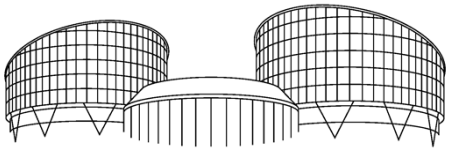

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRAND CHAMBER

CASE OF YÜKSEL YALÇINKAYA v. TÜRKİYE

(Application no. 15669/20)

JUDGMENT

Art 15 • Derogation in time of public emergency threatening the life of the nation

Art 7 • *Nullum crimen sine lege* • *Nulla poena sine lege* • Conviction for membership of an armed terrorist organisation based decisively on use of the encrypted messaging application ByLock without duly establishing offence's constituent material and mental elements in an individualised manner • Expansive and unforeseeable judicial interpretation inconsistent with essence of impugned offence which required specific intent • Art 7 requiring, for punishment purposes, existence of a mental link through which personal criminal liability might be established • Domestic courts' interpretation attached criminal liability in virtually automatic manner to ByLock users • Art 7 constitutes a non-derogable right and its safeguards could not be applied less stringently even in respect of terrorist offences allegedly committed in circumstances threatening the life of the nation • Convention required observance of Art 7 guarantees, including in the most difficult circumstances

Art 6 § 1 (criminal) • Fair hearing • Prejudice to the defence on account of non-disclosure of raw data obtained from encrypted messaging application server not counterbalanced by adequate procedural safeguards ensuring overall fairness of proceedings • Serious challenges in collection and handling of electronic evidence, increasingly used in criminal trials, did not call for a more strict or more lenient application of Art 6 § 1 safeguards • Defence's inability to have direct access to evidence and test its integrity and reliability first-hand placed a greater onus on the domestic courts to subject those issues to the most searching scrutiny • Domestic courts' failure to provide reasons for impugned non-disclosure of raw data and address core issues relating to integrity and evidential value of ByLock data • Access to decrypted ByLock material important for preserving defence rights • Shortcomings that undermined ability to conduct an effective defence on an equal footing with prosecution incompatible with very essence of applicant's procedural rights • Art 15 • Failure to comply with fair hearing requirements not strictly required by the exigencies of the situation

Art 11 • Freedom of association • Domestic courts' unforeseeable extension of scope of offence when relying on applicant's membership of a trade union and association considered as affiliated with the FETÖ/PDY, to corroborate conviction • Art 15 • Interference not strictly required by the exigencies of the situation

Art 46 • Execution of judgment • Individual measures • Reopening of criminal proceedings, if requested, most appropriate way of putting an end to violations found and affording redress • Respondent State required to take general measures as appropriate to address systemic problem regarding domestic courts' approach to use of ByLock

STRASBOURG

26 September 2023

This judgment is final but it may be subject to editorial revision.

TABLE OF CONTENTS

In the case of Yüksel Yalçınkaya v. Türkiye,

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Síofra O'Leary,
Georges Ravarani,
Gabriele Kucsko-Stadlmayer,
Pere Pastor Vilanova,
Arnfinn Bårdsen,
Carlo Ranzoni,
Georgios A. Serghides,
Lado Chanturia,
Ivana Jelić,
Gilberto Felici,
Saadet Yüksel,
Lorraine Schembri Orland,
Mattias Guyomar,
Frédéric Krenc,
Diana Sârcu,
Kateřina Šimáčková,
Davor Derenčinović*, judges*,

and Abel Campos, *Deputy Registrar,*

Having deliberated in private on 18 January and 28 June 2023,

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

INTRODUCTION

1. The case concerns the applicant's conviction for membership of an armed terrorist organisation described by the Turkish authorities as the "Fetullahist Terror Organisation/Parallel State Structure" (*Fetullahçı Terör Örgütü / Paralel Devlet Yapılanması*, hereinafter referred to as "the FETÖ/PDY"), considered by the authorities to be behind the coup attempt that took place in Türkiye on 15 July 2016. The conviction was based decisively on the applicant's use of an encrypted messaging application by the name of "ByLock", which the domestic courts held was designed for the exclusive use of the members of the FETÖ/PDY. Other evidence used against the applicant included his use of an account at Bank Asya, and his membership of a trade union and an association that were considered to be affiliated with the FETÖ/PDY. The applicant complained that his trial and conviction entailed a violation of Articles 6, 7, 8 and 11 of the Convention.

PROCEDURE

2. The case originated in an application (no. 15669/20) against the Republic of Türkiye lodged with the Court under Article 34 of the Convention

for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Turkish national, Mr Yüksel Yalçınkaya ("the applicant"), on 17 March 2020.

3. The applicant was represented by Mr J. Vande Lanotte and Mr J. Heymans, lawyers practising in Mariakerke, Belgium, Mr Ö. Akıncı, a lawyer practising in Kayseri, Türkiye, and Mr M. Öncü, who was given leave by the President of the Grand Chamber to represent the applicant in the proceedings before the Court (Rule 36 § 4 (a) *in fine* of the Rules of Court). The Turkish Government ("the Government") were represented by their Co-Agent, Mr H. A. Açıkgül, Head of the Department of Human Rights of the Ministry of Justice of the Republic of Türkiye.

4. The application was allocated to the Second Section of the Court (Rule 52 § 1 of the Rules of Court). On 19 February 2021 the Government were given notice of the applicant's complaints under Article 6 §§ 1 and 3 (concerning the collection, admission and assessment of the evidence against him, the independence and impartiality of the tribunals that tried him, and the right to effective legal assistance) and Articles 7, 8 (concerning the collection and use of the ByLock and Internet traffic data in his regard) and 11 of the Convention. The remainder of the application was declared inadmissible pursuant to Rule 54 § 3 of the Rules of Court.

5. The President of the Section granted leave to intervene in the proceedings to the International Commission of Jurists, which submitted written comments (Article 36 § 2 of the Convention and Rule 44 § 3).

6. On 3 May 2022 a Chamber of the Second Section decided to relinquish jurisdiction in favour of the Grand Chamber (Article 30 of the Convention and Rule 72).

7. The composition of the Grand Chamber was decided in accordance with the provisions of Article 26 §§ 4 and 5 of the Convention and Rule 24.

8. The applicant and the Government each filed further written observations on the admissibility and merits of the application (Rules 71 and 59 § 1).

9. A hearing took place in public in the Human Rights Building, Strasbourg, on 18 January 2023.

There appeared before the Court:

(a) *for the Government*

Mr	H.A. AÇIKGÜL,	*Co-Agent,*
Mr	S. TALMON,	
Mr	C. STAKER,	*Counsel,*
Ms	B. BAYRAK ŞENOCAK,	
Mr	İ. YUSUFOĞLU,	
Mr	K. ERSİNTANIK,	
Mr	F. YILMAZ,	*Advisers;*

(b) *for the applicant*
Mr J. HEYMANS,
Mr J. VANDE LANOTTE, *Counsel,*
Mr M. ÖNCÜ, *Adviser.*

The Court heard addresses by Mr Açıkgül, Mr Talmon and Mr Staker for the Government, and Mr Heymans and Mr Vande Lanotte for the applicant, as well as their replies to questions put by the judges.

THE FACTS

I. BACKGROUND AND CONTEXT OF THE CASE

A. *Coup d'état* attempt of 15 July 2016 and the declaration of a state of emergency

10. During the night of 15 to 16 July 2016 a group of members of the Turkish armed forces (also referred to as "the TAF") calling themselves the "Peace at Home Council" attempted to carry out a military coup aimed at overthrowing the democratically elected Parliament, Government and President of Türkiye.

11. During the attempted coup, more than 8,000 military personnel under the instigators' control bombarded several strategic State buildings, including the Parliament building and the presidential compound, attacked the hotel where the President was staying and the convoy in which the Prime Minister was travelling, held the Chief of General Staff hostage, attacked and occupied a number of public institutions, occupied television studios, blocked the bridges over the Bosphorus and the airports in Istanbul with tanks and armoured vehicles, and fired on demonstrators who had taken to the streets to oppose the coup attempt. According to the figures provided by the Government, more than 250 people, including civilians, were killed on the night in question and more than 2,000 people were injured. The Government also indicated that in the course of the coup attempt, some 70 military aircraft, including F-16 fighter jets and helicopters, 3 ships, 246 armoured vehicles and approximately 4,000 light arms were used.

12. The day after the attempted military coup, the national authorities blamed the network linked to Fetullah Gülen (hereinafter referred to as "F. Gülen"), a Turkish citizen living in Pennsylvania (United States of America) and considered to be the leader of the FETÖ/PDY. The authorities attributed responsibility for the coup attempt to members of the FETÖ/PDY who had infiltrated the Turkish armed forces.

13. On 16 July 2016 the Bureau for Crimes against the Constitutional Order at the Ankara Chief Public Prosecutor's Office initiated a criminal investigation into the attempted coup. Acting within the framework of that

investigation, the regional prosecutors' offices launched criminal investigations against those suspected of being involved in the coup attempt, as well as against others suspected of having links to the FETÖ/PDY.

14. On 20 July 2016 the Government declared a state of emergency for a period of ninety days as from 21 July 2016, which was subsequently prolonged on seven occasions, each time for further ninety-day periods.

15. On 21 July 2016 the Turkish authorities gave notice to the Secretary General of the Council of Europe of a derogation from the Convention under Article 15 (for the contents of the notice, see paragraph 205 below).

16. During the state of emergency, the Council of Ministers passed several legislative decrees. On the basis of one of these decrees, namely Legislative Decree no. 672, promulgated on 1 September 2016, some 50,875 civil servants were dismissed from their duties, as they were considered to belong to, be affiliated with or linked to terrorist organisations or other organisations, structures, or groups which had been deemed by the National Security Council to be engaging in activities detrimental to national security. Among those dismissed were 28,163 civil servants, mostly teachers, from the Ministry of National Education (for further information on the relevant legislative decree, see *Köksal v. Turkey* (dec.), no. 70478/16, § 7, 6 June 2017). Similarly, on the basis of Legislative Decree no. 667, which came into force on 23 July 2016, 104 foundations, 1,125 associations and 19 trade unions were shut down as they were considered as belonging, affiliated, or otherwise linked to the FETÖ/PDY.

17. On 18 July 2018 the state of emergency was lifted.

B. Measures taken against the FETÖ/PDY prior to the coup attempt

18. It appears from the domestic court judgments submitted by the parties that although the FETÖ/PDY, which was formerly known as the "Gülen movement" or the "Gülen community" (*cemaat*) internationally, was largely perceived as a religious group since its inception in the 1960s, its motivations and *modus operandi* had nevertheless been the subject of suspicion and public debate for many years (see the findings of the Turkish Constitutional Court in the case of *Ferhat Kara*, no. 2018/15231, noted in paragraph 172 below; see also paragraph 20 of the Memorandum by the Council of Europe Commissioner for Human Rights, set out at paragraph 198 below). In this connection, the leader of the movement, F. Gülen, was charged in 1999 with founding and leading a terrorist organisation on account of the activities of the "Gülen movement". Those proceedings ended in his acquittal by a final judgment, dated 24 June 2008, of the plenary criminal divisions of the Court of Cassation (see paragraphs 189-193 below for further details about those proceedings; see also *Akgün v. Turkey*, no. 19699/18, § 124, 20 July 2021).

19. As can be seen from the relevant domestic court judgments, the debate and controversy surrounding the FETÖ/PDY intensified after 2013,

particularly following the so-called "17-25 December investigations" and the "MİT trucks" incident, which reinforced misgivings about the motivations of the FETÖ/PDY and triggered numerous investigations of the suspected members of that movement on terrorism-related charges (for further details on these incidents, see paragraphs 15 and 16 of the Constitutional Court's *Ferhat Kara* judgment, set out at paragraph 172 below; see also *Sabuncu and Others v. Turkey*, no. 23199/17, § 23, 10 November 2020; *Murat Aksoy v. Turkey*, no. 80/17, § 12, 13 April 2021; and *Yasin Özdemir v. Turkey*, no. 14606/18, §§ 14 and 29, 7 December 2021).

20. At the same time, the State security services also considered that the FETÖ/PDY represented a threat to national security. The press statements issued following the regular bi-monthly meetings of the National Security Council, which is a consultative coordination body that provides policy advice on national security matters, reveal that as from early 2014, that body had raised the alarm about the FETÖ/PDY, with increasing intensity, as evidenced by the gradual change in the description of the organisation in the statements, from a "structure threatening public peace and security" in February 2014 to a "terrorist organisation" in May 2016 (see paragraphs 108-113 below for further details about the relevant statements; see also *Akgün*, cited above, §§ 39 and 40).

21. The information available in the case file further indicates that in parallel to these developments, the National Intelligence Agency of Türkiye (*Milli İstihbarat Teşkilatı*, hereinafter referred to as "the MİT") also engaged in intelligence-gathering activities in relation to the FETÖ/PDY prior to the coup attempt. In this respect, in early 2016 the MİT accessed the main server of the encrypted messaging application "ByLock", located in Lithuania, to gather information on the illegal activities of the FETÖ/PDY, apparently based on intelligence that this application was being used exclusively by the members of that organisation for internal communication. According to the information provided by the Government, as of May 2016 the data obtained by the MİT from the ByLock server, including the Internet Protocol ("IP") addresses of the persons who had connected to that server, were shared with the "relevant institutions", including the General Directorate of Security. On 24 October 2016 the MİT further shared with these "relevant institutions" an analytical report on the technical and organisational features of the ByLock application (hereinafter referred to as "the MİT technical analysis report", see paragraphs 114-116 below).

22. Subsequently, in December 2016, the MİT delivered the raw ByLock data in its possession to the Ankara Chief Public Prosecutor's Office. Upon the request of the latter, on 9 December 2016 the Ankara Fourth Magistrate's Court ordered the examination of that raw data pursuant to Article 134 of the Code of Criminal Procedure ("the CCP") (see paragraph 142 below). In particular, it ordered the making of copies of the material handed over by the MİT and the transcription of its contents. In the meantime, thousands of

investigations were commenced on the basis of the data disclosed by the MİT, with suspected users of the ByLock application being charged with membership of the FETÖ/PDY (for further information regarding the timeline of these developments, the technical reports prepared on ByLock by the national authorities and experts, as well as the ensuing investigative measures, see paragraphs 114-130 below, and the Constitutional Court's *Ferhat Kara* judgment noted at paragraphs 174 and 175 below).

II. CIRCUMSTANCES OF THE CASE

23. The applicant was born in 1966. On the date of lodging his application, he was serving a prison sentence in Kayseri.

A. The applicant's arrest and placement in pre-trial detention

24. On 22 July 2016 the applicant, who was a teacher at a public school in Kayseri, was suspended from the civil service. On 27 July 2016 he was dismissed from service by Legislative Decree no. 672, on account of his suspected affiliation with the FETÖ/PDY (see paragraph 16 above).

25. On 29 July 2016 the Kayseri Public Prosecutor's Office requested the Kayseri Security Directorate to inquire into whether the teachers dismissed from service in Kayseri, including the applicant, were among the members or executives of the FETÖ/PDY or whether they had links to that organisation; to investigate their social media accounts for any criminal content; to take any witness statements regarding these individuals; and to identify their address and contact details.

26. According to a record drawn up by the Kayseri Security Directorate on 18 August 2016, an anonymous call was placed to the police emergency line earlier on that same date, which reported the applicant, along with another person residing in Kayseri, as being members of the FETÖ/PDY.

27. On 5 September 2016 the Kayseri Security Directorate submitted its inquiry report to the Kayseri Public Prosecutor's Office concerning 147 teachers who had been dismissed from civil service in Kayseri. The report stated, in relation to the applicant, that he was identified as a user of ByLock (see paragraph 80 below for further information on the applicant's connection to ByLock). The report included no further information on the ByLock application, nor on how the applicant's use of that application had been established. It also indicated that the applicant was a member of the trade union "Aktif Eğitimciler Sendikası", also known as "Aktif Eğitim-Sen", and the association "Kayseri Voluntary Educators Association" (*Kayseri Gönüllü Eğitimciler Derneği*), which were deemed to carry out activities "in line with PDY". In the concluding part of the report, it was assessed that the suspects in question were members of the FETÖ/PDY, as they engaged in private encrypted communication with each other via ByLock, were in contact with

other members of the organisation, and some of them had accounts at Bank Asya, which supported the FETÖ/PDY. Accordingly, the Kayseri Security Directorate requested a search and seizure warrant in respect of the persons concerned, as well as warrants for their arrest and investigation.

28. On the same day, the Kayseri Public Prosecutor's Office lodged a request with the Kayseri Magistrate's Court for the search and seizure of digital evidence at the address and on the persons of the 147 individuals concerned, including the applicant, the search of their digital materials, such as computers, mobile phones and memory cards, and the temporary seizure of the digital materials for the purpose of their transcription and analysis.

29. The Kayseri Magistrate's Court granted the public prosecutor's requests on the same day, following which the latter instructed the police to perform the necessary procedures and arrest the suspects.

30. Accordingly, on 6 September 2016 the police conducted a search at the applicant's home. During the search the police seized, amongst other material, one mobile phone (IMEI[1] number: 351912067995747) together with its SIM card (with a specified telephone number). No elements of crime were found on the applicant's person or in his car. The applicant was placed under arrest at the end of the search and taken into police custody on suspicion of membership of the FETÖ/PDY.

31. On 8 September 2016 the applicant was interrogated by the police in the presence of his lawyer. In his statement, the applicant indicated that he had been using the same phone number for the past ten years. He denied having had any connection to associations, unions or institutions affiliated with the FETÖ/PDY, or having made any donations to such bodies. He stated that while he had joined a trade union named Aktif Eğitim-Sen, he had ended his membership in June 2016. When asked whether he had deposited any money with Bank Asya upon F. Gülen's call following its takeover by the Savings Deposit Insurance Fund ("TMSF") on 4 February 2014, the applicant claimed that he was not aware of any such call and therefore had not deposited any money with that bank in such circumstances. He explained, however, that when assigned to a school project conducted jointly with the Ministry of Education in 2014, he had been asked to open an account at Bank Asya in order to receive his remuneration, which was the extent of his involvement with that bank. Upon being informed by the police that he had been identified as a user of the ByLock application, the applicant stated that he had never heard of that application and had never used it. Lastly, as regards the anonymous call made in his respect, the applicant maintained that the accusations made against him were baseless and that he was not a member of the FETÖ/PDY.

1. "IMEI" stands for "International Mobile Equipment Identity", which is a unique number that is used to identify a mobile phone.

32. On 9 September 2016 the Kayseri Security Directorate sent a report to the Kayseri Public Prosecutor's Office, indicating the name of sixty-seven individuals, including the applicant, who had been identified as using the encrypted communication application ByLock. It was specified in the report that the information regarding the use of ByLock had been obtained "following coordination with other institutions".

33. On the same date, the applicant was questioned by the Kayseri Magistrate's Court in the presence of his lawyer. After reiterating the statements that he had previously made before the security directorate, the applicant asserted that he had not joined any associations or other bodies with the knowledge of their link to the FETÖ/PDY. At the close of the questioning, the Kayseri Magistrate's Court ordered the applicant's pre-trial detention having regard, *inter alia*, to the concrete pieces of evidence pointing to the existence of a strong suspicion that he had committed the offence of membership of an armed terrorist organisation.

B. Other reports included in the investigation file

34. On 12 October 2016 the Kayseri Security Directorate submitted a report to the Kayseri Public Prosecutor's Office concerning the 147 Kayseri-based teachers, including the applicant, who had been arrested on account of their alleged use of ByLock (hereinafter referred to as "the police ByLock report"). The report indicated the telephone (or the IP) number on which the application was used and the ByLock user-ID, together with a colour code assigned to each user (blue, orange or red). The information regarding the applicant indicated that he had connected to the ByLock application from the specified telephone number, that his ByLock user-ID was 408783, and that he was classified as an "orange" user. There was no explanation in the report as to how the data regarding the use of ByLock had been obtained, nor as to what the colour codes signified.

35. Following the Kayseri public prosecutor's request on 25 October 2016, on 16 November 2016 Bank Asya provided the prosecutor's office with the bank account details of a number of suspects, including the applicant. According to the information provided, two accounts were identified at Bank Asya in the applicant's name. While there had been no activity in relation to one of them, a deposit in the amount of 3,110.16 Turkish liras (TRY) (equivalent to approximately 1,020 euros (EUR) at the time) had been made to the other on 28 February 2014 – that is, after the alleged call by F. Gülen to support that bank (see paragraph 31 above). That money had been subsequently withdrawn, and a new deposit of TRY 1,520.50 (equivalent to approximately EUR 540 at the time) made on 12 December 2014. It was not indicated by whom the deposits had been made.

36. On an unspecified date, the Kayseri Public Prosecutor's Office transmitted a list of suspects, which included the applicant, to the Provincial

Directorate of Associations at the Kayseri Governor's office and requested information as to whether any of those persons had been members of associations or trade unions shut down by Legislative Decree no. 667 due to their affiliation with the FETÖ/PDY (see paragraph 16 above). On 1 December 2016 the Provincial Directorate replied that the applicant had been a member of the Kayseri Voluntary Educators Association and the Aktif Eğitim-Sen trade union, both of which had been shut down by Legislative Decree no. 667.

C. The applicant's prosecution

37. On 6 January 2017 the Kayseri public prosecutor filed a bill of indictment against the applicant with the Kayseri Assize Court, along with eight other persons, accusing them of membership of the armed terrorist organisation FETÖ/PDY under Article 314 § 2 of the Criminal Code. The bill of indictment was divided into three parts: the first part provided "general information" on the FETÖ/PDY; the second part examined the acts of the FETÖ/PDY in the terrorism context; and the third part dealt with the specific evidence against the suspects.

1. First part of the bill of indictment

(a) Founding of the FETÖ/PDY

38. According to the information provided in the first part of the bill of indictment, the foundations of the organisation had been laid in 1966 by F. Gülen, who was serving as an imam and preacher (*vaiz*) at the time. At its inception, the organisation concentrated its activities on young students, whom it reached via F. Gülen's talks recorded on cassettes or through "conversation meetings" (*sohbet*). By adapting himself to the socio-political conditions of the day, exploiting religious sentiments and maintaining his autonomy from political parties, F. Gülen was able to increase his effect in the "triangle of religion, politics and money", and to thus expand his organisation and his influence in religious circles. During this first phase of its existence preceding the *coup d'état* of 12 September 1980, the organisation focused on increasing its support base – particularly through the "houses of light" (*ışık evleri*) allocated to students, which were referred to in the bill of indictment as the "cell houses" of the organisation, and private tutoring centres (*dershane*) that targeted students – and infiltrating public institutions.

39. In the next phase, which followed the *coup d'état* of 1980, the organisation completed its mission of "staffing" public institutions, and prioritised its educational goals, while carrying on with other activities in secret. Targeting bright students and educating them formed a fundamental

part of the organisation's long-term project, as it was these students who were subsequently placed in important public institutions by the organisation.

40. In this second phase, the organisation replaced its ideology of "national, local Islam" with what the bill of indictment termed an "*étatist* discourse". From an economic perspective, the organisation also started operating in this phase like a holding company that connected companies; accordingly, it founded a bank and commenced activities in the health, finance, transport and media sectors, in addition to its presence in the area of education. This second phase also marked the period when the FETÖ/PDY expanded abroad.

41. According to the bill of indictment, the third phase of FETÖ/PDY leading to terrorism started after the incident of the so called "post-modern *coup d'état*" of 28 February 1997 (for some further insight into this incident, see *Dilipak and Karakaya v. Turkey*, nos. 7942/05 and 24838/05, §§ 6 and 54, 4 March 2014). In this phase, F. Gülen fled from Türkiye, and the organisation changed its rhetoric and adopted more universal expressions, entailing references to concepts such as "dialogue between religions" and "human rights". It was noted that by this phase the organisation had become active in 160 countries and had also brought all public institutions in Türkiye under its influence. Particularly after the constitutional changes adopted on 12 September 2010, the organisation began to perceive itself as the only *de facto* ruler of the State, which perception continued until 17 December 2013 (see paragraph 19 above in relation to the so-called "17-25 December investigations").

(b) Terminology, objectives and operation of the FETÖ/PDY

42. In this first part of the bill of indictment, the prosecutor's office also provided a description of the special terminology used by the organisation and its structure. It explained, in particular, the "cell-type organisation" of the FETÖ/PDY within public institutions, which consisted of a maximum of five persons, subordinated to their hierarchical superior, named the "brother" (*örgüt abisi*). This method of organisation was inspired by Hezbollah. The cells, which were the smallest organisational units within the FETÖ/PDY, were not aware of one another, so that if one cell was exposed, the others could continue their activities.

43. As for the organisation's objectives, the statements of persons who were formerly active in the FETÖ/PDY had revealed that the main goal was to take control of the constitutional bodies of the State through the use of its people and the financial power that it had accumulated by exploiting the religious feelings present in society. In order to infiltrate the public institutions and achieve this goal, the organisation had also resorted to clandestine acts, such as stealing university or civil-service entry exam questions, or arranging the dismissal of non-members from the civil service by fabricating evidence against them.

44. In arguing why the FETÖ/PDY should be classified as an "organisation", the prosecutor's office noted factors such as its use of code names and private telecommunication channels instead of handling its affairs openly and transparently, its unaccounted finances and the management of its activities from abroad, its resort to duress, blackmail and illegal methods to eliminate its opponents, its covert dealings with foreign diplomatic missions, its perception of the State as an adversary, and its interpretation of religious values in pursuance of its objectives, adapting this interpretation to the prevailing circumstances of the day.

45. The prosecutor's office noted that the hierarchical structure of the FETÖ/PDY was based on the system of imams, each of whom was responsible for their assigned "units" in their respective geographical, sectoral and institutional fields. Led by F. Gülen as "the universal imam", the FETÖ/PDY had organised and spread at the grassroots level through continental, country, regional, provincial, district, trades, neighbourhood, and house imams. The organisation also designated imams in the public sector, such as ministries, local authorities and universities, and the private sector. Due to the sensitive nature of their assignments, the imams operating in the civil service, law enforcement, army, judiciary and the MİT took more precautions to preserve their secrecy compared to other members of the organisation, including as regards their means of communication.

46. At the outermost layer of the organisation were its "sympathisers" who, while not properly part of the organisation, were essential to its function as its legitimacy depended on a large number of sympathisers.

47. The prosecutor's office further observed that having recognised early on the difficulties that waging an open fight against the State would involve, F. Gülen's aim was to reach his goals not by destroying the system, but by conquering all governmental structures from within. It had long been known to the public that the FETÖ/PDY was active in the police force, as well as in other public bodies, which had been instrumental in conducting its operations and furthering its goals.

(c) Communication methods used by the FETÖ/PDY and the ByLock application

48. The prosecutor's office indicated that the most important means of communication for the organisation was via "GSM lines". As a rule, these lines would be registered under the name of a third person or a FETÖ/PDY-controlled entity, which meant that the subscription information would not disclose the real user. A new GSM line would be obtained approximately every three months, and the mobile device would be replaced along with the GSM line. According to the public prosecutor's office, this arrangement alone was an important indication of the FETÖ/PDY's engagement in illegal activities that they wished to keep hidden.

49. The members of the organisation avoided using each other's names in their communications, and the provincial and district imams generally used code names.

50. Applications such as Skype, Tango, WhatsApp, Viber, Line and Kakao Talk were also favoured on account of the possibility of encrypted communication that they provided at low cost. However, members in critical positions eventually abandoned those applications in favour of ByLock, which had allegedly been developed upon the instruction of F. Gülen for the exclusive use of the members of the FETÖ/PDY. The bill of indictment did not provide much further information on the characteristics of ByLock, except for explaining that it was an encrypted messaging application with an automatic message deletion feature. It also stated that the ByLock application could not be downloaded from the Internet, as it required a special installation file which could only be obtained from another member, which also showed that the application could only be accessed by the members of the organisation.

2. Second part of the bill of indictment

51. The second part of the bill of indictment was devoted to a discussion of the meaning of terrorism under Turkish law and why the FETÖ/PDY had to be characterised as a terrorist organisation. After setting out the domestic legislative provisions governing the notions of "organisation" and "terrorism" (see paragraphs 146-149 below), the public prosecutor's office noted that three elements had to be present for a structure to be characterised as a "terrorist organisation", namely (i) an ideology or aim as set out in section 1 of the Prevention of Terrorism Act (Law no. 3713); (ii) an organised structure as per Article 220 of the Criminal Code, and (iii) resort to force and violence in order to reach its aims.

52. In the light of the foregoing explanations, the public prosecutor's office made the following observations as regards the FETÖ/PDY:

> "The Fetullahist Terror Organisation;
>
> 1) Harboured the aim of overthrowing the Government of the Republic of Türkiye by force, violence and other illegal methods or of preventing it wholly or partly from discharging its duties; of suppressing, weakening and redirecting State authority; [presenting itself] as an alternative authority; and eventually seizing State authority,
>
> 2) Had a continuous, covert and hierarchical structure involving persons who served for the same purpose but who would never otherwise act together in the normal course of life, including:
>
> - public officials and civil servants who were authorised by law to use arms [and] force and to enforce [the law], and who operated in an occupational hierarchy,
>
> ...
>
> 3) Was organised in a cell-type structure [with cells] independent from one another,

4) Individuals were assigned organisational responsibilities in accordance with the [identified] areas of activity, division of labour and responsibilities,

...

6) Secret organisational meetings would be regularly held in pre-designated houses in order to ensure the continuity of organisational activities and commitment to the leader,

...

8) Members of the organisation reported to [their hierarchy] in relation to organisational activities, and prepared documents/reports analysing the organisational areas of activity,

9) Secrecy was given particular importance in organisational activities and special coding procedures were used in communications, meetings, reporting, and in the preparation, storage and archiving of documents,

10) Owing to the qualified human resources that they had cultivated in their private tutoring centres and schools, and to the cautious and hypocritical policies that they had adopted, since the 1980s [they] found the opportunity to place their own staff in strategic bodies of the State and gradually took over/attempted to take over the decision-making and execution mechanisms in their employing bodies,

11) The public officers operating within the organisation utilised their office [and] the authority, tools, materials and personnel of [their office] in line with the organisation's aims,

12) They manipulated public opinion on political, legal, economic and current affairs in line with the organisation's aims through the [medium of the] books written by certain individuals acting within the organisation, or via the visual, print, and social media, [through] television series and films, and articles, declarations, commentaries, etc. published on the Internet;

By means of this method;

...

- they created/attempted to create public distrust and polarisation [resulting in] the disruption of public order [with the aim of] weakening the State's authority and, in this manner, garnered public support for all illegal interference in the politically elected government of the Republic of Türkiye by the members of the organisation,

- they also aimed to take under their control the judicial authorities [by instrumentalising] the pressure exerted by the public [thus] manipulated,

...

- they produced publications and broadcasts that aimed to disrupt our country's political and economic stability and to tarnish the reputation of our country in the international arena by creating the image of a State supporting terrorism ...,

- they violated the secrecy of State activities by publishing, via the Internet or media corporations, confidential documents exchanged between public institutions and [thus] attempted to hinder [such] activities,

...

13) It was stated in the judgment of the Erzincan Assize Court dated 16.06.2016 ... that 'having regard to the methods it adopted, it was considered that the characterisation of the FETÖ/PDY as an armed terrorist organisation was imperative',

...

19) Private and sensitive information/data [or] video [or] audio recordings pertaining to the political, philosophical or religious opinions, racial origins, moral dispositions, sexual lives, communication details (e-mail, telephone), [and the] state of health of members of the judiciary, academics, staff of the [armed forces], staff of the [law enforcement agencies], high level public officials, bureaucrats, journalists, etc. ... would be obtained illicitly and used for the purpose of blackmail in the pursuance of the organisation's goals,

...

In this framework;

It is assessed that ... the FETÖ/PDY is an organisation displaying the attributes of a terrorist organisation ... as set out in sections 1 and 7 of the Prevention of Terrorism Act.

[It is further assessed that] [T]his organisation had to use force and violence in order to achieve the above-listed aims, and that one of the most significant elements pointing to the existence of force and violence was the *coup d'état* attempt perpetrated by the FETÖ/PDY on 15.07.2016 ..."

3. Third part of the bill of indictment

53. In the third part of the bill of indictment, the public prosecutor's office set out the evidence against the applicant. It noted, accordingly, that;

(i) the applicant had used the ByLock application, which was used by the members of FETÖ/PDY for their internal organisational communication, on the specified mobile phone number registered in his name, and that the intensity of his use was at the "orange" level;

(ii) the applicant had an account at Bank Asya, and that his account balance was TRY 0 on 31 December 2013 and 31 January 2014, TRY 3,110.16 on 28 February 2014, TRY 2,953.68 on 31 March 2014, TRY 2,894.84 on 30 April 2014, TRY 0 between 31 May and 30 November 2014, TRY 1,520.50 on 31 December 2014, TRY 843.71 on 31 March 2015, TRY 573.77 on 30 June 2015, and TRY 7 between 31 December 2015 and 15 November 2016;

(iii) the applicant was a member of the trade union Aktif Eğitim-Sen and the association Kayseri Voluntary Educators Association, both of which had been declared in Legislative Decree no. 667 as belonging, affiliated, or linked to the FETÖ/PDY;

(iv) the applicant had been dismissed from public service by Legislative Decree no. 672; and

(v) information had been received from an anonymous caller that the applicant was a member of the FETÖ/PDY.

Having regard to the continuity, variety and intensity of these acts and activities, the public prosecutor's office found it established that the offence of membership of an armed organisation set out in Article 314 of the Criminal Code was made out in the applicant's case.

D. Criminal proceedings against the applicant

1. Proceedings before the Kayseri Assize Court

54. On 20 January 2017 the Kayseri Assize Court issued a preliminary report (*tensip zaptı*), where it accepted the bill of indictment filed against the applicant and set the date of the first hearing for 21 March 2017. It also requested the Anti-Smuggling and Organised Crime Department ("the KOM") of the Security Directorate, as well as its Kayseri branch, to provide information as to whether the applicant had used the ByLock application, and if so, the GSM line and the IMEI number of the telephone on which it had been used, the persons who had been contacted, the date of download and first use, the frequency of use and, if identified, the content of the exchanges made over the application.

55. On 9 February 2017 the KOM sent the Kayseri Assize Court a one-page report containing a table on which the applicant's name, identity number, GSM number and telephone IMEI number (35368406164487) were indicated (hereinafter referred to as "the KOM ByLock report"). It was also noted on the table that the "identification date" was "3 October 2015". According to the explanation provided by the Government, this referred to the date of the applicant's first connection to ByLock. The table was not accompanied by any explanation as to the source of the information provided.

(a) Hearing held on 21 March 2017

56. On 21 March 2017 the first hearing was held before the Kayseri Assize Court.

57. At the start of the hearing, the assize court admitted in evidence the ByLock report submitted by the KOM and noted that the report on the digital materials seized at the time of the search conducted on 6 September 2016 had not yet been submitted. After reading out the bill of indictment, the assize court invited the applicant to make his defence statements. The applicant stated, *inter alia*, that while he was the user of the GSM line indicated, he had never used ByLock, and pointed out that there was no information in the bill of indictment as to his alleged communication "content and [other] issues". As regards his bank account at Bank Asya, the applicant reiterated that he had opened that account in relation to his assignment to a project conducted by his school, and that he had no other connection to that bank. As for his membership of the Aktif Eğitim-Sen trade union, the applicant claimed that he had joined it in 2014, following the announcement of certain incentives by

the Government for trade union membership, but then had quit on 17 June 2016 and had not engaged in any illegal activities during his membership. He had also joined the Kayseri Voluntary Educators Association out of his interest in their activities, which offered various educational and cultural courses, and for the purpose of socialising. He had sought to leave that association in June 2016 as well, but was informed that it was in the process of liquidation, and it was subsequently closed down. The applicant lastly stated that he did not know about or understand the anonymous tip-off received regarding him, and that he did not accept it.

58. The applicant's lawyer added that there were no concrete data in the case file to establish that the structure in question was a terrorist organisation. According to the lawyer, it transpired from the statements of the President and the Prime Minister regarding this "structure" that its terrorist aims, as well as its aspirations to take over the State and any other illegal aims that it harboured, had been unknown to the State authorities; the applicant could not therefore have been expected to have knowledge of those matters. Accordingly, the material and mental elements of the crime had not materialised. He further claimed that the data regarding ByLock could not constitute "evidence" under the CCP, because (i) they were unlawful, in view of the method of their seizure, (ii) it was unclear how the raw data had been incorporated into the case file from a technical point of view, (iii) they were technically inadequate, and (iv) they could not be inspected. To the extent that the accusations brought against the applicant concerned his membership of a trade union and an association, the applicant's lawyer indicated that both had been established in accordance with the law and no illegal activities had been attributed to them.

59. The applicant's lawyer further requested the extension of the investigation so as to inquire about, *inter alia*, whether the said terrorist organisation had committed any crimes against the Turkish State, its institutions and its citizens, and how the ByLock data had been obtained and deciphered technically. The lawyer also requested that any specific ByLock data belonging to the applicant be included in the case file.

60. The Kayseri Assize Court dismissed the lawyer's request for the extension of the investigation, having regard to the evidence already available in the case file, including the various reports confirming the applicant's use of ByLock, and to the designation of the FETÖ/PDY as a terrorist organisation in a final judgment delivered by the Samsun Regional Court of Appeal on 7 March 2017.

61. Subsequently, the public prosecutor presented his submissions on the merits (*esas hakkında mütalaa*) and sought the applicant's conviction of the offence with which he was charged. Reiterating the arguments made in the bill of indictment, the public prosecutor claimed that in a bid to conceal its true aims, the FETÖ/PDY had made an effort to portray itself as a religious community (*dini cemaat*) or civil society movement, and had used

code-names and private communication methods in order to ensure secrecy. Against this background, and bearing in mind that people from all parts of society had sympathised with this organisation without being aware of its real motives and aims, had offered it financial support and had taken part in its activities, the public prosecutor found it imperative to establish who had truly been a part of the organisation's hierarchy and had acted in accordance with its common purpose. In this connection, having regard to the applicant's membership of a trade union and an association that was affiliated with the FETÖ/PDY, and noting his intensive use of an encrypted application employed for organisational communication amongst the FETÖ/PDY members, there was no doubt that the applicant had been a part of the organisation's hierarchical structure and a member of that organisation.

62. The applicant and his lawyer repeated their defence submissions in response to the public prosecutor's opinion.

(b) Ruling of the Kayseri Assize Court

63. At the end of the hearing held on 21 March 2017, the Kayseri Assize Court convicted the applicant as charged on the basis of the evidence indicated in the bill of indictment and sentenced him to six years and three months' imprisonment. It also decided to order his release having regard, *inter alia*, to the time that he already spent in detention.

64. The judgment was divided into five parts. In the first part titled "the FETÖ/PDY Armed Terrorist Organisation", the court made general remarks regarding the definition, types and components of a terrorist organisation, and then proceeded to examine, *inter alia*, the establishment, objectives, management and hierarchical structure of the FETÖ/PDY, as well as its financial structure and communication methods, largely along the same lines as the bill of indictment. The assize court stressed that the fact that the State security institutions infiltrated by the FETÖ/PDY were armed and were authorised to use those arms was a very important factor to demonstrate that the organisation was in fact armed and had a military tendency.

65. The second part of the judgment on the "Structure and Functioning of the Organisation" provided an overview of the unlawful methods commonly employed by the organisation in order to achieve its ulterior motives, such as stealing exam questions for their supporters, fabricating evidence and depriving people of their liberty based on trumped up charges. Stressing that maintaining secrecy was the key to the organisation's functioning, the assize court quoted some statements by F. Gülen allegedly instructing his followers to act discreetly and keep a low profile until they reached "all power centres", which showed that the organisation had infiltrated all public institutions as a strategic means of seizing control over the constitutional order (see paragraph 162 below for some of these instructions, as noted in the judgment of the Court of Cassation dated 26 September 2017). The assize court further noted that the veil of secrecy had been lifted with the "bureaucratic coup

attempt" of 17-25 December 2013 (see paragraph 19 above and the references therein), which had been performed to "redesign the government and politics". The assize court held that in view of its consequences, the 17-25 December events should be considered as a milestone for the recognition, at both the State and the public level, that the FETÖ/PDY was not an aid organisation or a "service" movement but a terrorist organisation.

66. The third part of the judgment was devoted to an examination of the ByLock application. The court indicated that the application had been subjected to technical studies, including "reverse engineering, crypto analysis, web behaviour analysis and server response codes", without providing further information as to who had carried out those analyses. It then provided a summary of the assessments made in the MİT technical analysis report (see paragraphs 114-116 below), without, however, referring expressly to that report, and concluded that under the guise of a global application, ByLock had been offered for the exclusive use of the members of the FETÖ/PDY.

67. In the fourth part of the judgment, the assize court examined the legal framework governing armed terrorist organisations in Türkiye and laid out the main elements of the offence of membership of an armed terrorist organisation, referring to the relevant provisions of the Criminal Code and the Prevention of Terrorism Act (see paragraphs 146-149 below). It noted, in particular, that membership of an organisation required voluntary submission and subordination to the organisation's hierarchical structure, as well as an "organic link" to the organisation and participation in its activities. The organic link rendered the person available for commands and determined his or her hierarchical position and hence was the most important element of membership. Mere sympathy for the organisation would not constitute an offence.

68. In the fifth and the final part of the judgment, the assize court assessed the evidence on which it relied in convicting the applicant. In this connection, it noted that despite the applicant's denial, the ByLock report prepared by the Kayseri Security Directorate during the investigation stage and the report drawn up subsequently by the KOM at the trial stage had established that the applicant had used the ByLock application on his GSM line from 3 October 2015 onwards, with a telephone bearing the IMEI number 35368406164487. It had also been established that the applicant had been a member of a trade union and an association, both of which had been shut down on account of their affiliation with the FETÖ/PDY, and that he had deposited money with Bank Asya, similarly affiliated with that organisation. Elaborating on the latter point, the assize court stated that in contrast to the minimal activity in his Bank Asya account in the previous periods, in February 2014, upon the organisation's instructions, the applicant had made a deposit with the bank of an amount proportionate to his income – that is,

TRY 3,110 – for the purpose of saving it from the economic hardships it encountered in the aftermath of the 17-25 December 2013 process.

69. Turning next to the applicant's allegations regarding the unlawfulness of the ByLock data on account of the failure to comply with the relevant provisions of the CCP in their collection, the assize court found that the data in question had been obtained by the MİT – within the framework of its powers under Law no. 2937 on Intelligence Services of the State and the National Intelligence Agency ("the Law on Intelligence Services") – from Lithuania, where the ByLock application's main server was located. Since the provisions of the CCP were not enforceable in Lithuania, it was not possible to argue that the data had been collected in an unlawful manner on account of non-compliance with the CCP in that respect. The court moreover explained that on 9 December 2016, the Ankara Fourth Magistrate's Court had ordered the analysis of the data handed over by the MİT in accordance with Article 134 of the CCP.

70. The assize court further stated that while membership of an association or trade union could not in itself constitute evidence of membership of an armed terrorist organisation, in the applicant's case membership of more than one entity affiliated with the FETÖ/PDY had been established, in addition to his use of the organisation's communication tool, ByLock. Having regard to the aims and the functioning of terrorist organisations, any facilities ensuring intra-organisational communication and allowing the flow of information regarding organisational activities "could not be assessed outside the organisational structure", for only people who were part of the organisational hierarchy would be admitted to the communication network. It therefore found it established that the applicant, by virtue of his use of the ByLock application and the other evidence in the case file, had been a part of the hierarchical structure of FETÖ/PDY.

(c) Applicant's appeal against his conviction

71. On 3 April 2017 the applicant appealed against the judgment of the Kayseri Assize Court. In his appeal, the applicant challenged, *inter alia*, what he deemed to be the retrospective classification of FETÖ/PDY as an armed terrorist organisation. According to the intelligence reports issued by the MİT, the aim of the FETÖ/PDY was to seize the State institutions and to replace the constitutional order. However, in its 50-year history, that organisation, which the applicant referred to as a "structure", had not been associated with any such acts. Referring to the judgment delivered by the plenary criminal divisions of the Court of Cassation on 24 June 2008 as regards F. Gülen's acquittal of terrorism charges (see paragraphs 189-193 below), the applicant argued that the activities carried out by the structure had been found to be in compliance with the law. It was unclear to him which concrete acts undertaken after the Court of Cassation's ruling had given rise to a contrary finding as regards the organisation's objectives. While the bill

of indictment referred to the "17-25 December operation" as an act of terror, opposition political parties considered the acts carried out on 17-25 December 2013 to be an anti-corruption operation; therefore, its classification as a terrorist act was a political decision, not a legal one.

72. The applicant further asserted that bearing in mind that membership of an armed terrorist organisation was a crime of specific intent (*özel kast*), it was primordial to establish when that organisation had come into existence, when individuals who were affiliated with the relevant structure – which used to be highly regarded by the State authorities – solely for religious reasons had become aware of the terrorist intent and goals harboured by certain members, and when, and by which means, he had knowingly and willingly become part of that organisation. Stressing in particular the lawful nature of the acts attributed to him, the applicant criticised the trial court's silence on these matters. In the applicant's view, the accusation of membership of an armed terrorist organisation made against him had to be supported by an investigation by the prosecutor's office into the organisation's hierarchical structure in the province of Kayseri, and his place in that hierarchy.

73. As regards the evidence concerning his use of the ByLock application, the applicant claimed that the ByLock data had not been obtained in accordance with the relevant procedures set out in Articles 134 and 135 of the CCP; in fact, the circumstances in which the data had been obtained were unclear. According to the information provided by the MİT, it had conducted an intelligence operation to obtain the data from the application's main server located in Lithuania; however, the technical details as to how exactly it had accessed and analysed the data remained unknown. In such circumstances, there was no possibility to inspect the data and to verify whether they had been modified; a person who had been added to the ByLock user list had no way to challenge that. The applicant highlighted here that the three user lists shared by the MİT with the judicial authorities did not match. In the applicant's opinion, the evidence regarding the use of ByLock was unreliable also from a purely technical point of view, given that it was possible for one IP address to be allocated to more than one person.

74. The applicant added that according to the MİT technical analysis report, the ByLock application had been downloaded some 500,000 to 1 million times from open sources, yet there had been no judicial examination to determine who had downloaded it for organisational purposes and who for other reasons.

75. To conclude, the applicant argued that the trial court's judgment had failed to comply with the rules of procedure and the rule of law, since it had been given on the basis of an insufficient investigation and without resorting to the opinions of competent and independent experts, particularly in respect of the ByLock data, and it had not established the material and mental elements of the crime at issue.

2. Proceedings before the Ankara Regional Court of Appeal

(a) Further material obtained at the pre-hearing stage

76. In its preliminary report dated 10 May 2017, the Ankara Regional Court of Appeal requested the KOM to provide information as to (i) the characteristics of the ByLock application, its downloading to communication devices and the means and conditions of its use; (ii) whether it could be downloaded and used by anyone; (iii) whether the application was specifically used by members of an organisation for their communications within the framework of the organisation's activities and how this had been established; (iv) the characteristics of the application that distinguished it from other means of communication; (v) the time period that and the frequency with which the applicant had used the application; (vi) on which GSM lines and from which devices (with IMEI numbers) the applicant had used the application; and (vii) if identified, the content of exchanges over the application and the identity and telephone contact details of the persons with whom the exchanges had been made.

77. In the same report, the court of appeal also requested the Information and Communications Technologies Authority ("the BTK") to provide information regarding (i) the base station data, pertaining to both the GSM line reported to be used by the applicant and the device(s) used with that line, indicating the dates on which ByLock IP addresses had been accessed in the period between 3 September 2015 and 15 July 2016; and (ii) the communication records indicating the incoming and outgoing calls, the messages sent and received, and the base stations used between 1 January 2015 and 15 July 2016, as well as the IMEI numbers of the device(s) used.

78. On 3 June 2017 a document issued by the KOM entitled "ByLock Identification Report" was included in the case file. The document bore the signature of two KOM officers, without further specifying their rank or functions. The report indicated that the ByLock database, which had been handed over by the MİT to the Ankara Chief Public Prosecutor's Office, had been transmitted to them by the latter on 16 December 2016 for examination. The analysis carried out on the ByLock subscriber lists had revealed that the applicant, who had been noted on the 114,060th line of the 129,862-line subscriber list, had used the specified GSM number, that the IMEI number belonging to the device used for connection was 35368406164487, that the first date of connection that could be identified was 3 October 2015 and that the examinations conducted so far had not disclosed any content of communication through messages or emails.

79. On 12 June 2017 the BTK also submitted the communication records requested from it.

80. Upon the court of appeal's request, an expert report was subsequently drawn up by a digital forensics expert on the basis of all the information and

records available in the case file and was submitted to the appeal court on 29 June 2017. According to this report, the applicant had accessed the ByLock application through his GSM line with the specified telephone number and that his ByLock user-ID number was 408783. The examination of the HTS ("Historical Traffic Search"[2]) records pertaining to this GSM line in the period between 1 January 2015 and 16 July 2016, which had been procured by the BTK, revealed that the line had been used in phones with three different IMEI numbers, including the device with IMEI number 35368406164487, on which the ByLock application had been found to have been used, but which had not been found in the applicant's home or on his person at the time of his arrest. Over the relevant period, a total of 13,450 call, SMS and MMS records and 38,166 GPRS[3] records were detected on the relevant GSM line, most of which concerned communication with persons believed to be the applicant's kin bearing the same surname. The report further indicated that in the period between 11 August 2014 and 10 January 2015, when the said GSM line was used with the phone with IMEI number 35368406164487, communication had been established with the IP number 46.166.164.181 that belonged to ByLock servers on six different dates for a total of 380 times. This expert report was served on the applicant's lawyer on 21 September 2017.

(b) Hearing held on 9 October 2017 and the ruling of the Ankara Regional Court of Appeal

81. At the hearing held on 9 October 2017, the applicant and his lawyer reiterated their previous defence statements. The lawyer further indicated that they did not accept the digital forensics expert's report described in paragraph 80 above, which was based on unlawfully obtained evidence, and requested the court to obtain a fresh report from a committee of three experts. He stressed that the material and mental elements of the crime of membership of an armed terrorist organisation had not materialised.

82. At the same hearing, the court dismissed the applicant's request for a new expert report. It also upheld the applicant's conviction based on the information and reports in the case file.

83. The court reviewed at the outset the different forms of organised crime under Turkish law and discussed the distinguishing factors of the offence of "membership of an armed organisation" under Article 314 § 2 of the Criminal Code, as also addressed at first instance (see paragraph 67 above). The appeal court specified that although it was not necessary for a "member" to have committed an actual crime in connection with the organisation's activities, the individual must nevertheless have made a specific material or moral

2. HTS records include signal information pertaining to the caller, the dialled number, the duration of the call, and the place and the time of the call.

3. "GPRS" stands for "General Packet Radio Service", which is a technology that provides moderate-speed data transfer and that is typically used for instant messaging.

contribution to the organisation's existence or reinforcement. The offences of aiding an organisation or committing a crime on behalf of the organisation also involved receiving orders from the organisation; however, the distinctive factor in the determination of membership of an organisation was the readiness of the suspected member to execute all instructions and orders given within the context of the organisational hierarchy, without questioning and with absolute submission. The member should have established an organic link with the organisation, which was the most important element of membership of an organisation, and taken part in its activities. In this connection, it was primordial to determine on the concrete facts of a case whether the individual's position within the armed organisation had reached a level warranting his consideration as a "member" of that organisation. The appeal court also noted that the offence of membership of an armed organisation required a specific intent besides general intent. Since the terrorist organisation was founded for a specific purpose, the perpetrator had to know of that purpose and had to have a specific intent for its realisation.

84. Moving on to the specific considerations concerning the FETÖ/PDY, the appeal court reiterated the distinct attributes which rendered that organisation an "armed terrorist organisation", following the same line of reasoning adopted by the first-instance court, and more recently by the Court of Cassation in its judgments of 24 April 2017 and 26 September 2017 (see paragraphs 162-163 below). It noted that the aim of this organisation was not to come to power through legitimate methods, but to dissolve the Parliament, the government and the other constitutional institutions by using force and violence, as demonstrated by the attacks carried out against several symbolic State buildings, including the Parliament building and the presidential compound, with heavy weaponry. It also stressed that the absence of a prior judicial ruling designating the FETÖ/PDY as a terrorist organisation did not preclude criminal liability for offences committed in connection with that organisation.

85. The appeal court next turned to the issue of the lawfulness of the ByLock evidence and held that, in accordance with the principle of free evaluation of evidence, all types of evidence, including electronic evidence, could be relied on in criminal proceedings, as long as it was obtained lawfully. It considered in this connection that the MİT had collected the relevant data in pursuance of its duties and powers under sections 4 (1) and 6 (1) of the Law on Intelligence Services (see paragraph 143-145 below), and that the judicial procedure had only started after the MİT's handover of the digital material to the judicial authorities, from which point onwards the investigation had to be carried out in accordance with the terms of the CCP. The Ankara Fourth Magistrates' Court had accordingly ordered the examination and processing of the data handed over by the MİT in accordance with Article 134 of the CCP. The acts undertaken to identify and assess the use of ByLock had therefore been lawful.

86. The appeal court then addressed the probative value of evidence demonstrating a person's use of ByLock and held as follows:

> "Before assessing whether the ByLock system constitutes organisational evidence or a communication system at the disposal of an organisation, it must first be established [under which circumstances] a communication system could be considered as being an organisational communication system.
>
> A person may join a special communication network and use [such] program on [his or her] mobile telephone device or computer. However, where it is established on the basis of concrete evidence that this communication network is one that was set up to commit crimes and is used exclusively by the members of a criminal organisation, the joining and use of that network ... for communication with the knowledge (intentionally) that [it was being used in this way by the members of a criminal organisation] must be taken as evidence of [the person's] connection with the organisation, even if the contents of the communication are not discovered."

87. The appeal court noted that the ByLock application was developed as a "special software that could only be used by the members [of the FETÖ/PDY] over a special server and that enabled communication by the [members] amongst themselves using a special encryption method". It observed that the application could be downloaded from the Internet, or obtained via memory cards or Bluetooth, and that while it was exceptionally available for download by all at the beginning of 2014, it was subsequently made available by members of the organisation by means of USB keys, memory cards or Bluetooth, as indicated in statements, messages and e-mails obtained. The downloading of the application was not sufficient to be able to use it for messaging; knowledge of the user-specific ID number assigned automatically by the system and the approval of the other party was required to engage in communication, which was in conformity with the cell-like structure of the organisation. Moreover, almost all of the transcribed content concerned organisational contact and activities of the FETÖ/PDY members and corresponded to the organisation's specific jargon. Based on the foregoing elements, and others noted at length previously by the MİT and the Court of Cassation (see paragraphs 115-116 and 158-160 below, respectively), the appeal court found that under the guise of a global application, ByLock was offered for the exclusive use of the members of the FETÖ/PDY armed terrorist organisation and had been used by its members since early 2014, as revealed by the members themselves. To that end, the appeal court held, echoing the Court of Cassation's landmark judgment of 26 September 2017 (see paragraph 160 below):

> "In the ByLock communication system, it is possible to determine the date of connection, the IP address from which the connection was made, the number of connections over a given period of time, the persons with whom the communications were made and the content of the communication. The date of connection, the establishment of the IP address from which the connection was made and the establishment of the number of connections within a given period of time are sufficient to establish that the person is part of a special communication system.

Given that the ByLock communication system is a network designed for the use of the members of the armed terrorist organisation FETÖ/PDY and is used exclusively by some members of this criminal organisation, as demonstrated by the concrete evidence described above, where it is established – beyond doubt by technical data capable of supporting a firm conviction – that [a person] has joined that network on the instructions of the organisation, and that [he or she] has used [ByLock] for communication to ensure secrecy, such finding would constitute evidence of the person's connection with the organisation."

88. Turning to the specific facts of the applicant's case, the appeal court made the following findings:

"A report was prepared by a digital forensics expert on the basis of the records obtained from [the BTK] and [the KOM] concerning the [specified] GSM number used by the applicant and the entire content of the case file; this report, which was submitted on 29 June 2017, is taken as the basis of [the court's] verdict in view of its consistency with the HTS records furnished by the BTK, the ByLock assessment and identification reports furnished by the KOM and the content of the case file, [as well as its] detailed, comparative and scrutinisable nature.

As explained in detail in the judgment no. 2015/3-2017/3 of the Sixteenth Criminal Division of the Court of Cassation dated 24 April 2017, which was upheld by the plenary Criminal Divisions of the Court of Cassation's judgment no. 2017/956-370 dated 26 September 2017, the ByLock application, under the guise of a global application, is a network designed for the use of the members of the armed terrorist organisation FETÖ/PDY and is used exclusively by some members of this criminal organisation. [For that reason] where it is established – beyond doubt by technical data capable of supporting a firm conviction – that [a person] has joined that network on the instructions of the organisation, and that [he or she] has used [ByLock] to ensure secrecy, such finding is taken to constitute evidence of the person's connection with the organisation.

The records and documents [obtained during] the investigation process, the actions undertaken and the hearings held by [this court] at the appeal stage, and the entire content of the case file [attest that] the defendant was registered in the ByLock communication system with a specified GSM number – which was registered in his name and which he stated had been in his use for a long time – and ByLock ID (identity number) 408783, that it had been established by the KOM and the BTK that the defendant had first joined the ByLock system on 3 October 2015 on a device bearing the IMEI number 353684061644870 [*sic*], that he had established connection with the IP number 46.166.164.181 that belonged to the ByLock servers/systems for 380 times on six different dates, that the connections made and the communications established [by him] had been explained in detail in the report prepared ... by a digital forensics expert on 29 June 2017, that the defendant had frequently communicated with GSM numbers used by his close relatives during the period covering the dates in question, and that it was not possible for the specified GSM number to have been used by anyone other than the defendant.

There is no doubt that the defendant – who, by virtue of his level of education [and] the knowledge, position and experience that he had gained through his job, is expected to have known of the ultimate purpose of the [FETÖ/PDY], of its organisation within the State institutions and armed forces, and of the fact that its members might use the weapons at their disposal in line with the purpose of the organisation when needed – is a member of the FETÖ/PDY armed terrorist organisation. The defendant had joined the ByLock communication system and had used it many times with the knowledge of

(intentionally) [the fact that] it was designed solely for the use of the members of the armed terrorist organisation FETÖ/PDY and was used exclusively by the members of this criminal organisation, in view of its technical specifications, downloading and utilisation method, and its users and content. [Based on that finding] and other evidence in the case file, the first-instance court disregarded the defendant's denial-oriented pleas and found that [he] was a member of the armed terrorist organisation FETÖ/PDY."

Holding that the first-instance court had not erred in its assessment and findings, the Ankara Regional Court of Appeal Court dismissed the applicant's appeal.

3. Applicant's appeal against the judgment of the Ankara Regional Court of Appeal and the judgment of the Court of Cassation

89. In his appeal against the judgment of the Ankara Regional Court of Appeal, the applicant mainly elaborated on the arguments made in his previous appeal against the trial court's ruling. In this connection, he denied having taken part in any activities – legal or illegal – of the FETÖ/PDY, and argued that his membership of that organisation had not been established on the basis of clear, definite and unambiguous evidence. The courts had furthermore failed to explain how the impugned offence had been individualised in his particular circumstances and had left open the questions as to whether his supposed position within the organisation had been of a nature and extent to render him a "member" in the legal sense, how he had been "organically linked" to the organisation, and where he had been situated in the organisation's hierarchy. The judgments of the lower courts were similarly silent as to how his intention to become a member of an armed terrorist organisation, in the full knowledge of the organisation's resolve to realise its aims by use of arms and to engage in criminal conduct, had been established. The applicant claimed on this basis that the domestic courts had failed to demonstrate the factual basis of their findings and that their reasoning failed to make a connection between the evidence and the verdict.

90. Noting that his conviction had been based to a decisive extent on his alleged use of the ByLock application, the applicant pointed out that this application had been available for download from various application stores until February 2016 without the requirement of any reference or prior authorisation, and had in fact been downloaded by some 600,000 people according to publicly available sources. Moreover, many of the technical features listed as proof of the "organisational" character of ByLock were in fact shared by other popular messaging applications. In these circumstances, to hold that the mere use of such an application could amount to proof of membership of an armed terrorist organisation, which offence would in principle require concrete evidence entailing the use of force and violence, would be tantamount to disregarding the material and mental elements of the offence. The applicant stressed in this regard that, according to the well-established case-law of the Court of Cassation, the offence of

membership of an armed terrorist organisation could only be committed by participating in the hierarchy of an organisation intentionally, embracing its end goals and activities, and required a continuous, diversified and uninterrupted link to the organisation, as well as concrete acts aimed at ensuring its sustainability. None of these had been made out in his case.

91. Besides the inherent insufficiency of the simple use of ByLock to serve as evidence of membership of an armed terrorist organisation, the applicant claimed that the procedure by which the MİT had obtained and processed the ByLock data was unlawful, as well as being obscure. He argued, on the latter point, that it remained unclear why only 115,000 ByLock users had been identified and pursued from among the approximately 600,000 people who had downloaded the application. This uncertainty was compounded by the fact that the MİT had shared with the judicial authorities a total of three user lists on different dates, and the names of the users in the three lists did not match. No technical explanation had, however, been provided as to why some persons who appeared in the initial list did not figure in the other lists.

92. In the applicant's view, the accuracy and integrity of the evidence to be used in criminal proceedings could only be ensured via procedural safeguards. For that reason, the collection of electronic evidence in criminal investigations had been subjected to a series of safeguards by the lawmaker under Article 134 of the CCP (see paragraph 142 below), each of which ensured the transparency of the data collection procedure and rendered it open to inspection and challenge. The collection of the digital data regarding ByLock had, however, been an act of intelligence gathering, which was not subject to any of the safeguards stipulated under Article 134 of the CCP. The fact that the Ankara Magistrates' Court had subsequently issued an authorisation on 9 December 2016 for the examination of the material handed over by the MİT did not retrospectively "regularise" that evidence as argued by the lower courts, bearing in mind particularly that he had been arrested for use of ByLock three months before the magistrate's order.

93. The applicant further argued that the technical details as to how the MİT had procured and analysed the relevant ByLock data had not been revealed in the MİT technical analysis report in the interest of preserving the confidentiality of the process, but this obscurity surrounding the MİT's collection and handling of the relevant data rendered it virtually impossible to verify their authenticity. The ByLock reports subsequently issued by the law enforcement authorities (noted in paragraphs 27, 32, 34, 55 and 78 above) were similarly lacking in important respects, as it was unclear by whom, and on the basis of what authority and criteria, those reports had been prepared, and whether their accuracy had been verified. Those reports also failed to provide any information as to whom he had communicated with over the ByLock application and why he had been classified as an "orange" user. In the absence of clear, comprehensible and technically adequate reports

on his alleged use of ByLock, he had not been able to exercise his defence rights effectively.

94. As regards the other evidence used against him, the applicant argued that to rely on trade union membership as evidence of membership of an armed terrorist organisation amounted to a violation of his right to freedom of association, given in particular the absence of any evidence of illegal activity on the union's part. He further asserted that the accusations regarding Bank Asya were similarly groundless. That bank had been founded on 24 October 1996 and, until the revocation of its operation licence on 23 July 2016, it had operated in accordance with the relevant legal framework. At no point in that 20-year period had its banking operations been restricted or banned, and none of his interactions with that bank had been carried out with the intention of committing a crime.

95. As for the classification of the FETÖ/PDY as a terrorist organisation, the applicant argued that the statements and opinions shared by this organisation with the public did not entail incitement to commit any of the acts listed in section 1 of the Prevention of Terrorism Act (see paragraph 149 below). If the organisation had covertly engaged in such activities, those had to be laid out in the judgment.

96. Lastly, the applicant argued that the independence and impartiality of the judiciary had been undermined by the recent changes in the structure and composition of the Court of Cassation and the possibility of removal of judges from duty by decision of the High Council of Judges and Prosecutors under Article 3 of Legislative Decree no. 667 (see paragraph 151 below), which he argued was contrary to the principle of the irremovability of judges.

97. Arguing that the proceedings before both the trial court and the appeal court had been conducted as a matter of form only, and that none of his appeals for further investigation and assessment had been accepted, the applicant requested from the Court of Cassation, *inter alia*, the log records obtained by the MİT from the ByLock server and an independent expert review of those records and data, including as to whether that data could be, or had been, manipulated. He also asked that court to establish his alleged activity on ByLock, such as the names and organisational status of the persons with whom he had communicated via that application, and the content of those communications, given in particular that, according to the MİT technical analysis report, 15 million messages out of a total of 17 million messages had been decrypted. He further requested that inquiries be conducted as to when he had become a member of the terrorist organisation, who he had reported to and what actions he had undertaken in keeping with the instructions received from the organisation's hierarchy.

98. On 30 October 2018 the Court of Cassation upheld the applicant's conviction, without commenting on his requests for further clarification or action. In the light of the expert report obtained at the appeal stage and the remaining contents of the case file, it held that all procedural acts undertaken

during the proceedings had been in accordance with the law and that the arguments regarding the unlawfulness of the evidence underlying the conviction had been duly assessed. The findings made in the applicant's regard had, therefore, been based on valid and consistent data. Moreover, the relevant acts had been accurately classified and had conformed to the offence set out under the law, and the verdict and sentence had been determined in an individualised manner. The Court of Cassation further found that the delivery of the appeal judgment without awaiting the submission of a detailed ByLock findings and evaluation report had not affected the outcome (see paragraph 107 below regarding this detailed findings and evaluation report, which was issued on 7 October 2020).

4. Proceedings before the Constitutional Court

99. On 13 December 2018 the applicant lodged an individual application with the Constitutional Court, in which he mainly invoked the arguments previously made during the criminal proceedings and raised the complaints under Articles 6, 7, 8 and 11 of the Convention that he subsequently brought before the Court. Once again, he drew attention to the irregularities in the collection of the ByLock data and their use as evidence in the criminal proceedings, which had not only been an arbitrary exercise of the courts' discretion in the assessment of evidence, but had infringed some of his procedural rights, such as the right to adversarial proceedings and equality of arms, and the right to a reasoned decision. He claimed in particular that the courts' evaluation of the ByLock evidence had been at variance with the material facts. He noted in this connection that convictions for membership of the FETÖ/PDY by reason of the sole use of ByLock were based on the premise that that application had been used exclusively by the members of that organisation; however, publicly available figures demonstrated that the application had been downloaded by some 600,000 people and the MİT technical analysis report revealed that 215,092 ByLock users had been initially identified, whereas the user ID numbers in the same MİT report went up to 493,000. The applicant argued that the "exclusive use" argument was not tenable in these circumstances.

100. Moreover, in securing his conviction, the courts had relied exclusively and unconditionally on reports drawn up by authorities operating under the executive branch of the government, such as the MİT, the BTK and the police, without directly examining or discussing the accuracy of the findings made in those reports or subjecting them to objective and independent expert examination. Nor had the data in the hands of the prosecution been shared with him, in disregard of the requirements of Article 134 of the CCP, which had created a disparity between the defence and the prosecution. The applicant claimed that his access to such data was imperative for him to be able to comment on their authenticity and integrity, as well as to challenge the "exclusive use" argument, with a view to

influencing the courts' decisions. In these circumstances, he had been strictly denied the possibility of proving his innocence.

101. The applicant further emphasised that although the courts had proceeded from the understanding that the ByLock data had been admitted and examined by the judicial authorities only following the authorisation granted by the Ankara Fourth Magistrate's Court on 9 December 2016, in reality, the data had been processed, and ByLock's allegedly exclusive use by the members of the FETÖ/PDY and the probative value of its data had been determined, long before that date. In this connection, he referred to indictments and official correspondence predating 9 December 2016, including a press statement made on 5 October 2016 by the then Deputy President of the High Council of Judges and Prosecutors, who had indicated that "ByLock is the communication software of the organisation and our strongest evidence. It is clear that ByLock is not a program that can be used by persons other than the members of the organisation...".

102. The applicant also argued that as a result of the restrictions introduced by Article 6 § 1 (d) of the Legislative Decree no. 667, all his meetings with his lawyer had either been held in the presence of a prison officer, or recorded, which destroyed the essence of his right to avail himself of the assistance of a lawyer within the meaning of Article 6 § 3 (c) of the Convention.

103. The applicant also complained, in a general manner, of a lack of independence and impartiality on the part of the Turkish courts, mainly on account of the systemic disregard of the principle of the irremovability of judges.

104. As regards his complaints concerning the unlawfulness of his conviction, within the meaning of Article 7 of the Convention, the applicant once again put emphasis on the importance of establishing when he had acquired the requisite "knowledge" that the formerly lawful "Gülen movement" had become the unlawful armed terrorist organisation "FETÖ/PDY". He underlined in this connection that the first act of violence attributed to this organisation was the coup attempt of 15 July 2016 and contended that the absence of knowledge regarding the "terrorist" nature of the FETÖ/PDY would exclude the establishment of the specific intent required for the offence of membership of an armed terrorist organisation.

105. Lastly, the applicant added that none of his aforementioned objections and arguments had been considered by the courts in duly reasoned judgments, which also amounted to a violation of his right to a fair trial.

106. On 26 November 2019 the Constitutional Court summarily dismissed the applicant's individual application as inadmissible, finding that his complaints were manifestly ill-founded and failed to comply with the other admissibility criteria.

5. Subsequent developments

107. On 7 October 2020 the KOM issued the detailed "Findings and Evaluation Report" in respect of the applicant's ByLock user profile, including his user ID number (408783), username and password and the date of his last connection (31 January 2016). The assessment in the report indicated that user ID 408783 had had six contacts in the ByLock application, had sent one message over the application on 20 June 2015 to a teacher, which read "Hello, I am Yüksel Yalçınkaya", and had received one message on 18 February 2016 from another teacher, which read "Hello teacher". A number of email messages forwarded to user ID 408783, among others, were also attached to the report, which mainly praised and referred to the hardships faced by the "Gülen movement", encouraged the collection of funds (*himmet*), or criticised the Government by reference to the Prophet Muhammad's sayings or to moral or religious anecdotes.

III. OTHER MATERIAL SUBMITTED BY THE PARTIES

A. Press statements issued following National Security Council decisions

108. In the press statements issued at the close of its meetings held between February 2014 and October 2015, the National Security Council noted the FETÖ/PDY among the threats posed to the national security of Türkiye, and referred to this organisation in the following terms:

- "the structure threatening public peace and national security" (26 February and 30 April 2014);
- "the illegal structure within the State" (26 June 2014);
- "parallel structures and illegal formations, conducting illegal acts under the guise of legality at home and abroad, that threaten our national security and disturb public order" (30 October 2014);
- "the parallel State structure and illegal formations" (30 December 2014);
- "the parallel State structure and illegal formations operating under the guise of legality" (26 February 2015);
- "the parallel State structure and illegal formations that threaten our national security" (29 April and 29 June 2015);
- "the parallel State structure ... operating outside of the law" (2 September 2015);
- "the parallel State structure that threatens our national security and that collaborates with other terrorist organisations" (21 October 2015).

109. The press statement released after the meeting held on 18 December 2015 provided as relevant:

> "It has been confirmed that the fight against the parallel State structure would continue with determination, domestically and abroad.

...

It has been stated that the fight against all terrorist organisations that exploit the religious, sectarian, ethnic notions and sensibilities, and the [power] groups that support them, will continue ... indiscriminately."

110. The relevant parts of the press statement issued after the meeting held on 27 January 2016 read as follows:

"... In this framework, the internal and external threats against our national security, and the efforts against the separatist terrorist organisation, the parallel State structure and Daesh at home and abroad, have been assessed.

It has been stated that regardless of from whom and where it originates, the decisive and principled fight against [terror] would continue until all forms of terror were eliminated."

111. The press statement issued following the meeting held on 24 March 2016 provided as relevant:

"... In this framework, the internal and external threats against our national security, and the efforts to combat terror and terrorists have been evaluated, and the implementation of the measures taken against the parallel State structure have been emphasised."

112. On 26 May 2016, following its last meeting prior to the coup attempt, the National Security Council issued the statement below, as relevant:

"Efforts undertaken to ensure the peace and security of our citizens and the public order, the achievements in the fight against terror and terrorist[s] and the measures taken against the parallel State structure, which threatens our national security and which is a terrorist organisation, have been discussed."

113. In the first meeting it held following the coup attempt on 20 July 2016, the National Security Council stated that the attempt had been instigated by the members of the FETÖ/PDY who served in the Turkish armed forces.

B. ByLock expertise reports

1. Reports submitted by the Government

(a) "Technical Analysis Report" prepared by the MİT

114. As mentioned in paragraph 21 above, in early 2016 the MİT accessed the databases of the ByLock server. Following the analysis of the digital data obtained from the server, the MİT issued an 88-page technical analysis report, which it shared with the "relevant institutions" on 24 October 2016.

115. According to the report, after getting hold of the relevant material, the MİT carried out elaborate technical analyses both on the mobile application itself and on the application servers, on matters such as the application's technical design, operation, its similarities and differences to applications that provided the same functions, and the decrypted user profiles.

In summary, the MİT's main findings regarding the ByLock application were:

- ByLock was first released on the Google Play store in early 2014 and had remained there until early 2016 with different versions, during which period it was installed more than 100,000 times;
- The application allowed for instant messaging, voice calls, group messaging, file sharing and email correspondence, all encrypted;
- Following the downloading of the application, a username/user code and cryptographic password was created; this information was transmitted to the application's server in encrypted form, so as to protect the user's information and communication security;
- 215,092 registered users had been identified on the server;
- No personal information was requested when creating a ByLock user account and, unlike similar global and commercial applications, no system for verifying the user account – such as by authentication via SMS or email – was provided, which was intended to ensure anonymity and to render user identification more difficult;
- Registration in the system was not sufficient to communicate with other users, nor was it possible to search and add users by their names; individuals could only contact one another after adding each other's usernames/codes, which suggested that the application was designed to allow communication only in conformity with the cell-like structure of the organisation;
- The automatic transfer of phone contacts to the application, a feature provided in similar messaging applications, was not available in ByLock;
- After its removal from the Google Play and Apple application stores, ByLock could still be installed from APK[4] download sites and according to the statistics available on those sites, the application had been downloaded 500,000 to 1 million times; while it was not possible to verify the accuracy of these figures, they did not appear to be inconsistent with the number of users found on the ByLock server (215,092), given that people may have (i) deleted and redownloaded the application; (ii) downloaded the application without creating a user account; and (iii) downloaded the application on more than one device;
- Statistically, the figures regarding the use of ByLock in Türkiye were much higher than the total sum of its use in other countries, although it was hardly known to the public or even to experts in the field before the coup attempt, which provided an important insight into the purpose of the application;
- The majority of the users who posted about ByLock on Twitter prior to 15 July 2016 had also posted content favourable to the FETÖ/PDY, which suggested that the Twitter users in question had been supporters of the

4. "APK", which stands for "Android Package Kit", is the file format for applications used on the Android operating system.

FETÖ/PDY, who knew about the application and who used it before the general public had ever heard about it; moreover, most of the Internet publications about ByLock were made from fictitious accounts that published pro-FETÖ/PDY material;

- While the application mainly provided service over the server with the IP number "46.166.160.137", eight additional IP addresses had also been rented in order to render the identification of the users more difficult;

- As it appeared from an announcement (in English) posted on the application's website by the system administrator on 15 November 2014, the access of some IP ranges, all of which originated from Türkiye, had been blocked; while the administrator had explained this as a precaution to cope with the high number of registered users (which had apparently reached one million at that stage) and the malicious connections detected from the relevant IP ranges, the MİT report claimed that the real aim had been to force users based in Türkiye to connect via a VPN ("Virtual Private Network") to prevent their identification;

- Virtually all "Google" searches on ByLock were performed by users from Türkiye and searches for "ByLock" on the Google search engine had increased significantly following the blocking of the access to the application by Turkish IP addresses;

- The developer and publisher of the application had no professional references for his previous work and, unlike similar messaging applications, the application had not been commercially promoted, nor had any efforts been made to increase its user base or to give it commercial value; the aim of ByLock had rather been to limit the number of users with an emphasis on anonymity. Moreover, the anonymous nature of the payments made to sustain the application – such as the rental of the server and the IP addresses – confirmed that the enterprise behind it was not institutional and commercial in nature;

- Instead of opting for an authority-signed SSL certificate[5] that was typically used by commercial messaging applications, the developer of the ByLock application had used a self-signed SSL certificate created under the name of "David Keynes", allegedly to prevent other parties from acquiring the user information;

- The application had a feature which deleted the messages and other content stored on the devices automatically, which ensured the privacy of communications even if the user omitted to delete any compromising exchanges;

- The storage of all the server and communication data in encrypted form in the application's database added an additional layer of security to prevent user identification and to secure communications;

5. Secure Sockets Layer (SSL) certificates, also called digital certificates, are used to secure the connection between the computer and the server with the use of a strong encryption.

- ByLock users took further steps to conceal their identities, such as using long passwords, downloading the application manually rather than from various application stores, and using their organisational code names in messages and contacts lists;

- While other messaging applications were used for daily and routine communications, the examination of the communication network and the content of the messages exchanged over ByLock revealed that the latter had been used for organisational purposes: almost all of the decrypted content – that is, approximately 15 million messages out of the 17 million messages recovered and 2 million emails out of the 3 million emails recovered – concerned organisational contact and activities pertaining to the FETÖ/PDY, using organisation-specific jargon;

- The source codes of the application included certain expressions in Turkish and the majority of decoded usernames, group names and passwords, and almost all of the decrypted content was in Turkish.

116. The report concluded that when taken as a whole, the above factors suggested that ByLock had served as a messaging system for the exclusive use of FETÖ/PDY members, under the guise of a global application, which was also corroborated by statements obtained from a number of suspected members of the organisation in investigations conducted after the coup attempt.

(b) "Analysis Report on Intra-Organisational Communication Application" prepared by the KOM

117. This report, dated 2 April 2020, was prepared by the KOM at the request of the Ankara Chief Public Prosecutor's Office. The report largely reiterated the findings in the MİT report, but also made the following observations:

- Although all versions of the application were available on various application stores and websites, the members of the organisation were urged to download the ByLock application from USB keys or via Bluetooth, so as to ensure organisational secrecy;

- On the devices where it was downloaded, the ByLock application could be hidden under the icons of other more common applications;

- While the application was available to download freely, its actual use required further operational information, which was provided by the organisation and which would not be shared outside the organisation; accordingly, it was physically impossible for a non-member to use the ByLock application;

- A review of the first 100 users of the application, 53 of whom had been identified, indicated that the application had been developed and offered for use by members of the organisation: for instance, the user ID 3 was a computer engineer employed at Turkish Institute of Scientific and Technical Research ("TÜBİTAK") facing charges of FETÖ/PDY membership on the

basis of evidence other than the use of ByLock; the user ID 49 was the private secretary of F. Gülen; and 15 of these 53 identified users were former police officers working in the police intelligence service, on trial for illegal phone tapping;

- The examination of the ByLock contents and user information had revealed that 175 people who had been identified as senior executives of the FETÖ/PDY, 52 of the judges who had taken part in the investigations and prosecutions referred to as "*Ergenekon*" (see, for further details regarding those proceedings, *Perinçek v. Switzerland* [GC], no. 27510/08, § 27, ECHR 2015 (extracts), and the cases cited therein, and *Eminağaoğlu v. Turkey*, no. 76521/12, § 6, 9 March 2021), "Sledgehammer" (*Balyoz*) and "Military Espionage" (*Askeri Casusluk*) (see *Ahmet Hüsrev Altan v. Turkey*, no. 13252/17, §§ 5-8, 29 and 56, 13 April 2021, and the cases cited therein on these investigations and prosecutions), and 5,922 people out of the 8,723 who faced charges for being part of the confidential structure within the law enforcement agencies were users of ByLock;

- The information obtained about the organisation from the application was consistent with the information gathered from other sources;

- ByLock contacts consisted of users' organisational networks, rather than family members or social acquaintances, and friends' groups, demonstrating that the organisational hierarchy had been detected over the application.

118. Based on the foregoing, and all the other information available, the report concluded that ByLock was a communication tool designed for the sole use of members of the FETÖ/PDY, that measures had been put in place to prevent the identification of users, and that it was not accessible to anyone outside the organisation.

119. The report also provided further insight as to how the ByLock user lists had been drawn up by the authorities. In the first stage, the MİT had identified, on the basis of the raw log data that it had obtained, the nine different IP addresses used by the ByLock server, the accuracy of which had been verified by the Department of Cyber Crimes of the General Directorate of Security. The Internet traffic data, also referred to as the CGNAT data[6], stored by the service providers in accordance with the relevant legislative framework had then been examined for the purpose of identifying the IP addresses that had connected to the ByLock server's nine IP addresses from Türkiye, although the user information thus obtained was limited to the connections that were made prior to the obligation to connect via VPN, or to instances where the VPN connection was momentarily disabled. The IP addresses thus identified were then matched to the respective GSM and ADSL subscribers. The first version of the user list was transmitted by the MİT to the Ankara Chief Public Prosecutor's Office on 16 December 2016.

6. "CGNAT" data provide information as to connections made to a target IP address, such as the date and frequency of the connection, and the IP address from which the connection was made.

Upon further analysis of the available data, an updated list was prepared by the MİT and shared with the authorities on 24 March 2017. That list, which included information pertaining to 129,862 users, was then verified using the CGNAT data procured by the BTK from the service providers as of 19 April 2017 and the ByLock user list was thus put together. Subsequently, on 28 December 2017, 11,480 people who were discovered to have been unwittingly directed to the ByLock server, via a trap application known as *Mor Beyin* ("Purple Brain"), were removed from the ByLock user list (for further information on *Mor Beyin*, see *Taner Kılıç v. Turkey (no. 2)*, no. 208/18, § 36, 31 May 2022).

120. In a supplementary report drawn up on 22 May 2020, officers from the KOM responded to some specific questions put by the Ankara Chief Public Prosecutor's Office. In response to a question on the measures taken to ensure the integrity of the ByLock data and to prevent their manipulation, it was reiterated that the ByLock data had been obtained from two different sources: (i) the raw log data obtained by the MİT from the ByLock server; and (ii) the CGNAT data (pertaining to the Internet traffic information) showing connections made to the ByLock IPs from Türkiye. The first set of data was subjected to a disk imaging process and accorded a hash value, and the data was kept in a safe by the judicial authorities and could not, therefore, be modified. As for the CGNAT data, they concerned internationally registered data which could not be altered or corrupted.

121. In response to another query as to whether an individual ByLock user could be given the digital (raw) ByLock data pertaining to him or her alone, the report explained that it was not possible to sort the raw data on a user ID basis without first processing them. The raw ByLock data were categorised under separate tables on a database, and the information belonging to a particular individual was obtained following the extraction of the relevant data from these tables, through the use of an interface. The information thus obtained was included in each individual's case file, in the form of a "ByLock Results and Evaluation Report". It was otherwise not possible to share the raw data in their entirety with any particular suspect, as that data contained information concerning many other suspects as well.

122. It was also indicated in this supplementary report that there had been no prosecutions for the mere download of ByLock and that evidence of the actual use of ByLock was required in each case.

(c) "Expert Report on the ByLock application" prepared by independent cyber security experts

123. On 10 July 2020 a group of cyber security experts, who were commissioned by the authorities, prepared an expert report on the ByLock application, on the basis of information obtained from open sources as well as from the reports prepared by the MİT and the KOM referred to above. While the expert report mainly reiterated the findings in those earlier reports,

it also included some further pertinent observations (for a more detailed account of this report, see *Akgün*, cited above, § 57).

124. In this connection, the report noted that the ByLock application used advanced encryption methods and that it was an anonymity-oriented messaging application, which enabled communication without leaving a digital fingerprint that could be detected by the law-enforcement authorities. Some of its features, such as the storage of all messages in the server in an encrypted manner and the special procedure for adding contacts, demonstrated that ByLock had been designed differently from other messaging applications and intended to serve not the general public but a specific purpose.

125. The report also noted that some "trap" applications (as mentioned in paragraph 119 above) that were used to establish inadvertent connections to the ByLock server had been identified. The technical analysis had shown that the CGNAT data pertaining to such inadvertent connections could be distinguished from the data produced following an ordinary connection to the ByLock server.

126. The report further emphasised that according to the information obtained from Google Trends on the searches conducted regarding ByLock on the Google search engine, virtually no searches had been made from September 2014 to February 2016. Given that ByLock worked very differently from other messaging applications, the absence of online searches suggested that this application was used by a specific group of people and that those people possessed detailed information on how the application worked and shared it with prospective users.

127. Lastly, as regards the number of users of the ByLock application, the report clarified that the figure "215,092" found in the MİT report indicated not the actual number of users, but the number of registrations with the application.

(d) "The Technical Report" prepared by IntaForensics

128. IntaForensics, a digital forensics and cyber security consultancy service based in the United Kingdom, prepared a forensic investigation and technical report on the ByLock application, dated 21 August 2020, at the request of the Ministry of Justice of Türkiye (for further details on the report, see *Akgün*, cited above, § 58).

129. The report, which was very similar in content to the reports outlined above, noted that despite the fact that ByLock was published on global application stores, for all intents and purposes the interest in it was limited to Türkiye. Moreover, given its difference in features when compared with other messaging applications, it would appear that anonymity as much as security was a primary goal for ByLock.

130. It was also observed in the report that the application had been removed from the Google Play store on 3 April 2016, yet no prior

announcements had been made to the users on this matter, nor were any complaints or comments from users identified on social media or elsewhere as to why the application had been unpublished without notice. According to the authors of the report, this suggested that the application was used by a specific group of people and that the developer had no commercial concerns.

2. Reports submitted by the applicant

(a) Expert opinion on the digital data concerning the applicant

131. On 5 September 2021 the applicant's lawyer commissioned a digital forensics expert based in Türkiye to examine the CGNAT data and HTS records included in the applicant's case file, as well as the "Findings and Evaluation Report" issued by the KOM on 7 October 2020 (see paragraph 107 above). In a report dated 11 October 2021, the expert noted that the IP addresses indicated in the CGNAT data pertaining to the applicant were all within the IP ranges blocked by the system administrator. He further found, *inter alia*, that while the relevant data suggested that connection with the ByLock server may have been established from the applicant's device, the nature of the data available did not rule out the possibility that the connections had been made other than by use of the ByLock application, i.e., inadvertently.

(b) Expert reports commissioned in the context of other criminal proceedings

132. The applicant also submitted a number of expert reports that had been prepared by independent experts in the context of other criminal proceedings concerning the use of ByLock.

133. One of those reports, which had been prepared by a Netherlands-based IT company on 13 September 2017 and which mainly involved an analysis of the MİT technical analysis report, found that the said report entailed no information that would enable the verification of the integrity of the data obtained, such as hash values or an audit trail, nor did it provide a description of the technical analysis undertaken. As such, it was difficult to scrutinise the analysis methods used.

134. Another report, issued on 1 September 2021 by two legal forensics experts from Türkiye, concerned specifically the question whether there was sufficient evidence to support the conclusion that the ByLock application had been used "exclusively" by members of the FETÖ/PDY. The report included the following findings, as relevant:

- All commonly used mobile messaging applications, such as "WhatsApp", "Telegram", "Skype" and "Signal", provided encrypted communication to varying degrees;

- ByLock could be downloaded from mobile application stores freely without the need for any reference, or other requirement;

- Some of the features cited as proof of "exclusiveness" of ByLock stemmed from the preferences of the developers of the application, and numerous messaging applications with similar features could be found;

- By way of example, access to the phone contacts was an optional feature in virtually all applications, and the requirement for prior approval to establish communication with another user could be found as an optional feature in many messaging applications, such as "Line"; automatic deletion of messages was similarly a feature available in many applications, such as "Snapchat" and "Telegram";

- While the lack of a dedicated application website, the use of self-signed certificates, and the lack of a password recovery option were not frequently encountered among the widely used applications, they were quite common for applications without a large user base.

135. Based on the foregoing, the report found that the ByLock features identified by the authorities as proof of its exclusive use did not prove beyond reasonable doubt, from a technical perspective, that the said application had been meant for "exclusive use". It added that any communication content which was not related to the organisation in question, of which there was plenty according to the records included in the case files, would undermine the "exclusiveness" argument.

C. Arrest of the licence owner of ByLock

136. On 9 June 2021 David Keynes, a Turkish and American dual national who was identified as the licence owner of ByLock (see the mention in the MİT technical analysis report noted in paragraph 115 above), was arrested and taken into police custody at Istanbul Airport.

137. According to his subsequent statements to the police, the public prosecutor and the magistrate's court, he had returned from the USA to Türkiye in order to share his knowledge of the ByLock application and the FETÖ/PDY with the Turkish authorities, in order to benefit from the "active repentance" provision in Article 221 of the Criminal Code, which provides for the possibility of reduction of sentence in exchange for information. He explained that, as a student, he had studied and briefly worked in the private tutoring centres owned by the FETÖ/PDY and had also frequented their student houses. He claimed to have cut all his connections with the FETÖ/PDY in 1997. In 2002 he went to the USA to study, shortly after which he made friends with a certain A.C., who was studying computer engineering in the USA and who appeared to maintain active ties with the FETÖ/PDY. In December 2013, David Keynes met with A.C. in Istanbul, who told him that he was in the process of developing some mobile applications but had encountered problems in uploading them to the application stores due to problems related to payment. A.C. requested to use David Keynes' card and also obtained his contact and identity information to complete the upload

process. At their next meeting in March 2014, A.C. told him about the ByLock application that he had uploaded to the application stores, with the use of his credit card, identity and communication details.

138. When they met again in August 2015, A.C. asked him to stop the payments for the domain name, reportedly because the number of downloads had dropped. He therefore stopped payment in October 2015, yet according to his knowledge the domain name remained available until February 2016. When the police asked David Keynes why A.C. had wanted to discontinue the domain payments in August 2015, he stated that from what he heard after the coup attempt, the MİT had discovered the ByLock application in July 2015, which was probably why A.C. wanted to stop the flow of information over ByLock after that time.

139. David Keynes stated that having regard to the configuration and the impracticality of the application, which had been designed to prioritise confidentiality, and to A.C.'s connection to the organisation, he had realised with hindsight that the ByLock application had been developed by A.C. for the use of the FETÖ/PDY.

140. On 14 June 2021 David Keynes was placed in pre-trial detention on suspicion of membership of an armed terrorist organisation. According to a news report submitted by the applicant, which was not refuted by the Government, David Keynes was released from pre-trial detention on 3 November 2021, in view of the evidence collected, the absence of a risk of absconding, and the prospect of the application of the active repentance provision in his case. The parties did not provide the Court with further information on the outcome of the criminal proceedings against this person.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. DOMESTIC LAW AND PRACTICE

A. Domestic law

1. The Constitution

141. The provisions of the Constitution relevant to the present case provide as follows:

Article 15

"In times of war, mobilisation, or state of emergency, the exercise of fundamental rights and freedoms may be partially or entirely suspended, or measures derogating [from] the guarantees [enshrined] in the Constitution [in relation to those rights and freedoms] may be taken to the extent required by the exigencies of the situation, [provided that] obligations under international law are not violated.

Even under the circumstances indicated in the first paragraph, the individual's right to life [and] the right to [physical] and spiritual [integrity] shall be inviolable, except

where death occurs through acts in conformity with the law of war; no one shall be compelled to reveal [their] religion, conscience, thought or opinion, nor be accused on account of them; offences and penalties shall not be made retroactive; nor shall anyone be held guilty until so proven by a court ruling."

Article 36

Everyone has the right of litigation either as plaintiff or defendant and the right to a fair trial before the courts ...

Article 38

"No one shall be punished for any act which [did] not constitute a criminal offence under the law in force at the time committed; no one shall be given a heavier penalty for an offence other than the penalty applicable at the time when the offence was committed.

...

Findings obtained through illegal methods shall not be considered evidence.

Criminal responsibility shall be personal."

Article 90 § 5

"International agreements duly put into effect have the force of law. No appeal to the Constitutional Court shall be made with regard to these agreements, on the grounds that they are unconstitutional. In the case of a conflict between international agreements, duly put into effect, concerning fundamental rights and freedoms and the laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail."

2. Relevant domestic law relating to the collection of electronic evidence, the interception of communications and the evaluation of evidence

(a) Code of Criminal Procedure (Law no. 5271 of 4 December 2004)

142. The relevant provisions of the Code of Criminal Procedure read as follows at the material time:

Article 134
Search, copying and seizure of computers, computer programs and logs

"(1) In the context of an investigation conducted in relation to a crime, where there exist strong suspicions based on concrete evidence that an offence has been committed, and there are no other means of obtaining [additional] evidence, a search may be performed on the computer used by the suspect as well as the computer programs and logs, and copies of the computer records may be obtained and the records in question may be analysed and transcribed by order of the judge upon the request of the public prosecutor.

(2) If computers, computer programs and computer logs are inaccessible due to inability to decipher the passwords or if the hidden information is unreachable, then these devices and equipment may be seized with a view to deciphering and taking the necessary copies. Seized devices shall be returned without delay [in the event that] the password has been deciphered and the necessary copies have been taken.

(3) During the seizure of the computer or computer logs, a backup of all the data in the system shall be created.

(4) The suspect or his/her lawyer shall be provided with a copy of the backup created in accordance with paragraph 3 and a report [indicating provision of such copy] shall be drawn up and signed.

(5) The data in the system may also be copied, partially or in its entirety, without seizing the computer or the computer logs. The copied data shall be printed on paper, which shall be recorded in writing and [the record] shall be signed by the concerned persons."

Article 135
Interception, wiretapping and recording of communications

"(1) The judge or, in cases where a delay would be detrimental, the public prosecutor, may decide to ... wiretap or record the telecommunications or evaluate the signal information of a suspect or an accused person if, in the context of an investigation or prosecution conducted in relation to a crime, there is strong suspicion based on concrete evidence that a criminal offence has been committed and there are no other means of obtaining [additional] evidence. The public prosecutor shall immediately submit his or her decision to the judge for approval and the judge shall take a decision within 24 hours. Upon the expiry of this period or if the judge decides to the contrary, the measure shall be lifted immediately by the public prosecutor.

...

(4) The decision to be rendered in accordance with the provisions of the first paragraph shall state the type of the imputed offence, the identity of the individual to whom the measure is to be applied, the means of communication, the telephone number, or the code which makes it possible to identify the connection of the communication, the type of the measure, its scope and its duration...

...

(6) Interception of the communications of the suspect and the accused person shall be carried out upon the order of the judge or, in cases where a delay would be detrimental, the public prosecutor at the investigation stage and on the basis of the court order at the prosecution stage. The decision shall state the type of the imputed offence, the identity of the individual to whom the measure is to be applied, the means of communication, the telephone number, or the code which makes it possible to identify the connection of the communication, and the duration of the measure. The public prosecutor shall submit his or her decision within 24 hours to the judge for approval and the judge shall take a decision within 24 hours. Upon the expiry of this period or if the judge decides to the contrary, the records shall be destroyed immediately.

...

(8) The provisions contained in this article relating to the wiretapping, recording and evaluation of signal information shall only be applicable to the offences listed below:

(a) ...

16. Offences against the Constitutional order and its functioning (Articles 309, 311, 312, 313, 314, 315, 316 [of the Criminal Code])

..."

Article 206
Production and rejection of evidence

"…

(2) A request to produce evidence shall be denied in the cases mentioned below:

a) If the evidence was obtained unlawfully ..."

Article 217
Discretion to evaluate evidence

"(1) A judge shall base his or her decision only on evidence brought to the hearings [*duruşmaya getirilen*] and assessed in his or her presence. That evidence shall be evaluated freely through the inner conviction of the judge.

(2) The imputed offence may be proven by using all kinds of lawfully obtained evidence."

(b) Law on Intelligence Services of the State and the National Intelligence Agency (Law no. 2937 of 1 November 1983)

143. Section 4 (1) of the Law provides as follows, as relevant:

"The functions of the National Intelligence Agency are:

a) To obtain national security intelligence about existing and potential future activities directed, from within or outside [the country], against the unity of the nation and the territorial integrity, existence, independence, security [and the] constitutional order of the Republic of Türkiye as well as the other elements which comprise the national strength [of the Republic of Türkiye] and to communicate such intelligence to the President, the Chief of the General Staff, the Secretary General of the National Security Council and related public institutions,

...

i) To collect, record, and analyse information, documents, news and data by using all kinds of technical intelligence and human intelligence methods, tools and systems on foreign intelligence, national defence, counterterrorism, international crime and cyber security, and to communicate the generated intelligence to the relevant bodies."

144. Sections 6 (1) and (2) of the same Law read as follows, insofar as relevant:

"(1) In performing its duties hereunder, the National Intelligence Agency shall be empowered:

...

b) to receive information, documents, data and records from public institutions and organisations, ... and other legal persons and institutions with no legal personality; to avail itself of, and establish contact with, the archives, electronic data processing centres and communication infrastructure of these institutions and organisations. The institutions and organisations which receive such requests may not abstain from fulfilling the request by relying on their own legislation,

...

d) To employ covert working procedures, principles and techniques in the performance of its duties,

...

g) To collect data running through telecommunication channels in relation to foreign intelligence, national defence, terrorism, international crimes and cyber security.

...

(2) "For the purpose of performing the duties set out in section 4 of this Law and in the event of a serious threat against the fundamental values set out in Article 2 of the Constitution and the democratic [State governed by the] rule of law, a decision by a judge or, in cases where a delay would be detrimental, a written order by the Undersecretary or Deputy Undersecretary of the Agency, will be issued to intercept, wiretap, evaluate signal information [and] record [electronic] communications with a view to protecting national security, preventing acts of terrorism, espionage and the divulging of state secrets. The written order, given in cases where a delay would be detrimental, shall be submitted to the competent judge within 24 hours..."

145. Additional section 1 of the same Law provides as follows, as relevant:

"The information, documents, data and records in the possession of the National Intelligence Agency relating to intelligence, as well as the analysis undertaken [by the latter], may not be requested by judicial authorities, unless in relation to offences indicated in [Book 2, Chapter 4 and Part 7] of the Turkish Criminal Code."

3. Relevant domestic law governing organised crime and terrorism

(a) Criminal Code (Law no. 5237 of 26 September 2004)

146. Article 220 of the Criminal Code, which concerns the offence of forming an organisation with the aim of committing a criminal offence, provides as follows, as relevant:

"(1) Anyone who forms or leads an organisation established to carry out acts defined by law as criminal offences shall be sentenced to a term of imprisonment of four to eight years, provided that the structure of the organisation, the number of its members, and its tools and equipment are found to be appropriate for the commission of the intended offences. However, for an organisation to exist there must be at least three members.

(2) Anyone who becomes a member of an organisation established for the purpose of committing a criminal offence shall be sentenced to a term of imprisonment of two to four years.

(3) If the organisation is armed, the sentence to be imposed in accordance with the above paragraphs shall be increased by between one quarter and one half."

147. Article 314 §§ 1 and 2 of the Criminal Code provides for the offence of membership of an armed organisation:

"(1) Anyone who forms or leads an armed organisation with the purpose of committing the offences listed in the fourth and fifth parts of this chapter shall be sentenced to a term of imprisonment of ten to fifteen years.

(2) Any member of an organisation referred to in the first paragraph shall be sentenced to a term of imprisonment of five to ten years."

Parts four and five of the chapter to which Article 314 § 1 refers list offences against State security and against the constitutional order and its functioning.

148. Article 30 of the Criminal Code reads as follows:

Mistake
Article 30

"(1) Any person who, while performing an act, is unaware of matters which constitute the *actus reus* of an offence as defined in the law, is not considered to have acted intentionally. Culpability for recklessness arising from such mistake shall be preserved."

(b) Prevention of Terrorism Act (Law no. 3713 of 12 April 1991)

149. The relevant provisions of the Prevention of Terrorism Act provide as follows:

Definition of Terrorism
Section 1
(before amendment by Law no. 4928 of 15 July 2003)

"(1) Terrorism is any kind of act committed by one or more persons belonging to an organisation with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, undermining the territorial integrity of the State and the unity of the nation, endangering the existence of the Turkish State and Republic, weakening or destroying or usurping the authority of the State, eliminating fundamental rights and freedoms, undermining the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat."

Section 1
(as amended by Law no. 4928 of 15 July 2003)

"(1) Terrorism is any kind of criminal act committed by one or more persons belonging to an organisation with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, undermining the territorial integrity of the State and the unity of the nation, endangering the existence of the Turkish State and Republic, weakening or destroying or usurping the authority of the State, eliminating fundamental rights and freedoms, undermining the internal and external security of the State, public order or general health by using force and violence and through one of the methods of pressure, terror, intimidation, oppression or threat."

Terrorist Offenders
Section 2

"(1) Any member of an organisation founded to attain the aims defined in section 1 who commits a crime in furtherance of these aims, individually or together with others, or any member of such an organisation, even if he or she does not commit such crime, shall be deemed to be a terrorist offender."

Terrorist Offences
Section 3

"The offences indicated in Articles 302, 307, 309, 311, 312, 313, 314, 315 and 320, as well as paragraph 1 of Article 310, of the Turkish Criminal Code [no. 5237] are terrorist offences."

Terrorist Organisations
Section 7

"(1) Those who form, lead or become members of a terrorist organisation in order to commit crime [that is] directed at the purposes set out under section 1, by use of force and violence, and by means of pressure, terror, intimidation, oppression or threat, shall be punished in accordance with the provisions of Article 314 of the Turkish Criminal Code..."

4. Relevant domestic law concerning the judiciary

(a) Law no. 6723 amending the Law establishing the Supreme Administrative Court and certain laws (1 July 2016)

150. On 1 July 2016 the Turkish Parliament enacted Law no. 6723, which amended certain laws, including the Court of Cassation Act (Law No. 2797). Section 22 of Law no. 6723, which entered into force on 23 July 2016, added a provisional article to Law no. 2797. This section mainly provided for the cessation, with certain exceptions, of the terms of office of the members of the Court of Cassation as of the date of its entry into force and reduced the total number of members to be re-elected. It further stipulated that those judges who were not re-elected as members of the Court of Cassation would be appointed by the High Council of Judges and Prosecutors to another position in accordance with their class and grade.

(b) Legislative Decrees nos. 667 and 685

151. Article 3 § 1 of Legislative Decree no. 667, which came into force on 23 July 2016 as part of the state of emergency measures, provided, *inter alia*, that judges and prosecutors, including the members of the Constitutional Court and the higher courts, would be dismissed from office if they were considered to belong to, be affiliated with or linked to terrorist organisations or organisations, structures or groups which the National Security Council had established were engaged in activities prejudicial to national security. The dismissal decision was to be taken by the absolute majority of the Constitutional Court, sitting in plenary formation, in respect of the members of the Constitutional Court, by the First Presidency Board of the Court of Cassation in respect of the members of the Court of Cassation, and by the High Council of Judges and Prosecutors in respect of prosecutors and judges who were not members of the high courts.

152. On 18 October 2016, the Turkish Parliament adopted Law no. 6749 (published in the Official Gazette on 29 October 2016), approving Legislative

Decree no. 667. Article 3 § 1 of Legislative Decree no. 667 was incorporated into Article 3 § 1 of Law no. 6749.

153. Legislative Decree no. 685 adopted on 2 January 2017 provided in its Article 11 that persons who had been dismissed from their duties under Article 3 § 1 of Legislative Decree no. 667 and Law no. 6749 could challenge the measure before the Supreme Administrative Court, acting as a court of first instance.

5. Other relevant domestic law

154. Article 6 § 1 (d) of Legislative Decree no. 667 introduced some restrictions, to be applied during the course of the state of emergency, on the right to legal assistance of persons detained in relation to certain offences against the Nation and the State set out in the fourth chapter of Book Two of the Criminal Code (including the offence of membership of an armed organisation under its Article 314), the offences falling within the scope of the Prevention of Terrorism Act, and collective offences. Article 6 § 1 (d) provided, *inter alia*, that the meetings of persons in detention with their lawyers could be recorded, that the meetings could be attended by an officer to monitor the exchanges, or that the documents and files exchanged and the records kept by the detainees or their lawyers could be seized upon the decision of the public prosecutor, where it was deemed necessary for the reasons listed therein. This article was incorporated into Article 6 § 1 (d) of Law no. 6749 adopted on 18 October 2016 and published in the Official Gazette on 29 October 2016 (see paragraph 152 above).

B. Domestic practice

1. Case-law of the Court of Cassation

(a) Judgments of 24 April 2017 and 26 September 2017

155. On 24 April 2017 the Sixteenth Criminal Division of the Court of Cassation ("the Sixteenth Criminal Division"), sitting as a first-instance court, delivered a judgment (E.2015/3, K.2017/3), whereby it convicted two judges, namely M.Ö. and M.B., of membership of the FETÖ/PDY and abuse of office. This was the first judgment by the Court of Cassation holding the said organisation to be a "terrorist organisation". In reaching this verdict, the high court relied on the use of the ByLock messaging system by the judges concerned, as well as on evidence demonstrating that they had adopted judicial decisions – which involved releasing sixty-three suspects detained in connection with FETÖ/PDY-related charges – on the basis of an encrypted instruction by F. Gülen published on a FETÖ/PDY-affiliated website (see *Başer and Özçelik v. Türkiye*, nos. 30694/15 and 30803/15, 13 September 2022 for further details relating to the charges brought against these two

judges). On 26 September 2017 the plenary criminal divisions of the Court of Cassation upheld this judgment (no. E. 2017/16-956, K. 2017/370).

156. In these two judgments (hereinafter referred to as the "the landmark judgments"), which shaped the course of all ensuing criminal proceedings involving the use of ByLock, the Court of Cassation made important findings as regards the legal framework regulating the collection of the ByLock data, the nature and features of the ByLock application and its probative value, and the structure of the FETÖ/PDY.

(i) Findings regarding the legal basis for the collection of the ByLock data

157. In both judgments, the Court of Cassation reiterated at the outset that by virtue of Article 217 § 2 of the CCP (see paragraph 142 above), courts could rely on all types of evidence, whether physical or electronic, to establish guilt, as long as the evidence at issue was obtained lawfully. It further found, for the reasons subsequently relied on by the Ankara Regional Court of Appeal (see paragraph 85 above), that the collection and processing of the ByLock data had been carried out in compliance with the relevant legal framework.

(ii) Findings regarding the characteristics of the ByLock application and the probative value of its use

158. The Court of Cassation next examined the nature of the ByLock application and the elements that it considered relevant to determine whether it was a commercial application or had been used exclusively by the FETÖ/PDY. The Court of Cassation's examination here largely reflected the findings that had been made by the MİT (see paragraphs 114-116 above; see also *Akgün v. Turkey*, no. 19699/18, §§ 68-81, 20 July 2021), which had subsequently been verified by the KOM following the handover of the relevant data to the judicial authorities. In this respect, the Court of Cassation noted that while the ByLock application was publicly available and accessible at the application stores in early 2014, the members of the organisation downloaded it through external hard drives, memory cards and Bluetooth after its removal from those stores, as revealed by the statements, messages and e-mails included in the relevant investigation files.

159. The Court of Cassation further established that almost all the transcribed contents of the communication via ByLock concerned organisational contacts and activities and listed some of the conversation topics as follows: changes of meeting places; prior notice of the operations to be conducted; provision of secret hiding places for members; plans for fleeing abroad; meetings for collection of money (*himmet*) and financial support for organisation members suspended or dismissed from office; conveying instructions and opinions of F. Gülen; sharing of websites which operate for the purpose of portraying Türkiye as a country supporting terrorism; ensuring

the release of suspects or accused persons, by certain judges and prosecutors, within the scope of the investigations conducted into and the prosecutions brought against the FETÖ/PDY; ensuring the appointment of lawyers to assist members of the organisation; providing information on the places where operations might be conducted and sending warnings that important digital data in such places be disposed of; informing the members that if disclosed, the use of ByLock should be discontinued, and alternative programs such as Eagle, Dingdong and Tango should be used instead; and preparation of legal texts which would be used in the defence of organisation members.

160. Having regard to the technical features of the application and the special procedures relating to its use, as well as to the profile of the users and the content of the decrypted messages exchanged, the Court of Cassation arrived at the conclusion in both judgments that, under the guise of a universal messaging application, ByLock was in fact a communication system intended for the exclusive use of the members of the armed terrorist organisation FETÖ/PDY, and had been used as such. The relevant excerpt from the judgment of the plenary criminal divisions of the Court of Cassation reads as follows:

> "In the ByLock communication system, it is possible to determine the date of connection, the IP address from which the connection was made, the number of connections over a given period of time, the persons with whom the communications were made and the content of the communication. The date of connection, the establishment of the IP address from which the connection was made and the establishment of the number of connections within a given period of time are sufficient to establish that the person is part of a special communication system. The persons with whom the communications were made and the determination of the content of these communications is information that can be useful in determining the person's place within the structure [terrorist organisation]. In other words, it is information that can be used to establish the person's position in the organisation's hierarchy (leader of the organisation/member of the organisation).
>
> Given that the ByLock communication system is a network designed for the use of the members of the armed terrorist organisation FETÖ/PDY and is used exclusively by some members of that terrorist organisation, where it is established – beyond doubt by technical data capable of supporting a firm conviction – that [a person] has joined that network on the instructions of the organisation, and that [he or she] has used [ByLock] for communication to ensure secrecy, such finding would constitute evidence of the person's connection with the organisation."

(iii) Findings regarding the FETÖ/PDY

161. In both judgments, the Court of Cassation provided an overview of the concepts of terror, criminal organisation and terrorist organisation on the basis of the relevant legal provisions of the Criminal Code and the Prevention of Terrorism Act, and also engaged in an examination of the offence of founding, leading and membership of an armed terrorist organisation set out in Article 314 of the Criminal Code, which it considered to be a distinct form of organised criminality (see paragraphs 146-149 above). It noted that for a

structure to be classified as an "armed terrorist organisation", it would not only have to fulfil the criteria set out under Article 220 of the Criminal Code in relation to the offence of "forming an organisation with the aim of committing a criminal offence", but also had to embrace the aims and methods indicated in sections 1 and 7 of the Prevention of Terrorism Act. It stressed that the requirement of use of "force and violence" in section 7 of the relevant Act did not necessarily mean the actual use of force and violence, and that an existing threat that such force and violence may be used would suffice. The Court of Cassation further maintained that the armed terrorist organisation had to be in possession of a sufficient amount of arms to carry out its aims, or to have the means of access to such arms, and it did not matter for the purposes of the offence under Article 314 of the Criminal Code whether those arms had been obtained unlawfully or were State property.

162. The Court of Cassation then proceeded to examine the history, nature and characteristics of the FETÖ/PDY, which it described as a "*sui generis* terrorist organisation". The relevant findings were noted in the judgment of the plenary criminal divisions of the Court of Cassation as follows:

> "The FETÖ/PDY is an atypical/*sui generis* armed terrorist organisation which uses religion as a front and a means to attain its non-religious earthly purposes; which acts in line with the instructions of the organisation leader having the intent of establishing a new political, economic and social order; which, to that end, primarily aims at having power and acts with great secrecy – instead of transparency and openness – with a view to being strong and establishing a new order; which uses ... codenames, special communication channels, and money from unknown sources; which tries to convince everyone that such structure does not exist and has grown and gained strength to the extent that it has succeeded in giving such an impression; which considers those who are not affiliated to it as an enemy ...; which, instead of clashing with the system, penetrates the State from bottom to top in pursuit of the seizure of the system, through its members named 'Golden Generation'; which, after gaining a certain power [following the penetration of various State institutes] eliminates its adversaries by means of illegal methods that appear legal; which thereby aims at ensuring social transformation by taking whole sub-elements of the State under its control and seizing the system as well as by using the public power it has gained; and which also performs espionage activities.
>
> The FETÖ/PDY armed terrorist organisation, which harbours the aim of taking over all constitutional institutions of the Republic of Türkiye by using its human and financial resources ... is founded on the principles of 'living covertly, always fearing, not telling the truth, denying the truth'.
>
> Fetullah Gülen, the leader of the organisation ... has given the following instructions to the members of the organisation, [which] demonstrate the utmost importance attached to confidentiality within the organisation:
>
> 'Be flexible. Move through their vital points without [being noticed]! Progress towards the vital points of the system until reaching all power centres without letting anyone notice you!'
>
> 'Existence of our fellows in the courthouses, the civil service or other critical institutions and organisations must not be regarded as individual existence. They are

our guarantees in these units for the future. To some extent, they are guarantors of our existence.'

'The time is not yet appropriate. You must wait until the moment we can shoulder the world, until the moment we are ready and the conditions are favourable! We must be ahead of [our] adversaries particularly as regards obtaining information.'

'..., you do not dominate ..., there are other powers. It is advisable to proceed in a balanced, attentive, cautious manner by taking into account the various powers in this country so that we do not take steps backwards...'

'Each step is early until the moment we can get a hold of the power and strength in all constitutional institutions of Türkiye. ... if you disclose [your secret], you would be taken captive by [that] secret.'

...

'Tell me one day that we have a thousand houses in Ankara, then I will seize the State by the legs, and when the State 'wakes up', there would be nothing left to do'.

...

The organisation has a layered hierarchical structure. Transfers between the layers is possible; that said, transfers above the fourth layer are determined by the leader. The layers are constituted as follows:

a) First Layer (Common tier): Consists of those who are connected to the organisation by faith and ties of affection and who provide actual and material support. This layer mostly consists of persons who are not part of the organisation's hierarchical structure, but who nevertheless serve [it], knowingly or unknowingly.

b) Second Layer (Faithful tier): The group of faithful people composed of those working at schools, private tutoring centres, student dormitories, banks, newspapers, foundations and institutions. These are people who attend organisational conversation meetings (*sohbet*), who regularly pay dues, and who are more or less familiar with the organisation's ideology.

c) Third Layer (Ideological organisation tier): Persons who undertake duties in unofficial activities, who adopt the organisational ideology and who accordingly disseminate the propaganda of the organisation.

d) Fourth Layer (Inspection and control tier): Persons who are in this layer supervise all [organisational] service (legal and illegal). Those who attain the required rank in terms of commitment and obedience may be promoted to this layer. [Members of] this layer are those who joined the organisation at a young age; those who join the organisation later on can usually not undertake duties in this layer or the layers above.

e) Fifth Layer (Organising and executing tier): Requires a high level of confidentiality. Those in this layer barely know each other. They are appointed by the organisation's leader and organise and oversee [the activities] at the State level.

f) Sixth Layer (Special/Private tier): Consists of those who are personally appointed by Fetullah Gülen and who ensure communication between the leader and subordinate layers and who have the power, within the organisational structure, to reassign and dismiss.

g) Seventh Layer (Senior tier): This is the most eminent layer of the organisation consisting of seventeen people chosen directly by the leader of the organisation.

The organisation has been careful to observe cell-type horizontal structuring in order not to be disclosed and to prevent the State from deciphering the organisational structure...

...

Although the FETÖ/PDY militants who had penetrated into the TAF [Turkish Armed Forces], the Security Directorate and the MİT are public officers in appearance, their sense of organisational belonging surpasses all other commitments. It has been understood that the FETÖ/PDY uses the public force, which should remain at the State's disposal, for its own organisational interests. The members of the organisation who have entered into public service at the TAF, the Security Directorate and [the MİT] ..., as a "soldier" of the FETÖ/PDY, undergo an ideological training according to which they are ready to employ their weapons and their authority to use force in line with the instructions given by their hierarchical superior ...

The FETÖ/PDY, which has organised itself in the operative units of the Security Directorate and the TAF, instrumentalises the oppression and intimidation emanating from the authority to use force and violence inherent in the [aforementioned bodies]. The organisation members' capacity to have recourse to arms as needed is essential, and sufficient, for the constitution of the offence of 'armed terrorist organisation'; during the coup attempt of 15 July 2016, weapons were used by the members of the organisation, who ... appeared to be TAF officers but who acted in line with the orders and instructions of the organisation leader, as a result of which many civilians and public officials were martyred.

... "

In the light of the foregoing considerations, and noting in particular that certain members of the organisation were employed in State bodies possessing the power to use arms, and would not hesitate to use those arms if instructed to do so by the hierarchy of the organisation, the plenary criminal divisions of the Court of Cassation found it self-evident that the FETÖ/PDY was an armed terrorist organisation within the meaning of Article 314 of the Criminal Code.

163. The plenary then went on to examine the circumstances under which a purported member of this armed terrorist organisation could escape liability by invoking the defence of mistake under Article 30 of the Criminal Code (see paragraph 148 above) and held the following, as relevant:

"A criminal organisation may be an illegal structure which is established at the outset to commit an offence. [Similarly], a non-governmental organisation which functions on a legal basis may subsequently turn into a criminal organisation and even into a terrorist organisation. In this connection, while the legal existence of an organisation – which has already been in existence unbeknownst to the public on account of the absence of a judicial decision [acknowledging its existence] – is contingent upon a decision to be issued by the courts, the founder, the executives or the members of the organisation would be held responsible in criminal law as from its foundation or from the date on which it became a criminal organisation despite having being founded for legitimate aims.

Regard being had to the fact that the offence of membership of an armed terrorist organisation [is an offence that] may [only] be committed with direct intent [*doğrudan kast*], an assessment would need to be undertaken under the mistake provision set out

in Article 30 § 1 of the Turkish Criminal Code in circumstances where some of the members of an organisation, who are part of structures which carry out their activities on a legal basis [but which harbour an] ultimate purpose that is not clearly known due to its concealment, claim that they were unaware of the fact that the relevant structure was a terrorist organisation.

...

Intent refers to the materialisation of the elements in the legal description of the offence wilfully and knowingly, and a lack of knowledge, or incomplete or incorrect information, about those elements amounts to a mistake related to the material elements. If the mistake is to such an extent that would prevent the existence of an intent, no penalty would be imposed on the accused...

...

There is no doubt that the FETÖ/PDY terrorist organisation possesses the necessary and sufficient organisational power, considering that it has been organised [clandestinely] in order to achieve its ultimate goal of altering the constitutional order of the State by force and violence, and [given its] presence in the armed forces of the State. It is also clear that the members of the organisation who know its goals and methods will be punished on the basis of their positions within the organisation. According to the organisational pyramid, it must be accepted that the members in the fifth, sixth and seventh layers and, as a rule, those in the third and fourth layers, fall into this category. However, a factual assessment must be carried out under Article 30 of the Turkish Criminal Code as to whether the members of the organisation pertaining to the other layers – who were utilised as the so-called legitimacy front of the organisation – were aware of the relevant [goals and methods], in view of the fact that the FETÖ/PDY first turned into a religious cult and subsequently into a terrorist organisation despite having initially emerged, and been widely perceived, as a moral and educational movement, that the organisation concealed its illegal objectives and tried to avoid being criminalised in the public eye, and that a decision of acquittal had been delivered by the Ankara Eleventh Assize Court in respect of Fetullah Gülen.

In this connection, while undertaking this assessment, it is necessary to take into consideration the ongoing investigations and prosecutions [concerning the FETÖ/PDY] throughout the country, the [General Security Directorate] reports and other documents in the relevant case files concerning the FETÖ/PDY, the judgments delivered by [various] courts, the confessions made by the accused in the relevant cases, the witness statements, and the intense discussions that have occupied the public agenda for a long period over [some] sensational incidents that have ... revealed the ultimate goal of the organisation. Among these incidents, [one may] note the MİT crisis of 7 February 2012, the so-called 17-25 December operations ..., and the interception of MİT trucks on 1 and 19 January 2014.

It should moreover be noted that in the National Security Council decisions taken on 30 October 2014 and thereafter, which were shared with the public, the FETÖ/PDY was assessed to be a terrorist organisation that threatened national security and disrupted public order, that conducted illegal activities under a legal appearance within the State, that had an illegal economic aspect and that cooperated with other terrorist organisations. [It was moreover] decided to wage an effective fight against this terrorist organisation with the entire State apparatus, and [these decisions] and statements were espoused at the highest ranks of the State and Government and shared with the public."

164. Having regard to the special status of M.Ö. and M.B. as judges in the organisational structure – who were considered to belong to the "private"

(*mahrem*) part of the organisation, along with members of the armed forces and law enforcement agencies –, their level of education, and the knowledge and information that they had acquired through their profession, the Sixteenth Criminal Division held that they were in a position to know the organisation's ultimate goal, its configuration within the armed forces and, consequently, the fact that it was an armed terrorist organisation. The mistake provision stipulated under the Criminal Code would not, therefore, be applied in their case. They were accordingly convicted of, *inter alia*, membership of an armed terrorist organisation, on account of their use of the ByLock application that had been created for the exclusive use of the FETÖ/PDY members, and of their conduct in respect of the mass release of FETÖ/PDY suspects, which they had carried out in accordance with the instructions issued by the FETÖ/PDY, an act which the court deemed could only be carried out by a devoted member of the organisation.

165. In upholding their conviction for membership of an armed terrorist organisation, the plenary criminal divisions of the Court of Cassation emphasised that M.Ö. and M.B.'s use of ByLock was evidence that they were a part of the FETÖ/PDY's hierarchical structure. It further added that the absence of a final judicial ruling determining that the FETÖ/PDY was a terrorist organisation at the time of the commission of the offence did not prevent establishing the criminal liability of the accused, who had carried out the relevant acts knowingly and willingly.

(b) Other relevant judgments of the Court of Cassation

166. The judgment delivered by the plenary criminal divisions of the Court of Cassation on 27 June 2019 (E.2018/16-418, K.2019/513) provided further information on how the raw data obtained from the ByLock server and the CGNAT data had been assessed in establishing whether a person had used the ByLock application. The relevant paragraph from this judgment provides as follows:

> "CGNAT ... data, which contain the Internet traffic records of the subscribers who have connected to the nine IP addresses of the ByLock server from IP addresses in Türkiye, and which are retained by the operators, are a kind of metadata. As such data reveal that the subscriber's IP address has connected to IP addresses of the ByLock server, they constitute an important indication of the relevant person's involvement in the ByLock system; however, they do not provide any information ... as to whether the relevant subscriber has been assigned a user ID..."

167. According to the Court of Cassation, the presence of CGNAT data showing a person's connection to the ByLock IP addresses, in circumstances where no ByLock user ID had been discovered, could mean one of these two things: either the KOM inquiry on the data obtained from the ByLock server had not yet been completed – or the relevant data could not be recovered or transcribed –, or the person in question had been unwittingly diverted to the ByLock server through traps such as via the application known as *Mor Beyin*

(see paragraph 119 above), which was apparently developed and used to deliberately direct users of certain applications – mainly of an Islamic nature – to ByLock servers.

168. In the same vein, an earlier judgment delivered by the Sixteenth Criminal Division of the Court of Cassation on 29 April 2019 (E.2019/98, K.2019/3057) maintained that the presence of a user ID would demonstrate that a person had connected to the ByLock server directly, without any routing, and a detailed ByLock assessment and identification report would provide information on the identity of the real user, as well as his or her position within the organisation and activities. The Court of Cassation quashed the conviction in that case since, despite the presence of CGNAT data and a ByLock user report issued by the KOM, which constituted "significant indications" as to the use of ByLock, the individual's user ID had not been identified and the possibility of inadvertent connections had therefore not been ruled out.

2. Case-law of the Constitutional Court

169. The Constitutional Court has delivered a number of key judgments in the context of the criminal proceedings brought in the aftermath of the military coup attempt. A number of those judgments, such as *Aydın Yavuz and Others*, dated 20 June 2017 (application no. 2016/22169) and *M.T.*, dated 4 June 2020 (application no. 2018/10424) have been cited at length by the Court in the cases of, *inter alia*, *Baş v. Turkey* (no. 66448/17, §§ 91-97, 3 March 2020), *Ahmet Hüsrev Altan* (cited above, §§ 88 and 89) and *Akgün* (cited above, §§ 83-101). Below is a summary of other Constitutional Court judgments, which are deemed to be particularly relevant for the purposes of the present case.

(a) Judgment of *Ferhat Kara* dated 4 June 2020 (application no. 2018/15231)

170. On 4 June 2020 the Plenary of the Constitutional Court delivered a judgment in the case of *Ferhat Kara*, which concerned the alleged violation of the right to a fair trial on the ground that the data regarding the use of ByLock had been obtained unlawfully and were relied on as sole or decisive evidence for conviction for membership of the FETÖ/PDY, and that the relevant digital data were not brought before the trial court.

171. The Constitutional Court commenced its examination by setting out the facts and the background to the case, providing an overview of the FETÖ/PDY and of the ByLock application, both in terms of its technical features and the manner in which the application data had been obtained and processed by various authorities. It then examined the admissibility and merits of Mr Kara's complaints.

(i) Constitutional's Court's findings regarding the facts and the background to the case

172. The Constitutional Court held that beyond its legal activities, the FETÖ/PDY was an illegal structure and that its actions and activities had been a matter of debate in society for a long time. In keeping with its purpose, its members had committed acts such as destroying evidence, wiretapping the phones of public institutions and high-level State officials, disclosing the State's intelligence activities, and obtaining questions in advance of the exams held for recruitment or promotion in public institutions, to be distributed amongst its members. It had accordingly been the subject of many investigations and prosecutions, particularly after 2013. The Constitutional Court continued to list the illegal activities of the FETÖ/PDY as follows:

> "14. In this context, it was alleged that many cases leading to intense public debates such as '*Şemdinli*', '*Ergenekon*', 'Sledgehammer' [*Balyoz*], 'Military Espionage' [*Askeri Casusluk*], 'Revolutionist Military Headquarters' [*Devrimci Karargah*], 'Oda TV' and 'Match-fixing' [*Şike*], have been used [by the FETÖ/PDY] to dismiss public officials, particularly within the Turkish Armed Forces, who were not members of the organisation, or to neutralise persons who were considered to act against the interests of the organisation in civilian circles...
>
> 15. In the same vein, an investigation was launched by the public prosecutors, judges and law enforcement officers considered to be affiliated with the FETÖ/PDY against certain politicians, their relatives and certain businessmen ..., on the ground that they had allegedly been involved in corruption, and certain preventive measures were taken with regard to these persons during the operations carried out at the end of 2013. These operations, which are known to the public as the 17-25 December investigations, were considered by the public authorities as well as the investigation and judicial authorities as an organisational activity orchestrated by the FETÖ/PDY to overthrow the Government. Afterwards, administrative/judicial measures and sanctions were imposed on the members of the judiciary and law enforcement officers who were involved in these operations...
>
> 16. In addition, trucks loaded with supplies belonging to the National Intelligence Agency ('the MİT') were stopped and searched, respectively ... on 1 January 2014 and ... 19 January 2014, by law enforcement officers who were considered to be members of the FETÖ/PDY, in accordance with the instructions given by the public prosecutors who were stated to be affiliated with this structure. The public authorities as well as the investigation and judicial authorities considered the events pertaining to the stopping and searching of the MİT trucks as an organisational activity intended to create a public perception that the State of the Republic of Türkiye aided terrorist organisations, to thereby enable the prosecution of Government officials. Subsequently, the members of the judiciary and law enforcement officers involved in these operations were subject to judicial/administrative measures and sanctions.
>
> 17. [By way of] an indictment issued by the Ankara Chief Public Prosecutor's Office on 6 June 2016 in respect of the senior executives of the organisation, a criminal action was filed against 73 [persons] including Fetullah Gülen, on the ground that they had founded an armed organisation and attempted to overthrow the Government of the Republic of Türkiye and to prevent it from performing its duties...
>
> 18. In addition, the threat posed by the FETÖ/PDY at national level was also discussed in the decisions, statements and practices of the security units of the State. In

this sense, the State officials explained that the structure in question had been posing a threat to the security of the country. Such assessments were also included in the decisions of the National Security Council... On 8 January 2016, the Gendarmerie General Command included the FETÖ/PDY in the ... list of terrorist organisations.

19. Moreover, disciplinary proceedings were conducted against a great number of public officials due to their relations with the FETÖ/PDY, notably members of the judiciary and police officers, and various disciplinary sanctions including dismissal from public service or administrative sanctions were imposed in respect of many public officials. Furthermore, various administrative measures were also applied in respect of certain business organisations, financial institutions and media outlets considered to have connections with the FETÖ/PDY.

...

21. It was accepted in many judicial decisions that the FETÖ/PDY had been organised in parallel to the current administrative system with a view to taking over the constitutional institutions of the State and re-shaping the State, society and citizens in accordance with its ideology ..."

173. The Constitutional Court stressed that the FETÖ/PDY was an organisation based on confidentiality and, for that reason, it favoured communication through encrypted programs, such as ByLock, where face-to-face communication was not possible. The Constitutional Court then went on to provide a chronological account of how the ByLock program had been identified, notified to the judicial authorities and processed by the latter.

174. In this connection, the MİT had submitted to the Ankara Chief Public Prosecutor's Office the hard disk containing the digital data obtained on the ByLock program and the flash drive containing the list of the ByLock subscribers who had connected to the application as well as the technical report that it had issued. Following the order of the Ankara Fourth Magistrate's Court for the analysis of the relevant material in accordance with Article 134 of the CCP, the public prosecutor's office had instructed the KOM to conduct the necessary examination. Accordingly, the KOM had put together a working group – consisting of their personnel and that assigned by the Anti-Terrorism Department and the Departments of Intelligence and Cyber Security – for the analysis of the received data. To this end, an interface program was used to export the ByLock data. The public prosecutor's office had also requested the BTK to provide information showing the number of connections made to the ByLock IP addresses (CGNAT data) by the persons noted in the list of subscribers provided by the MİT.

175. In the meantime, a new version of the subscriber list, updated by the MİT through a detailed examination, was sent to the Ankara Chief Public Prosecutor's Office and processed by the judicial authorities in the same manner, resulting in an updated user list of 123,111 users. The Constitutional Court explained that since connections made via VPN did not have Türkiye-based IPs, the CGNAT data pertaining to those connections could not be accessed. It added that:

> "The CGNAT data that could be accessed belonged to the connections that had been made from Türkiye-based IPs to the target IPs on the ByLock server without using a VPN or that could be identified as a result of ... the VPN being disabled during the connection from Türkiye."

The Constitutional Court also underlined that an investigation was launched by the Ankara Chief Public Prosecutor's Office into the allegations that some people, who were not actually ByLock users, had inadvertently connected to the ByLock IP on account of a software named *Mor Beyin*. The software had been developed by the FETÖ/PDY with the aim of preventing the disclosure of the real users of the ByLock application and to reduce the reliability of the ByLock evidence by directing irrelevant persons to this program.

176. Basing itself mainly on the reports prepared by the investigating authorities and the earlier Court of Cassation judgments, the Constitutional Court went on to provide some information on the installation and use of the ByLock application, as well as the features distinguishing it from other messaging applications. In doing this, the Constitutional Court also referred to the statements made by some suspects in the context of FETÖ/PDY-related investigations, with a view to shedding further light on that application's use by FETÖ/PDY members, a few of which are noted below, as relevant:

> "'In March or April 2014, those on duty were asked to use the communication program called ByLock. This [instruction] was conveyed to us by the Regional EC [Education Consultant,] and he installed this program on my phone via the Internet or Bluetooth at the regional EC meeting ... Provincial supervisors installed this program, and then everyone installed it for those in their lower level, thereby expanding the communication network. The ByLock program was not installed for everyone, but rather for senior officials. The persons at the lower levels, who heard of the program from each other, also started using it over time. As far as I know, this program was used by special units and was later expanded to the regional units. This program was used by people who added each other mutually, ...'
>
> ...
>
> 'In the past three years, as there was a crisis environment, the community started increasing its pressure on prudence... As the Gaziantep Regional Meetings had not been attended intensively for precautionary purposes since 2015, the Provincial ECs attending these meetings were instructed ... about the use of ByLock. As a result of these instructions, the Provincial EC... had given the flash memory card in which the program had been installed to another EC... She told me that according to the ... instruction, I had to install the ByLock program; .... Along with the ByLock program, a phone-reset program as well as an encrypted note-taking program were installed on my phone. She said that owing to this program, ... no documents could be found [on my phone] in a police operation... When the [ByLock] program is installed, it assigns an ID [number] ... In order to add someone, the 'Add' tab is opened and the ID of the person to be added, consisting of 6-digit numbers, is written. The name of the person you want to add is written in the section 'Name of the person to be added' in the line below; since the community uses code names, generally the code name of the relevant person is written in this section. In the next line, it is requested to write a joint number in the section 'Keyword between you and the person you will add'. We were told that the longer this number was, the more difficult it would be to decipher the system. After

entering this number, when you press the 'Invite' button at the bottom, a message is sent to the phone of the person to be added. When the message is opened, the button 'Enter verification' appears and it is requested to enter the keyword. Since the keyword is determined mutually, the program will be installed on the phone by entering the keyword.

As far as I learned, the ByLock program was previously used only by private service units, namely military personnel, police officers, judges and prosecutors and court personnel. It has been used by civilians for about a year. At the time when this program was installed on our phones, we were told that 'It is a program developed by our brothers, it is safe'... The person who has the ByLock program on his phone must be in a certain position in the community, that is, he must be in a high position. ... there was another program in the flash card in which ByLock had been downloaded; it was a VPN program. After this program is installed on the phone, if it is opened before ByLock, a key image appears on the top of the screen, which shows that the program is running. Then a country name is entered, which is the country from which the user appears to be connected to Internet. Whatever the entered country is, it is shown as if the user connected to the Internet from that country...'

'... As far as I recall, we were told around March-April 2015 that ByLock had been found out and that it was not safe, and we were [therefore asked] to uninstall it... At that time, ByLock was installed for everyone who belonged to the *cemaat*.'

'Following the decline in the meetings in the aftermath of 17-25 December, a program named ByLock was introduced, in order to motivate the members and prevent fall outs... we were told to download it to people whom we trusted...'

'...This [ByLock] program was different from the normal WhatsApp program; it was closed to the 'outside', only people who had specially downloaded it could use it.'

'People within the *cemaat* structure initially used Line, Coco, WhatsApp. Lately, some had started using the ByLock program...'

'At a conversation meeting, M.Ö. told us that we had to use a program named ByLock in order not to be exposed...'

'... The ByLock program appeared under the [icon] Gmail on the phone screen...'

'Those who were in important senior positions in the *cemaat*, [such as] State imams, grand regional imams ... used the ByLock program. Regional imams at lower levels, such as me, were contacted over the phone, but at some point [H.Y.] told all regional imams to download ByLock on their phones...'

'... particularly, the more senior people downloaded two separate ByLock programs on their phones. In one of them [they registered] people who could be related to the organisation but whom they could account for and in the second one, there were people related to their duties; when the police caught them, they would show the former ...'

'I ... downloaded the ByLock program in the summer of 2014 from the Google Play store... I heard about the use of this program from my friends in the *cemaat.*'

'We received discussion topics and meeting information on this program... The discussion topics concerned F. Gülen books and videos, and religious matters ...'

'As for the content of the exchanges, we shared [over ByLock] information regarding those ... arrested, and exchanged ideas on how we would act in the event of arrest.'

'I was told to install this program on the following grounds: there were some powers within the State that were hostile against the 'service movement' and that wanted to

> destroy it; we could be implicated in crimes after manipulations on digital platforms, Internet or our telephones, and that we should be protected against [such acts] by using this program... Religious messages were received over this program, [as well as] motivating messages concerning the ongoing process of conflict...'"

In addition, the Constitutional Court referred to the organisational nature of the content of the decrypted communications over the ByLock application, as had been set out in the Court of Cassation judgments (see paragraph 159 above), and also noted the exchanges between some senior members of the organisation as to how the Government could be overthrown illegally, and how the members of the judiciary and security units connected to the organisation could be employed for that purpose.

177. After recapitulating the findings in various reports and Court of Cassation judgments concerning the link between ByLock and the FETÖ/PDY, and its "organisational" features (see paragraphs 114-122 and 158-160 above), the Constitutional Court discussed the different sources of data that the authorities had relied on to establish the use of ByLock, how such data had been processed and how they had been attributed to the real users. It clarified at the outset that the ByLock data was essentially based on two sources: the primary source was the raw log data obtained by the MİT, comprising information on ByLock users, user IDs, messages, emails and voice calls and the log records pertaining to the foregoing; the second source consisted of the CGNAT data pertaining to the Internet traffic records showing access to the ByLock IPs from Türkiye. The raw data submitted to the Ankara Chief Public Prosecutor's Office were subjected to a disk imaging process and accorded a hash value, apparently as a safeguard against subsequent data alteration; one copy was submitted to the KOM for examination, the other copy was locked in a safe by the evidence unit. As for the CGNAT data, the forensics units had confirmed that they could not be altered or impaired, and they could be cross-checked from other sources.

178. The Constitutional Court moreover noted that according to the reports issued by the investigating authorities, the raw data submitted by the MİT to the Ankara Chief Public Prosecutor's Office were not as such decipherable; therefore, an interface had been developed to make sense of the data and to associate them with the different user IDs.

(ii) Constitutional Court's findings regarding Mr Kara's complaints

179. Having set out the factual and legal background governing the case, the Constitutional Court proceeded to examine Mr Kara's complaints.

180. The Constitutional Court dealt in the first place with Mr Kara's allegation that he had been convicted on the basis of unlawful evidence, on account of the failure of the MİT and subsequently the judicial authorities to comply with the relevant laws in the procurement and processing of the digital ByLock data. As regards the data obtained by the MİT from the ByLock server in Lithuania, the Constitutional Court reiterated that at the

time when the investigating authorities and the security units of the State had started acknowledging the threat posed by the FETÖ/PDY to national security, the MİT had also conducted inquiries, within its own mandate under sections 4 and 6 of the Law on Intelligence Services, on the activities of the FETÖ/PDY. These inquiries had led it to the relevant ByLock data, which it had duly shared with the investigating authorities to ascertain whether they involved any criminal elements. The MİT's conduct, which merely involved the transmission to competent judicial authorities of concrete data – and not hearsay intelligence information of an abstract nature – that was discovered lawfully and that related to a matter falling within its mandate (counter-terrorism), could not be construed as engaging in law enforcement activities with the aim of collecting evidence. The judicial authorities were always entitled to test the authenticity and reliability of the digital materials handed over to them, which they had duly done in the present case in accordance with the procedure set out in Article 134 of the CCP. Besides, the defence had been granted the opportunity to challenge the veracity and the use of such digital data, as required by the principles of equality of arms and adversarial proceedings.

181. The Constitutional Court next examined whether the courts' reliance on the ByLock data as the sole or decisive evidence for conviction had rendered the procedural guarantees of a fair trial devoid of any effect and had been manifestly arbitrary. Referring to the various features of the ByLock application as outlined mainly in the judgment of the plenary criminal divisions of the Court of Cassation (dated 26 September 2017 – see paragraphs 158-160 above), the Constitutional Court stated that the findings and assessments regarding ByLock, including as regards its "exclusive" use by the members of FETÖ/PDY and the probative value of the evidence showing such use, could not be considered to have been devoid of a factual basis. The Constitutional Court further emphasised that the finding as to the use of ByLock did not stem from a single set of data, but was based on the verification of such data using information, documents, records and data obtained from other sources. In these circumstances, and bearing in mind that it fell principally on the trial courts to assess whether a single piece of evidence sufficed for a finding that the offence of membership of an armed terrorist organisation had been committed, the Constitutional Court concluded that reliance on the ByLock evidence in the circumstances of the case had not rendered the procedural guarantees wholly ineffective or been manifestly arbitrary.

(b) Judgment of *Adnan Şen* dated 15 April 2021 (application no. 2018/8903)

182. On 15 April 2021 the Constitutional Court, sitting in plenary, delivered another judgment concerning an individual convicted of membership of the FETÖ/PDY on the basis of his use of ByLock. It principally examined an alleged violation of the principle of *nullum crimen,*

nulla poena sine lege on the ground that the judicial interpretations as to the offence of membership of an armed terrorist organisation had not been foreseeable and that the conviction had been based on acts that did not constitute an offence. The applicant in that case argued in particular that the structure previously known as the "Gülen movement" had been declared a terrorist organisation by a decision of the National Security Council dated 26 May 2016, with no mention of it being a terrorist organisation in the previous decisions, and that there was no evidence of any acts of violence before the said date that could suggest that the relevant structure was a terrorist organisation.

183. Similar to its approach in the *Ferhat Kara* case, the Constitutional Court first embarked on an examination of the characteristics and activities of the FETÖ/PDY. Reiterating that the clandestine activities of that organisation had already been the subject of investigations and prosecutions as of 2013, the Constitutional Court listed the incidents that had revealed the ulterior aims of this organisation, as noted in *Ferhat Kara* (see paragraph 172 above). It also referred to some other criminal proceedings initiated against suspected FETÖ/PDY members prior to the coup attempt, such as the proceedings brought in 2015 against the police officers who had refrained from taking any measures to prevent the murder of Hrant Dink despite their knowledge of the murder plans, allegedly in pursuance of the objectives of the organisation; the espionage proceedings brought in 2014 and 2015 against a number of public officials for bugging the residence and offices of the Prime Minister, as well as some high-level confidential meetings, and for wiretapping the encrypted telephones of senior State officials; and the many investigations launched regarding the allegations of the leaking of the questions for civil service entry and promotion exams to the members of the organisation.

184. The Constitutional Court then reviewed the relevant domestic law and practice in respect of the offence of membership of an armed terrorist organisation. It noted that, according to the settled case-law of the Court of Cassation, conviction for membership of an armed terrorist organisation would only follow where the courts could (i) establish the suspect's organic link with the organisation, based on the continuity, diversity and intensity of his or her activities; and (ii) demonstrate that he or she had acted knowingly and willingly within the organisation's hierarchical structure. Amongst many Court of Cassation judgments, the Constitutional Court cited the following passage from the Sixteenth Criminal Division (E.2019/521, K.2019/4679, 5 July 2019), as relevant:

> "A member of an organisation is a person who embraces the objectives of an organisation, who adheres to [its] hierarchy, and who submits to the will of the organisation by [his or her] readiness to discharge the duties entrusted to [him or her] ... A member of the organisation must have an organic link with it and must participate in its activities. An organic link, which is the most important element of membership, is a link which is live, transitive, and active: it makes a perpetrator available for

commands and instructions and determines [his or her] hierarchical position. [The offences of] aiding an organisation or committing a crime on behalf of an organisation [also] involve commands or instructions [from the organisation]. However, the distinctive factor in the determination of membership of an organisation is the readiness of the member to comply, in full submission, with all orders and instructions issued within the organisational hierarchy, without calling them into question.

...

Although the commission of an actual crime in connection with the organisation's activities and for the achievement of its aims is not required for punishment for membership of a terrorist organisation, the [individual] must nevertheless have made a concrete material or mental contribution to the organisation's actual existence or reinforcement...

...

According to the established judicial practice, ... in order for the offence of membership of an armed organisation to be constituted, there must exist an organic link with the organisation and, as a rule, there must exist acts and activities of a continuous, diverse and intense character. However, despite the lack of such 'continuity, diversity and intensity', the perpetrators of acts which – given their nature, the method of their commission, the weight of the resulting harm and danger, and their contribution to the aims ... of the organisation – may only be committed by a member, would also be considered as members of the organisation...

...

Mental element: The mental element of the crime is direct intent and the 'aim/objective of committing a crime'. A person partaking in an organisation must know that the organisation is one that commits crimes [or] aims to commit crimes.

..."

The Constitutional Court also referred to a number of Court of Cassation judgments where acts such as attendance at conversation meetings (primarily before 2013), communicating (via telephone) with the district imam and other suspected members of the organisation, subscription to newspapers issued by the organisation and enrolment of children in schools affiliated with the organisation were considered as acts not going beyond mere sympathy and affiliation with the FETÖ/PDY, as they did not suggest an organic link to it or participation in its hierarchy.

185. The Constitutional Court noted that the concepts of "terror" and "terrorism" did not have universally accepted definitions; nevertheless, the courts were under an obligation to interpret the domestic law in a foreseeable manner that did not undermine the essence of the principle of *nullum crimen, nulla poena sine lege* when ruling on terror offences. The main issue in the case before it, from the perspective of the said principle, was whether acts performed in connection with the FETÖ/PDY in the period prior to the coup attempt could be taken as evidence of membership of that organisation, given that the FETÖ/PDY's criminal activities were not widely known in the relevant period.

186. In this connection, the Constitutional Court acknowledged that under Turkish law, the classification of a structure as a terrorist organisation was only possible by way of a judicial decision. It also reiterated, however, that prior to the characterisation of the FETÖ/PDY as a terrorist organisation by a judicial decision, the threat posed by the FETÖ/PDY had already been recognised in the decisions of the National Security Council, as well as in the 2014 National Security Policy Document, and many investigations had been launched before the coup attempt on suspicion of membership of the FETÖ/PDY.

187. The Constitutional Court further emphasised that the absence of a judicial ruling declaring an organisation "terrorist" would not exclude the criminal liability of the members of such organisation, since an approach to the contrary would lead to impunity of all members in the period preceding the judicial ruling. That said, when assessing an individual's membership of the FETÖ/PDY it had also to be borne in mind that a significant proportion of the population had known and supported this organisation for many years as a religious group carrying out activities beneficial to society, such as in the field of education, without being aware of its illegal nature. An allegation as to the lack of knowledge of the true nature of the FETÖ/PDY would accordingly be examined in the light of the mistake provision under Article 30 of the Criminal Code (see paragraph 148 above), having regard to factors such as the accused's position in the organisation and the nature of the acts attributed to him or her. Moreover, acts performed prior to the period when the activities of the FETÖ/PDY had started being denounced at different levels of the State and among the public would not be considered by judicial authorities as falling within the scope of criminal "organisational" activities, unless there were concrete facts and evidence suggesting that those acts had served the terrorist organisation, in view of their nature and substance. In other words, the courts would seek to establish, on the basis of concrete evidence, whether the acts at issue had been carried out with "organisational" aims and within the framework of an "organisational" relationship.

188. Turning to the facts before it, the Constitutional Court stated that the applicant Adnan Şen had not been convicted for the act of using ByLock, but because his use of ByLock had been considered to be evidence demonstrating his membership of the FETÖ/PDY. Based on the recognition that ByLock had been utilised by members of the FETÖ/PDY since early 2014 to conceal themselves and to ensure their organisational communication, the courts had found it established that the applicant had used that "organisational" application for "organisational" purposes, and therefore had full knowledge of the criminal intentions of that organisation. Consequently, the requisite conditions of continuity, diversity and intensity had been met. The applicant was also in a position to know the elements of the offence of membership of an armed terrorist organisation. The Constitutional Court emphasised that the

courts' findings in the applicant's respect had not unduly extended the scope of the relevant offence in contravention of the principle of *nullum crimen, nulla poena sine lege* and had therefore been foreseeable.

3. Criminal proceedings brought against F. Gülen in 1999

189. Following the initiation of an investigation in 1999, on 31 August 2000 the Ankara Chief Public Prosecutor's Office issued a bill of indictment against F. Gülen, charging him with founding and leading a terrorist organisation. Referring mainly to its organisation, strategy and activities, the public prosecutor claimed that the accused had established a structure that aimed at insidiously demolishing the democratic, secular and social State based on the rule of law, and replacing it with a regime based on Sharia in line with his world view, despite appearing externally to support rationalism, science and technology. There was no indication in the bill of indictment that the organisation in question had used force, violence, intimidation or threats to reach its aims.

190. By a judgment dated 10 March 2003, the Ankara Second State Security Court decided to suspend the delivery of a definitive finding on the merits of the case by virtue of section 4 of Law no. 4616, which provided for such suspension in respect of certain offences committed before 23 April 1999 (see *Urat v. Turkey*, nos. 53561/09 and 13952/11, § 38, 27 November 2018).

191. Following the amendment of section 1 of the Prevention of Terrorism Act on 15 July 2003 (see paragraph 149 above), the accused requested the re-examination of the case file and the review of the suspension decision, arguing that the acts attributed to him no longer constituted a crime under the Prevention of Terrorism Act.

192. Upon the acceptance of the request for re-examination, on 5 May 2006 the Ankara Eleventh Assize Court decided to acquit the applicant. It held that following the amendment of section 1 of the Prevention of Terrorism Act, terrorism would henceforth be confined to acts that were "criminal" and were committed "by using force and violence" by at least two or more people and with the purpose of changing the constitutional order. The Assize Court found, on the basis of the evidence in the case file, that the accused's aim of changing the constitutional order had not been established and that the allegations of the existence of such an aim were based on estimations and inferences. Even supposing that such an aim had existed, there was no evidence to suggest that the accused, or the organisations affiliated with him, had embraced the use of force and violence, or had actually used force and violence, or had committed any acts that constituted a distinct crime. Moreover, an "organisation" had to consist of at least two people under the Prevention of Terrorism Act, whereas there was only one defendant in the file. Accordingly, in the absence of a "terrorist act" or a "terrorist organisation" as defined under section 1 of the Prevention of

Terrorism Act, there was no question that the accused could have founded or lead an organisation within the meaning of section 7 (1) of that Act.

193. The judgment of the Assize Court was upheld by the Court of Cassation on 5 March 2008. Subsequently, on 24 June 2008 the plenary criminal divisions of the Court of Cassation dismissed the objection of the chief public prosecutor's office at the Court of Cassation, and the judgment became final.

II. INTERNATIONAL LAW AND PRACTICE

A. The United Nations

194. Article 15 of the International Covenant on Civil and Political Rights 1966 (ICCPR) provides:

Article 15

> "1. No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence, under national or international law, at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time when the criminal offence was committed."

195. In the decision *Nicholas v Australia* (HRC, UN Doc. CCPR/C/80/D/1080/2002), adopted during its 80th session held on 15 March and 2 April 2004, the United Nations Human Rights Committee indicated that, for a conviction to be entered in relation to any criminal offence, the prosecution must demonstrate that every element of that offence has been proven to the necessary standard:

> "7.5 ... [Th]e Committee observes that article 15, paragraph 1, requires any 'act or omission' for which an individual is convicted to constitute a 'criminal offence'. Whether a particular act or omission gives rise to a conviction for a criminal offence is not an issue which can be determined in the abstract; rather, this question can only be answered after a trial pursuant to which evidence is adduced to demonstrate that the elements of the offence have been proven to the necessary standard. If a necessary element of the offence, as described in national (or international) law, cannot be properly proven to have existed, then it follows that a conviction of a person for the act or omission in question would violate the principle of *nullum crimen sine lege*, and the principle of legal certainty, provided by article 15, paragraph 1."

196. At its 82nd session held between 20-24 August 2018, the United Nations Working Group on Arbitrary Detention ("the WGAD") adopted an opinion (no. 42/2018) in respect of a person who had been detained on suspicion of membership of the FETÖ/PDY on the basis of, *inter alia*, his alleged use of the ByLock application. The relevant findings of the WGAD read as follows (footnotes omitted):

> "87. The Working Group also notes the failure on behalf of the Government to show how the mere use of such a regular communication application as ByLock by Mr. Yayman constituted an illegal criminal activity...

> 88. In fact, it appears to the Working Group that even if Mr. Yayman did use the ByLock application, an allegation that he denies, it would have merely constituted exercise of his right to freedom of opinion and freedom of expression.
>
> ...
>
> 107. The Working Group notes that the present case is but one of a number of cases concerning individuals with alleged links to the Gülen group that have come before it in the past 18 months. In all these cases, the connection between the individuals concerned and the Gülen group has not been one of active membership and support of the group and its criminal activities but rather, as described by the Council of Europe Commissioner for Human Rights, activities of 'those who were sympathisers or supporters of, or members of legally established entities affiliated with the movement, without being aware of its readiness to engage in violence'. In all those cases, the Working Group has found the detention of the individuals concerned to be arbitrary and it thus appears to the Working Group that a pattern is emerging whereby those who have been linked to the group are being targeted, despite never having been active members of the group or supporters of its criminal activities."

197. During its 135th session held between 27 June and 27 July 2022, the United Nations Human Rights Committee ("HRC") adopted its views in respect of the communication *Alakuş v. Türkiye* (CCPR/C/135/D/3736/2020), which concerned a conviction for membership of the FETÖ/PDY on the basis of, *inter alia*, the use of ByLock and transactions at Bank Asya. In respect of the complaint that the conviction had violated Article 15 § 1 of the ICCPR, by reason of the fact that it had been based on acts which were not defined as crimes nor prohibited under domestic law, the HRC made the following findings, as relevant (footnotes omitted):

> "10.6 The Committee recalls that the principle of legality in the field of criminal law, as one of the fundamental principles of the rule of law, requires both criminal liability and punishment to be limited to clear and precise provisions in the law at the time the act or omission took place. In doing so, the Committee limits itself to the question of whether the author's acts, at the material time of commission, constituted sufficiently defined criminal offences under the Penal Code or under international law... The Committee considers that, as a matter of principle, merely using or downloading a means of encrypted communication or owning a bank account cannot indicate, in themselves, evidence of membership of an illegal armed organisation, unless supported by other evidence, such as conversation records. In the absence of documentary evidence provided by the State party, the Committee finds, in these circumstances, that the rights of the author under article 15(1) have been violated."

B. The Council of Europe

1. Council of Europe Commissioner for Human Rights

198. On 7 October 2016 the then Commissioner for Human Rights, Mr Nils Muižnieks, published a memorandum (CommDH(2016)35) on the human rights implications of the measures taken under the state of emergency in Türkiye, following his visit between 27 and 29 September 2016. The relevant parts of the memorandum read as follows (footnotes omitted):

"13. The Commissioner is convinced that it is in the interest of the Turkish authorities to conduct this fight while fully upholding human rights, as well as general principles of law such as, among others, presumption of innocence, individuality of criminal responsibility and punishment, no punishment without law, non-retroactivity of criminal law, legal certainty, right to defence and equality of arms...

...

19. The authorities pointed out to the Commissioner that the danger posed by this organisation became clear to the government and the public already previously, for example during the period of 17-25 December 2013. The Commissioner also took note of the information that the National Security Council had already designated FETÖ/PDY as a terrorist organisation in 2015, while noting that the conclusions of this body are not addressed to the public, but to the Council of Ministers.

20. Nevertheless, the Commissioner must also take note of the fact that this organisation's readiness to use violence, a *sine qua non* component of the definition of terrorism, had not become apparent to Turkish society at large until the coup attempt. Furthermore, it has not yet been recognised as a terrorist organisation in a final judgment of the Turkish Court of Cassation which, according to the Turkish authorities, is a crucial legal act in the Turkish legal system when it comes to the designation of an organisation as terrorist. Despite deep suspicions about its motivations and *modus operandi* from various segments of the Turkish society, the Fethullah [*sic*] Gülen movement appears to have developed over decades and enjoyed, until fairly recently, considerable freedom to establish a pervasive and respectable presence in all sectors of Turkish society, including religious institutions, education, civil society and trade unions, media, finance and business. It is also beyond doubt that many organisations affiliated to this movement, which were closed after 15 July, were open and legally operating until that date. There seems to be general agreement that it would be rare for a Turkish citizen never to have had any contact or dealings with this movement in one way or another.

21. The Commissioner stresses that these considerations do not address the nature or motivations of FETÖ/PDY itself, but point to the need, when criminalising membership and support of this organisation, to distinguish between persons who engaged in illegal activities and those who were sympathisers or supporters of, or members of legally established entities affiliated with the movement, without being aware of its readiness to engage in violence...

22. The Commissioner therefore urges the authorities to dispel these fears by communicating very clearly that mere membership or contacts with a legally established and operating organisation, even if it was affiliated with the Fethullah [*sic*] Gülen movement, is not sufficient to establish criminal liability and to ensure that charges for terrorism are not applied retroactively to actions which would have been legal before 15 July.

...

28. It also needs to be borne in mind that all measures taken under the state of emergency must be derogating from the ECHR only to the extent strictly required by the situation, and therefore must be proportionate to the aim pursued. This aim, in the context of Turkey's derogation to the ECHR, was to counter the severe dangers to public security and order, amounting to a threat to the life of the nation, 'posed by the coup attempt and its aftermath together with other terrorist acts'. In this connection, when it comes to the public sector, the threat posed by a public employee wielding the sovereign power of the State, such as military personnel, an intelligence officer, a police

officer or a judge, cannot be compared to the risk represented by a teacher, academic or an unqualified worker...”

199. The Commissioner for Human Rights, Ms Dunja Mijatović, carried out a visit to Türkiye from 1 to 5 July 2019. The report (CommDH(2020)1) from her visit, published on 19 February 2020, reads in so far as relevant (footnotes omitted):

1.2.1 General observations on Turkish criminal law and its application

“36. ... In particular, the work of the Commissioner’s Office on Turkey has consistently pointed to an overbroad interpretation by the Turkish judiciary of what constitutes terrorism or membership of an armed criminal organisation despite all the changes over the years.

...

43. ... The state of emergency and the criminal proceedings concerning membership of FETÖ/PDY appear to have had a particularly negative legacy [in respect of the increased legal uncertainty]: in most cases, membership of FETÖ/PDY was primarily determined by such acts as the use of a smartphone application called ‘ByLock’, deposits in Bank Asya, and links with or using the services of schools or hospitals associated with Fethullah [*sic*] Gülen. This approach overlooks the fact that these institutions were operating under licenses delivered by the relevant State bodies until the coup attempt in July 2016 and is based on the assumption that the persons concerned should have known not to trust these licenses and severed their ties with these institutions...

44. The Commissioner considers that the implications of this approach are worrying for the principles of legal certainty, foreseeability of criminal offences and the rule of law in general, as anyone can retroactively be considered a member of a criminal organisation long after the events in question.

...

48. In her third-party intervention concerning [*Kavala v. Turkey*, no. 28749/18, 10 December 2019] before the EctHR, the Commissioner also made more general observations on the state of criminal justice in Turkey, pointing out that in this and similar cases, the prosecutors and courts impute a criminal motive or presumed intention to the suspect first, before collecting or examining the available evidence, rather than going from evidence towards guilt. This approach manifests itself at every stage of the criminal proceedings, including investigations, arrests and detentions, but also increasingly when it comes to trials, convictions and sentencing. This contributes to a situation where actions which should be considered lawful in a democratic society, including statements and acts protected under the ECHR, are re-interpreted as circumstantial evidence used to prove criminal intent to commit very serious offences, thus undermining legal certainty and reinforcing the serious chilling effect on all sectors of Turkish society. For the Commissioner, this entails a clear risk of resulting in judgments of intentions (‘*procès d’intention*’), where no amount of material evidence can prove the person’s innocence.”

2. The European Commission for Democracy through Law (Venice Commission)

200. The Report on the Democratic Oversight of the Security Services adopted by the Venice Commission at its 71st Plenary Session (Venice, 1-2 June 2007) (CDL-AD(2007)016-e) and updated at the 102nd Plenary Session (Venice, 20-21 March 2015) (CDL-AD(2015)010), contains the following passages, as relevant:

> "1. The maintenance of the internal and external security of the State is vital and essential for the protection of the other values and interests of the State. In order to anticipate, prevent or protect itself against threats to its national security, a State needs effective intelligence and security services: intelligence is thus an inescapable necessity for modern governments.
>
> ...
>
> 3. ... Intelligence is one of the main weapons the State has in the struggle against terrorism ..."

201. On 11 and 12 March 2016, at its 106th Plenary Session, the Venice Commission adopted its opinion on Articles 216, 299, 301 and 314 of the Turkish Criminal Code (CDL-AD(2016)002). The relevant parts of the opinion read as follows (footnotes omitted):

> "**1. Membership of an armed organisation (Article 314)**
>
> ...
>
> 100. There is a rich case-law of the Court of Cassation in which the high court developed the criterion of 'membership' in an armed organisation. The Court of Cassation examined different acts of the suspect concerned, taking account of their 'continuity, diversity and intensity' in order to see whether those acts prove that the suspect has any 'organic relationship' with the organisation or whether his or her acts may be considered as committed knowingly and wilfully within the 'hierarchical structure' of the organisation...
>
> 101. If this 'organic relationship' with the organisation cannot be proven on the basis of acts attributed to the defendant, which do not present any 'continuity, diversity or intensity', the paragraphs on 'aiding and abetting an armed organisation' or 'committing crime on behalf of an armed organisation' under Article 220 may be applied...
>
> 102. According to non-governmental sources, in the application of Article 314, the domestic courts, in many cases, decide on the membership of a person in an armed organisation on the basis of very weak evidence, which would raise questions as to the 'foreseeability' of the application of Article 314...
>
> ...
>
> 105. ... [T]he Commission reiterates that conviction on the basis of weak evidence in the application of Article 314 may create problems in the field of Article 7 ECHR since this provision embodies, *inter alia*, the principle that the criminal law must not be extensively construed to an accused's detriment, for instance by analogy... Any allegation of membership to an armed organisation must be established with convincing evidence and beyond any reasonable doubt.

106. In conclusion, the Venice Commission recommends, first, that the established criteria in the case law of the Court of Cassation that acts attributed to a defendant should show 'in their continuity, diversity and intensity', his/her 'organic relationship' to an organisation or they should prove that he/she acted knowingly and willingly within the 'hierarchical structure' of the organisation, should be applied strictly. The loose application of these criteria may give rise to issues concerning in particular the principle of legality within the meaning of Article 7 ECHR.

...".

202. The opinion on the Protection of Human Rights in Emergency Situations adopted by the Venice Commission at its 66th Plenary Session (Venice, 17-18 March 2006) (CDL-AD(2006)015) provides as follows, as relevant (footnotes omitted):

"8. The balance that has to be struck between national security and public safety, on the one hand, and the enjoyment of fundamental rights and freedoms, on the other hand, cannot be determined by use of any mathematical calculation or fixed scale... The assessment of the fairness and proportionality of the balancing of public and private interests has to be determined by the concrete situation and circumstances... The bottom line, however, is that the right or freedom concerned may not be curtailed in its essence. This also holds true for the rights and freedoms of those who have committed, or are suspected of having committed, acts against State security or public safety.

...

13. Even in genuine cases of emergency situations the rule of law must prevail."

3. Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism

203. The Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (CETS no. 217), which entered into force on 1 July 2017 and which was ratified by Türkiye on 13 February 2018 (entry into force on 1 June 2018), reads as follows in its Article 2:

Article 2 – Participating in an association or group for the purpose of terrorism

"1. For the purpose of this Protocol, 'participating in an association or group for the purpose of terrorism' means to participate in the activities of an association or group for the purpose of committing or contributing to the commission of one or more terrorist offences by the association or the group.

2. Each Party shall adopt such measures as may be necessary to establish 'participating in an association or group for the purpose of terrorism', as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law".

The Explanatory Report to the Additional Protocol provides that the offence set out in its Article 2 must be committed intentionally and unlawfully for criminal liability to apply, the term "intentionally" being left to interpretation under domestic law. In addition, the offence requires a further subjective element of "terrorist purpose", that is, the activities must have as their purpose the contribution to the commission of one or more terrorist

offences by the association or group, or the commission of one or more such offences on its behalf. According to the Explanatory Report, Article 2 does not define the precise nature of the association or group, as the criminalisation depends on the commission of terrorist offences by the group regardless of its officially proclaimed activities. The Parties to the Protocol may qualify or define the associations or groups within the meaning of Article 2, including by interpreting the terms "association or group" to mean "proscribed" organisations or groups in accordance with its domestic law.

4. The Reykjavík Summit and Declaration

204. On 16 and 17 May 2023 the 4th Summit of Heads of State and Government of the Council of Europe was held in Reykjavík. Appendix IV to the Declaration adopted at the Summit reads as below, in so far as relevant:

> "**Recommitting to the Convention system as the cornerstone of the Council of Europe's protection of human rights**
>
> We, the Heads of State and Government,
>
> ...
>
> Underlining the primary obligation for all High Contracting Parties to the Convention to secure to everyone within their jurisdiction the rights and freedoms defined in the Convention in accordance with the principle of subsidiarity, the importance of taking into account the case law of the Court in a way that gives full effect to the Convention, and the unconditional obligation to abide by the final judgments of the Court in any case to which they are parties;
>
> ...
>
> Consequently, undertake to,
>
> ...
>
> Recommit to resolving the systemic and structural human rights problems identified by the Court and to ensure the full, effective and prompt execution of the final judgments of the Court, taking into account their binding nature and the obligations of the High Contracting Parties under the Convention while also recalling the importance of involving national parliaments in the execution of judgments;
>
> ...".

III. NOTICE OF DEROGATION BY TÜRKİYE

205. On 21 July 2016 the Permanent Representative of Türkiye to the Council of Europe sent the Secretary General of the Council of Europe the following notice of derogation:

> "I communicate the following notice of the Government of the Republic of Turkey.
>
> On 15 July 2016, a large-scale coup attempt was staged in the Republic of Turkey to overthrow the democratically-elected government and the constitutional order. This despicable attempt was foiled by the Turkish State and people acting in unity and solidarity. The coup attempt and its aftermath together with other terrorist acts have

posed severe dangers to public security and order, amounting to a threat to the life of the nation in the meaning of Article 15 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

The Republic of Turkey is taking the required measures as prescribed by law, in line with the national legislation and its international obligations. In this context, on 20 July 2016, the Government of the Republic of Turkey declared a State of Emergency for a duration of three months, in accordance with the Constitution (Article 120) and the Law No. 2935 on State of Emergency (Article 3/1b). ...

The decision was published in the Official Gazette and approved by the Turkish Grand National Assembly on 21 July 2016. Thus, the State of Emergency takes effect as from this date. In this process, measures taken may involve derogation from the obligations under the Convention for the Protection of Human Rights and Fundamental Freedoms, permissible in Article 15 of the Convention.

I would therefore underline that this letter constitutes information for the purposes of Article 15 of the Convention. The Government of the Republic of Turkey shall keep you, Secretary General, fully informed of the measures taken to this effect. The Government shall inform you when the measures have ceased to operate.

..."

206. The notice of derogation was withdrawn on 8 August 2018, following the end of the state of emergency.

THE LAW

I. PRELIMINARY QUESTION CONCERNING THE DEROGATION BY TÜRKİYE

207. The Government emphasised at the outset that the applicant's complaints under Articles 6, 8 and 11 of the Convention should be examined with due regard to the derogation notified under Article 15 of the Convention to the Secretary General of the Council of Europe on 21 July 2016. Article 15 provides:

"1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under [the] Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

2. No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Articles 3, 4 (paragraph 1) and 7 shall be made under this provision.

3. Any High Contracting Party availing itself of this right of derogation shall keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefore. It shall also inform the Secretary General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed."

A. The parties' submissions

208. The Government submitted that Türkiye had experienced a public emergency threatening the life of the nation on account of the risks posed by the attempted military coup, as also acknowledged by the Court in a number of judgments. They observed that the threat arising from the FETÖ/PDY had continued for a long time, and that the measures taken by the national authorities in response to the emergency – and in the context of the fight against terrorism – had been strictly required by the exigencies of the situation. Accordingly, in availing itself of its right to derogate from the Convention under Article 15, Türkiye had not breached the provisions of the Convention. Referring to the measures taken by the legislative decrees enacted during the state of emergency, the Government further argued that Türkiye had observed the principles of necessity, proportionality and legality throughout the relevant period in keeping with its international human rights obligations. The Government therefore invited the Court to examine the applicant's complaints under Articles 6, 8 and 11 of the Convention from the perspective of Article 15 of the Convention.

209. In respect, in particular, of the applicant's complaint under Article 6 § 3 (c) of the Convention (see paragraphs 358 and 366 below), the Government argued that the relevant restrictions imposed by Article 6 § 1 (d) of Legislative Decree no. 667 on the right to legal assistance of persons detained for certain offences (see paragraph 154 above) had been justified by the circumstances of the state of emergency to the extent required by those circumstances. The Constitutional Court had subjected the restrictions in question to thorough scrutiny, including in the context of the right to a fair trial, and had found in a number of judgments that they had been proportionate to the conditions of the state of emergency. Echoing the findings of the Constitutional Court, the Government claimed that in view of the characteristics of the FETÖ/PDY – such as its secrecy, cellular structure, and presence in all public institutions – and the continuing danger it posed in the aftermath of the coup attempt, there was a real risk that persons detained for offences related to the coup attempt or the FETÖ/PDY would continue their organisational activities in detention and that organisational communication would be ensured through meetings with their lawyers. The measures taken within the framework of Article 6 § 1 (d) of Legislative Decree no. 667 had, therefore, been reasonable and had not been of a nature to undermine the fairness of the relevant criminal proceedings as a whole. They added that the applicant's release on 21 March 2017 by the Kayseri Assize Court while the state of emergency was still in effect showed "that the state of emergency was not determinative in the decisions of the judicial authorities, and that judicial activities were carried out by [their] own principles and rules".

210. The applicant submitted in reply that the extensive measures taken by the Government in the aftermath of the coup attempt, such as the dismissal, arrest and conviction of thousands of individuals, amounted to an arbitrary witch hunt against the supporters of the Gülen movement, and had therefore not been "strictly required by the exigencies of the situation". He further claimed that even in a state of emergency, the fundamental principle of the rule of law had to prevail. It would accordingly not be consistent with the rule of law in a democratic society to investigate, prosecute and convict a person – who had not committed any offence – based on the allegation of using an encrypted messaging application, depositing money to a lawfully operating bank, and membership of a trade union and an association established and operating in accordance with the law, all of which acts fell within the scope of the exercise of fundamental rights. He further observed that while the numerous legislative decrees adopted during the state of emergency had imposed significant limitations on the rights of individuals, Article 314 of the Criminal Code, under which he had been charged, had remained unchanged in the relevant period.

B. The Court's assessment

211. The Court notes that the notice of derogation by Türkiye, indicating that a state of emergency had been declared in order to tackle the threat posed to the life of the nation by the severe dangers resulting from the attempted military coup and other terrorist acts, did not explicitly mention which Articles of the Convention were to form the subject of a derogation. Instead, it announced in a general manner that "measures taken may involve derogation from the obligations under the Convention".

212. It also notes its finding in *Mehmet Hasan Altan v. Turkey* (no. 13237/17, § 93, 20 March 2018) and *Şahin Alpay v. Turkey* (no. 16538/17, § 77, 20 March 2018), and in many other cases that followed (see, for instance, *Alparslan Altan v. Turkey*, no. 12778/17, § 74, 16 April 2019; *Pişkin v. Turkey*, no. 33399/18, § 59, 15 December 2020; and *Ahmet Hüsrev Altan v. Turkey*, no. 13252/17, § 102, 13 April 2021), that the attempted military coup amounted to a "public emergency threatening the life of the nation" within the meaning of the Convention and that the formalities required by Article 15 § 3 had been respected.

213. The Court sees no reason to depart from that finding in the present case. As to whether the specific actions taken against the applicant were strictly required by the exigencies of the situation and consistent with the respondent State's other obligations under international law, these points will be considered as part of the examination of the relevant complaints on the merits (see *Mehmet Hasan Altan*, cited above, § 94; see also paragraphs 347-355 and 398-401 below).

II. ALLEGED VIOLATION OF ARTICLE 7 OF THE CONVENTION

214. The applicant complained that the acts that formed the basis of his conviction were lawful at the relevant time and that holding him criminally liable for those acts entailed an extensive and arbitrary interpretation of the relevant laws, in violation of the principle of no punishment without law enshrined in Article 7 of the Convention.

215. He further complained under Article 6 § 2 that despite the absence of any court rulings declaring the FETÖ/PDY structure a terrorist organisation at the time of the acts attributed to him or when he was subsequently charged, the said structure had been proscribed as an armed terrorist organisation by the executive and its members accused of membership of an armed terrorist organisation.

216. The applicant lastly complained under Article 4 of Protocol No. 7 to the Convention that the designation of the FETÖ/PDY as a terrorist organisation on the basis of acts going back to 1966, which had been found by the Court of Cassation in 2008 not to constitute a criminal offence in the context of the criminal proceedings brought against F. Gülen in 1999, was in violation of the principle of *ne bis in idem*.

217. Having regard to its case-law and the nature of the applicant's complaints, the Court, being master of the characterisation to be given in law to the facts of a case (see, for instance, *Molla Sali v. Greece* [GC], no. 20452/14, § 85, 19 December 2018, and *S.M. v. Croatia* [GC], no. 60561/14, §§ 241-43, 25 June 2020), considers that the complaints raised by the applicant should be examined solely from the perspective of Article 7 of the Convention, as they all essentially concern the foreseeability of the applicant's conviction for membership of an armed terrorist organisation and are thus intrinsically linked (see, amongst many others, *Del Río Prada v. Spain* [GC], no. 42750/09, §§ 91-93, ECHR 2013, *Pessino v. France*, no. 40403/02, §§ 35-36, 10 October 2006, *Dragotoniu and Militaru-Pidhorni v. Romania*, nos. 77193/01 and 77196/01, §§ 40-45, 24 May 2007, and *Jorgic v. Germany*, no. 74613/01, §§ 103-14, ECHR 2007-III, where the Court dealt with the issue of the foreseeability of a criminal conviction under Article 7 of the Convention). Article 7, in so far as relevant, reads as follows:

> "1. No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed.
>
> ..."

A. Admissibility

218. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes

that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) Submissions of the applicant

219. The applicant stated that the offence for which he had been convicted, namely membership of an armed terrorist organisation, required the presence of a number of elements such as: the existence beyond reasonable doubt of an armed terrorist organisation; knowledge on the part of the suspect of the nature of that organisation; and the suspect's actual membership of that organisation, based on some qualitative requirements, as well as specific intent for the realisation of its aims. The applicant maintained that none of these elements had been established in his case and that, as a result, his prosecution for membership of an armed terrorist organisation had not been foreseeable. He therefore claimed that his conviction had been in contravention of Article 7 of the Convention.

220. He argued that the Gülen movement could not have been characterised as having been, beyond reasonable doubt, a "terrorist organisation" at the time of the acts attributed to him, between 2014 and 2015. He claimed in this regard that following the indictment of F. Gülen on 31 August 2000 on the charges of founding and leading a terrorist organisation, all activities of the Gülen movement had been extensively investigated, resulting in acquittal of all the charges on 5 May 2006. When upholding the acquittal on 24 June 2008, the plenary criminal divisions of the Court of Cassation had confirmed that it had not been established that the accused, and the organisations allegedly linked to him, had harboured the goal of overthrowing the constitutional order, or had resorted to violence. From then on, the Gülen movement had maintained its activities without facing any other investigations until the end of 2013, when it was held responsible for several high-level political scandals. However, even at that point the Gülen movement was not categorised by the Government as a terrorist organisation.

221. Emphasising that under Turkish law only a court could decide whether a structure was a terrorist organisation, the applicant pointed out that there had been no final court judgments to this effect with respect to the Gülen movement at the time of his conviction by the Kayseri Assize Court on 21 March 2017. He further contended that neither in that judgment, nor in other judgments – against him or other suspects – that followed, were the elements of violence, pressure, intimidation or threat, which were essential to the definition of "terrorism" under Turkish law, discussed in respect of the Gülen movement's activities preceding the coup attempt.

222. The applicant next argued that according to domestic law and practice, the offence of membership of an armed terrorist organisation necessitated not only the existence of an organisation that aimed at committing the offences listed in the Criminal Code, but also required that the organisation operate in a hierarchical structure and that the alleged members have performed acts of a certain continuity, diversity and intensity, none of which had been established in his case. He claimed that at no point in their judgments had the domestic courts laid out the hierarchical structure of the alleged armed terrorist organisation, other than in abstract and general terms, or his position therein. Many questions, such as whom he had taken orders from or to whom he had reported, with whom he had attended the meetings of the terrorist organisation, the offences he had committed on its behalf, and the degree of intensity and diversity of his involvement in the acts of the terrorist organisation had been left unanswered when establishing the elements of the offence attributed to him.

223. The applicant noted in this connection that even if it were to be accepted that the Gülen movement was a terrorist organisation, it was of the utmost importance to determine whether he had personally been aware of that fact at the time of the acts attributed to him, this state of awareness being one of the intrinsic elements of the offence of membership of an armed terrorist organisation. He contended that establishing the ultimate goal of an organisation was altogether different from establishing an individual's knowledge and acceptance of that goal. In arguing that he could not have been aware of the terrorist nature and intentions of the Gülen movement the applicant referred once again to the judgment of 2008 confirming the acquittal of F. Gülen of all crimes and to the many statements made by high-level Government officials publicly declaring their support for and appreciation of that movement over the years.

224. He further maintained that none of the acts attributed to him were such as to indicate membership of an armed terrorist organisation. The material elements of the offence of membership of an armed terrorist organisation were construed extremely broadly due to the very wide interpretation of the offence set out in in Article 314 § 2 of the Criminal Code, which had been wholly unforeseeable and had expanded the scope of criminal liability for the offence in question.

225. To the extent that his conviction was based on his alleged use of the ByLock application, an allegation which he denied, the applicant drew the Court's attention to the fact that the domestic courts had not examined the content of the messages that he had purportedly exchanged over the application, the instructions he had allegedly received, or how he had followed those instructions. He was, moreover, accused of having used that application only on six days, which fell short of the "continuity" requirement for a hierarchical membership. He argued that, in any event, the domestic courts' finding that the application was exclusively designed for and used by

members of the Gülen movement, and that its use could serve as proof of a person's hierarchical position within the Gülen movement, was unfounded. He stressed in this connection that the application had been downloaded some 600,000 times just from application stores – that is, without counting the downloads made from different APK sites – and that certain technical features of ByLock that had been portrayed as unique to that application to ensure its organisational use were in fact to be found in other comparable applications as well.

226. In the applicant's view, even if it were to be accepted that the evidence against him demonstrated his association with the Gülen movement, it still needed to be proven beyond reasonable doubt that he had acted with the requisite specific intent. The "specific intent" in this context required the accused to have acted with the knowledge that the organisation had been established to commit certain offences and with the purpose of committing those offences. Establishing these points was particularly important in the present context bearing in mind that the Gülen movement was a social structure which had been supported by all segments of the society for decades. Holding ordinary members of that structure criminally liable for illegal activities carried out by the executives of the organisation, without establishing their individual intent, was contrary to the principle of individual criminal responsibility and amounted to collective punishment. The applicant claimed that he had been convicted essentially for allegedly associating with a community, some members of which had allegedly committed certain crimes.

(b) Submissions of the Government

227. The Government stated at the outset that although under Turkish law the designation of a structure as a "terrorist organisation" was contingent upon a judicial finding to this effect, this was not a prerequisite for a conviction for membership of an armed terrorist organisation, as also noted by the Court in the case of *Parmak and Bakır v. Turkey* (nos. 22429/07 and 25195/07, § 71, 3 December 2019). According to domestic case-law, the founders, directors or members of a terrorist organisation could be held criminally liable from the date of the foundation of the organisation, or from the date on which it had transformed into a criminal organisation, even in the absence of a prior judicial decision proscribing it. To hold otherwise would mean that a person would go unpunished for the offences he had committed prior to a court decision designating a structure as a terrorist organisation, which would seriously imperil the fight against terrorism.

228. As to the relevance for the applicant's complaints under Article 7 of the confirmation of F. Gülen's acquittal by the Court of Cassation on 24 June 2008, and whether that acquittal had rendered his punishment for membership of FETÖ/PDY unforeseeable, the Government stressed that the scope of those proceedings had been limited to acts carried out and/or

detected by the authorities prior to 31 August 2000, that is, the date on which the bill of indictment had been filed against F. Gülen. It therefore followed that the finding made in 2008 that, up to 2000, the impugned structure was not an armed terrorist organisation, did not necessarily render unforeseeable a later finding to the contrary, one that was based on acts that took place or evidence that surfaced after 2000.

229. The Government underlined in this connection that after 2013 many investigations into the illegal acts undertaken by the members of the FETÖ/PDY had been initiated, such as the "17-25 December investigations" or the "MİT trucks investigations". Furthermore, the National Security Council had declared the structure in question a "terrorist organisation" in its meetings held between 26 February 2014 and 26 May 2016. The FETÖ/PDY had therefore started showing its true colours publicly by the time the applicant had committed the acts forming the basis of his conviction. They contended, accordingly, that the domestic courts' finding that the FETÖ/PDY was a terrorist organisation could reasonably have been foreseen by the applicant at the time of the acts on which his conviction rested, irrespective of F. Gülen's acquittal in 2008.

230. The Government next reviewed the constituent elements of the crime of membership of an armed terrorist organisation, which they claimed were formulated with sufficient precision in the relevant legislative framework and the case-law of the Court of Cassation, as referred to in detail in the judgments delivered in the applicant's respect. Based on those elements, the domestic courts had examined the FETÖ/PDY, including its purpose, functioning, socio-cultural and hierarchical structure, model of organisation and attempts to establish a parallel State structure, and had concluded that it was an armed terrorist organisation, albeit a *sui generis* one. In arriving at this conclusion, the domestic courts had taken into account the fact that the FETÖ/PDY had not aimed to come to power through legitimate methods, but had intended to abolish Parliament, the Government and other constitutional institutions by coercion, violence and other undemocratic methods, through its members that it had strategically placed within the State bureaucracy. The members placed in institutions authorised to use force, such as the army, the police and the MİT, had – during the coup attempt – used weapons belonging to the State against public institutions, the security forces and civilians with a view to bringing about their intended aims.

231. As for the applicant's specific situation, the Government stated that in view of the public awareness that had emerged, particularly after 2013, about the FETÖ/PDY's illegal activities, the domestic courts had found that the applicant had been in a position to know the ultimate purpose of the organisation, its structuring within the State institutions and the armed forces, and the fact that the members of the organisation, who had at their disposal every kind of weapon of the State, would use this force when necessary in line with the purpose of the organisation, given in particular his level of

education, knowledge and professional experience. The courts had concluded against this background, and given the nature of the evidence against the applicant, that he had committed the acts attributed to him wilfully and with full knowledge of the illegal purposes of the FETÖ/PDY.

232. The Government referred in this connection to the domestic courts' reasons for finding why the use of the ByLock application was considered to meet all the constituent requirements of the offence of membership of an armed terrorist organisation, such as continuity, diversity, intensity and hierarchical link, irrespective of the content of the exchanges made over that application. The Government stressed that in case of secretive terrorist organisations, retrieving the contents of the messages in relation to individual users and establishing the context in which they were exchanged were often impossible because of the secure forms of the communications used; yet the judicial authorities had nevertheless duly established that ByLock was used exclusively by the executives and members of the terrorist organisation and had been developed by the FETÖ/PDY for secret intra-organisational communication. They explained that as an organisation based on secrecy, the FETÖ/PDY favoured face-to-face communication; however, where that was not possible, the organisation chose to conduct its communication via encrypted means. The friends' groups established in ByLock demonstrated the existence of a hierarchical structure and cell-type organisation, which were features of terrorist organisations. Based on those findings, the Government – while confirming at the hearing that the technical means by which the applicant had acquired the ByLock application were unknown to them – stated that it was not possible for a person who had no link to the organisation to download and use the ByLock application, and that ByLock users were already aware of the illegal purposes of the organisation, wanted those to be achieved and participated in organisational activities to that end. According to the Government, if a person had downloaded that application, which had been developed by the organisation and exclusively used by its members, and used it despite all technical difficulties, that showed that such a person fully submitted to the will of the organisation and adhered to its hierarchy. The mental element of the crime had, therefore, materialised in the applicant's case, who had established organisational communication with the members of the FETÖ/PDY via ByLock in line with the instructions of the organisational hierarchy, without ever calling into question those instructions. As such, the applicant could not benefit from the "mistake" provision in Article 30 of the Criminal Code. Referring to the Court of Cassation's landmark judgments, the Government indicated that the use of ByLock would therefore be sufficient in itself for a conviction for membership of the FETÖ/PDY.

233. In response to the applicant's argument that he had not engaged in any criminally reprehensible conduct through his alleged use of ByLock, which was a lawful act, the Government contended that where membership

of an armed terrorist organisation was proven, it was the act of membership itself that constituted the criminally reprehensible conduct. The applicant's use of ByLock was not a physical act forming part of the *actus reus* of the crime of which he was convicted. The domestic courts had not found the mere fact of the applicant's use of ByLock to amount to participation in an armed terrorist group as a member. The *actus reus* of the offence was rather the act of becoming part of the hierarchical structure of the organisation, by making himself available for commands and instructions. The applicant's use of ByLock was merely evidence demonstrating that he had become part of that structure. In other words, while the applicant had not become part of the hierarchical structure of the organisation by his use of ByLock, his use of that application was evidence that he had otherwise become a part of that hierarchy.

234. In these circumstances, it was immaterial to ask for the purposes of the "foreseeability" requirement under Article 7 whether the applicant could have foreseen that the use of ByLock would be construed as evidence of the offence of membership of an armed terrorist organisation. According to the Government, the use in a criminal trial of a form of evidence, the use of which was unforeseen at the time of the acts in question, did not in itself raise issues under Article 7 of the Convention.

235. The Government argued that the finding that use of ByLock satisfied by itself the elements of the offence in question was not a novel interpretation; the Court of Cassation had long acknowledged, in the context of other terrorist organisations, that the performance of certain acts, by their nature, could in themselves constitute the offence of membership of an armed terrorist organisation. The Government referred in this connection to a judgment of the plenary criminal divisions of the Court of Cassation dated 26 June 2001, holding that the act of submitting a *curriculum vitae* to Hezbollah, an illegal armed organisation, had been considered as evidence of an organic link with the organisation, as it had demonstrated the accused's readiness to discharge the duties to be entrusted to him.

236. The Government indicated that the above arguments similarly applied, as relevant, in respect of the deposits that the applicant had made with Bank Asya, which was considered by the authorities to be a part of the financial structure of the terrorist organisation, and his membership of FETÖ/PDY-affiliated entities, which were used as corroborative evidence to prove his membership of that organisation. They acknowledged, however, that even "suspect" deposits of funds with Bank Asya, which appeared to have been made upon the call of F. Gülen with the sole aim of benefiting the organisation, or membership of a trade union or association affiliated with the FETÖ/PDY, would not on their own suffice to prove membership of the FETÖ/PDY, but would only serve as corroborating elements when taken together with other substantial evidence, as in the present case.

2. The Court's assessment

(a) General principles

237. The guarantee enshrined in Article 7 of the Convention, which is an essential element of the rule of law, occupies a prominent place in the Convention system of protection, as is underlined by the fact that no derogation from it is permissible under Article 15 of the Convention in time of war or other public emergency. It should be construed and applied, as follows from its object and purpose, in such a way as to provide effective safeguards against arbitrary prosecution, conviction and punishment (see *Scoppola v. Italy (no. 2)* [GC], no. 10249/03, § 92, 17 September 2009, and *Del Río Prada*, cited above, § 77, each with further references).

238. Article 7 of the Convention is not confined to prohibiting the retroactive application of criminal law to the disadvantage of an accused. It also embodies, more generally, the principle that only the law can define a crime and prescribe a penalty (*nullum crimen, nulla poena sine lege*) and the principle that criminal law must not be extensively construed to the detriment of an accused, for instance by analogy. From these principles it follows that an offence must be clearly defined in law. This requirement is satisfied where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him criminally liable. When speaking of "law", Article 7 alludes to the very same concept as that to which the Convention refers elsewhere when using that term, a concept which comprises written as well as unwritten law and implies qualitative requirements, notably those of accessibility and foreseeability (see, among other authorities, *Streletz, Kessler and Krenz v. Germany* [GC], nos. 34044/96, 35532/97, 44801/98, § 50, ECHR 2001-II, and *Del Río Prada*, cited above, § 91).

239. In any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Indeed, in the Convention States, the progressive development of the criminal law through judicial law-making is a well-entrenched and necessary part of legal tradition. Article 7 of the Convention cannot be read as outlawing the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen. The lack of an accessible and reasonably foreseeable judicial interpretation can lead to a finding of a violation of Article 7 rights. Were that not the case, the object and purpose of this provision – namely that no one should be subjected to arbitrary prosecution, conviction or punishment – would be defeated (see *Del Río Prada*, cited above, § 93, with further references).

240. The Court reiterates that, in principle, it is not its task to substitute itself for the domestic jurisdictions. It is primarily for the national authorities, notably the courts, to resolve problems of interpretation of domestic legislation. The Court's role is confined to ascertaining whether the effects of such an interpretation are compatible with the Convention (see, among others, *Korbely v. Hungary* [GC], no. 9174/02, §§ 72-73, ECHR 2008; and *Kononov v. Latvia* [GC], no. 36376/04, § 197, ECHR 2010).

241. The Court has stressed, however, that its powers of review must be greater when the Convention right itself, Article 7 in the present case, requires that there was a legal basis for a conviction and sentence (see, amongst others, *Advisory opinion on the applicability of statutes of limitation to prosecution, conviction and punishment in respect of an offence constituting, in substance, an act of torture* [GC], request no. P16-2021-001, Armenian Court of Cassation, § 71, 26 April 2022). Article 7 § 1 requires the Court to examine whether there was a contemporaneous legal basis for the applicant's conviction and, in particular, it must satisfy itself that the result reached by the relevant domestic courts was compatible with the object and purpose of that provision. To accord a lesser power of review to this Court would render Article 7 devoid of purpose (see *Kononov*, cited above, § 198, and *Rohlena v. the Czech Republic* [GC], no. 59552/08, § 52, ECHR 2015).

242. Lastly, the Court has found that the requirement of accessibility and foreseeability entails that, in principle, a measure can only be regarded as a penalty within the meaning of Article 7 where an element of personal liability on the part of the offender has been established. Accordingly, Article 7 requires, for the purposes of punishment, the existence of a mental link through which an element of liability may be detected in the conduct of the person who physically committed the offence (see *G.I.E.M. S.r.l. and Others v. Italy* [GC], nos. 1828/06 and 2 others, §§ 242 and 243, 28 June 2018). This requirement does not preclude the existence of certain forms of objective liability stemming from presumptions of liability, provided that they comply with the Convention. More specifically, a presumption should not have the effect of making it impossible for an individual to exonerate himself from the accusations against him (ibid., § 243).

(b) Application of the general principles to the present case

243. The Court points out at the outset that it is not its task under Article 7 of the Convention to establish whether the applicant actually performed the acts imputed to him – in particular, whether he actually used the ByLock application, which he denies – or to rule on his individual criminal responsibility, those being primarily matters for the domestic courts (see *Streletz, Kessler and Krenz*, cited above, § 51; *Navalnyye v. Russia*, no. 101/15, § 58, 17 October 2017; and *Khodorkovskiy and Lebedev v. Russia (no. 2)*, nos. 51111/07 and 42757/07, § 572, 14 January 2020). The Court's task is rather to consider, from the standpoint of Article 7, whether his

conviction complied with the principles of legality and foreseeability enshrined in that provision.

244. The applicant in the present case was convicted of the offence of membership of an armed terrorist organisation. The Court will therefore first verify whether at the time of the acts attributed to him such an offence was clearly set out in domestic law.

245. It notes that the applicant's conviction was based on Article 314 § 2 of the Criminal Code, which provides for a sentence of five to ten years for those found to be members of an armed organisation formed with the purpose of committing one of the offences referred to in the first paragraph of that provision, i.e., offences against State security and the constitutional order (see paragraph 147 above).

246. Article 314 § 2 of the Criminal Code does not itself provide a definition of terrorism or terrorist organisation, which is set out in the Prevention of Terrorism Act. Under Section 1 of this Act, in its present wording, terrorism is defined as any kind of criminal act committed by use of force and violence, through one of the methods of pressure, terror, intimidation, oppression or threat, in pursuit of any of the aims listed in that same provision (see paragraph 149 above). Section 3 of the same Act further provides that the offences indicated in, *inter alia*, Article 314 of the Criminal Code are terrorist offences (ibid.). Section 7 of the Prevention of Terrorism Act in turn stipulates that those who become members of a terrorist organisation in order to commit crime in pursuance of the purposes set out under Section 1, by use of force and violence, and through the methods of pressure, terror, intimidation, oppression or threats, shall be punished in accordance with Article 314 of the Criminal Code (ibid.).

247. The legal framework governing the offence of membership of an armed terrorist organisation is complemented by the Court of Cassation's case-law, which provides further clarity on both the elements of an armed terrorist organisation, and that of the offence of membership of such an organisation (see paragraph 161 above). The Court of Cassation has specified that for the purposes of the offence set out in Article 314 § 2 of the Criminal Code, the "organisation" is not an abstract gathering but one that is based on a hierarchical structure. In ascertaining the existence of the organisation, it has to be assessed whether it has, or had, sufficient members, tools and equipment to enable it to commit the intended offence, as required under Article 220 of the Criminal Code. In particular, it must be verified whether the organisation possesses, or possessed, a sufficient amount of arms to carry out its aims, or the means to access such arms.

248. The Court of Cassation has further clarified that conviction for membership of an armed terrorist organisation follows only where the accused's organic link with the armed organisation is established, based on the continuity, diversity and intensity of his or her activities, and where it is demonstrated that he or she acted knowingly and willingly within the

organisation's hierarchical structure and embraced its objectives (see paragraph 184 above). It has moreover specified the mental element of the offence as being "direct intent and the aim or objective of committing a crime". It therefore follows that a person taking part in an organisation has to know that it is one that commits, or aims to commit, crimes (ibid.), and has to possess a specific intent for the realisation of that purpose (see paragraph 83 above). Although the commission of an actual crime in connection with the organisation's activities and for the achievement of its aims is not required to establish the offence of membership of an armed terrorist organisation, the individual must nevertheless have made a concrete material or mental contribution to the organisation's actual existence or reinforcement (see paragraph 184 above).

249. Having regard to the legal provisions described above, and to their interpretation by the domestic courts, the Court considers that the offence of which the applicant was convicted is codified and defined under Turkish law, in keeping with the principle of legality under Article 7 of the Convention. Article 314 § 2 of the Criminal Code, particularly when read in conjunction with the Prevention of Terrorism Act and the case-law of the Court of Cassation, is, in principle, formulated with sufficient precision to enable an individual to know, if need be with appropriate legal advice, what acts and omissions would make him criminally liable.

250. The applicant nevertheless argued that his conviction was not compatible with Article 7 of the Convention, mainly for two reasons. He claimed that the FETÖ/PDY had not been recognised as an "armed terrorist organisation" at the time of the acts attributed to him. He also argued that he had been convicted on the basis of lawful acts following an extensive interpretation of the relevant laws. The existence of the constituent elements of the offence of membership of an armed terrorist organisation as defined under the domestic law, in particular the mental element, had not been duly made out in his case. The Court will address these claims in turn.

(i) Whether the FETÖ/PDY was recognised as a terrorist organisation at the time of the acts attributed to the applicant

251. According to the domestic judgments and the Government's observations, under Turkish law the official designation of a structure as a "terrorist organisation" is contingent upon a decision by the courts (see paragraphs 163 and 227 above, respectively). In this connection, while the Erzincan Assize Court (first instance) declared this organisation to be terrorist in nature on 16 June 2016 – that is, one month prior to the coup attempt (see the reference to this judgment in paragraph 52 above) –, the first final judgment to that effect was delivered by the Samsun Regional Court of Appeal on 7 March 2017 (see paragraph 60 above). The first rulings of the Court of Cassation in that regard followed on 24 April and 26 September 2017 (see paragraphs 155 and 156 above). While certainly of factual

relevance, the assessments of the National Security Council or other public authorities prior to these judgments as to the terrorist nature of that organisation did not have legal force, *stricto sensu* (see the press statements of the National Security Council noted in paragraphs 108-113 above, in particular the statement of 26 May 2016 in which it expressly referred to the FETÖ/PDY as a terrorist organisation for the first time).

252. The applicant argues, and the Government do not contest, that the acts underpinning his conviction preceded the above court judgments. In this connection, the various ByLock reports relied on by the domestic courts indicated that the applicant connected to the ByLock application between 3 and 23 October 2015, and that the application was taken down in early 2016. Moreover, the applicant's allegedly suspicious account activities at Bank Asya took place mainly between 28 February 2014 and 31 December 2014. As for his membership of the Kayseri Voluntary Educators Association and the Aktif Eğitim-Sen trade union, the applicant states that he ended both in June 2016, prior to their closure on 23 July 2016 by Legislative Decree no. 667.

253. The Court therefore acknowledges that the FETÖ/PDY had not yet been designated, in the manner provided for in domestic law, as an armed terrorist organisation when the applicant carried out the various acts held against him. It does not however consider this sufficient to render the applicant's conviction incompatible with Article 7 of the Convention. This is essentially because, as can be seen from the relevant rulings of the domestic courts cited above, the rule in Turkish law regarding the legal designation of a terrorist organisation does not have the effect of precluding the criminal liability of the founders or members of the organisation for acts undertaken before such designation, to the extent that they acted "knowingly and willingly" (see paragraphs 84, 163, 165 and 187 above). As pointed out by the Government, this has already been accepted by the Court in *Parmak and Bakır* (cited above, § 71). Moreover, and regard also being had to the arguments put forth by the Government in paragraph 228 above, the Court can accept that F. Gülen's earlier acquittal of the charge of founding an armed terrorist organisation did not *per se* exclude the possibility of a different verdict regarding the nature of the FETÖ/PDY at a later time on the basis of subsequent developments.

254. The Court considers accordingly that the relevant question for the purposes of the present case is not whether the FETÖ/PDY had been proscribed as a terrorist organisation at the time of the acts attributed to the applicant. It is whether his conviction for membership of an armed terrorist organisation was sufficiently foreseeable given the requirements of the domestic law, in particular as regards the cumulative constituent material and mental elements of the offence such as they appear in Article 314 § 2 of the Criminal Code, the Prevention of Terrorism Act and in the relevant case-law of the Court of Cassation.

(ii) Whether the applicant's membership of an armed terrorist organisation was established in keeping with the requirements of the domestic law

255. The Court reiterates that it is not its task to substitute itself for the domestic courts as regards the interpretation of domestic legislation or the assessment of the facts and their legal classification (see *Kononov*, cited above, § 198, and *Rohlena*, cited above, § 51). It also stresses, however, that when exercising its supervisory function under Article 7 of the Convention, it will only defer to the conclusions reached by the domestic courts to the extent that they are compatible with the object and purpose of Article 7. As indicated in paragraph 241 above, the Court's powers of review are necessarily greater when the Convention right itself, such as Article 7 in the present context, requires that there was a sufficiently clear and foreseeable legal basis for a conviction and sentence.

256. As a natural extension of this principle, it is not sufficient for the purposes of Article 7 that an offence is set out clearly in domestic law. A failure on the part of the domestic courts to comply with the relevant law, or an unreasonable interpretation and application thereof in a particular case, could in itself entail a violation of Article 7 of the Convention (see *Del Río Prada*, cited above, § 93; *Khodorkovskiy and Lebedev v. Russia*, nos. 11082/06 and 13772/05, § 781, 25 July 2013; *Žaja v. Croatia*, no. 37462/09, §§ 91 and 92, 4 October 2016; and *Pantalon v. Croatia*, no. 2953/14, § 48, 19 November 2020, all with further references). The Court considers that the requirement that criminal offences be strictly defined by law would be thwarted if the domestic courts were to circumvent the law in its interpretation and application to the specific facts of a case.

257. Turning to the applicant's conviction for membership of the FETÖ/PDY, the Court notes that it stemmed from his alleged use of the ByLock messaging application. The position taken by the domestic courts and by the Government was that the establishment of the use of ByLock was sufficient on its own for conviction (see paragraphs 87, 88, 160, 165, 181, 188, 232 and 233 above). It is, furthermore, not contested that the remaining acts attributed to the applicant – namely his use of an account at Bank Asya and membership of a trade union and an association – served only as a source of corroboration. The Government expressly confirmed in this respect that those remaining acts would not have sufficed on their own to prove membership of the FETÖ/PDY, but could only have been used in support of other "substantial" evidence (see paragraph 236 above).

258. It was emphasised by the domestic courts, as well as in the Government's submissions, that the use of ByLock was not regarded as the *actus reus* of the crime of membership of an armed terrorist organisation – that is to say, the use of ByLock was not as such criminalised and sanctioned –, but was only relied on as evidence to establish guilt (see the Constitutional Court's judgment in the case of *Adnan Şen*, referred to in paragraph 188 above; see also the Government's statement to this effect in

paragraph 233 above). It was, however, also made clear that the mere fact of having used the ByLock application would serve, on its own, as conclusive proof of the presence of all of the constituent elements of the crime of membership of an armed terrorist organisation as defined in domestic law, irrespective of the content of the messages exchanged or the identity of the persons with whom the exchanges were made (see paragraphs 160 and 188 above).

259. The Government argued that it was not possible for a person who had no link to the organisation to download and use the ByLock application (see paragraph 232 above; see also the observations in the KOM report noted in paragraph 117 above). The Court is mindful of the ample material produced by the domestic authorities and courts to demonstrate the link between the ByLock application and the FETÖ/PDY. In this regard, it notes in particular the findings regarding the profile of some users of the application, the content of the decrypted communications, statements made by suspects in other FETÖ/PDY-related investigations confirming its use within the organisation, and the statements of the licence owner of the application noting, with hindsight, that it had been developed for the use of the FETÖ/PDY (see paragraphs 115, 117, 159, 176 and 139 above, respectively). It acknowledges, accordingly, that although it could be downloaded from open sources and that its allegedly unique features were in fact shared by some widely available applications (see the applicant's arguments to this effect in paragraph 225 above), ByLock was not just any ordinary commercial messaging application, and that its use could *prima facie* suggest some kind of connection with the Gülen movement.

260. The Court also notes, however, that the act that is penalised under Article 314 § 2 of the Criminal Code in question is not mere connection with an allegedly criminal network, but membership of an armed terrorist organisation, to the extent that such membership is established on the basis of the constituent – objective and subjective – elements set out in the law as noted in detail in paragraphs 245-248 above, and as confirmed in the Constitutional Court's judgment in the *Adnan Şen* case (see paragraphs 184-187 above). Accordingly, and as pointed out by the Ankara Regional Appeal Court (see paragraph 83 above), only persons whose position within a terrorist organisation had reached a level warranting their consideration as a "member" of that organisation could be convicted under Article 314 § 2. It therefore falls to the Court to verify whether the relevant constituent elements, and in particular the subjective, or mental, element, were duly established in the applicant's respect, in keeping with the requirements of the applicable law, and whether the assessment by the domestic courts of these constituent elements in the applicant's case represented a foreseeable, and not an expansive, interpretation and application of the said criminal provision (see, for a similar examination, *Korbely*, cited above, §§ 84 and 85, and *Navalnyye*, cited above, §§ 59-69).

261. In this connection, the Government explained that having particular regard to developments from the end of 2013 onwards, which revealed the criminal activities and the ultimate goal of the FETÖ/PDY, ByLock users, including the applicant, were in a position to be aware of the illegal purposes of the organisation, given that ByLock had become operational in early 2014 (see paragraphs 88, 163, 172, 229 and 231 above). Moreover, they wanted those purposes to be achieved and participated in organisational activities to that end, while using ByLock to ensure the confidentiality of their intra-organisational communication (see paragraph 232 above). The domestic courts had considered that if a person downloaded that application, which they determined had been developed by the organisation for the exclusive use of its members, and used it despite all technical difficulties, that showed his or her full submission to the will of the organisation and submission to its hierarchy. The Government contended, against this background, that the mental element of the crime had materialised in the applicant's case and that he could not resort to the "mistake" (*hata*) provision under Article 30 of the Criminal Code claiming lack of the requisite intent (ibid.; see also the findings of the Court of Cassation and the Constitutional Court in this regard in paragraphs 163, 187 and 188 above).

262. The Court notes from the foregoing that although the domestic courts referred to the applicant's membership of a trade union and an association and his account at Bank Asya (see paragraphs 68 and 70 above), all of the constituent elements of the relevant offence were considered to be manifested through the applicant's alleged use of ByLock, which was taken as sufficient in itself to establish his membership of an armed terrorist organisation and notably the requisite mental link allowing his personal criminal liability to be established. Admittedly, the assessment of the relevance or the weight attached to a particular piece of evidence is not, in principle, within the remit of the Court under Article 7 of the Convention. It considers, however, that over and above its evidential value, the finding regarding the use of ByLock here effectively replaced an individualised finding as to the presence of the constituent material and mental elements of the offence, thereby bypassing the requirements of Article 314 § 2 of the Criminal Code – as interpreted by the Court of Cassation itself – in contravention of the principle of legality and bringing the matter within the realm of Article 7.

263. The Court points in this connection to the absence of any meaningful explanation in the relevant domestic court judgments as to certain matters that went to the essence of the offence, such as how the mere use of ByLock, irrespective of what that use had actually entailed, led directly to the conclusion that the applicant knew that the FETÖ/PDY harboured terrorist aims that it intended to achieve by the use of force and violence, or that he had submitted himself to the will of the FETÖ/PDY, possessed the specific intent for the realisation of its purposes, and participated in its activities as a part of its hierarchy, or made any other concrete material or mental

contribution to the organisation's actual existence or reinforcement, as required under national law.

264. The interpretation adopted by the domestic courts rather seems to presuppose the very conclusions to which it purports to lead, in that it treats them as flowing automatically from the mere use of ByLock. In so doing, it effectively imputes criminal responsibility to a user of that application without establishing that all the requirements of membership of an armed terrorist organisation (including the necessary intent) have been fulfilled. In the Court's view, this is not only incompatible with the essence of the offence in question, which requires proof of an organic link based on continuity, diversity and intensity (see paragraph 184 above) and the presence of a very specific mental element, but is also irreconcilable with the right of an individual, under Article 7 of the Convention, not to be punished without the existence of a mental link through which an element of personal liability may be established (see *G.I.E.M. S.r.l. and Others*, cited above, §§ 242 and 244).

265. That is not to contest that the ByLock application was used by some, and even many, people as a tool for "organisational communication", within the meaning ascribed to that term by the national authorities. However, it is not only unforeseeable but also against the principle of legality and individual criminal responsibility to draw decisive conclusions from the profile and exchanges of such users for the entire user base, in the absence of concrete content or other relevant information pertaining to a particular accused. As pointed out by the Government (see paragraph 232 above), the Court takes into account the significant challenges involved in accessing the content of secure communications, which are increasingly resorted to for illicit purposes. It also notes the arguments regarding the *sui generis* nature of the FETÖ/PDY as an organisation operating in secrecy (see paragraphs 162 and 230 above). However, the difficulties encountered by the State authorities in penetrating a communication tool allegedly used by an organisation designated as terrorist after use of that tool are not sufficient reason to attach criminal liability in a virtually automatic manner to those who previously used that tool, in disregard of the guarantees laid down in Article 7 of the Convention.

266. The Court considers that the need to establish the presence of the elements of the relevant offence on an individual basis was all the more compelling in the present context, given the organisation's pervasive presence in all sectors of Turkish society for a considerable period of time, as noted by the domestic judicial authorities (see paragraphs 41, 52, 162, 163 and 187 above; see also the memorandum of the Commissioner for Human Rights noted in paragraph 198 above). The Court of Cassation itself accepted that not all members of the organisation could be considered as possessing the knowledge and direct intent required for a finding of guilt under Article 314 § 2 of the Criminal Code. In this connection, it noted that the organisation was made up of seven layers, and that the members in the first

and second layers – who were utilised as the so-called legitimacy front of the organisation – were not necessarily aware of the goals and methods rendering it an "armed terrorist organisation" and could, in principle, benefit from the mistake provision stipulated under Article 30 of the Criminal Code (see paragraphs 162 and 163 above). Statements made by some suspects in other FETÖ/PDY-related investigations further revealed that while ByLock was indeed used within the organisation, including and in particular by those at higher levels (as noted in paragraph 176 above), the use had over time spread to those in the "lower levels" and had at one point been used across the "*cemaat*" (ibid.; see also paragraph 18 above as to the meaning of "*cemaat*"). In these circumstances, and in the absence of sufficient elucidation by the domestic courts, it is difficult to understand how it could be ascertained with such certainty and automaticity that all alleged users of ByLock, such as the applicant, were individuals who could be validly considered to be "members of an armed terrorist organisation" within the meaning of domestic law as previously interpreted and applied by the domestic courts (see also, to this effect, the observations of the UNWGAD noted in paragraph 196 above; see further the Explanatory Report on the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism mentioned in paragraph 203 above – which was not in force in respect of Türkiye at the time of all the relevant domestic judgments taken into consideration in the present case – where the significance of the elements of "intention" and "terrorist purpose" is emphasised in relation to the analogous offence of "participating in an association or group for the purpose of terrorism" provided for under Article 2 of the Additional Protocol).

267. Having regard to the foregoing, the Court cannot but find that the applicant's conviction for membership of an armed terrorist organisation was secured without duly establishing the presence of all constituent elements of that offence in an individualised manner, in contravention of the requirements under domestic law and the principles of legality and foreseeability that is at the core of the protection under Article 7. It notes in this regard that although the use of ByLock was technically not part of the *actus reus* of the impugned offence, the domestic courts' interpretation had in practice the effect of equating the mere use of ByLock with knowingly and willingly being a member of an armed terrorist organisation.

268. The Court stresses that this finding under Article 7 does not as such concern the relevance of the ByLock evidence to establishing the applicant's guilt to the required standard of proof. The issue here is rather that, to all intents and purposes, the factual finding regarding the use of ByLock alone was considered to have made out the constituent elements of the offence of membership of an armed terrorist organisation. It is moreover clear from the domestic court judgments and the Government's submissions that the other acts attributed to the applicant had very limited bearing on the outcome (see paragraph 257 above). The effect of this unforeseeable and expansive

interpretation of how the provisions of Article 314 § 2 of the Criminal Code and the Prevention of Terrorism Act should apply was to create an almost automatic presumption of guilt based on ByLock use alone, making it nearly impossible for the applicant to exonerate himself from the accusations (*see G.I.E.M. S.r.l. and Others*, cited above, § 243, with further references). It flows from the object and purpose of Article 7, which seeks to ensure that no one should be subjected to arbitrary prosecution, conviction or punishment, that whatever the factual basis for the offence, the substantive guarantees of legal certainty should be satisfied.

(c) Conclusion

269. The Court is acutely aware of the difficulties associated with the fight against terrorism and those that States encounter in the light of the changing methods and tactics used in the commission of terrorist offences (see *Parmak and Bakır*, cited above, § 77). It has, furthermore, already acknowledged the unique challenges faced by the Turkish authorities and courts in the context of their efforts against the FETÖ/PDY, having regard to the atypical nature of that organisation, which, according to the domestic authorities and courts, pursued its aims covertly rather than through traditional terrorist methods. The Court reiterates in this connection the finding it has made in a number of cases, and endorsed in the present case (see paragraph 213 above), that the attempted military coup in Türkiye disclosed the existence of a "public emergency threatening the life of the nation" within the meaning of the Convention (see, for instance, *Mehmet Hasan Altan*, cited above, § 93, and *Baş v. Turkey*, no. 66448/17, § 115, 3 March 2020). Therefore, the urgency and severity of the situation that the authorities and courts had to grapple with in the aftermath of the coup attempt are recognised.

270. It should also be emphasised, however, that none of these considerations mean that the fundamental safeguards enshrined in Article 7 of the Convention, which is a non-derogable right that is at the core of the rule of law principle, may be applied less stringently when it comes to the prosecution and punishment of terrorist offences, even when allegedly committed in circumstances threatening the life of the nation. The Convention requires the observance of the Article 7 guarantees, including in the most difficult of circumstances.

271. The Court considers that it is up to the States to adapt their terrorism laws to be able to combat effectively the evolving threats of terrorism and non-traditional terrorist organisations, within the bounds of the *nullum crimen, nulla poena sine lege* principle. The offence of membership of an armed terrorist organisation under Turkish law was at the material time, and still remains, an offence of specific intent. The presence of some specific subjective elements is therefore a *conditio sine qua non*. Despite that, the finding by the domestic courts, through expansive interpretation of the applicable provisions of the Criminal Code and the Prevention of Terrorism

Act, that the use of ByLock denoted membership of an armed terrorist organisation, without seeking to establish the presence in the applicant's specific case of the knowledge and intent required under the legal definition of the crime in domestic law, effectively attached objective liability to the use of ByLock. The Court is of the view that this expansive and unforeseeable interpretation of the law by the domestic courts had the effect of setting aside the constituent – notably the mental – elements of the offence and treating it as akin to an offence of strict liability, thereby departing from the requirements clearly laid down in domestic law. The scope of the offence was, therefore, extended to the detriment of the applicant in an unforeseeable manner, contrary to the object and purpose of Article 7.

272. The Court concludes, in the light of the foregoing, that there has been a violation of Article 7 of the Convention.

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

273. The applicant complained under Article 6 § 1 of the Convention that the data regarding his use of the ByLock application, which had been the decisive evidence to secure his conviction, had been obtained unlawfully and should therefore have been inadmissible. He further complained that the relevant data had not been made available for him to examine or challenge, in breach of the principles of equality of arms and adversarial proceedings as well as the clear requirements under Article 134 of the CCP (the Code of Criminal Procedure), and that the domestic courts had relied exclusively on the unilateral assessment of the prosecution and other public authorities of that data without examining them directly or subjecting them to other independent assessment. He claimed, moreover, that the evidence underpinning his conviction, and in particular that regarding his use of ByLock, had been assessed arbitrarily by the domestic courts, and that his objections and requests before the Ankara Regional Court of Appeal and the Court of Cassation regarding the evidence had been ignored by those courts in judgments that lacked reasoning.

274. The relevant parts of Article 6 § 1 of the Convention read as follows:

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

A. Admissibility

1. The parties' submissions

275. The Government claimed that the applicant had not complained before the Court, or before the competent domestic courts, of (i) the lack of safeguards to protect the integrity and authenticity of the ByLock data obtained by the MİT in the period preceding their submission to the judicial authorities; (ii) the denial of his request for the ByLock data to be submitted

to independent expert examination; and (iii) the lack of any possibility to refute the allegations against him. The Government requested, accordingly, that the Court refrain from examining these matters or declare them inadmissible for non-exhaustion of domestic remedies.

276. The applicant stated at the outset that while the case before the Court was limited to the facts complained of by an individual, it was untenable that the Court should limit itself to the exact words and expressions used in the application form. According to the applicant, any complaint submitted to the Court, at least in substance, had to be examined. He further argued that in any event, and contrary to the Government's allegations, he had clearly complained in his application form that the domestic courts had failed to question the factual authenticity and the integrity of the ByLock data and that they had been content to rely on documents produced by public bodies that were neither independent nor impartial, without submitting the data to independent examination. He had also expressly stated in his application form that the ByLock data had not been submitted to his review and that he had thus been put in a position in which he had no means to produce his counter-arguments regarding that data, in breach of the principle of equality of arms. Consequently, the Government's argument that he had not complained before the Court of his inability to refute the allegations against him was ill-founded.

277. The applicant added that the complaints in question had also been raised before the domestic courts, including the Constitutional Court, and that the latter had dismissed them as manifestly ill-founded without specifically citing any other grounds of inadmissibility, such as non-exhaustion of the available remedies.

2. The Court's assessment

278. The Court refers at the outset to the findings in *Radomilja and Others v. Croatia* ([GC], nos. 37685/10 and 22768/12, §§ 123-26, 20 March 2018) as regards its powers in examining an application and the limits thereto, and reiterates that the scope of a case before the Court remains circumscribed by the facts as presented by the applicant.

279. In this connection, it is noted, and the Government do not deny, that the applicant complained before the Court that the ByLock data had been retrieved by the MİT unlawfully outside the procedural safeguards provided under the CCP for the collection of electronic evidence, that the relevant data had not been shared with him or his lawyer in breach of the principles of adversarial proceedings and equality of arms, and that the domestic courts had relied exclusively on the reports prepared by various public bodies – that did not enjoy the guarantees of independence and impartiality – without submitting the data to other examination.

280. When these complaints are viewed against the background of the facts as presented by the applicant, it cannot reasonably be argued that he did

not in substance call into question the integrity of the ByLock data procured by the MİT, the lack of submission of that data to independent examination, or the lack of access to potentially exculpatory material on account of the non-disclosure of that data. It is stressed in this regard that applicants are not expected to present their complaints, either before domestic instances or before the Court, using a particular terminology or particular line of legal reasoning that reflects the Court's approach to the relevant Convention issues, and that it is sufficient that a complaint is raised in substance (see *Radomilja and Others*, cited above, §§ 116 and 117). Accordingly, the Court does not consider that its consideration of these matters would be tantamount to ruling beyond the scope of the case. This is particularly so noting that, contrary to the Government's arguments, the matters at issue were also raised by the applicant before domestic instances, including before the Constitutional Court (see paragraphs 73, 75, 92, 93, 97 and 100 above), and were also addressed in detail in his observations submitted to the Court. It is recalled in this regard that applicants are not prevented from clarifying or elaborating on their initial submissions during the Convention proceedings (see *Radomilja and Others*, cited above, § 122).

281. Accordingly, the Court rejects the Government's preliminary objections noted in paragraph 275 above. It further considers that the applicant's complaints under this head are not manifestly ill founded within the meaning of Article 35 § 3 of the Convention, nor are they inadmissible on any other grounds. They must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) Submissions of the applicant

282. The applicant maintained his argument that the data pertaining to his use of ByLock had been collected unlawfully by the MİT and could therefore not be used as evidence to convict him, since the use of unlawful evidence was prohibited under domestic law. He argued that according to additional section 1 of the Law on Intelligence Services (see paragraph 145 above), information collected as part of intelligence activities could not be requested by judicial authorities for use as evidence in criminal proceedings, with the exception of certain specific offences which were not at issue in his case. Moreover, according to section 6 (2) of the same Law (see paragraph 144 above), a prior court order was required for the MİT to intercept communications via telecommunication networks, which had not been obtained before the MİT acquired the ByLock data. In holding that the MİT had acted lawfully, the domestic courts had erroneously relied on the MİT's powers set out in very broad terms in the first paragraph of section 6, ignoring

the requirements under the second paragraph, and had failed to sufficiently explain why the rule under additional section 1 had not been observed.

283. The applicant further noted that in accepting the use of the ByLock data as lawful evidence in the criminal proceedings, the domestic courts – led by the Court of Cassation's landmark judgments – had based themselves on the fact that the examination and use of that data for judicial purposes had been authorised by the order issued by the Ankara Fourth Magistrate's Court on 9 December 2016 on the basis of Article 134 of the CCP. The applicant considered this finding to be problematic for a number of reasons. He claimed, in particular, that contrary to the domestic courts' reasoning, the analysis and use of the ByLock evidence for judicial purposes had predated the Ankara Fourth Magistrate's Court's order of 9 December 2016, as evidenced by the fact that he had been placed in pre-trial detention on 9 September 2016 for membership of the FETÖ/PDY on account of his use of ByLock. He gave similar examples from other proceedings initiated in relation to the use of ByLock throughout Türkiye and claimed that ByLock users were identified on the basis of the raw data collected by the MİT long before any judicial order. In the applicant's view, this meant that examination of the digital data and other ensuing measures were carried out within the scope of intelligence activities without any judicial warrant. This was in blatant disregard of the procedural safeguards laid down in domestic law, which had been put in place for the very purpose of providing protection against abuse and ensuring the integrity and reliability of the data seized. Despite this, the domestic courts had not subjected the admissibility and lawfulness of the main evidence to sufficient scrutiny.

284. In the applicant's view, this absence of judicial oversight of the collection and processing of the ByLock data had left them vulnerable to alterations and had made it impossible to verify their authenticity and integrity. This deficiency was further compounded by the fact that the MİT had not provided an account of the steps that it had taken to ensure the integrity of the data in a verifiable manner. In these circumstances, the ByLock data could neither be regarded as reliable nor conclusive. The applicant pointed in this connection to the alleged discrepancies between the different user lists prepared by the MİT, as well as between the number of downloads and that of individuals identified as users.

285. The applicant added that the CGNAT data and HTS records relied on by the Ankara Regional Court of Appeal to verify the accuracy of the ByLock data in his regard had similarly been unlawful and unreliable. He argued that whereas under the relevant legal framework Internet traffic data could be retained and stored for a maximum period of one year, the CGNAT data and HTS records submitted by the BTK to the appeal court in his respect had included information dating back more than one year. As for the reliability issue, the applicant referred in the first place to the alleged IP-based attribution challenges, claiming that the same IP address could be used by

more than one person at a time, and also argued, relying on an expert report (see paragraph 131 above), that CGNAT data were in general not reliable indicators that a connection had been established by a certain individual with a certain target IP address. The same expert had also noted that the CGNAT data and HTS records in his case file did not conclusively suggest that he had connected to the ByLock server deliberately. The applicant further alleged that the BTK had fabricated log records by adding data to and removing data from the original traffic records that it had received from the network providers. By way of proof, he submitted some documents pertaining to another criminal investigation, where the missing target IP numbers in the original document issued by a service provider had been filled in by the BTK when transmitting that document to the trial court.

286. As regards his claims that he had not been able to duly challenge the evidence against him, the applicant maintained that despite being the decisive evidence for his conviction, and contrary to the requirement flowing from Article 134 § 4 of the CCP, a copy of the ByLock data pertaining to his alleged use of that application had not been disclosed to him or submitted to independent expert examination by the domestic courts. He could, therefore, neither verify the reliability of the data in question and refute the claims made by the MİT, nor use them to uncover any potentially exculpatory information and to contest the veracity of the "exclusive use" argument. The ByLock reports made available to him instead contained very general, indirect and non-verifiable information that had been put together by officials whose ranks or functions had not been specified. What is more, those reports were highly cryptic and failed to explain how the relevant information had been put together from a technical point of view, which made them impossible to challenge in practice. The applicant further argued that the additional expert report commissioned by the Ankara Regional Court of Appeal merely summarised the findings already available in the case file, without any added value, and that his request for an independent examination of the raw data had been turned down. He contended that in these circumstances, his right to adversarial proceedings and equality of arms conferred by Article 6 of the Convention had been breached, as he had been at a substantial disadvantage *vis-à-vis* the prosecution. The applicant stressed that the circumstances of his case had to be distinguished from others similarly involving large amounts of electronic data, such as *Rook v. Germany* (no. 1586/15, 25 July 2019), where the lack of full disclosure of the data in the hands of the prosecution was not found to have breached the fair trial requirements under Article 6 § 1. He claimed that unlike in that case, the evidence used against him was not collected within the framework of a judicial procedure subject to independent oversight, and was thus inherently unreliable.

287. The applicant also complained that both the Ankara Regional Court of Appeal and the Court of Cassation had rejected his appeals without addressing his objections regarding issues that had been decisive for the

outcome of the proceedings, including those of the lawfulness and admissibility of the ByLock evidence and the organisational nature of the ByLock application. He stressed the lack of satisfactory reasoning in respect of the finding that ByLock had been used by the Gülen movement exclusively, despite the centrality of that presumption to his conviction, as well as the failure of the domestic courts to duly establish his mental and material link to the serious offence that he had been charged with. The applicant argued that alongside him, thousands of others had been convicted of membership of an armed terrorist organisation as their alleged use of ByLock was deemed to be conclusive evidence of that crime in the landmark judgments of the Court of Cassation, despite the absence of any concrete evidence revealing the requisite link. According to the applicant, such unfettered arbitrariness on the part of the domestic courts, based not only on inadmissible but also totally irrelevant evidence and hypothetical findings, amounted to a blatant violation of fundamental rights and freedoms.

288. The applicant further underlined in this regard that the bank that he had dealt with and the trade union and association that he had been a member of had been operating with the permission and under the control of the State at the material time, which had also been ignored by the domestic courts.

(b) Submissions of the Government

289. The Government recalled at the outset that according to the subsidiarity principle that constituted the foundation of the Convention system, it was primarily for the domestic courts to assess the evidence available, and it was not for the Court to act as a court of "fourth instance" by questioning the conclusions reached by domestic courts or to substitute its own views for their findings. Noting that the applicant's complaints under Article 6 mainly concerned the admissibility of the evidence indicating his use of ByLock and the assessment of the evidential value of the use of that application, the Government maintained that those matters had been duly reviewed by the domestic courts in a comprehensive manner. They further contended that the trial against the applicant had been fair overall and had been conducted in accordance with the principles of equality of arms and adversarial proceedings, and that he had been convicted on the basis of lawful and objective evidence. The Government then went on to address the specific claims raised by the applicant under this head.

290. They submitted that contrary to the applicant's arguments, the MİT had been mandated and authorised to collect the ByLock data by virtue of section 4 (1) (a) and (i) and section 6 (1) (d) and (g) of the Law on Intelligence Services (see paragraphs 143 and 144 above). The work conducted by the MİT in this respect was not an act of law enforcement or judicial investigation to collect evidence for use in criminal proceedings, but intelligence work carried out to detect terrorist threats before they materialised, which was a significant need in democratic societies and which did not require judicial

oversight. They specified that the actual judicial process had started in December 2016 after the handover of the relevant digital data by the MİT to the judicial authorities, who had processed that data in keeping with Article 134 of the CCP and had provided judicial oversight.

291. The Government argued that the applicant had not put forth any concrete arguments as to why the relevant data could not be considered to be reliable and that, therefore, they should not be required to defend their reliability in the abstract. Nevertheless, they provided the Court with an account of the measures taken to ensure the reliability and authenticity of the ByLock data.

292. In this connection, the Government explained that the MİT had obtained the raw data from the ByLock server as a file automatically created by the MySQL software – an open-source relational database management system – without any human intervention. The hash value of the file was computed before its delivery to the judicial authorities to ensure the data integrity. Upon its subsequent receipt by the judicial authorities, the hard disk containing the raw ByLock data was subjected to examination pursuant to Article 134 of the CCP. Accordingly, it was copied by two appointed experts in accordance with the digital forensics standards, in the presence of a judge and recorded by camera, and one copy was sent to the KOM, and the other was secured at a safe deposit. Sufficient measures were therefore in place to ensure the integrity and reliability of the ByLock data. Moreover, the judicial authorities had the power to put the data in their possession to the test and to assess their authenticity and reliability.

293. The Government further explained that the action carried out by the MİT and subsequently the KOM had been limited to rendering the raw data intelligible in order to be able to extract meaningful information from them – as the raw data file generated automatically by the MySQL was not readable without further processing with the assistance of an interface program – and had not involved any modification of their content. The analysis carried out by the MİT in this respect had not been subject to any judicial authorisation or oversight, as it remained within the domain of intelligence activities. However, the fact that the end-product retrieved separately by the MİT and by the KOM matched was proof that no manipulation of the raw data had taken place. It was further observed that in many investigations subsequently carried out, the statements given by the accused regarding the usernames, passwords and roster information matched the ByLock data retrieved by the MİT and the judicial authorities.

294. However, in the Government's opinion, the most telling indication of the integrity of the raw ByLock data was that the CGNAT data – which gave information about the date, the number of times and the address from which a connection had been made to the target IP address of the ByLock server – included in the applicant's case file at the appeal court stage tallied with his ByLock data. The Government contended that there was no question

regarding the reliability of CGNAT data *per se*, as this was data produced by the service providers' systems following the generation of traffic flow and after the calculation of the hash value, and thus were not corruptible. What is more, the appeal court had verified the CGNAT data against the HTS records – which indicated, *inter alia*, the call history and the times and durations of the calls made – and had also appointed an independent digital forensics expert to examine all the available data. The Government pointed out that the applicant had had the right under Article 68 of the CCP to request the hearing of this expert in the trial, yet he had not exercised that right. Nor had he explained why he objected to that expert and requested the re-examination of the evidence by a panel of three experts instead.

295. The Government further contested the applicant's argument that he had not been able to duly challenge the evidence against him. They argued that the applicant's use of ByLock had been established on the basis of various reports drawn up by the police, the BTK and the aforementioned independent expert, and that all of those reports had been made available to him in keeping with the principles of equality of arms and adversarial proceedings. They stressed that the applicant's access to the investigation file had not been restricted in any way. They moreover added that the applicant could also challenge the finding in the landmark judgments of the Court of Cassation regarding the "exclusive use" of ByLock by members of the FETÖ/PDY, which he had failed to do.

296. As for the applicant's claim that he had not been able to obtain a copy of the original or raw ByLock data, the Government argued that whereas the procedure set out under Article 134 of the CCP for the seizure of digital material required the sharing with the suspect of the copies of the material seized, that requirement only applied where the suspect was the owner of the computer, computer program or the log from which the data had been seized. The data at issue in the present case did not, however, belong to the applicant, but had been obtained from the ByLock server. The Government stressed that the ByLock data obtained by the MİT contained millions of data items relating to more than a hundred thousand users. Moreover, it was not intelligible in the form in which it had been collected. Information pertaining to a user was not found in one place but was scattered in different tables, making it impossible to extract the raw data for individual users, and the authorities had therefore had to develop an interface program to make the data meaningful in relation to each user. In these circumstances, the disclosure of the entire body of raw data to the applicant would entail sharing data relating to all users, thereby creating a security risk and potentially prejudicing the investigations, not to mention the interference that it would constitute with the privacy rights of other users. Moreover, special software had to be used in order to render the raw data meaningful. The Government noted that in any event, the applicant had failed to explain how his inability to obtain a copy of

the raw data in its entirety had put him at a disadvantage and how this data would have impacted the decision to be delivered in his respect.

297. The Government lastly contended that the domestic courts' interpretations and conclusions regarding the evidential value of the ByLock evidence, involving extensive evaluations of the technical and organisational aspects of ByLock, did not entail any manifest error or arbitrariness and that they had duly reasoned their judgments. They claimed in this regard that the domestic judgments in the present case were based on findings of fact and the relevant case-law of the Court of Cassation, which had established that ByLock had been used exclusively by the FETÖ/PDY. Having regard to the constraints under which the judicial system was operating at the material time as noted by the Constitutional Court in its *Aydın Yavuz and Others* judgment (as noted in *Baş*, cited above, § 93) and the derogation in place, it was consistent with Article 6, and strictly required within the meaning of Article 15 of the Convention, for domestic courts to rely on earlier case-law in this manner without engaging in a fresh examination of the matter themselves – provided that it was open to an accused to challenge those findings.

298. Accordingly, when the Ankara Regional Court of Appeal had deemed the evidence leading to the applicant's conviction at first instance – that is, ByLock user reports prepared on the basis of the raw data – to be insufficient, it had requested complementary reports from the BTK concerning the applicant's CGNAT data and HTS records, and had thus verified the finding regarding the applicant's use of ByLock in a manner consistent with the Court of Cassation's case-law. The appeal court had also responded to the applicant's claims concerning the unlawfulness of the evidence at issue, and had engaged in a detailed assessment of the elements of the offence of membership of an armed terrorist organisation and discussed why the use of ByLock was deemed sufficient to prove membership of that organisation. This finding was, moreover, supported by other corroborating evidence. The Court of Cassation had in turn endorsed the appeal court's duly reasoned judgment, which the appellate courts were allowed to do under the Court's case-law (see *García Ruiz v. Spain* [GC], no. 30544/96, § 26, ECHR 1999-I).

299. To the extent that the applicant complained that the impugned evidence was insufficient to sustain a conviction, the Government reiterated that the Court was not a court of fourth-instance before which an applicant could raise issues of the sufficiency of evidence. They emphasised that, as per Article 217 of the CCP, an imputed offence could be proven by any evidence obtained lawfully, including circumstantial evidence, and that it was primarily for the domestic courts to assess the evidence and reach the necessary conclusions in the context of criminal proceedings.

2. The Court's assessment

(a) Preliminary remarks

300. The Court has established above, under Article 7 of the Convention, that the applicant's conviction for membership of an armed terrorist organisation was based on an expansive and unforeseeable interpretation of the relevant domestic law. It found that this interpretation, whereby the domestic courts effectively imputed objective liability to the users of ByLock, had the effect of assuming instead of establishing the constituent elements of the offence at issue as set out under the relevant domestic law and practice. It therefore contravened the object and purpose of that provision to provide effective safeguards against arbitrary prosecution, conviction and punishment.

301. The applicant's complaints regarding his conviction on the basis of his alleged use of ByLock are not however limited to the question of the conformity of such conviction with the principles enshrined in Article 7 of the Convention. As set out in paragraph 273 above, the applicant also complained under Article 6 § 1 of the alleged irregularities in the collection and admission in evidence of the ByLock data, as well as the difficulties he encountered in challenging them and the inadequacy of the reasoning in the courts' decisions *vis-à-vis* that evidence, producing an arbitrary outcome. To the extent that the applicant's complaints relate to the deficiencies in the domestic proceedings in the establishment of the material and mental elements of the offence of membership of an armed terrorist organisation on the basis of his alleged use of ByLock, that matter has already been dealt with under Article 7 and no separate issue arises under Article 6 § 1. However, the applicant has raised some distinct fair trial issues, particularly of a procedural nature, that do not fall to be addressed under Article 7. The Court is therefore called upon to determine under Article 6 § 1 whether the applicant's defence rights were prejudiced on account of the various shortcomings alleged.

(b) General principles

302. It is not for the Court to deal with alleged errors of law or fact committed by the national courts unless and in so far as they may have infringed rights and freedoms protected by the Convention (see, amongst others, *García Ruiz*, cited above, § 28, and *Perez v. France* [GC], no. 47287/99, § 82, ECHR 2004-I), for instance where it can, exceptionally, be said that they are constitutive of "unfairness" incompatible with Article 6 of the Convention. While this provision guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence or the way in which evidence should be assessed, these being primarily matters for regulation by national law and the national courts (see *Moreira Ferreira v. Portugal (no. 2)* [GC], no. 19867/12, § 83, 11 July 2017).

303. It is therefore not the role of the Court to determine, as a matter of principle, whether particular types of evidence – for example, evidence obtained unlawfully in terms of domestic law – may be admissible or, indeed, whether the applicant was guilty or not. The question which must be answered is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair (see *Bykov v. Russia* [GC], no. 4378/02, § 89, 10 March 2009, and the cases cited therein). It must be examined, *inter alia*, whether the applicant was given the opportunity to challenge the evidence and to oppose its use. From the perspective of the rights of the defence, issues under Article 6 may arise in terms of whether the evidence produced for or against the defendant was presented in such a way as to ensure a fair trial (see *Erkapić v. Croatia*, no. 51198/08, § 73, 25 April 2013), because a fair trial presupposes adversarial proceedings and equality of arms; thus, possible flaws in the process of administration of evidence may be examined under Article 6 § 1 (see *Mirilashvili v. Russia*, no. 6293/04, § 157, 11 December 2008). In addition, the quality of the evidence must be taken into consideration, including whether the circumstances in which it was obtained cast doubt on its reliability or accuracy (see *Bykov*, cited above, § 90). While no problem of fairness necessarily arises where the evidence obtained is unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker (ibid.). In undertaking this examination, the Court also has regard to the state of the other evidence in the case file and attaches weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (see ibid., and *Gäfgen v. Germany* [GC], no. 22978/05, § 164, ECHR 2010).

304. Issues such as the weight attached by the national courts to particular items of evidence or to findings or assessments submitted to them for consideration are not for the Court to review. The Court should not act as a fourth-instance body and will therefore not question under Article 6 § 1 the national courts' assessment unless their findings can be regarded as arbitrary or manifestly unreasonable (see *Bochan v. Ukraine (no.2)* [GC], no. 22251/08, § 61 and 62, ECHR 2015; see also the cases cited therein: *Dulaurans v. France*, no. 34553/97, §§ 33-34 and 38, 21 March 2000; *Khamidov v. Russia*, no. 72118/01, §§ 170-75, 15 November 2007; and *Anđelković v. Serbia*, no. 1401/08, §§ 24-29, 9 April 2013; as well as the application of this case-law in more recent judgments: *Moreira Ferreira*, cited above, §§ 83-100; *Pavlović and Others v. Croatia*, no. 13274/11, § 49, 2 April 2015; *Tsanova-Gecheva v. Bulgaria*, no. 43800/12, § 91, 15 September 2015; *Navalnyy and Ofitserov v. Russia*, nos. 46632/13 and 28671/14, §§ 103-20, 23 February 2016; *Navalnyye*, cited above, §§ 81-84; and *Ballıktaş Bingöllü v. Turkey*, no. 76730/12, §§ 78-84, 22 June 2021). It transpires from this case-law that a domestic judicial decision cannot be qualified as arbitrary to the point of prejudicing the fairness of proceedings

unless no reasons are provided for it or if the reasons given are based on a manifest factual or legal error committed by the domestic court, resulting in a "denial of justice" (see *Moreira Ferreira*, cited above, § 85).

305. The Court reiterates in this regard that according to its established case-law reflecting a principle linked to the proper administration of justice, judgments of courts and tribunals should adequately state the reasons on which they are based. The extent to which this duty to give reasons applies may vary according to the nature of the decision and must be determined in the light of the circumstances of the case (see *García Ruiz*, cited above, § 26). Without requiring a detailed answer to every argument advanced by the complainant, this obligation presupposes that parties to judicial proceedings can expect to receive a specific and explicit reply to the arguments which are decisive for the outcome of those proceedings (see, among other authorities, *Moreira Ferreira*, cited above, § 84, and the cases cited therein). It must be clear from the decision that the essential issues of the case have been addressed (see *Taxquet v. Belgium* [GC], no. 926/05, § 91, ECHR 2010). In view of the principle that the Convention is intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective, the right to a fair trial cannot be seen as effective unless the requests and observations of the parties are truly "heard", that is to say, properly examined by the tribunal (see *Ilgar Mammadov v. Azerbaijan (no. 2)*, no. 919/15, § 206, 16 November 2017; *Carmel Saliba v. Malta*, no. 24221/13, § 65, 29 November 2016, with further references therein; *Ayetullah Ay v. Turkey*, nos. 29084/07 and 1191/08, § 127 and 195, 27 October 2020; and *Pişkin*, cited above, §§ 147, 149 and 151).

306. It is further reiterated that a fundamental aspect of the right to a fair trial is that criminal proceedings, including the elements of such proceedings which relate to procedure, should be adversarial and that there should be equality of arms between the prosecution and defence. The right to an adversarial trial means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party (see, for instance, *Murtazaliyeva v. Russia* [GC], no. 36658/05, § 91, 18 December 2018). The accused must have the opportunity to organise his or her defence in an appropriate way and without restriction as to the possibility of putting all relevant defence arguments before the trial court and thus of influencing the outcome of the proceedings (see *Rook*, cited above, § 56). The facilities which everyone charged with a criminal offence should enjoy include the opportunity to acquaint him or herself, for the purposes of preparing his or her defence, with the results of investigations carried out throughout the proceedings (ibid., § 57).

307. The right to an adversarial trial also requires, in a criminal case, that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused (see *Rowe and Davis v. the United*

Kingdom [GC], no. 28901/95, § 60, ECHR 2000-II). The term "material evidence" cannot be construed narrowly, in the sense that it cannot be confined to evidence considered as relevant by the prosecution. Rather, it covers all material in the possession of the authorities with potential relevance, also if not at all considered, or not considered as relevant (see *Rook*, cited above, § 58). Failure to disclose to the defence material evidence which contains such particulars as could enable the accused to exonerate him- or herself or have his or her sentence reduced would constitute a refusal of facilities necessary for the preparation of the defence (see *Natunen v. Finland*, no. 21022/04, § 43, 31 March 2009, and *Matanović v. Croatia*, no. 2742/12, § 157, 4 April 2017).

308. However, the entitlement to disclosure of relevant evidence is not an absolute right. In any criminal proceedings there may be competing interests, such as national security or the need to keep secret police methods of investigation of crime, which must be weighed against the rights of the accused (see, for the relevant principles, *Jasper v. the United Kingdom* [GC], no. 27052/95, § 52, 16 February 2000). In some cases, it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. That said, in principle, only such measures restricting the rights of the defence which are strictly necessary are permissible under Article 6 § 1. Moreover, in order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities (ibid., with further references). In making its assessment of the relevant procedural guarantees, the Court must have regard to the importance of the undisclosed material and its use in the trial (see *Matanović*, cited above, § 155). The accused may, however, be expected to give specific reasons for his request and the domestic courts are entitled to examine the validity of these reasons (ibid., § 157, and *Rook*, cited above, § 59).

(c) Application of the general principles to the present case

(i) The evidence regarding the applicant's alleged use of ByLock

309. The essence of the applicant's complaint under the present head is that despite their inadmissibility as evidence on account of their unlawful procurement by the MİT, the data regarding his alleged use of ByLock were relied on as the decisive element to secure his conviction by the domestic courts, without duly addressing his concerns regarding their integrity and evidential value and in disregard of the principles of equality of arms and adversarial proceedings.

310. The Court considers at the outset that, having regard to its limited role in determining the admissibility of a piece of evidence or reviewing its assessment by national courts, it is not necessary, for the purposes of its

present examination under Article 6, to determine whether the contested evidence was actually obtained lawfully in terms of domestic law and was admissible, or whether the domestic courts made any substantive errors in their assessment of the relevant evidence. Its task under Article 6 § 1 is rather to assess the fairness of the proceedings as a whole, taking into account the specific nature and circumstances of the case, including the way in which the evidence was taken and used, and the manner in which any objections concerning the evidence were dealt with (see *Bykov*, cited above, §§ 88-90; *Huseyn and Others v. Azerbaijan*, nos. 35485/05 and 3 others, §§ 199, 200 and 211, 26 July 2011; *SA-Capital Oy v. Finland*, no. 5556/10, § 78, 14 February 2019; *Kobiashvili v. Georgia*, no. 36416/06, § 56, 14 March 2019; and *Ayetullah Ay*, cited above, §§ 124 and 125). The Court notes in this regard that there is a distinction between the admissibility of evidence – that is to say the question of which elements of proof may be submitted to the relevant court for its consideration – and the rights of the defence in respect of evidence which in fact has been submitted to the court (see *SA-Capital Oy*, cited above, § 74 and the references therein, and *Ayetullah Ay*, cited above, § 125). In assessing the overall fairness of the proceedings, particular regard must be had to whether the rights of the defence were respected in a manner consonant with Article 6, in the light of all of the relevant elements of the case (see *Bykov*, cited above, § 90, and *SA-Capital Oy*, cited above, § 78; see also the principles recalled in paragraph 303 above).

311. Turning to the facts of the present case, it has already been established, in the context of the examination conducted under Article 7, that the applicant's conviction for membership of an armed terrorist organisation rested decisively on the finding that he had used the ByLock application, which finding was primarily based on the data obtained by the MİT, the remaining evidence serving only as a source of corroboration. In these circumstances, the quality of the evidence in question and the applicant's ability to effectively challenge it in proceedings that complied with the guarantees of Article 6 § 1 were all the more important. These matters will accordingly be examined in turn. However, before proceeding with this examination, the Court wishes to clarify whether the specific nature of the evidence at issue, that is encrypted electronic data stored at the server of an Internet-based communication application, requires it to adapt the application of the relevant guarantees under Article 6 § 1 in any way.

312. The Court acknowledges that electronic evidence has become ubiquitous in criminal trials in view of the increased digitalisation of all aspects of life. It notes more pertinently, and without prejudice to its subsequent examination in the present case, that recourse to electronic evidence attesting that an individual is using an encrypted messaging system which had been specially designed for and used exclusively by a criminal organisation in the internal communications of that organisation, can be very important in the fight against organised crime (see *Akgün v. Turkey*,

no. 19699/18, § 167, 20 July 2021). It also notes that electronic evidence differs in many respects from traditional forms of evidence, including as regards its nature and the special technologies required for its collection, securing, processing and analysis. Most significantly, it raises distinct reliability issues as it is inherently more prone to destruction, damage, alteration or manipulation. The Court also reiterates that the use of untested electronic evidence in criminal proceedings may involve particular difficulties for the judiciary as the nature of the procedure and technology applied to the collection of such evidence is complex and may therefore diminish the ability of national judges to establish its authenticity, accuracy and integrity (ibid.). Moreover, the handling of electronic evidence, particularly where it concerns data that are encrypted and/or vast in volume or scope, may present the law enforcement and judicial authorities with serious practical and procedural challenges at both the investigation and trial stages.

313. That said, these factors do not in the abstract call for the safeguards under Article 6 § 1 to be applied differently, be it more strictly or more leniently. The Court's main concern is, once again, to assess whether the overall fairness of the proceedings was ensured through the lens of the procedural and institutional safeguards and the fundamental principles of a fair trial inherent in Article 6 of the Convention (see *Al-Khawaja and Tahery v. the United Kingdom* [GC], nos. 26766/05 and 22228/06, § 118, ECHR 2011, and *Ayetullah Ay*, cited above, § 194).

(α) Quality of the evidence

314. According to the applicant, the detailed requirements set out in Articles 134 and 135 of the CCP (see paragraph 142 above) regarding the collection of electronic data pursued the aim of protecting against abuse and ensuring the authenticity and integrity of such data. He claimed, on that basis, that the fact that the State intelligence service had obtained and processed the relevant ByLock data in total secrecy and without any judicial oversight or other procedural guarantees envisaged under the CCP had put into question the reliability of the data.

315. The Court notes that electronic or other data collected by intelligence services, whose activities in that regard may or may not be subject to the standard rules of procedure applicable to the collection of evidence, may be increasingly resorted to in criminal proceedings as direct or indirect evidence. As indicated by the Venice Commission, "in order to anticipate, prevent or protect itself against threats to its national security, a State needs effective intelligence and security services" and that intelligence constitutes "one of the main weapons the State has in the struggle against terrorism" (see paragraph 200 above). The Court also notes that it is a natural consequence of the forms taken by present-day terrorism that governments resort to

cutting-edge technologies in pre-empting such attacks (see *Szabó and Vissy v. Hungary*, no. 37138/14, § 62, 12 January 2016).

316. It is not for the Court to pronounce on whether and in what circumstances and format intelligence information may be admitted in criminal proceedings as evidence. It refers in this connection to the observations above concerning the limits of the Court's power as regards the admissibility and assessment of evidence, which is a matter that primarily remains within the discretion of national courts and other competent authorities (see paragraphs 303, 304 and 310 above). It acknowledges, however, that in cases where the collection or processing of such information is not subject to prior independent authorisation or supervision, or a *post factum* judicial review, or where it is not accompanied by other procedural safeguards or corroborated by other evidence, its reliability may be more likely to be called into question.

317. Turning to the examination of the facts before it, the Court notes that the whole structure of the Convention rests on the general assumption that public authorities in the Contracting States act in good faith (see, for instance, *Kavala v. Türkiye* (infringement proceedings) [GC], no. 28749/18, § 169, 11 July 2022, and *Khodorkovskiy v. Russia*, no. 5829/04, § 255, 31 May 2011). There are no objective indications before it to doubt that the MİT or other public authorities acted in good faith in relation to the ByLock data. That said, it transpires from the information in the case file that sections 4 (1) and 6 (1) of the Law on Intelligence Services, invoked by the domestic courts and the Government as the legal basis for the MİT's conduct, do not envisage procedural safeguards akin to those set out under Article 134 of the CCP with respect to the collection of electronic evidence, including independent authorisation or oversight. Moreover, nothing in the case file suggests that the Ankara Fourth Magistrate's Court's subsequent order for the examination of the ByLock data pursuant to Article 134 of the CCP entailed a *post factum* judicial review of the MİT's data collection activity. On that basis, and given that the MİT had apparently retained the relevant data for many months prior to their submission to the judicial authorities, the Court does not agree with the Government that the applicant's doubts regarding the reliability of the ByLock data may be readily dismissed as being abstract or baseless, and will examine whether any measures were taken by the MİT or the judicial authorities to allay those doubts.

318. The Court refers in this connection to the Government's account of the forensic precautions taken by the MİT and the investigating authorities to ensure the integrity and reliability of the relevant data, as explained in paragraphs 292 and 293 above. It considers that it is not in a position to assess whether those measures presented sufficient guarantees of integrity and reliability, given in particular that the domestic courts did not engage in such an assessment.

319. The Court also notes, however, that the accuracy of the ByLock data obtained by the MİT, at least to the extent that it concerned the applicant, was tested by other means as indicated by the Government (see paragraph 294 above). In this connection, whereas the first-instance court judgment delivered in the applicant's respect rested solely on the reports derived from the data handed over by the MİT, at the appeal stage the Ankara Regional Court of Appeal requested the BTK to furnish the CGNAT data and HTS records to verify that the applicant, whose user ID had been detected on the basis of the raw data obtained by the MİT, had actually connected to the ByLock target IP address from his phone. This metadata obtained by the BTK from the service providers, which was also confirmed by an expert, were taken as showing that the applicant had indeed connected to that application. The regional appeal court's finding in this regard was upheld by the Court of Cassation.

320. The lawfulness, accuracy and reliability of these complementary CGNAT data and HTS records were also contested by the applicant both before the domestic courts and the Court, as indicated in paragraphs 92 and 285 above. The Court does not, however, consider those arguments to be sufficient to call into question the assessment undertaken by the domestic courts for the reasons indicated below.

321. Firstly, even assuming that the CGNAT data and HTS records were indeed obtained outside the statutory time-limit as alleged, this would not have any bearing on the technical accuracy of those records, in the absence of any arguments to the contrary by the applicant.

322. Secondly, as concerns the allegations regarding the reliability of the CGNAT data, the Court notes that the applicant did not advance any manipulation claims before the domestic courts or the Court pertaining to his individual records, which were all available in the case file for his review. Moreover, apart from voicing some general concerns regarding the possible allocation of the same IP address to multiple users, the applicant did not advance any tangible claims before the domestic courts that would call into question his personal CGNAT data indicating the connection from his telephone to the ByLock IP addresses. The expert report that he subsequently submitted to the Court (see paragraph 131) pointed to the inconclusive nature of those records. The Court indeed acknowledges that the *Mor Beyin* incident, which demonstrated that the CGNAT data could be misleading (see paragraphs 119 and 167 above), did raise well-founded doubts regarding the possibility of inadvertent connections to the ByLock server. It also notes, however, the Court of Cassation's finding that such risk was not present in cases where, in addition to the CGNAT data showing connections to the ByLock server, an individual's ByLock user ID was identified on the basis of the information obtained from the ByLock server (see, in particular, the Court of Cassation judgments, noted in paragraphs 167 and 168 above).

323. It therefore follows that the domestic courts in the applicant's case assessed the CGNAT data not in isolation from but in conjunction with the data obtained from the ByLock server and with the HTS records, and arrived at the conclusion that these separate sets of data, when viewed together, established that he had used the ByLock application. Accordingly, although it is recognised that the circumstances in which the ByLock data was retrieved by the MİT did *prima facie* raise doubts as to their "quality" in the absence of specific procedural safeguards geared to ensuring their integrity until the handover to the judicial authorities, the Court does not have sufficient elements to impugn the accuracy of those data – at least to the extent that they established the applicant's use of the ByLock application.

(β) The applicant's ability to challenge the evidence in proceedings that complied with the guarantees of Article 6 § 1 of the Convention

324. The Court reiterates that a review of the overall fairness of the proceedings must also incorporate an assessment as to whether the applicant was given the opportunity of challenging the evidence and of opposing its use in circumstances where the principles of adversarial proceedings and equality of arms between the prosecution and the defence were respected (see *Kobiashvili*, cited above, § 56). It is stressed that the question whether the applicant's challenges to the evidence were properly examined by the domestic courts, that is whether the applicant was truly "heard", and whether the courts supported their decisions with relevant and adequate reasoning, are also factors to be taken into account in conducting this assessment (see, *mutatis mutandis*, *Taxquet*, cited above, § 91, and *Ilgar Mammadov (no. 2)*, cited above, § 206). In this regard, it should be reiterated that while courts are not obliged to give a detailed answer to every argument raised, it must be clear from the decision that the essential issues of the case have been addressed (see *Taxquet,* cited above, § 91).

325. The applicant mainly complained that he had been unable to properly challenge the ByLock evidence in his regard as the data collected by the MİT from the ByLock server had not been shared with him or submitted to independent examination in accordance with the principles of equality of arms and adversarial proceedings, and as required under Article 134 § 4 of the CCP. He claimed that it was essential for him to have access to those data so as to verify their reliability and integrity, as well as to access potentially exculpatory information, and to contest the veracity of the arguments about "exclusive" and "organisational" use that were relied on by the domestic courts in support of his conviction (see paragraphs 97, 100 and 286 above).

326. The Court notes, as also pointed out by the Government, that the applicant had available to him all the ByLock reports relied on by the domestic courts in the criminal proceedings, and that the accuracy of the ByLock data pertaining to him had been verified on the basis of data obtained from other sources. The Court further notes that a technical report produced

in 2020 explained that it was not possible to sort the raw data on a user ID basis without first processing them (see paragraph 121 above). While the Court does not ignore the significance of these factors, it considers that they are not determinative of the question whether the applicant's defence rights *vis-à-vis* the ByLock evidence were duly respected in the present case.

327. The Court reiterates in this connection that the requirement of disclosure to the defence of "all material evidence" for or against the accused, which is an aspect of the right to adversarial proceedings (see *Rowe and Davis*, cited above, § 60), cannot be construed narrowly, in the sense that it cannot be confined to evidence considered as relevant by the prosecution. Rather, it covers all material in the possession of the authorities with potential relevance for the defence, even if not at all considered, or not considered as relevant by the prosecution authorities (see *Rook*, cited above, § 58). Accordingly, the fact that the applicant had access to all the ByLock reports included in the case file does not necessarily mean that he had no right or interest to seek access to the data from which those reports had been generated.

328. Similarly, the fact that the domestic courts found the ByLock data pertaining to the applicant to tally with another set of data that had been verified by an expert (see paragraph 80 above) did not necessarily remove the applicant's procedural rights with respect to those former data. It is stressed in this connection that the ByLock data in question were critical in the applicant's case, as it was those data which triggered the criminal proceedings against him. Essentially, they served not only to gather the individualised information on the applicant's alleged use of ByLock, but also constituted the basis for it to be characterised as an exclusively organisational communication tool (see the findings in the MİT report noted in paragraph 115 above) and thus led directly to the applicant's conviction. It may, moreover, not be excluded that the ByLock material potentially contained elements which could have enabled the applicant to exonerate himself, or to challenge the admissibility, reliability, completeness or the evidential value of that material (see *Matanović*, cited above, § 161).

329. The Court must nevertheless emphasise that the entitlement to disclosure of evidence is not an absolute right. As noted in paragraph 308 above, there may be a variety of reasons which may require the withholding of evidence from the defence, including concerns over national security or the preservation of the fundamental rights of others. Moreover, where the evidence in the hands of the prosecution relates to a large mass of electronic information, it may not be possible, or even necessary, to disclose that information to the defence in its entirety. The applicant's right to disclosure must not be confused with a right of access to all that material (see, for instance, *Sigurður Einarsson and Others v. Iceland*, no. 39757/15, §§ 87-93 4 June 2019). The Court is accordingly able to accept that there may have been legitimate reasons for not sharing the raw data with the applicant in the

present case. It is further reiterated that in cases where evidence has been withheld from the defence on public interest grounds, it is not the role of this Court to decide whether or not such non-disclosure was strictly necessary since, as a general rule, it is for the national courts to assess the evidence before them (see *Rowe and Davis*, cited above, § 62).

330. That said, even in such circumstances, the Court must examine whether any prejudice sustained by the applicant on account of the non-disclosure of the relevant ByLock data was counterbalanced by adequate procedural safeguards and whether he was given a proper opportunity to prepare his defence, as required by Article 6 of the Convention (see *Matanović*, cited above, §§ 153 and 165). The nature and adequacy of the safeguards required will depend on the alleged prejudice sustained on account of the non-disclosure, which, in the present case, consisted of the applicant's purported inability to verify first-hand the integrity of the evidence in question and to challenge the relevance and significance attributed to it. The Court will now examine whether these alleged difficulties experienced by the applicant in contesting the evidence against him were otherwise offset – or exacerbated – during the criminal proceedings.

331. The Court notes firstly that according to the information in the case file, the reasons advanced by the Government before the Court (in paragraph 296 above) to justify the non-disclosure of the relevant data to the applicant were never actually adverted to in the domestic courts' judgments, either in his case or in the earlier judgments of the Court of Cassation; the applicant's request that the data be admitted to the case file simply went unanswered. The complementary analysis report submitted by the Government to the Court, which provided further insight into how the ByLock user lists had been drawn up and why the raw data pertaining to individual ByLock users could not be isolated and shared with the relevant users, was similarly not available to the applicant during the course of the criminal proceedings against him (see paragraphs 119 and 121 above). Accordingly, while the Court acknowledges that it is in no position to determine whether, in what form and to what extent the relevant data should have been shared with the applicant, it cannot but note that the applicant was given no explanation by the domestic courts as to why, and upon whose decision, the raw data – particularly to the extent that they concerned him specifically – were kept from him. He was therefore deprived of the opportunity to present any counter-arguments, such as to contest the validity of those reasons or to dispute that all efforts had been made to strike a fair balance between the competing interests at play and to ensure the rights of the defence. The Court reiterates that maintaining the need for disclosure under the assessment of the competent court, keeping the defence duly informed and permitting the accused to make submissions and participate in the decision-making process as far as possible are important safeguards in this regard (see *Matanović*, cited above, § 183).

332. Secondly, the applicant's request that the raw data be submitted to an independent examination for the verification of their content and integrity was also not entertained by the domestic courts. The Court acknowledges that Article 6 does not impose on domestic courts an obligation to order an expert opinion to be produced or any other investigative measure to be taken solely because it is sought by a party, and that it is primarily for the national court to decide whether the requested measure is relevant and essential for deciding a case (see *Mirilashvili*, cited above, § 189). On the instant facts, the domestic courts' exclusive reliance on the information and reports provided by the MİT and the KOM in determining the applicant's guilt, without submitting the raw data to direct examination, does not alone suffice to render the proceedings unfair, having regard particularly to the technical competencies required to examine the ByLock data in their raw form.

333. That said, given in particular the absence of any concrete information in the case file to suggest that the data in question had at any point been subjected to examination for verification of their integrity, whether at the time of their submission to the judicial authorities in December 2016 or subsequently, the Court considers that the applicant had a legitimate interest in seeking their examination by independent experts and that the courts had the duty of properly responding to him. In this regard, the Government's explanations as to the measures taken by the judicial authorities upon receipt of the data from the MİT (see paragraph 292 above) suggest that they were aimed at preserving the integrity of the data as on the day received, rather than involving an assessment as to whether their integrity had been kept intact before the handover, which was the crux of the applicant's concern. In these circumstances, and recalling once again the critical importance of the raw ByLock data to the applicant's case beyond the question of his personal use of that application (as discussed in paragraph 328 above), the domestic courts' failure to respond to his request for such independent examination – even if only to explain why such independent examination was not deemed necessary – was problematic (see, *mutatis mutandis*, *Vidal v. Belgium*, 22 April 1992, § 34, Series A no. 235-B). The Court notes the Government's argument that the applicant did not make use of his right provided under Article 68 of the CCP to question the expert commissioned by the Ankara Regional Court of Appeal (see paragraph 294 above). It also stresses, however, that the examination conducted by that expert did not entail the examination of the raw data obtained by the MİT, as sought by the applicant, but was limited in its scope to an assessment of the various reports and records already available in the case file (see paragraph 80 above).

334. Thirdly, a number of other arguments raised by the applicant to point to his concerns regarding the reliability of the ByLock evidence – such as the inconsistency between the different ByLock user lists issued by the MİT, as well as between the number of users identified and eventually prosecuted and the number of downloads – were similarly left unanswered by the domestic

courts. The Court considers that, in principle, the inability of the defence to have direct access to the evidence and to test its integrity and reliability first-hand places a greater onus on the domestic courts to subject those issues to the most searching scrutiny. In this regard, the applicant consistently argued before the domestic courts that the ByLock data had not been collected or shared with him, in accordance with Article 134 of the CCP, which stipulates various safeguards to ensure the accuracy and integrity of the data, and thereby contested not only the lawfulness but also the reliability of that evidence (see paragraphs 58, 73, 91 and 92 above). The Court notes, however, that other than confirming the lawfulness of the data collection procedure and verifying that the applicant had established a connection with the ByLock server, the domestic courts did not address the separate matter of how the integrity of the data obtained from the server had been ensured in all respects – that is, beyond the issue of the applicant's individual use –, particularly in the period prior to their transmission to the judicial authorities on 9 December 2016. Nor did they refer to any other judgments or procedures where this matter was addressed. More specifically, they did not account for the fact that between their collection by the MİT and the magistrate's court's subsequent order for their examination, the ByLock data had already been processed and used not only for intelligence purposes, but as criminal evidence to initiate investigations and arrest suspects, including the applicant. His allegations that the MİT lacked the authority to collect data to be used as evidence in criminal proceedings and that the court order issued on 9 December 2016 could not retrospectively render the evidence thus collected "lawful" and reliable, was examined neither by the Ankara Regional Court of Appeal nor by the Court of Cassation (see paragraphs 91 and 92 above).

335. Fourthly, while it may not have been possible to share the raw data with the applicant, the requirement of "fair balance" between the parties would have at least required the proceedings to be conducted in a manner that would enable the applicant to comment on the full extent of the decrypted material concerning him, including, in particular, the nature and content of his activity over that application. The Court notes in this connection that the Ankara Regional Court of Appeal requested the KOM to provide the content of the exchanges engaged in by the applicant over ByLock, as well as information regarding the individuals that he had communicated with. However, it then delivered its judgment without waiting for the submission of those data, which were eventually included in the file after the applicant's conviction had become final. The applicant's objections regarding the absence of those data were moreover dismissed by the Court of Cassation, which held that the delivery of the appeal judgment without awaiting the submission of the detailed ByLock findings and evaluation report had not affected the outcome (see paragraph 98 above).

336. The Court observes that in making this finding, the Court of Cassation appears to have concerned itself only with the outcome of the

criminal proceedings, at the expense of an examination of the fairness of the procedure leading to it (see, *mutatis mutandis*, *Pullicino v. Malta*, (dec.), no. 45441/99, ECHR 2000-II). While it is not the Court's task to determine whether the applicant's full access to the ByLock material concerning him – in particular the content of his messages and contacts – could have affected the outcome, it cannot be ruled out that it could have served to substantively reinforce the defence arguments, including to challenge the validity of the inferences drawn from the use of the ByLock application. The Court is accordingly of the view that giving the applicant the opportunity to acquaint himself with the decrypted ByLock material in his regard would have constituted an important step in preserving his defence rights. This is all the more so considering, once again, the preponderant weight of the ByLock evidence in securing the applicant's conviction.

337. Fifthly, the Court considers that the prejudice sustained by the defence on the basis of the foregoing shortcomings was compounded by the deficiencies in the domestic courts' reasoning *vis-à-vis* the ByLock evidence. As noted above, the applicant deemed it important to access all the ByLock material to be able to contest the accuracy of the allegations made in his regard, in particular to refute the argument that the ByLock application had been used "exclusively" by the members of the FETÖ/PDY, or that he had used it for "organisational" purposes. In such circumstances, and to the extent that the applicant could not challenge those arguments directly on the basis of the ByLock data at the prosecution's sole disposal, it was primordial for the domestic courts to support them with sufficient and pertinent reasoning, and to address the applicant's objections regarding their veracity, which they failed to do.

338. In this connection, the contention that the applicant had used the ByLock application for organisational purposes was not based on any specific factual findings made in his regard, such as the discovery of incriminating ByLock content or other information suggesting a hierarchical link, but was subsumed under the argument initially made by the MİT and accepted in the landmark judgments of the Court of Cassation that ByLock had been used "exclusively" by the members of the FETÖ/PDY. It appears that this exclusivity argument, which the applicant did challenge contrary to the Government's contention (see paragraphs 74, 90, 91 and 99 above), was mainly supported by the technical features of the application – such as its encrypted nature, the special arrangements required to enter into communication with other users, the requirement to use a VPN and the automatic deletion of content –, as well as the decrypted user profiles and content (see paragraphs 115-116 and 158-160 above). The Court cannot but note, however, that the applicant drew attention during the domestic proceedings to the fact that the ByLock application could be downloaded from publicly available application stores or sites until early 2016 – that is, for approximately two years – without any control mechanism, which he

claimed weakened the exclusivity argument and necessitated the examination of the specific activity carried out over that application for each alleged user to verify if it had been used for "organisational purposes" as alleged (see paragraphs 74, 90 and 99 above).

339. The Court indeed notes the findings in the MİT technical analysis report that the ByLock application had been downloaded more than 100,000 times from Google Play store and 500,000 to 1 million times from APK download sites (see paragraph 115 above). As noted above, the technical analysis indicated that while it was not possible to verify the accuracy of these figures, they did not appear to be inconsistent with there being 215,092 users on ByLock servers, considering, *inter alia*, the number of people who may have downloaded it on multiple devices or deleted and re-downloaded it (ibid.). It observes moreover from the expert report submitted by the applicant (see paragraph 134 above), which was not refuted by the Government, that the configurations required to establish communication with other users following download, as well as many other technical features relied on to support the exclusivity argument, were not of a nature to limit the use only to a defined group, but were in fact found in many widely available applications, a point that the applicant also raised before the domestic courts (see paragraph 90 above). It further refers to statements from some FETÖ/PDY suspects, cited in the Constitutional Court's *Ferhat Kara* judgment, explaining how they had downloaded ByLock from an application store after hearing about it from "friends in the *cemaat*" and how its use had spread across the *cemaat* at some point (see paragraph 176 above), suggesting that the application may have also been downloaded and used outside a strict organisational hierarchy. It is important to highlight in this regard that while the original test set out in the landmark Court of Cassation judgments indicated that the use of ByLock would constitute proof of connection with the FETÖ/PDY if it was established that a person had "joined the network on the instructions of the organisation" (see paragraph 160 above), neither the Court of Cassation itself, nor the courts in the applicant's specific case, subsequently engaged in a separate assessment to that effect. Nor did they provide any explanation as to why that assessment was not deemed necessary in the circumstances.

340. While it is not the Court's intention to draw any substantive conclusions from these factual assertions, they point to some palpable lacunae in the "exclusivity" and "organisational use" argument, which called for further explanation by the domestic courts as to how it was ascertained that ByLock was not, and could not have been, used by anyone who was not a "member" of the FETÖ/PDY within the meaning of Article 314 § 2 of the Criminal Code (see, for a similar finding, in the context of Article 5 § 1 of the Convention, *Akgün*, cited above, § 173). This is particularly so bearing in mind, once again, the apparently layered structure of the organisation, as noted in paragraph 266 above. The Court notes that the domestic courts,

including the Court of Cassation in their landmark judgments, accepted the findings made primarily by the MİT, in an extrajudicial context, regarding the allegedly exclusive and organisational nature of ByLock and did not thoroughly scrutinise those findings.

341. The Court considers, in the light of the foregoing, that there were not enough safeguards in place to ensure that the applicant had a genuine opportunity to challenge the evidence against him and conduct his defence in an effective manner and on an equal footing with the prosecution (see *Horvatić v. Croatia*, no. 36044/09, § 84, 17 October 2013). Moreover, the domestic courts' failure to respond to the applicant's specific and pertinent requests and objections raised a legitimate doubt that they were impervious to the defence arguments and that the applicant was not truly "heard". In view of the importance of duly reasoned decisions for the proper administration of justice, the domestic courts' silence on vital matters that went to the heart of the case also raised well-founded concerns on the applicant's part regarding their findings and the conduct of the criminal proceedings "as a matter of form" only (see the applicant's argument on paragraph 97 above).

(ii) The remaining evidence

342. Having regard to the above findings, and to the limited significance of the remaining evidence in the case file – namely, the applicant's use of an account at Bank Asya and membership of a trade union and an association, which were merely invoked as circumstantial elements reinforcing the finding that he had been a member of the FETÖ/PDY as demonstrated by his use of ByLock –, the Court considers that it is dispensed from examining further whether the domestic courts carried out a proper examination of the applicant's objections regarding that remaining evidence.

343. Nevertheless, the Court cannot but note the lack of any meaningful discussion in the domestic courts' judgments as to how those acts could be evidence of criminal conduct, even in an ancillary manner. It observes in this regard that, at the time they were undertaken, the acts in question were all seemingly lawful acts that benefited from the presumption of legality (see *Taner Kılıç*, cited above, § 105) and that moreover pertained to the applicant's exercise of his Convention rights, in so far as the membership of a trade union and an association were concerned (see the further discussions within the framework of Article 11 of the Convention in paragraphs 385-397 below). The domestic courts were therefore required to clarify how these acts had reinforced the finding regarding the applicant's membership of an armed terrorist organisation. The Court notes in particular that the explanation provided by the applicant to account for his Bank Asya transactions was never verified or otherwise addressed by the domestic courts.

(d) Preliminary conclusion under Article 6 § 1 of the Convention

344. The Court reiterates that electronic evidence attesting to an individual's use of an encrypted messaging system that was allegedly designed by a terrorist organisation for the purposes of its internal communications may, in principle, be very important in the fight against terrorism or other organised crime (see, for a similar finding, *Akgün*, cited above, § 167). However, while the fight against terrorism may necessitate resorting to such evidence, the right to a fair trial, from which the requirement of the proper administration of justice is to be inferred, applies to all types of criminal offence, from the most straightforward to the most complex. The right to the fair administration of justice holds so prominent a place in a democratic society that it cannot be sacrificed for the sake of expediency (see *Ramanauskas v. Lithuania* [GC], no. 74420/01, § 53, ECHR 2008) and the evidence obtained, whether electronic or not, may not be used by the domestic courts in a manner that undermines the basic tenets of a fair trial.

345. Accordingly, and despite the specific features of the criminal proceedings at issue – both in terms of the context in which they were conducted and the nature and scope of the main evidence at their origin, which entailed a high volume of encrypted electronic data relating to thousands of other individuals –, the domestic courts were required to take adequate measures to ensure the overall fairness of the proceedings against the applicant. As demonstrated above, this they failed to do. In the Court's view, the domestic courts' failure to put in place appropriate safeguards *vis-à-vis* the key piece of evidence at issue to enable the applicant to challenge it effectively, to address the salient issues lying at the core of the case and to provide reasons justifying their decisions was incompatible with the very essence of the applicant's procedural rights under Article 6 § 1. These failings had the effects of undermining the confidence that courts in a democratic society must inspire in the public and of breaching the fairness of the proceedings (see *Ayetullah Ay*, cited above, § 192).

346. In the Court's view, the foregoing considerations are sufficient to lead to the conclusion that the criminal proceedings against the applicant fell short of the requirements of a fair trial in breach of Article 6 § 1 of the Convention.

(e) Considerations under Article 15 of the Convention

347. The Court notes at the outset that the right to a fair trial, as protected by Article 6 of the Convention does not feature among the non-derogable rights listed in Article 15 § 2. It is therefore a derogable right. Thus, the breach of certain procedural safeguards in criminal proceedings which is susceptible of giving rise to a violation of that provision under "normal" circumstances may still be regarded as compatible with that provision in time of war or other public emergency threatening the life of the nation, provided that the

conditions stipulated in Article 15 § 1 are met, that is to say that it was strictly required by the exigencies of the situation and consistent with the State's other obligations under international law.

348. The Court reiterates in this regard that it falls to each Contracting State, with its responsibility for "the life of [its] nation", to determine whether that life is threatened by a "public emergency" and, if so, how far it is necessary to go in attempting to overcome the emergency. By reason of their direct and continuous contact with the pressing needs of the moment, the national authorities are in principle in a better position than the international judge to decide both on the presence of such an emergency and on the nature and scope of derogations necessary to avert it. Accordingly, in this matter a wide margin of appreciation should be left to the national authorities (see *Ireland v. the United Kingdom*, 18 January 1978, § 207, Series A no. 25).

349. Nevertheless, Contracting Parties do not enjoy an unlimited power of appreciation. The Court, which is responsible for ensuring the observance of the States' engagements under Article 19 of the Convention, is empowered to rule on whether the States have gone beyond the "extent strictly required by the exigencies" of the crisis. The domestic margin of appreciation is thus accompanied by European supervision (ibid.). At the same time, in exercising its supervision the Court must give appropriate weight to such relevant factors as the nature of the rights affected by the derogation, the circumstances leading to, and the duration of, the emergency situation (see *Brannigan and McBride v. the United Kingdom*, 26 May 1993, § 43, Series A no. 258-B).

350. The Court considers that its supervision in this framework must be guided primarily by the rule of law, which is one of the fundamental principles of a democratic society that is inherent in all the Articles of the Convention, and which is expressly referred to in the Preamble to the Convention (see *Grzęda v. Poland* [GC], no. 43572/18, § 339, 15 March 2022, with further references). A derogation under Article 15, even if it may be justified by the circumstances surrounding it, does not have the effect of dispensing the States from the obligation to respect the principle of the rule of law and its attendant guarantees. As the Court has previously pointed out, even in the context of a state of emergency, the fundamental principle of the rule of law must prevail (see, for instance, *Pişkin*, cited above, § 153, and *Ahmet Hüsrev Altan*, cited above, § 165; see also the Venice Commission opinion noted in paragraph 202 above). Similarly, a valid derogation under Article 15 does not give the State authorities *carte blanche* to engage in conduct that may lead to arbitrary consequences for individuals. The Court reiterates in this regard that arbitrariness on the part of State authorities entails a negation of the rule of law (see, *mutatis mutandis*, *Al-Dulimi and Montana Management Inc. v. Switzerland* [GC], no. 5809/08, § 145, 21 June 2016) and may not be tolerated, whether in respect of substantive or procedural rights (see for a case to this effect not relating to Article 15 of the Convention, *Muhammad and Muhammad v. Romania* [GC], no. 80982/12, § 118,

15 October 2020). As it has often noted, the rule of law and the avoidance of arbitrary power are principles underlying the Convention and, in the judicial sphere, they serve to foster public confidence in an objective and transparent justice system (see *Taxquet*, cited above, § 90). Accordingly, when determining whether a derogating measure that encroaches upon the right to a fair trial was fully justified in that it was strictly required by the exigencies of the situation, the Court must also examine whether adequate safeguards were provided against abuse and whether the measure undermined the rule of law.

351. The Court further reiterates that Article 6 should not be applied in such a manner as to put disproportionate difficulties in the way of the authorities in taking effective measures to counter terrorism or other serious crimes in discharge of their duty to protect the right to life and the right to bodily security of members of the public (see *Ibrahim and Others v. the United Kingdom* [GC], nos. 50541/08 and 3 others, § 252, 13 September 2016). It refers, in this regard, to its considerations under Article 7 concerning the difficulties faced by the States in their struggle against terrorism in view of the dynamic nature of this threat and, more specifically, the serious predicament faced by Türkiye as a result of the attempted coup and the allegedly unorthodox nature of and methods employed by the FETÖ/PDY. The Court is also mindful of the heavy burden faced by the judicial authorities in Türkiye in the aftermath of the coup attempt. It refers in this connection to the findings of the Constitutional Court, in the case of *Aydın Yavuz and Others* in the context of the right to liberty and security, that the judicial and investigating authorities had had to handle an unforeseeably heavy workload, given that they had suddenly been required to initiate and conduct investigations in respect of tens of thousands of suspects because of the unexpected situation brought about by the coup attempt. Furthermore, thousands of judges and prosecutors had been dismissed from office for alleged connections with that organisation, some of whom have applications pending before the Court (see *Baş*, cited above, §§ 92 and 93).

352. Turning to the specific facts of the present case, the Government invited the Court to examine the applicant's complaints under Article 6 with due regard to the derogation notification and referred, in a general manner, to all the legislative decrees enacted during the state of emergency. However, when it came to substantiating their arguments regarding the fair trial issues raised by the applicant in relation to the ByLock evidence, they did not in any way claim that those issues resulted, even indirectly, from the specific measures adopted by the aforementioned legislative decrees (compare *Pişkin*, cited above, §§ 121-25 and 153).

353. The Government did however submit that the reliance of the domestic courts in the applicant's case on the Court of Cassation's landmark judgments as regards the "exclusivity" argument, without engaging in a fresh examination of this matter themselves, was consistent with the exigencies of

the state of emergency and strictly required within the meaning of Article 15 of the Convention, given the constraints under which the judiciary was operating at the material time (see paragraph 297 above). The Court notes, however, that the problem it has identified under Article 6 § 1 was not the fact that the domestic courts relied on the precedent created by the landmark judgments of the Court of Cassation when examining the applicant's case. It was rather that the applicant was deprived of adequate means to challenge those findings, the importance of which the Government also acknowledged in their relevant submissions (ibid.). In this regard, neither the Government nor the domestic courts – including the Court of Cassation in its landmark judgments – claimed that any specific measures had been taken, or been required, at the relevant period to restrict the rights of the defence in that respect. What is more, there is no indication in the landmark judgments of the Court of Cassation that the "exclusivity" argument at issue had been developed by reason of the special circumstances of the state of emergency.

354. The Court observes in this connection that none of the domestic courts involved in the applicant's case examined the fair trial issues relating to the ByLock evidence from the standpoint of Article 15 of the Convention or Article 15 of the Turkish Constitution, which similarly regulates derogations in times of emergency (see paragraph 141 above), or mentioned, even as a contextual factor framing their approach to those issues, the threats or difficulties giving rise to the state of emergency. The Government did not claim otherwise. Nor did they submit any other judicial rulings delivered at the relevant period in which the domestic courts had in fact engaged in an assessment of the implications of the state of emergency and the derogation for the fair trial issues examined in the present case, similar to the judgments in which the Constitutional Court had closely examined those matters in the context of the right to liberty and security (see paragraph 351 above, as well as *Baş*, cited above, §§ 92 and 93) and the right to legal assistance (see paragraph 209 above). The Court further notes the Government's statement made as part of their submissions under Article 6 § 3 (c) of the Convention that "the state of emergency had not been determinative in the decisions of the judicial authorities, and that judicial activities were carried out by [their] own principles and rules", as evidenced by the fact that the applicant had been released from detention by the first-instance court on 21 March 2017 – that is, while the state of emergency was still in effect (see paragraph 209 above). The Court acknowledges the limited significance of this statement for the purposes of the present examination, given the specific context in which it was made and the fact that the Article 6 § 3 (c) complaint will not be examined in the present judgment for the reasons indicated below (see paragraphs 366-367). It nevertheless considers this statement to be consistent with the Government's observations regarding the fair trial issues raised by the applicant in relation to the ByLock evidence that the criminal proceedings had been conducted by the domestic courts in a manner that duly observed

the applicant's procedural rights (see the Government's observations in paragraphs 289-299 above and, in particular, paragraph 289).

355. The Court is mindful that it is not its role to substitute its view as to what measures were most appropriate or expedient in dealing with an emergency situation for that of the State authorities, which have direct responsibility for establishing the balance between effectively combatting terrorism on the one hand and respecting individual rights on the other (see *Brannigan and McBride*, cited above, § 59). It further accepts that the difficulties facing Türkiye in the aftermath of the attempted military coup of 15 July 2016 are undoubtedly a contextual factor which must be taken into account. The Court also notes, however, that in contrast to their submissions in relation to Article 6 § 3 (c) of the Convention (see paragraph 209 above), the Government have not adduced any detailed reasons before it as to whether the specific fair trial issues identified above originated in the special measures taken during the state of emergency and, if so, why they were necessary to avert it or whether they were a genuine and proportionate response to the emergency situation (see *A. and Others v. the United Kingdom* [GC], no. 3455/05, § 184, ECHR 2009, and *Alparslan Altan*, cited above, §§ 116-18). In these circumstances, the Court considers that the limitations on the applicant's fair trial rights at issue – which, as indicated in paragraph 345 above, were incompatible with the very essence of his procedural rights under Article 6 § 1 and had the effect of undermining the confidence that courts in a democratic society must inspire in the public – cannot be treated as having been strictly required by the exigencies of the situation. A finding to the contrary in such circumstances would negate the safeguards provided by Article 6 § 1 of the Convention, which must always be construed in the light of the rule of law (see *Nicolae Virgiliu Tănase v. Romania* [GC], no. 41720/13, § 192, 25 June 2019).

(f) Conclusion

356. The Court concludes, in view of the above considerations, that there has been a violation of Article 6 § 1 of the Convention on the facts of the present case.

IV. OTHER ALLEGED VIOLATIONS OF ARTICLE 6 OF THE CONVENTION

357. The applicant further complained under Article 6 § 1 of the Convention that he had not been tried by independent and impartial tribunals, mainly on account of various legislative and factual developments in recent years that allegedly undermined the principle of the irremovability of judges.

358. He also claimed under Article 6 § 3 (c) of the Convention that he had been denied the right to effective legal assistance, having regard to the

restrictions imposed by Article 6, paragraph 1 (d) of Legislative Decree no. 667 on his communication with his lawyer in private.

A. Allegations under Article 6 § 1 concerning the independence and impartiality of the domestic courts

359. The applicant argued under Article 6 § 1 of the Convention that the courts that had tried him were not independent and impartial, alleging in particular that the principle of irremovability of judges had been eroded on account of certain legislative and factual developments that had taken place particularly in the aftermath of the coup attempt. He claimed more specifically that following the entry into force of Law no. 6723 on 23 July 2016 (see paragraph 150 above), all of the members of the Court of Cassation had been replaced before their terms had come to an end, which had tainted the independence and impartiality of that instance. Moreover, by virtue of Article 3 of Legislative Decree no. 667 (see paragraph 151 above), judges or prosecutors who were considered to "belong to, be affiliated with or linked to" terrorist organisations or other organisations considered by the National Security Council to be engaging in activities prejudicial to national security could be dismissed from office. Accordingly, some 3,000 judges and public prosecutors had been dismissed shortly after the coup attempt and arrested, and a great number of judges transferred to different posts or suspended from office on account of the judgments that they had delivered that were favourable to the FETÖ/PDY, including as regards the ByLock evidence. The applicant claimed that the High Council of Judges and Prosecutors, which issued the relevant decisions on transfers and suspensions, lacked structural independence and impartiality, as pointed out by many international bodies.

360. The Government submitted that the applicant's complaints regarding the independence and impartiality of the domestic judicial organs had not been duly raised before the domestic courts, that they did not relate to his case and were moreover abstract and speculative, particularly as regards the allegations of transfers and suspensions of judges on account of their judicial activities. The Government specified that appointments, transfers and all other administrative matters concerning judges and prosecutors were under the responsibility of the High Council of Judges and Prosecutors, an independent body with constitutional status. They moreover stressed that the change in the membership of the Court of Cassation pointed out by the applicant had been enacted prior to the coup attempt as part of an overhaul of the Turkish judiciary from a two-tier to a three-tier system, and that the salaries and other rights of the judges concerned had remained protected under the Constitution, which safeguarded the independence and impartiality of the judiciary and their security of tenure. As regards the measures introduced by Article 3 of Legislative Decree no. 667, the Government

contended that in no democratic State could a judge who was found to have links with a terrorist organisation be permitted to exercise that profession. Besides, the dismissal decisions were subject to judicial review.

361. The ICJ argued in their third-party submissions that the independence of the Turkish judiciary, which had already been under threat for some time, had further deteriorated after the attempted coup, particularly in view of the mass dismissals of the members of the judiciary in an arbitrary fashion, and of the structural changes made to the High Council of Judges and Prosecutors as part of the April 2017 constitutional reform.

362. The Court notes at the outset that, contrary to the Government's argument, the applicant did in fact make his claims regarding the independence and impartiality of the Turkish judiciary before the Court of Cassation and the Constitutional Court (see paragraphs 96 and 103 above).

363. It further notes the legislative changes introduced in Türkiye in recent years with respect to the organisation of the judiciary (see paragraphs 150-153 above), as well as the findings made by various international bodies regarding the perceived erosion of the independence of the Turkish judiciary and the concerns over undue interference by the executive (see, for instance, the opinions and reports noted in *Selahattin Demirtaş v. Turkey (no. 2)* [GC], no. 14305/17, § 434, 22 December 2020, and *Baş*, cited above, §§ 252-54 and 277). It stresses, however, that it is not called upon to make general findings about the Turkish judicial system in the abstract or to rule on the permissible limits of relations and interaction between the various State powers, but to determine, on the facts of the specific case before it, whether the requirements of the right to a fair trial have been met (see, *mutatis mutandis*, *Kleyn and Others v. the Netherlands* [GC], nos. 39343/98 and 3 others, § 193, ECHR 2003-VI; *Thiam v. France*, no. 80018/12, § 62, 18 October 2018; and *Baş*, cited above, § 277).

364. It observes in this regard that the arguments advanced by the applicant in the present case entail a criticism of the judiciary in a general manner (see paragraph 359 above for the applicant's arguments in this regard), without any specific allegations, either during the domestic proceedings or before the Court, relating to the judges who participated in the examination of his case and producing concrete consequences in his individual trial. The Court considers that the more immediate issue that lies at the heart of the present case is rather the uniform and global approach adopted by the Turkish judiciary *vis-à-vis* the ByLock evidence in convictions for membership of the FETÖ/PDY, which has led to findings of violations of Articles 7 and 6 § 1 of the Convention.

365. Accordingly, the Court considers that the complaints under this head do not require a separate examination as to their admissibility and merits.

B. Allegations under Article 6 § 3 (c) concerning the right to effective legal assistance

366. As regards the applicant's allegation under Article 6 § 3 (c) that he had not been able to communicate with his lawyer in private by reason of the restrictions imposed by Article 6 § 1 (d) of Legislative Decree no. 667 (see paragraph 154 above), the Court refers to its well-established case-law on the inter-relationship between this provision and the broader fair trial guarantee under Article 6 § 1. In its evaluation of the overall fairness of criminal proceedings, the Court may take account, as appropriate, of the extent to which the minimum rights listed in Article 6 § 3, which represent specific aspects of the concept of a fair trial, were respected. However, these specific procedural rights are not aims in themselves: their intrinsic aim is always to contribute to ensuring the fairness of the criminal proceedings as a whole (see, *mutatis mutandis*, *Ibrahim and Others*, cited above, §§ 250 and 251, with further references, and *Correia de Matos v. Portugal* [GC], no. 56402/12, § 120, 4 April 2018).

367. The Court considers that the Article 6 complaint in this case primarily and fundamentally concerns the lack of fairness, as established above (see paragraph 356 above), of the proceedings leading to the applicant's conviction of a serious criminal offence carrying a heavy sentence. Against this background, the Court does not consider it necessary to address separately the admissibility and merits of the complaint under this head (see *Navalnyy and Ofitserov*, cited above, §§ 120 and 121).

V. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

368. The applicant complained under Article 8 of the Convention that (i) the ByLock data in his regard had been collected and used by the MİT without a court order and in breach of the relevant legal framework, and (ii) his Internet traffic data (CGNAT) had been obtained by the BTK outside the statutory time-limit.

369. The Government claimed, *inter alia*, that the applicant's complaints under this head did not as such involve an allegation of interference with his private life due to the obtaining and processing of the relevant ByLock and Internet traffic data, but rather related to the fact that the said data had been used as evidence to convict him. They therefore contended that the complaint under this head needed to be examined from the standpoint of Article 6 of the Convention. Moreover, to the extent that the applicant had complained of the retention of the Internet traffic data outside the maximum time-limit, the Government reiterated that the relevant time-limit concerned only the Internet service providers. In any event, it would have been possible for the applicant to bring an administrative action against the State authorities that he held responsible for the allegedly unlawful retention, which he had failed to do.

370. In his observations submitted with respect to the first limb of his Article 8 complaints, the applicant stated, *inter alia*, that "[t]he genuine problem in this case is not the acquisition of the alleged ByLock data by an intelligence service and its repercussion to the right to respect for private life, but the obtainment by an intelligence service of data in disregard of guarantees provided for under the criminal procedure, and then the use of this data as evidence for the sole ground of [his] conviction."

371. The Court notes from the applicant's observations that at the heart of his complaints presented under Article 8 of the Convention lies his conviction on the basis of the ByLock and Internet traffic data that were allegedly obtained unlawfully, rather than the interference with his private life occasioned by reason of such unlawful action. It further observes that the Government were also of the same opinion.

372. The fact that the Article 8 aspect was regarded as a peripheral issue by the applicant himself is also evident from the scope of his arguments made both before domestic courts and the Court, which concentrated on the fairness of his conviction on the basis of the evidence at issue. Private life considerations – whether in relation to the ByLock or the Internet traffic data – were largely invoked only to the extent that they related to the use of the relevant evidence in the criminal proceedings.

373. Having regard to the foregoing, and to the fact that the main issues raised by the applicant under Article 8 as regards his conviction on the basis of unlawfully obtained evidence have been addressed under Article 6 § 1, the Court considers that there is no need to give a separate ruling on the admissibility and merits of these complaints from the standpoint of Article 8 in the specific circumstances of the instant case.

VI. ALLEGED VIOLATION OF ARTICLE 11 OF THE CONVENTION

374. The applicant complained that there had been a breach of Article 11 of the Convention in so far as the domestic courts had relied in their decision to convict him on his membership of a lawfully established trade union (Aktif Eğitim-Sen) and an association (Kayseri Voluntary Educators Association), which was no more than the exercise of his fundamental rights protected by that provision. Article 11 of the Convention reads as follows:

> "1. Everyone has the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.
>
> 2. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, 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. This Article shall not prevent the imposition of lawful restrictions on the exercise of these rights by members of the armed forces, of the police or of the administration of the State."

A. Admissibility

375. This complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) Submissions of the applicant

376. The applicant submitted at the outset that the judicial bodies' decision to convict him of a terrorism offence and to sentence him to six years and three months' imprisonment, on the grounds, *inter alia*, of his membership of a trade union and an association had constituted a direct, clear, and severe interference with his rights guaranteed under Article 11 of the Convention. In that regard, the applicant asserted that, contrary to the Government's allegation, the trial court had not accorded any special weight to the individual pieces of evidence that formed the basis of its decision to convict him. Moreover, even the Government themselves had not denied that his membership of the impugned trade union and association directly related to his exercise of fundamental rights under both domestic and international law. Accordingly, the Government's argument that there had been no interference was untenable.

377. As regards the question whether the interference was justified, the applicant pointed out, firstly, that the Government did not contest that both the trade union and the association in question had been established and had operated in accordance with the laws of Türkiye. Indeed, Aktif Eğitim-Sen had been a trade union representing public servants in the field of education. Kayseri Voluntary Educators Association had been dedicated to providing "voluntary educational services" to children. In this context, the applicant had given free chess courses to children. Furthermore, the applicant stated that by becoming a member of the trade union and association, he had not shown any intent or motive to commit a terrorist offence. More importantly, the trial court had not mentioned or even implied that he had undertaken or taken part in any illegal activity. Nor had the trade union or the association at issue ever been involved in any such activity. There was therefore no rational link between his memberships of these bodies and the terrorism offence of which he had been convicted.

378. In view of the foregoing considerations, the applicant took the view that the trial court's interpretation of Article 314 § 2 of the Criminal Code – under which he had been found guilty – was so vague and arbitrary that the interference with his rights under Article 11 of the Convention had not been prescribed by law.

379. Lastly, the applicant stated that the facts of the present case were entirely different from those of *Ayoub and Others v. France* (nos. 77400/14 and 2 others, 8 October 2020), on which the Government relied, and he asked the Court to dismiss that argument.

(b) Submissions of the Government

380. Referring to their submissions concerning the ByLock application under Articles 6 and 7 of the Convention, the Government contended that there had been no interference with the applicant's rights under Article 11 because the decisive evidence relied on for his conviction had been his use of ByLock. Moreover, the trial court had taken into account the fact that the applicant had deposited money with Bank Asya upon the instructions of the ringleader of the FETÖ/PDY along with the fact that he had been a member of a trade union and an association which had been shut down by Legislative Decree no. 667 in the context of the measures taken during the state of emergency. Considering that the trade union and the association in question had the purpose of carrying out the FETÖ/PDY's organisational activities under a legal appearance, the judicial bodies had merely relied on the applicant's membership thereof as corroborative evidence. Therefore, when taken as a whole, the elements of evidence relied on by the trial court for the applicant's conviction had not contradicted each other; on the contrary, they had complemented and confirmed one another. That being the case, the trial court had established that the material and mental elements of the offence of which the applicant had been convicted had been made out. Accordingly, the applicant had not been punished for simply being a member of an association or a trade union, nor had he faced any obstruction in the enjoyment of his right to respect for his freedom of assembly and association.

381. If the Court were to consider that there had been an interference with the applicant's rights under Article 11 of the Convention, the Government took the view that the interference had been prescribed by law, namely Article 314 § 2 of the Criminal Code and the case-law of the Court of Cassation. In that regard, the Government submitted that the well-established case-law of the Court of Cassation demonstrated that membership of a trade union or an association would not, without more, be sufficient to convict a person of being a member of an armed terrorist organisation, provided that the acts committed by the accused did not meet the continuity, diversity and intensity criteria or otherwise indicate his or her involvement in the hierarchical structure of the armed terrorist organisation. However, the case-law of the Court of Cassation demonstrated that it was appropriate to convict an individual who had used ByLock, had deposited money with Bank Asya in accordance with the instructions of the FETÖ/PDY and who had been a member of a trade union that had been considered to be affiliated with the FETÖ/PDY.

382. As regards the purpose of the alleged interference, the Government argued that this had been the protection of national security and public safety and the prevention of disorder or crime, given that the FETÖ/PDY – of which the applicant had been found to have been a member – had attempted to overthrow the Republic of Türkiye. The Government further stressed that any interference had been necessary in a democratic society, arguing that the trial court had approached the applicant's membership of the trade union and the association in question with caution, and had taken them into account only as "corroborative" or "complementary" evidence.

383. The Government further argued that in many different parts of the world, criminal organisations pursued illegal activities under the cloak of legal structures which exploited the advantages offered by democracy and human rights. In that regard, the Government referred to the Court's judgment in *Ayoub and Others* (cited above) in support of their contention that some such organisations had also been identified in the Court's case-law. They submitted that there was no reason for the Court to depart from this line of case-law in view of the activities performed by the FETÖ/PDY and of its purpose, namely to abolish the constitutional order.

2. The Court's assessment

384. The Court has found under Article 7 of the Convention that the applicant's conviction for membership of an armed terrorist organisation, which was based to a decisive extent on his alleged use of the ByLock application, contravened the requirements of that provision as it effectively imputed objective liability to the users of ByLock through an expansive and unforeseeable interpretation of the domestic law. In making this finding, the Court noted – on the basis of the relevant domestic judgments and the submissions of the Government (see paragraphs 87, 88, 160, 165, 181, 188, 232 and 233 above) – that the remaining acts attributed to the applicant, including his membership of a trade union and an association, served only as a source of corroboration and had very limited bearing on the outcome (see paragraphs 257, 262 and 268; see also the Government's submissions in this regard within the framework of Article 11 of the Convention in paragraphs 380 and 381 above). Nevertheless, since these memberships represented the exercise by the applicant of his right to freedom of association, which is protected by Article 11 of the Convention, the fact that this was used, even to the limited extent described above, to convict him warrants examination of this complaint by the Court.

(a) Whether there has been an interference

385. The right to freedom of association laid down in Article 11 incorporates the right to form an association. The ability to establish a legal entity in order to act collectively in a field of mutual interest is one of the

most important aspects of freedom of association, without which that right would be deprived of any meaning (see *Gorzelik and Others v. Poland* [GC], no. 44158/98, § 88, ECHR 2004-I, and *Sidiropoulos and Others v. Greece,* 10 July 1998, § 40, Reports of Judgments and Decisions 1998-IV).

386. Indeed, the state of democracy in the country concerned can be gauged by the way in which this freedom is secured under national legislation and in which the authorities apply it in practice (see *Gorzelik and Others*, cited above, § 88). In its case-law, the Court has on numerous occasions affirmed the direct relationship between democracy, pluralism and the freedom of association and has established the principle that only convincing and compelling reasons can justify restrictions on that freedom. All such restrictions are subject to a rigorous supervision by the Court (ibid.).

387. The Court notes that in cases where there are no objective grounds capable of establishing the constituent elements of the offence of being a member of an armed terrorist organisation, such as in the instant case, the use by domestic courts of statements or acts that were manifestly non-violent – and that should in principle be protected by the Convention – in determining criminal liability may entail an interference with the rights concerned. The corroborative or complementary nature of the use made of these statements or acts in the criminal proceedings does not detract from that conclusion. In the present case, the judicial authorities' reliance in the bill of indictment and in the judgments on the applicant's membership of Aktif Eğitim-Sen and the Kayseri Voluntary Educators Association, even if only in an ancillary manner, was sufficient to constitute an interference with his rights under Article 11 of the Convention.

(b) Whether the interference was justified

388. According to the Court's settled case-law the expressions "prescribed by law" and "in accordance with the law" in Articles 8 to 11 of the Convention not only require that the impugned measure should have some basis in domestic law, but that it should also be compatible with the rule of law, which, as indicated above, is inherent in all its Articles (see paragraph 350 above; see also *Maestri v. Italy* [GC], no. 39748/98, § 30, ECHR 2004-I). For the general principles with regard to the question whether an interference with the rights protected by those Articles was prescribed by law, the Court refers to its judgment in *Selahattin Demirtaş* (cited above, §§ 249-54).

389. In the present case, the Government argued that the purported interference had been prescribed by law, namely Article 314 § 2 of the Criminal Code as interpreted by the Court of Cassation. While the applicant did not contest that the interference had a basis in domestic law, he contended that the interpretation and application of the relevant provision on the present facts had fallen short of the requirement of lawfulness under Article 11 § 2 of the Convention. What is at stake in the present case is, therefore, the "quality"

of the law in question, in particular, whether it was foreseeable as to its effects (see, for instance, *Kudrevičius and Others v. Lithuania* [GC], no. 37553/05, § 108, ECHR 2015) and complied with the rule of law criterion under the second paragraph of Article 11 of the Convention.

390. It is common ground that the trade union and the association in question were established and were operating lawfully prior to their dissolution by Legislative Decree no. 667 after the attempted *coup d'état* on the ground that they posed a national security threat on account of their affiliation with the FETÖ/PDY. The Court considers that acts which appear on their face to come within the scope of Article 11 of the Convention and which do not incite violence or otherwise reject the foundations of a democratic society should benefit from a presumption of legality (compare, for a similar assessment made in the context of Article 5 of the Convention, *Taner Kılıç*, cited above, § 105). That being said, it is open to the domestic authorities to rebut this presumption in a given case. It should thus be ascertained whether the domestic authorities did so in the present case.

391. In that regard, the Court notes that there is no explanation in the trial court's judgment in respect of the nature of the actions of the trade union and the association in question which brought about their dissolution by Legislative Decree no. 667. The trial court's assessment on that point was limited to observing that they had been shut down pursuant to the said Legislative Decree on account of their affiliation with the FETÖ/PDY (see, for a similar finding, *Adana TAYAD v. Turkey*, no. 59835/10, §§ 33-34, 21 July 2020). Nor did the trial court's judgment contain any explanation as to whether the applicant had undertaken any acts within those structures, and, if so, what the nature of such acts was (see, for a similar situation in the context of a detention order under Article 5 of the Convention, *Atilla Taş v. Turkey*, no. 72/17, § 129, 19 January 2021). Moreover, the Ankara Regional Court of Appeal upheld the trial court's judgment, including as regards the evidence relied on, without shedding further light on these matters. Lastly, in their submissions before the Court, the Government did not submit any other domestic court judgment which offered further explanation in respect of these matters, but simply submitted that the trade union and the association in question had acted in accordance with the objectives of the FETÖ/PDY.

392. Accordingly, it appears that at no point during the criminal proceedings against the applicant did the domestic courts assess whether he had, in the context of his membership of Aktif Eğitim-Sen and Kayseri Voluntary Educators Association, engaged in any action which could be interpreted as inciting violence or otherwise rejecting the foundations of a democratic society. In that regard, it should further be noted that the Government did not put forward any specific evidence to rebut the presumption of legality (described above) in respect of the applicant's memberships of the trade union and association (see *Atilla Taş*, cited above,

§ 134). The Court considers that where no such elements are forthcoming, the mere fact of being a member of the trade union and the association in question, even when used only to corroborate the applicant's membership of an armed terrorist organisation, is not sufficient to rebut the presumption of legality.

393. At this juncture, the Court reiterates that in *Selahattin Demirtaş* (cited above), where that applicant's pre-trial detention in connection with serious offences punishable under Article 314 of the Criminal Code was based on his political statements and his involvement in a lawful organisation, it held that the range of acts that may have justified the applicant's detention was so broad that the content of that Article, coupled with its interpretation by the domestic courts, did not offer adequate protection against arbitrary interference by the national authorities (see also paragraph 201 above for the Venice Commission's opinion in that regard). The Court took the view that such a broad interpretation of a provision of criminal law could not be justified where it entailed equating the exercise of the right to freedom of expression with belonging to, forming or leading an armed terrorist organisation, in the absence of any concrete evidence of such a link (see *Selahattin Demirtaş*, cited above, §§ 277-80).

394. The question therefore arises whether the conclusions in the *Selahattin Demirtaş* judgment may be transposed to the instant case in the context of Article 11 of the Convention. In order to answer that question, careful consideration should be given to the factual circumstances of the two cases with a view to ascertaining whether they are such as to be regarded as sufficiently comparable to each other. The Court acknowledges that in *Selahattin Demirtaş*, the evidence underlying that applicant's detention and prosecution consisted solely of his speeches or acts that came within the exercise of his freedom of expression under Article 10 of the Convention. In the present case, the acts that enjoyed the protection of Article 11 were only relied on by the domestic courts as corroborating factors for the applicant's conviction. However, this is a difference in degree only, and the fact remains that the scope of Article 314 of the Criminal Code was extended unforeseeably to include membership of a trade union and an association – which were both operating lawfully at the material time – as indications of criminal conduct, without concrete elements which would fulfil the continuity, diversity and intensity criteria required in case-law interpreting that provision and demonstrating membership of an armed terrorist organisation. Accordingly, this factual difference does not seem sufficient to distinguish the present case from that of *Selahattin Demirtaş*.

395. Lastly, as regards the Government's argument that the present complaint should be rejected on the basis of *Ayoub and Others* (cited above), the Court considers that that case was materially different from the instant case, concerning the dissolution of three paramilitary-type far-right associations. The dissolution of the first of those associations had been based

not on expressions of political views, but on, *inter alia*, an act of violence, namely the killing of an individual, whereas the second and third associations had been dissolved on the grounds that the objectives actually promoted and put into practice by their members, including on various occasions by violent means, had indisputably contained elements of incitement to hatred and racial discrimination aimed in particular at Muslim immigrants, Jews and homosexuals. Having regard to the considerable differences between the facts of the two cases, the Government's argument that the Court should adopt the same stance here as in *Ayoub and Others* (cited above) must be rejected.

396. In view of the foregoing considerations, the Court finds that the manner in which Article 314 § 2 of the Criminal Code was interpreted in the present case in relation to the applicant's membership of Aktif Eğitim-Sen and Kayseri Voluntary Educators Association extended the scope of that provision in an unforeseeable manner, did not afford the requisite minimum protection against arbitrary interference and cannot therefore be regarded as being "prescribed by law" as required by Article 11 § 2 of the Convention.

397. In view of the above finding, it is unnecessary to examine whether the interference pursued one or more of the legitimate aims listed in paragraph 2 of Article 11 and was "necessary in a democratic society".

(c) Considerations under Article 15 of the Convention

398. In assessing the applicant's complaints under Article 6 from the standpoint of Article 15 of the Convention, the Court has already stressed that the need to ensure compliance with the principle of rule of law is indispensable at all times and that no derogation from it would be possible even in situations of emergency (see paragraph 350 above). Given that the rule of law is the principle underlying the Convention and all its provisions (see *Grzęda*, cited above, § 341), these considerations also hold true in respect of Article 11. Accordingly, when determining whether a derogating measure that encroaches upon the right to freedom of assembly and association was fully justified by the special circumstances of the emergency and was strictly required by the exigencies of the situation, the Court must also examine whether safeguards against arbitrary interferences by public authorities with the rights guaranteed by the Convention were provided and whether the measure undermined the rule of law.

399. The Government's request that the complaint under Article 11 be examined with due regard to the derogation notified on 21 July 2016 was based on the argument that the trade union and the association in question had been shut down by Legislative Decree no. 667 in the context of the measures taken during the state of emergency. The Court notes, however, that the breach of Article 11 at issue in the present case does not result from the shutting down of the relevant trade union and association, but from the fact that the applicant's membership of that trade union and association was used as corroborating evidence in securing his conviction for membership of an

armed terrorist organisation. Be that as it may, the Government did not advance any explanations as to whether the specific use made by the domestic courts of the applicant's membership of the trade union and association in question had been strictly required by the exigencies of the situation giving rise to the state of emergency in Türkiye. Nor did they point to any domestic judgments where such assessment had been undertaken, in the context of the applicant's case or elsewhere.

400. The finding that the reliance placed on those acts breached the requirement of lawfulness on account of its unforeseeability meant that the domestic courts overly extended the scope of Article 314 § 2 of the Criminal Code, thereby depriving the applicant of the minimum protection against arbitrary interference, which protection is fundamental to safeguarding the rule of law (see paragraph 350 above, as relevant).

401. In view of the above, the Court holds that the Government have failed to demonstrate that the interference with the applicant's rights protected under Article 11 of the Convention could be regarded as being strictly required by the exigencies of the situation under Article 15.

(d) Conclusion

402. In view of the foregoing considerations, the Court holds that there has been a violation of Article 11 of the Convention on the facts of the present case.

VII. APPLICATION OF ARTICLES 41 AND 46 OF THE CONVENTION

A. Article 46 of the Convention

403. Article 46 of the Convention provides as follows:

> "1. The High Contracting Parties undertake to abide by the final judgment of the Court in any case to which they are parties.
>
> 2. The final judgment of the Court shall be transmitted to the Committee of Ministers, which shall supervise its execution."

1. General principles

404. In the context of the execution of judgments in accordance with Article 46 of the Convention, a judgment in which the Court finds a breach of the Convention imposes on the respondent State a legal obligation to put an end to the breach found and make reparation for its consequences in such a way as to restore as far as possible the situation existing before the breach (see, among many authorities, *Kurić and Others v. Slovenia* (just satisfaction) [GC], no. 26828/06, § 79, ECHR 2014). The Court's judgments are, however, essentially declaratory in nature. Accordingly, the Contracting States that are parties to a case are in principle free to choose, subject to supervision by the

Committee of Ministers, the means whereby they will comply with a judgment in which the Court has found a breach – including any general and/or, if appropriate, individual measures to be adopted in their domestic legal order –, provided that the execution is carried out in good faith and in a manner compatible with the "conclusions and spirit" of the judgment (see, for instance, *Ilgar Mammadov v. Azerbaijan* (infringement proceedings) [GC], no. 15172/13, § 149, 29 May 2019).

405. That being said, in certain special circumstances the Court has found it useful to indicate to a respondent State the type of measures that might be taken to put an end to the situation – often a systemic one – which has given rise to the finding of a violation. Even in such cases, however, it is the Committee of Ministers that has the exclusive competence to evaluate the implementation of such measures under Article 46 § 2 of the Convention (see *Ilgar Mammadov* (infringement proceedings), cited above, §§ 153-55, and *Kavala* (infringement proceedings), cited above, § 134).

406. With regard in particular to the reopening of proceedings, the Court has clearly stated that it does not have jurisdiction to order such measures (see, among other authorities, *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland (no. 2)* [GC], no. 32772/02, § 89, ECHR 2009, and *Moreira Ferreira*, cited above, § 48). However, where an individual has been convicted following proceedings that have entailed breaches of the requirements of Article 6 of the Convention, the Court may indicate that a retrial or the reopening of the case, if requested, represents in principle an appropriate way of redressing the violation, and often the most appropriate one (see, respectively, *Verein gegen Tierfabriken Schweiz (VgT)*, cited above, § 89, and *Moreira Ferreira*, cited above, §§ 49 and 52). This is in keeping with the guidelines of the Committee of Ministers, which in Recommendation No. R (2000) 2 called on the Contracting Parties to the Convention to introduce mechanisms for re-examining the case and reopening the proceedings at domestic level, finding that in exceptional circumstances such measures represented "the most efficient, if not the only, means of achieving *restitutio in integrum*" (see *Verein gegen Tierfabriken Schweiz (VgT)*, cited above, §§ 33 and 89).

407. The Court confirms that the foregoing principles relating to the reopening of criminal proceedings are also relevant in situations in which it has found a violation of Article 7 of the Convention (see, for instance, *Dragotoniu and Militaru-Pidhorni*, cited above, § 55, and *Sinan Çetinkaya and Ağyar Çetinkaya v. Turkey*, no. 74536/10, § 49, 24 May 2022).

408. Lastly, the Court's rulings serve not only to decide those cases brought before it but, more generally, to elucidate, safeguard and develop the rules instituted by the Convention, thereby contributing to the observance by the States of the engagements undertaken by them as Contracting Parties (see, for instance, *Jeronovičs v. Latvia* [GC], no. 44898/10, § 109, 5 July 2016).

2. Application of the general principles to the case

(a) Individual measures to be taken in respect of the present applicant

409. The findings of violation made in the present case, particularly those under Articles 7 and 6 of the Convention, entail an obligation on the respondent State to take appropriate measures to remedy these infringements of the applicant's rights.

410. As acknowledged in its case-law, there is a wide range of remedies in Europe enabling individuals to apply, following a finding by the Court of a violation of the Convention, for the reopening of a criminal case which has been concluded by a final judgment; however, there is no uniform approach among the Contracting States as regards the right to apply for reopening (see *Moreira Ferreira*, cited above, § 53).

411. Under Turkish law, domestic legislation explicitly provides for such a right under Article 311 § 1 (f) of the CCP, which stipulates, as relevant, that the reopening may be requested within one year following a final judgment of the Court finding a violation of the Convention or Protocols thereto. The Court has therefore often made reference to the possibility of reopening criminal proceedings in cases against Türkiye where an individual was found to have been convicted following proceedings that had entailed breaches of the requirements of Articles 6 or 7 of the Convention (see, for instance, *Balta and Demir v. Turkey*, no. 48628/12, § 70, 23 June 2015; *Fikret Karahan v. Turkey*, no. 53848/07, § 64, 16 March 2021; *Faysal Pamuk v. Turkey*, no. 430/13, § 79, 18 January 2022; and *Sinan Çetinkaya and Ağyar Çetinkaya*, cited above, § 49).

412. In the light of the principles set out above, and without prejudice to any general measures that may be required to prevent or redress other similar violations (see paragraph 418 below), the reopening of the criminal proceedings, if requested, would be the most appropriate way of putting an end to the violations found in the present case and of affording redress to the applicant. As indicated in the case of *Sejdovic v. Italy* ([GC], no. 56581/00, § 127, ECHR 2006-II), it is not for the Court to indicate how any new trial is to proceed and what form it is to take, the choice of means to discharge their legal obligations remaining at the discretion of the Government, provided that such means are compatible with the conclusions and spirit of the Court's judgment.

(b) Measures to be taken in respect of similar cases

413. The Court observes that in the present case, the violations under Articles 7 and 6 of the Convention resulted notably from the domestic courts' characterisation of the use of ByLock. Under this approach, anyone whose use of that application was or is established by the domestic courts could, in principle, be convicted on that sole basis of membership of an armed terrorist organisation pursuant to Article 314 § 2 of the Criminal Code.

414. The Court therefore considers that the situation that led to a finding of violations of Articles 7 and 6 of the Convention in the present case was not prompted by an isolated incident or attributable to the particular turn of events, but may be regarded as having stemmed from a systemic problem. This problem has affected – and remains capable of affecting – a great number of persons (see, *mutatis mutandis*, *Broniowski v. Poland* [GC], no. 31443/96, § 189, ECHR 2004-V). This is evidenced by the fact that there are currently over 8,000 applications in the Court's docket involving similar complaints raised under Articles 7 and/or 6 of the Convention relating to convictions that were based on the use of ByLock as in the present case.

415. Following the relinquishment of jurisdiction in the present case to the Grand Chamber, the Government were requested to indicate the approximate number of criminal cases still pending before the domestic courts, including the Constitutional Court, involving charges under Article 314 § 2 of the Criminal Code on the basis of, in particular, the use of the ByLock messaging application as in the present case. The Government replied that the official statistics pertaining to the criminal cases pending before domestic courts did not include information that would enable them to respond to the Court's specific query. However, having regard to the number of ByLock users identified by the authorities, which was around one hundred thousand (see, for instance, paragraph 119 above), the Court notes that many more applications with similar complaints under Articles 7 and/or 6 of the Convention may potentially be lodged with it.

416. It is clear from the Court's case-law that where a violation originates in a systemic problem affecting a large number of people, general measures at national level will be called for in the execution of such a judgment (see, for instance, *Broniowski*, cited above, §§ 188-94, and *Vălеanu and Others v. Romania*, nos. 59012/17 and 27 others, §§ 269-73, 8 November 2022). Although commonly resorted to in the framework of a pilot-judgment procedure as codified under Rule 61 of the Rules of Court, the Court has also indicated general measures in cases where that procedure was not applied (see, among many examples, *Lukenda v. Slovenia*, no. 23032/02, § 98, ECHR 2005-X; *Hasan and Eylem Zengin v. Turkey*, no. 1448/04, § 84, 9 October 2007; *Manole and Others v. Moldova*, no. 13936/02, § 117, ECHR 2009 (extracts); *Grudić v. Serbia*, no. 31925/08, § 99, 17 April 2012; *Zorica Jovanović v. Serbia*, no. 21794/08, §§ 92 and 93, ECHR 2013; *Abdullah Yaşa and Others v. Turkey*, no. 44827/08, § 61, 16 July 2013; *Shishanov v. the Republic of Moldova*, no. 11353/06, §§ 123-39, 15 September 2015; and *Tunikova and Others v. Russia*, nos. 55974/16 and 3 others, §§ 149-59, 14 December 2021). Whether made within the framework of a pilot judgment or otherwise, the aim with such indications is to assist the Contracting States in fulfilling their role in the Convention system by resolving systemic problems at national level.

417. The Court points in this regard to the States' general obligation to resolve the problems underlying any violations of the Convention, as indicated in Recommendation Rec(2004)6 of the Committee of Ministers (see *Burmych and Others v. Ukraine* (striking out) [GC], nos. 46852/13 et al., § 110, 12 October 2017). It further notes the Contracting States' recommitment to resolving the systemic and structural human rights problems identified by the Court and ensuring the full, effective and prompt execution of its final judgments, taking into account their binding nature, as expressed unequivocally during the recent Summit of Heads of State and Government held in Reykjavík (see Appendix IV to the Reykjavík Declaration cited as relevant at paragraph 204 above). The Court's concern is to facilitate the rapid and effective correction of a defect identified in the national system of human-rights protection and, as indicated in paragraph 408 above, its judgments serve not only to decide those cases brought before it. It therefore follows that once such a defect has been identified, the national authorities have the task, subject to supervision by the Committee of Ministers, of taking – retrospectively if need be – the necessary measures of redress in accordance with the principle of subsidiarity, which underpins the Convention system, so that the Court does not have to reiterate its finding of a violation in a series of comparable cases (see, *Broniowski*, cited above, § 193, and *Scordino v. Italy (no. 1)* [GC], no. 36813/97, § 236, ECHR 2006 V). The Court refers in this regard to its pertinent findings in the decision of *E.G. v. Poland and 175 other Bug River applications* ((dec.), no. 50425/99, § 27, ECHR 2008 (extracts)), as relevant:

> "It is also to be recalled that the Court's principal task under the Convention is, as defined by Article 19 of the Convention, 'to ensure the observance of the engagements undertaken by the High Contracting Parties in the Convention and the Protocols thereto'. A requirement to deliver, continually, individual decisions in cases where there is no longer any live Convention issue cannot be said to be compatible with this task. Nor does this judicial exercise contribute usefully or in any meaningful way to the strengthening of human rights protection under the Convention; ..."

418. The Court is therefore of the opinion that in order to avoid it having to establish similar violations in numerous cases in the future, the defects identified in the present judgment need, to the extent relevant and possible, to be addressed by the Turkish authorities on a larger scale – that is, beyond the specific case of the present applicant. It accordingly falls to the competent authorities, in accordance with the respondent State's obligations under Article 46 of the Convention, to draw the necessary conclusions from the present judgment, particularly in respect of, but not limited to, the cases currently pending before the domestic courts, and to take any other general measures as appropriate in order to resolve the problem identified above that has led to the findings of violation here (see paragraph 414 above; see also, *mutatis mutandis*, *Guðmundur Andri Ástráðsson v. Iceland* [GC], no. 26374/18, § 314, 1 December 2020). More specifically, the domestic

courts are required to take due account of the relevant Convention standards as interpreted and applied in the present judgment. The Court underlines in this respect that Article 46 of the Convention has the force of a constitutional rule in Türkiye in accordance with Article 90 § 5 of the Turkish Constitution, according to which international agreements duly put into effect have the force of law and no appeal lies to the Constitutional Court to challenge their constitutionality (see paragraph 141 above).

B. Article 41 of the Convention

419. 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."

1. Damage

420. The applicant requested 50,000 euros (EUR) in respect of pecuniary damage, in view of his loss of earnings due to his imprisonment as well as the expenses related to his incarceration, including the travel expenses incurred by his relatives to visit him. He did not, however, submit any documents in support of these claims. He also claimed EUR 50,000 in respect of non-pecuniary damage.

421. The Government considered that there was no causal link between the alleged violations of the Convention and the losses the applicant claimed to have sustained, and that the request was unsubstantiated. As regards non-pecuniary damage, the Government claimed that the request was similarly unsubstantiated and excessive.

422. The Court reiterates that the awarding of sums of money to applicants by way of just satisfaction is not one of its main duties but is incidental to its task under Article 19 of the Convention of ensuring the observance by States of their obligations under the Convention (see *Nagmetov v. Russia* [GC], no. 35589/08, § 64, 30 March 2017). The Court enjoys a certain discretion in the exercise of that power, as the adjective "just" and the phrase "if necessary" attest (see *Molla Sali v. Greece* (just satisfaction) [GC], no. 20452/14, § 32, 18 June 2020, with further references). Depending on the circumstances, the Court may also consider that a finding of violation constitutes sufficient just satisfaction and thus dismiss related claims (see *Nagmetov*, cited above, § 70, and the cases cited therein).

423. The Court's guiding principle, in particular as regards just satisfaction on account of non-pecuniary damage, is equity, which involves flexibility and an objective consideration of what is just, fair and reasonable in all the circumstances of the case, including not only the position of the applicant but the overall context in which the breach occurred (see

Varnava and Others v. Turkey [GC], nos. 16064/90 and 8 others, § 224, ECHR 2009; *Al-Jedda v. the United Kingdom* [GC], no. 27021/08, § 114, ECHR 2011; and *Nagmetov*, cited above, § 73).

424. Turning to the applicant's claims in respect of pecuniary damage, the Court notes that according to its settled case-law, it is for applicants to show that such damage has resulted from the violations alleged and to produce documents in support of their claims (see, for instance, *Selahattin Demirtaş*, cited above, § 447). The Court observes that the applicant was dismissed from his job on 27 July 2016 – that is, some two months before his arrest – by way of Legislative Decree no. 672, on account of his suspected affiliation with the FETÖ/PDY (see paragraph 24 above). It further notes that the violations found in the present judgment concern the applicant's conviction and do not relate to his dismissal. In these circumstances, the Court finds that there is no causal link between these violations and the pecuniary damage complained of. Moreover, any claim regarding the alleged loss of earnings during the term of imprisonment is speculative. It therefore rejects the applicant's claim for pecuniary damage.

425. As regards non-pecuniary damage, the Court acknowledges that the applicant may have suffered some distress and anxiety on account of the violations that have been found. However, it also notes, as indicated in the framework of its findings under Article 46, that the applicant has the possibility under Article 311 § 1 (f) of the CCP to have the domestic proceedings reopened following the delivery of the present judgment, and that the reopening of the proceedings in accordance with the requirements of the Convention provisions at issue in the present case would in principle constitute the most appropriate form of redress, should he so request. The Court accordingly considers that a finding of a violation can be regarded as sufficient just satisfaction in the present case, and thus rejects the applicant's claim under this head.

2. Costs and expenses

426. While the case was still pending before the Chamber, the applicant sought EUR 10,000 for the costs and expenses that he had incurred before the domestic courts and the Court, which included lawyer's fees in the amount of 30,000 Turkish liras (TRY) (equivalent to approximately EUR 7,650 at the material time), as well as translation, postal and stationery expenses. To support his claim, the applicant submitted a legal services agreement dated 17 March 2017, signed between him and his lawyer, Mr Akıncı, for the aforementioned sum TRY 30,000, which concerned his representation before the domestic courts and the Court. He also submitted payment orders and receipts for a total sum of EUR 250 in respect of certain expenses incurred before the domestic courts.

427. Following the relinquishment of jurisdiction, the applicant additionally claimed EUR 7,000, inclusive of VAT, in costs and expenses,

which amount included the cost of legal representation before the Grand Chamber by Mr Heymans and Mr Vande Lanotte, as well as travel and accommodation expenses related to the hearing, which was indicated to be EUR 1,000. In support of this additional claim, the applicant submitted a "request for provision" (*verzoek tot provisie*) dated 8 July 2022, issued by the Belgium-based law firm Van Steenbrugge Advocaten for the sum of EUR 7,000, inclusive of VAT.

428. As regards the claim for costs and expenses incurred in the Chamber proceedings, the Government claimed that these expenditures had not been necessarily incurred, in the absence of proof of payment. Moreover, they were excessively high, given in particular the lack of complexity of the procedure and the limited number of issues in question. As for the applicant's claim for costs and expenses in the Grand Chamber proceedings, the Government argued that the applicant had not justified that the additional costs and expenses had been reasonably incurred and had, in particular, not explained why he needed to be represented before the Grand Chamber by three lawyers, and why two of them had to be based in Belgium. He had also not submitted any document showing that he had paid, or was under an obligation to pay, the additional costs he was claiming. For these reasons, the Government invited the Court not to award any costs and expenses to the applicant.

429. 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 have been actually and necessarily incurred and are reasonable as to quantum. In accordance with Rule 60 §§ 2 and 3 of the Rules of Court, itemised particulars of all claims must be submitted, failing which the Court may reject the claim in whole or in part (see *Karácsony and Others v. Hungary* [GC], nos. 42461/13 and 44357/13, § 189, 17 May 2016). A representative's fees are actually incurred if the applicant has paid them or is liable to pay them pursuant to a legal or contractual obligation (see *Merabishvili v. Georgia* [GC], no. 72508/13, § 371, 28 November 2017 and the cases cited therein). As for the number of representatives necessitated by the case, and the rates charged, those are matters taken into consideration by the Court as relevant within the framework of its assessment as to whether the costs and expenses have been reasonably incurred (see, for instance, *Iatridis v. Greece* (just satisfaction) [GC], no. 31107/96, § 55, ECHR 2000-XI).

430. In the present case, the Court considers that the legal services agreement submitted by the applicant for his representation by Mr Akıncı before the domestic courts and the Chamber constitutes sufficient proof that he was under a legal obligation to pay the fees charged by the latter (see, among many examples, *Toptanış v. Turkey*, no. 61170/09, §§ 60-62, 30 August 2016, and *Bilgen v. Turkey*, no. 1571/07, §§ 104-06, 9 March 2021 for a similar finding), given in particular the absence of any arguments by the Government contesting the enforceability of that agreement (see

Merabishvili, cited above, § 371). The Court further considers that the amount claimed is not excessive having regard, in particular, to the length and detail of the pleadings submitted by the applicant in response to the complex legal questions put by the Court at the time of the communication of the case and the equally voluminous submissions made by the Government, which demonstrate that a considerable amount of work was carried out on his behalf (see, *mutatis mutandis*, *Kyprianou v. Cyprus* [GC], no. 73797/01, § 197, ECHR 2005-XIII). Having regard to the documents in its possession and to its case-law, the Court considers it reasonable to award the applicant the sum of EUR 8,000 in respect of the costs incurred before the domestic courts and the Chamber.

431. As for the additional expenses incurred following the relinquishment of the case to the Grand Chamber, the Court considers that the applicant's decision to appoint additional counsel to represent him before the Grand Chamber can be regarded as justified in view of the complex nature of the case. In these circumstances, regard being had to the documents in its possession and the above considerations, the Court considers it reasonable to award the applicant the amount claimed in full (namely EUR 7,000) in relation to the proceedings before the Grand Chamber.

432. The Court therefore awards the applicant the total sum of EUR 15,000 in respect of costs and expenses.

3. Default interest

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

FOR THESE REASONS, THE COURT,

1. *Declares*, unanimously, the complaint under Article 7 of the Convention, the complaint under Article 6 § 1 of the Convention as concerns the rights of the defence in respect of the evidence underlying the conviction, and the complaint under Article 11 of the Convention admissible;

2. *Holds*, by eleven votes to six, that there has been a violation of Article 7 of the Convention;

3. *Holds*, by sixteen votes to one, that there has been a violation of Article 6 § 1 of the Convention;

4. *Holds*, unanimously, that there has been a violation of Article 11 of the Convention;

5. *Holds*, by sixteen votes to one, that there is no need to examine the admissibility and merits of the remaining complaints under Article 6 of the Convention and the complaint under Article 8 of the Convention;

6. *Holds*, by ten votes to seven, that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant;

7. *Holds*, by fourteen votes to three,
   (a) that the respondent State is to pay the applicant, within three months, EUR 15,000 (fifteen thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

8. *Dismisses*, by ten votes to seven, the remainder of the applicant's claim for just satisfaction.

Done in English and in French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 26 September 2023, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Abel Campos	Síofra O'Leary
Deputy Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) partly dissenting opinion of Judge Schembri Orland, joined by Judges Pastor Vilanova and Šimáčková;
(b) joint statement of partial dissent of Judges Krenc and Sârcu;
(c) partly concurring, partly dissenting opinion of Judge Serghides;
(d) joint partly dissenting opinion of Judges Ravarani, Bårdsen, Chanturia, Jelić, Felici and Yüksel;

(e) partly dissenting opinion of Judge Felici;
(f) partly dissenting, partly concurring opinion of Judge Yüksel.

S.O.L.
A.C.

PARTLY DISSENTING OPINION OF JUDGE SCHEMBRI ORLAND, JOINED BY JUDGES PASTOR VILANOVA AND ŠIMÁČKOVÁ

1. The present case concerns the applicant's conviction for membership of an armed terrorist organisation described by the Turkish authorities as the "FETÖ/PDY" ("Fetullahist Terror Organisation / Parallel State Structure"), considered by the authorities to be behind the coup attempt that took place in Türkiye on 15 July 2016. The conviction was based decisively on the applicant's use of an encrypted messaging application by the name of "ByLock", which the domestic courts regarded as having been designed for the exclusive use of members of the FETÖ/PDY. Other evidence used against the applicant included his account activities at Bank Asya and his membership of a trade union and an association that were considered to be affiliated with the FETÖ/PDY. The applicant was convicted and given a prison sentence of six years and three months.

2. The majority found a violation of Articles 7 and 6 § 1of the Convention, while the finding of a violation of Article 11 was unanimous. Whilst agreeing with those findings, as well as with the dismissal of the applicant's claim for pecuniary damage, we respectfully voted against the dismissal of the applicant's claim in respect of non-pecuniary damage (see point 6 of the operative provisions and paragraph 425 of the judgment). The majority determined that the finding of a violation constituted in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant.

3. We start with the premise that the finding of a violation cannot of itself be sufficient to dispense the Court from making a monetary award to the injured party under Article 41 of the Convention. That Article contains further pre-requisites, namely, that the domestic law of the member State allows only partial reparation to be made and that such an award is necessary.

4. In the present case, the Court arrived at its conclusion on just satisfaction by relying on its judgment in *Nagmetov v. Russia* ([GC], no. 35589/08, § 64, 30 March 2017), and thus considered that the awarding of monetary compensation to the applicant by way of just satisfaction was "not one of its main duties" but was "incidental to its task under Article 19 of the Convention of ensuring the observance by States of their obligations under the Convention". The Court, moreover, referred to its discretion in the exercise of that power, this conclusion being supported by the use of the adjective "just" and the phrase "if necessary" in Article 41 of the Convention (see paragraph 422 of the judgment).

5. Despite the discretionary aspect of Article 41, we are nevertheless of the opinion that individual just satisfaction should have been awarded in this case. It must be pointed out that there was no doubt that the applicant sustained non-pecuniary harm arising from the violation of the relevant Articles of the Convention (see paragraph 425 of the judgment

acknowledging that the applicant "may have suffered some distress and anxiety on account of the violations that have been found"), or that there was a causal link between the violation and the harm. The issue here concerns the refusal to award compensation for the violations suffered. The gravity of the violations sustained by the applicant, as further explained below, should, in our opinion, be a compelling consideration for the granting of such compensation.

6. In the first place, whilst recognising that Article 41 uses the term *just satisfaction* and not *just compensation,* this does not exclude the granting of compensation as a form of just satisfaction, but, rather, allows for the possibility of recourse to other effective forms of individual redress, including compensatory reparation. Indeed the Court's jurisprudence is replete with monetary awards of compensation for non-pecuniary damage. The Court has sometimes held that a public vindication of the wrong is sufficient in itself. In this particular case, the Court indicated that the reopening of the criminal proceedings, if requested, would be the most appropriate way of putting an end to the violations found and of affording redress to the applicant. This possibility already exists under Turkish law[1] and recourse to it will be an inevitable consequence of the judgment in this case. Moreover the Grand Chamber has made general recommendations, applying Article 46 of the Convention for appropriate measures to be taken in relation to those who have been treated in the same way as the applicant, drawing the necessary conclusions from the violations of Articles 7 and 6 established in this judgment (see paragraph 414 in conjunction with paragraph 418 of the judgment).

7. It is our opinion that individual redress, in addition to collective redress, is central to human rights. Non-pecuniary, non-material damage is the more typical harm caused by human rights violations. Of particular relevance to the present case, it consists in the trauma, anxiety, and anger consequential to the attack on human dignity, the loss of trust in State institutions, the mental and physical pain lasting after imprisonment, censorship, separation from family members and other manifestations of harm which would merit compensation (see, for example, *Varnava and Others v. Turkey* [GC], nos. 16064/90 and 8 others, § 224, ECHR 2009). Although such non-material harm can by definition never be "remedied" by money, most legal systems or legal instruments, including the European Convention on Human Rights, foresee the possibility of a monetary award to persons who have sustained such harm.

8. The application before the Court in *Yüksel Yalçınkaya* was brought by an individual, under Article 34 of the Convention, and a finding of multiple violations has been made, almost unanimously in respect of a violation of Article 6 § 1 of the Convention, and by a substantial majority of the Court in respect of a violation of Article 7 of the Convention. The possibility of the

1. Article 311 § 1 (f) of the Code of Criminal Procedure.

reopening of proceedings would be an effective way of addressing the applicant's conviction and subsequent sentencing, which had abusively relied on the use of the Bylock application as a decisive element, independently of any intentional element of the offence, contrary to Articles 7 and 6 § 1 of the Convention, in addition to Article 11. However, the availability of the option of reopening the proceedings would not necessarily guarantee an immediate, certain or expeditious outcome and would not substantially erase the distress and anxiety that the applicant has hitherto suffered.

9. We note that the decisive reliance on the use of the Bylock application by the domestic courts in the context of the offence of membership of an armed terrorist group is not a novel situation for the Court. The Court has repeatedly found the courts of Türkiye to be in violation of Article 5 § 1 and 5 § 3 of the Convention (see, for example, *Akgün v Turkey* no. 19699/18, § 173, 20 July 2021), by simply relying on the use of this application as the decisive basis on which to justify the "reasonable suspicion" requirement of that Article. Consequently, the applicant was not alone in falling foul of the systemic flawed reasoning of the Turkish domestic courts. This reasoning, deemed to have been insufficient to sustain a mere suspicion of the commission of that offence, was then conclusively adopted to sustain his conviction for a crime which was a serious one and carried harsh penalties.

10. The issue is not, therefore, simply one of reopening a prosecution in respect of which it would be impossible to speculate on the outcome. For the purposes of ensuring a fair hearing, a reopening of the proceedings would redress the lack of procedural guarantees, resulting, to name a few examples, from a flawed weighting of evidence or from a lack of sufficient evidence, or from a refusal to admit evidence in cross-examination, but here the issue stems, rather, from a conviction which failed to give due consideration to the intentional element of the alleged crime, the *mens rea*, as was specifically required by law. The breach here is not of a straightforward due-process nature, but one that goes to the very essence of the rule of law and the consequential grievous sense of injustice this has caused to the applicant.

11. It is true that the decisive reliance on the Bylock application for arrest, detention, prosecution and conviction for the offence of membership of an armed terrorist organisation reveals a systemic problem within the domestic courts. Indeed over 8,000 similar applications are pending before the Court (see paragraph 414 of the judgment). However, whilst we are mindful of the volume of applications pending, and the consequential impact of multiple compensatory awards on the respondent State, this should not detract from the right of the applicant currently before the Court to individual redress, commensurate with the serious nature of the violations he has suffered. It is no consolation to him that he is the first in a series, if he is then to be deprived of equitable recognition of his distress and suffering. Such a restrictive interpretation of Article 41 of the Convention runs the risk of relegating the award for non-pecuniary damage to the side-lines of justice. The

discretionary application of Article 41 in the form of monetary compensation and the reopening of proceedings are not necessarily mutually exclusive. These awards serve the interests of the aggrieved individuals. They are not intended to serve some collective interest, such as the public interest in a systemic reform, or in rendering respect for human rights more effective in general.

12. On the contrary, the granting of compensation for non-pecuniary damage is envisaged by Article 41 of the Convention, which itself empowers the Court to afford the injured party such satisfaction as appears to it to be appropriate. In *Selahattin Demirtaş (No. 2) v Turkey* ([GC], no. 14305/17, 22 December 2020) the Grand Chamber awarded satisfaction for non-pecuniary damage despite and in addition to having provided for the specific individual measure of the applicant's release. Under that head, the Grand Chamber awarded him EUR 25,000 having considered the multiple and serious violations of the Convention that it had found to have indisputably caused him substantial damage (ibid., § 449).

13. In the present judgment, the majority, relying on *Nagmetov* (cited above), disregarded the principle therein cited whereby it was held that it was "in keeping with the role of the Court under Article 34 of the Convention to 'render justice' in individual cases by way of recognising violations of an injured party's rights and freedoms under the Convention and Protocols thereto and, if necessary, by way of affording just satisfaction" (ibid., § 64). The Court in *Nagmetov* then went on to award monetary compensation in respect of a claim for just satisfaction which had not been specifically articulated. Indeed, the Court held, citing numerous judgments, that it had "previously found it necessary, in rare cases, to make a monetary award in respect of non-pecuniary damage, even where no such claim had been made or where the claim was belated, taking into account the exceptional circumstances of the cases, for instance the absolute or fundamental character of the right or freedom violated". Moreover, the Court in *Nagmetov* further stated (ibid., § 69, emphasis added):

> "In a case concerning Article 8 of the Convention, the Court ordered under Rule 39 of the Rules of Court that the respondent State was to appoint a representative to the applicant, who was entirely divested of the capacity to act and was not capable under domestic law of choosing her own legal representative. When it later transpired that the representative so appointed had omitted to claim just satisfaction, the Court made a non-pecuniary award, having regard to the **trauma, anxiety and feelings of injustice that the applicant must have experienced** as a result of the procedure leading to the adoption of her daughter (see *X v. Croatia*, no. 11223/04, §§ 61-63, 17 July 2008)."

14. The Court has held that, as regards just satisfaction on account of non-pecuniary damage, its guiding principle is equity, which involves flexibility and an objective consideration of what is just, fair and reasonable in all the circumstances of the case, including not only the position of the applicant but the overall context in which the breach occurred (see *Varnava and Others*,

cited above, § 224). The Court's awards in respect of non-pecuniary damage serve to give recognition to the fact that non-material damage occurred as a result of a breach of a fundamental human right and reflect in the broadest of terms the severity of the damage (ibid.). The purpose of awards of just satisfaction has been explained by the Court as follows: They "serve to give recognition to the fact that moral damage occurred as a result of a breach of a fundamental human right and reflect in the broadest of terms the severity of the damage; they are not, nor should they be, intended to give financial comfort or sympathetic enrichment at the expense of the Contracting Party concerned" (ibid.).

15. In conclusion, we consider that the declaration of a violation both of Article 7 and of Article 6 § 1 of the Convention, as well as of Article 11 of the Convention, is an important recognition of a systemic problem which needs to be redressed in Türkiye. However, this cannot of itself serve as a basis for the rejection of a request for just satisfaction in respect of the non-pecuniary damage sustained by the applicant. This is a matter for the Committee of Ministers in conjunction with the respondent State to address. In this respect, the Grand Chamber has given an important judgment defining the applicability, particularly of Article 7, to the expansive interpretation of domestic law, and the interplay with Article 6 § 1 of the Convention. We strongly affirm, however, that the Court's findings also called for individual redress in the form of a monetary award for non-pecuniary damage, given the context and the circumstances of the present case.

JOINT STATEMENT OF PARTIAL DISSENT OF JUDGES KRENC AND SÂRCU

(Translation)

Having regard to the content of the findings of violations of the Convention set out in the present judgment, we are unable to consider that those findings constitute in themselves sufficient just satisfaction for the non-pecuniary damage sustained by the applicant.

PARTLY CONCURRING, PARTLY DISSENTING OPINION JUDGE SERGHIDES

Introduction

1. As stated in the introduction to the judgment, this case concerns the applicant's conviction for membership of an armed terrorist organisation described by the Turkish authorities as the "FETÖ/PDY" ("Fetullahist Terror Organisation/Parallel State Structure"), considered by the authorities to be behind the coup attempt that took place in Türkiye on 15 July 2016. The conviction was based decisively on the applicant's use of an encrypted messaging application by the name of "ByLock", which the domestic courts regarded as having been designed for the exclusive use of the members of the FETÖ/PDY. Other evidence used against the applicant included his account activities at Bank Asya and his membership of a trade union and an association that were considered to be affiliated with the FETÖ/PDY. The applicant was sentenced to six years and three months' imprisonment (see paragraph 63 of the judgment) and he complained before the Court that his trial and conviction had entailed a violation of Articles 6, 7, 8 and 11 of the Convention.

2. While I voted in favour of points 1, 2, 3, 4 and 7 of the operative provisions, I nevertheless voted against the other operative provisions, namely, points 5, 6 and 8. In particular, I respectfully disagree with the majority: (a) "that there is no need to examine the admissibility and merits of the remaining complaints under Article 6 of the Convention and the complaint under Article 8 of the Convention" (point 5 of the operative provisions); (b) "that the finding of a violation constitutes in itself just satisfaction for any non-pecuniary damage sustained by the applicant" (point 6 of the operative provisions); and (c) that "the remainder of the applicant's claim for just satisfaction" is to be dismissed (point 8 of the operative provisions).

3. Lastly, for the reasons I will explain below, I concur with the judgment in finding that there has been a violation of Article 6 § 1 of the Convention (see paragraphs 346 and 356 of the judgment and point 3 of its operative provisions).

1. Where I concur as to finding a violation of Article 6 § 1 of the Convention

4. I agree with the judgment that there has been a violation of Article 6 § 1 of the Convention as a result, in the criminal proceedings, of the failure to ensure an equality of arms between the prosecution and the applicant and to uphold the principle of adversarial proceedings – guarantees which I consider to be linked.

5. However, my disagreement with the judgment here is that it seeks to ascertain whether there were adequate or appropriate safeguards counterbalancing the lack of equality of arms and adversarial proceedings and thus ensuring the overall fairness of the proceedings against the applicant (see paragraphs 330 *et seq.*); only after establishing that there were no such safeguards (see paragraphs 341 and 345) does it then conclude that the trial was unfair overall, and, therefore, that there has been a violation of Article 6 § 1 of the Convention (see paragraph 346). By way of parenthesis here, it is noteworthy that the judgment does not engage in an analysis of the proceedings as a whole, examining all the alleged shortfalls in guarantees, but only performs a review of the overall fairness of the trial in respect of the complaint in question, in connection with any possible safeguards that might address this complaint, such as those summarised in paragraph 345 of the judgment.

6. By contrast, I consider that the breach of the guarantees of equality of arms and adversarial proceedings, mainly due to the complete prohibition barring the applicant from access to the relevant data and evidence on the basis of which he had been convicted and sentenced, rendered his trial unfair *per se* and therefore entailed a violation of Article 6 § 1, without there being any need to examine whether there were any adequate safeguards to counterbalance the absence of these guarantees.

7. In my submission, *there can be no safeguard for a lack of a safeguard*. In the present case, there could be no safeguard for the lack of the Article 6 § 1 safeguards or guarantees of equality of arms and adversarial proceedings, which are indispensable components or elements of the right to a fair trial. On these two guarantees, I had the opportunity to state my views in my Partly Dissenting Opinion in *Regner v. the Czech Republic* ([GC], no. 35289/11, 19 September 2017), to which I simply refer here without setting them out again.

8. The view I am expressing here may also be supported by the case-law of the Court regarding certain Article 6 § 1 guarantees. I can name at least four guarantees – albeit not including the guarantees of equality of arms and adversarial proceedings – in respect of which the Court does not search for counterbalancing safeguards if the guarantee in question is lacking. These are the three institutional and explicit guarantees of a tribunal established by law, of an independent tribunal, and of an impartial tribunal, as well as the guarantee of not using evidence obtained by torture, the latter being an implicit guarantee. Regarding the first three, the institutional guarantees, the Court's practice, when finding that one of them is breached, is not to proceed to examine any other complaints under Article 6 but to consider the trial unfair, finding a violation of the said provision (see, for the guarantee of a tribunal established by law, *Guðmundur Andri Ástráðsson v. Iceland* [GC], no. 26374/18, § 295 and point 2 of the operative provisions, 1 December 2020; see, for the guarantees of an independent and impartial tribunal, *Ergin*

v. Turkey (no. 6), no. 47533/99, §§ 54-56, 4 May 2006, and *Çıraklar v. Turkey,* no. 19601/92, §§ 40-41, 28 October 1998)[1]. Turning now to the guarantee of not using evidence obtained by torture, the Court will find a violation of Article 6 when such evidence has been taken, thus considering the trial as unfair, even if the admission of the evidence in question had not been decisive in securing the suspect's conviction (see *Jalloh v. Germany* [GC], no. 54810/00, §§ 104-05, 1 June 2010)[2], and, of course, without examining any other complaint under Article 6.

9. The above approach regarding these four guarantees, I submit, should apply also regarding the guarantees of equality of arms and adversarial proceedings, as well as any other Article 6 guarantees, and the notion or review of the overall fairness of the trial should not merely be understood as a yardstick by which to assess all relevant factual circumstances so as to ensure the fairness of the proceedings against the applicant, but rather be understood as requiring that all Article 6 guarantees are fully respected and satisfied, as required by the rule of law and the principle of effectiveness – both as a method of interpretation and as a norm of international law – without accepting any compromises by way of counterbalancing with possible safeguards. This view, which is not, however, one which reflects the current practice of the Court, including its approach in the present case, has received extensive and persuasive academic support[3] and is the one that I

1. See more on this, the "hierarchy" of Article 6 guarantees and the principle of effectiveness, in §§ 22-31 of my dissenting opinion in *Angerjärv and Greinoman v. Estonia*, nos. 16358/18 and 34964/18, 4 October 2022. See also Ryan Goss, *Criminal Fair Trial Rights – Article 6 of the European Convention on Human Rights* (Bloomsbury, 2016), pp. 160-161.

2. See also on this guarantee of not taking evidence by torture, Paul Lemmens, "The Right to a Fair Trial and its Multiple Manifestations", in Eva Brems and Janneke Gerards (eds.), *Shaping Rights in the ECHR – The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press, 2013), 294, at p. 309.

3. See, *inter alia,* Yvonne McDermott, *Fairness in International Criminal Trials* (OUP, 2016), 36-37; Nikos Vogiatzis, "Interpreting the Right to Interpretation under Article 6 (3) (e) ECHR: A Cautious Evolution in the Jurisprudence of the European Court of Human Rights", *Human Rights Law Review,* 2022, 22, 1, at pp. 12-14; Ryan Goss, *Criminal Fair Trial* Rights – *Article 6 of the European Convention on Human Rights* (Bloomsbury, 2016), at p. 125; Ryan Goss, "The Undermining of Article 6 ECHR", in P. Czech, L. Heschl, M. Nowak and G. Oberleitner (eds.), *The European Yearbook on Human Rights* (Intersentia, 2019), 295 at pp. 298-299, 304, 311-312; Andreas Samartzis, "Weighing Overall Fairness: A Critique of Balancing under the Criminal Limb of Article 6 of the European Convention on Human Rights", in *Human Rights Law Review,* 2021, 21, 409, p. 410; Ioannis Sarmas, "Fair Trial and Search for Truth in the Case Law of the European Court of Human Rights", in R. Spano, I. Motoc, B. Lubarda, P. Pinto de Albuquerque, M. Tsirli (eds), *Fair Trial: Regional and International Perspectives*, Liber Amicorum Linos-Alexandre Sicilianos (Anthemis, 2020), at p. 500; Georghios M. Pikis, *Justice and the Judiciary* (Martinus Nijhoff Publishers, 2012), at § 145 (p. 63); and Stefan Trechsel, "The Character of the Right to a Fair Trial" in J. Jackson and S. Summers (eds), *Obstacles to Fairness in Criminal Proceedings – Individual Rights and Institutional Forms* (Hart, Oxford, 2018), 19, at p. 25. See also some

would take here. In a Chamber case[4] concerning another implicit guarantee of Article 6 § 1, I considered myself bound by the current case-law of the Court as regards the quest for adequate safeguards to compensate for the lack of the guarantee in question, though I also expressed my preference for the opposite view, as I indeed explained there. In the present case, however, being in the composition of a Grand Chamber case, I consider that I am not compelled to follow the current case-law and feel free to express my preferred view, in the hope that the case-law will evolve in the future so that "no deviation or shortfall of a fair trial should be countenanced"[5].

2. My dissent as to holding that there is no need to examine the admissibility and merits of the remaining complaints under Article 6 or the complaint under Article 8

(a) The applicant's complaint that there had been a breach of the Article 6 § 1 guarantee to have his case heard by an independent and impartial tribunal

10. I respectfully disagree with the majority's finding that there is no need to examine the admissibility and merits of the applicant's complaint that he had not been tried by an independent and impartial tribunal. According to its case-law (see, for instance, *Ergin*, cited above), the Court firstly examines any complaint based on an alleged infringement of the applicant's right to a hearing by an independent and impartial tribunal, and if it concludes that there was such an infringement, it holds that there is no need or cause to examine any other Article 6 complaint.

11. In paragraph 364 of the judgment, the Court provides the following explanation as to why the complaints in question do not require a separate examination of their admissibility and merits:

> "The Court considers that the more immediate issue that lies at the heart of the present case is rather the uniform and global approach adopted by the Turkish judiciary vis-à-vis the ByLock evidence in convictions for membership of the FETÖ/PDY, which has led to findings of violation under Articles 7 and 6 § 1 of the Convention."

This, of course, could also be an explanation as to why the Court proceeded to examine and decide on other Article 6 § 1 complaints, without examining the complaints as to a lack of guarantees of an independent and impartial tribunal.

12. However, in my view, the Court should have proceeded by examining first the applicant's complaints as to a lack of an independent and impartial tribunal for the following reasons: (a) there had been an objection by the

---

pertinent academic works cited in paragraphs 36 and 37 of my partly dissenting opinion in *Xenofontos and Others v. Cyprus*, nos. 68725/16 et al., 25 October 2022.

4. See *Xenofontos*, cited in note 3 above.

5. See Pikis, cited in note 3 above, at § 145 (p. 63).

Government as to the admissibility of these complaints (see paragraph 360 of the judgment) and therefore this objection should have been examined and decided upon by the Court; (b) the guarantees of an independent and impartial tribunal are institutional ones, and together with the guarantee of a tribunal established by law, are conditions *sine qua non* for the existence of any other guarantee under Article 6; (c) if these guarantees (or any one of them) are absent, then the Court automatically (*per se*) finds a violation of Article 6, without needing to examine any safeguards or any other complaints under Article 6; and (d) what the Court considers in its judgment as the more immediate issue at the heart of the present case is an issue concerning administration of evidence and justice, respect for which would follow or presuppose, as said in point (b) above, the existence of an independent and impartial tribunal.

13. For my part, I began by examining the complaints about the lack of a hearing by an independent and impartial tribunal, and I found them inadmissible, because the applicant had not raised them before the judges who had decided on his case; subsequently, I examined the complaints as to the lack of equality of arms and adversarial proceedings under Article 6 § 1, complaints which the judgment itself examines and in respect of which finds a violation. In paragraph 364 of the judgment, the Court observes that the arguments invoked by the applicant in the present case entail a criticism of the judiciary in a general manner (see paragraph 359 of the judgment for the applicant's arguments in this regard), without any specific allegations, either during the domestic proceedings or before the Court, relating to the judges who participated in the examination of his case and producing concrete consequences in his individual trial. The Court's observation in paragraph 364 amounts in my view to a separate examination of the complaints in question as to their admissibility and the only thing that is missing is a clear finding by the Court that the complaints are inadmissible. However, the judgment, instead of stating the obvious conclusion which clearly follows from its observation in paragraph 364, states in paragraph 365 that it considers these complaints not to require a separate examination as to their admissibility and merits.

(b) The applicant's complaint that the guarantee under Article 6 § 3 (c) concerning the right to effective legal assistance had been breached

14. Regarding the above complaint under Article 6 § 3 (c) of the Convention, I agree with the judgment, which does not consider it necessary to address separately its admissibility and merits (see paragraph 367 of the judgment). This is so because the Court had already found a violation of Article 6 § 1 of the Convention owing to a lack of some other guarantees, namely the guarantees of equality of arms and adversarial proceedings in the criminal proceedings (see paragraphs 356 and 367 of the judgment), which,

though implicit guarantees, when breached could lead to the same result, namely a violation of Article 6 § 1, as could the explicit guarantee and minimum right under Article 6 § 3 (c) if it is breached.

15. However, I respectfully disagree with paragraph 366 of the judgment – which represents the current case-law of the Court – stating that the guarantees or minimum rights of Article 6 § 3 of the Convention are not aims in themselves but that their intrinsic aim is always to contribute to ensuring the fairness of the criminal proceedings as whole. In my humble view, each Article 6 guarantee is an indispensable element or component of the concept of a fair trial, and any lack of or shortfall in such a guarantee completely nullifies the fairness of the trial. With due modesty, I would point out that this view, which is in line with the rule of law and the principle of effectiveness, follows the view I have explained above (see paragraph 7) regarding the preferred meaning of the overall fairness of the trial, namely, that all Article 6 guarantees are fully respected and satisfied. I will not proceed however to further explain my view and my disagreement with the judgment on this point, since the judgment does not ultimately consider it necessary to address separately the admissibility and merits of the complaint under Article 6 § 3 (c) of the Convention.

16. Since the complaint in question was placed in point 5 of the operative provisions of the judgment together with other complaints which, unlike myself, the majority consider that there was no need to examine on their admissibility and merits, my vote regarding point 5 could not be in the affirmative but only in the negative.

(c) The applicant's complaint that his rights under Article 8 had been violated

17. I respectfully disagree with the judgment that there is no need to give a separate ruling on the admissibility and merits of the applicant's complaint from the standpoint of Article 8 in the specific circumstances of the instant case.

18. In his application form, the applicant argued that as the ByLock data had been collected and used without a judicial warrant, contrary to Article 6 § 2 of the Law on Intelligence Services of the State and the National Intelligence Agency and Articles 134 and 135 of the Code of Criminal Procedure, his right to respect for private life had been violated owing to the interference with his freedom of communication, which lacked any legal basis. In his observations before the Court, the applicant repeated the above and also argued that the violation of Article 8 of the Convention had been brought before the Court of Appeal in substance and explicitly before the Court of Cassation and the Constitutional Court, and that therefore in his view his complaint under Article 8 was admissible.

19. As to the merits of his complaint, the applicant argued the following in his observations. Any interference with the rights under Article 8 can only

be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more legitimate aims to which that paragraph refers, and is necessary in a democratic society in order to achieve any such aim. But this was clearly not the case here in his view. The National Intelligence Agency (*Milli İstihbarat Teskilati,* MİT) and the Police had interfered with his right to respect for correspondence without any legal basis and the Internet traffic records (HTS) had been illegally stored for more than one year and had subsequently been used in the instant case. The ByLock operation organised by MİT had been completely disproportionate and had simply been a fishing expedition to collect personal and sensitive data in an indiscriminate manner. Furthermore, the entire procedure had not provided any guarantees against abuse by the MİT. The interference with his right to respect for correspondence had been unlawful and manifestly disproportionate and had therefore violated Article 8. In any event, to consider the mere fact of downloading an ordinary communication application onto a smartphone (a fundamental right) to be a crime had constituted in itself a violation of Article 8.

20. In view of the above very convincing observations and submissions of the applicant, I disagree with what is said in paragraphs 372-373 of the judgment, namely, that the Article 8 aspect was a peripheral issue to that of Article 6 and did not need a separate ruling on its admissibility and merits.

21. In conclusion, in my humble view, the complaint under Article 8 was admissible, and there has also been a violation of this Article, particularly with regard to the applicant's right to respect for his private life and his correspondence.

3. My dissent as to the decision not to award the applicant any amount in respect of non-pecuniary damage and the dismissal of the remainder of his just satisfaction claim

22. The applicant requested 50,000 EUR in respect of non-pecuniary damage (see paragraph 420 of the judgment), but the Court decided not to award him any amount for such damage, explaining its approach in paragraph 425 of its judgment as follows:

> "As regards non-pecuniary damage, the Court acknowledges that the applicant may have suffered some distress and anxiety on account of the violations that have been found. However, it also notes, as indicated in the framework of its findings under Article 46, that the applicant has the possibility under Article 311 § 1 (f) of the CCP to have the domestic proceedings reopened following the delivery of the present judgment, and that the reopening of the proceedings in accordance with the requirements of the Convention provisions at issue in the present case would in principle constitute the most appropriate form of redress, should he so request. The Court accordingly considers that a finding of a violation can be regarded as sufficient just satisfaction in the present case, and thus rejects the applicant's claim under this head."

23. In point 6 of the operative provisions the Court holds "that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant".

24. I have had the opportunity to read in advance the partly dissenting opinion of my eminent colleagues, namely Judges Schembri Orland, Pastor Vilanova and Šimáčková, who also voted against point 6 of the operative provisions. I adhere to their opinion almost in its entirety and would have joined it, but I decided to express my own separate opinion in order to add some further important legal arguments and dimensions to those provided by my colleagues. For this reason, as well as because my separate opinion covers issues on which I dissent and concur which are not covered by that opinion, I have decided to include the issue of non-pecuniary damage in my opinion and will endeavour to develop it in a manner that entails both conceptual and practical dimensions. In respect of just satisfaction the two opinions, in my view, are to a great extent complementary and mutually reinforced.

25. It is my submission that Article 41 of the Convention, as worded, cannot be interpreted as meaning that "[the] finding [of] a violation of a Convention provision" can in itself constitute sufficient "just satisfaction for the injured party". This is because "the finding of a violation" is one of the prerequisites "for affording just satisfaction" and the Court cannot treat them as being on a par (see, similarly, paragraph 7 of the Joint Partly Dissenting Opinion that I wrote with Judge Felici in *Grzęda v. Poland* [GC], no. 43572/18, 15 March 2022, and paragraph 3 of the Partly Dissenting Opinion of Judge Schembri Orland, joined by Judges Pastor Vilanova and Šimáčková in the present case).

26. Article 41 of the Convention sets out the following three requirements or criteria which must be met cumulatively for the Court to award just satisfaction, including, of course, satisfaction for non-pecuniary damage (the numbering is mine): (a) the Court finds that there has been a violation of the Convention or the Protocols thereto; (b) the internal law of the High Contracting Party concerned allows only partial reparation to be made; and (c) the Court considers it necessary to afford just satisfaction.

27. The Court in the present case confines itself to the first requirement of Article 41, namely, the finding of a violation, and it regrettably considers, without any justification or explanation, that the fulfilment of this requirement in itself constitutes sufficient just satisfaction for non-pecuniary damage. What the Court is engaging in here is a circular argument: the finding of a violation, which is a *sine qua non* for just satisfaction, becomes the just satisfaction itself. In my opinion, such an interpretation and application of Article 41 has no foundation either in the wording or in the purpose of that provision.

28. Thus, since Article 41 asks for three requirements to be satisfied in order for the Court to afford just satisfaction, there is a logical fallacy in

deciding that the existence of one of them in itself constitutes sufficient satisfaction.

29. To my regret, point 6 of the operative provisions reflects a failure to see that the purpose of Article 41, albeit related, is not the same as the purpose of the substantive provisions of the Convention securing human rights, such as Articles 6, 7 and 11 which the judgment finds to have been violated in the present case. If their purpose were the same, then Article 41 would be rendered futile, which would lead to absurd results.

30. Consequently, with all due respect, the reason provided in point 6 of the operative provisions of the judgment does not seem to be a legitimate and valid ground, having no legal basis in Article 41 and erroneously confusing the merits of the case with the just satisfaction.

31. The failure to award the applicant a sum in respect of non-pecuniary damage for the violation of his rights amounts, in my view, to rendering the protection of his rights illusory and fictitious. This runs counter to the Court's case-law to the effect that the protection of human rights must be practical and effective and not theoretical and illusory, as required by the principle of effectiveness which is inherent in the Convention (see *Artico v. Italy*, 13 May 1980, §§ 33 and 47-48, Series A no. 37). For the applicant's rights under Articles 6, 7, 8 and 11 to be practical and effective and not theoretical and illusory, these substantive Articles together with Article 41 of the Convention must be applied by the Court, not only by finding a violation of the relevant Articles but also by awarding the applicant just monetary compensation for non-pecuniary damage under Article 41.

32. As stated above, all three requirements of Article 41 must be met cumulatively. Since the Court held that there had been a violation of Articles 6, 7 and 11 of the Convention, it is clear that the first requirement of Article 41 is met. I should point out that I have also found that there has been a violation of Article 8.

33. Let us now examine the second requirement of Article 41, namely, that "the internal law of the High Contracting Party concerned allows only partial [and therefore not full] reparation to be made". In paragraph 425 of the judgment, the Court bases its approach on the possibility of reopening the proceedings in accordance with the requirements of the Convention provisions at issue in the present case and argues that this "would in principle constitute the most appropriate form of redress, should [the applicant] so request". By saying the above, the Court does not expressly state that it is dealing with the second requirement of Article 41; however, it is apparent that it is doing so. In my humble view, however, the possibility of reopening the proceedings cannot dispense the Court from finding the second requirement to be satisfied, and therefore from making a monetary award of just satisfaction in the present case, for the following three reasons: (a) by its nature, this measure may not be an appropriate form of redress; (b) reopening

cannot amount to a full reparation; and (c) reopening is an uncertain measure (even the Court uses the word "possibility", which reflects uncertainty).

34. The reopening of proceedings would be an uncertain measure, since the Court in the present case decides on both the merits and just satisfaction in the same judgment and cannot have the opportunity to assess such a measure after it is taken. In other words, the Court in the present case did not first deliver its judgment on the merits and then adjourn its decision on just satisfaction, so as to ensure that this measure of reopening would indeed be adopted by the respondent State. As Ichim observes: "In order for the judges to consider whether domestic law permits any reparation, they should give the state the occasion to prove it [, which] was facilitated in the past by the practice of delivering a first judgment on the merits and then a subsequent judgment on just satisfaction"[6]. In view of the above, even if reopening were an appropriate form of redress amounting to full reparation, the Court would not be able to find out whether this measure is actually taken by the respondent State or, if so, whether it is successful and capable of compensating the applicant for the distress and anxiety he suffered regarding the former proceedings which are the subject-matter of the present judgment. Hence, since there is no full reparation under the internal law, the second requirement of Article 41 is also met.

35. The judgment in paragraph 425, after suggesting the reopening measure, and without elaborating on the first requirement of Article 41, concludes that "the Court accordingly considers that a finding of a violation can be regarded as sufficient satisfaction in the present case, and thus rejects the applicant's claim under this head". With all due respect, by stating this, the judgment erroneously confuses the first and the second requirements of Article 41 of the Convention and actually treats them as one and the same, even though the Court does not expressly refer when dealing with just satisfaction to the requirements under that Article. In any event, in point 6 of the operative provisions, only an implicit reference to the first requirement of Article 41, entailing *per se* the rejection of the claim for non-pecuniary damage, is made, even though the word "requirement" is again not mentioned by the Court.

36. Turning now to the third requirement of Article 41, namely, that it is necessary to afford just satisfaction (the necessity requirement), it is obvious that this requirement is also satisfied in the present case, because the applicant suffered distress and anxiety on account of the violations that have been found. What is even more important, these violations were indeed of a serious nature and must have caused the applicant such feelings and sentiments. As to this requirement, no mention is made of it in paragraph 425 of the judgment, the only paragraph of the judgment dealing with the issue of non-

6. See Octavian Ichim, *Just Satisfaction under the European Convention on Human Rights* (Cambridge University Press, 2015), at p. 67.

pecuniary damage. Nor are there any reasons indicated as to why, despite the distress and anxiety caused to the applicant, the discretion of the Court can be exercised in such a manner as not to award any sum for non-pecuniary damage. If the Court wishes to apply this requirement, it should state and explain it clearly, thus conferring transparency, clarity and consistency on its pronouncement. If the Court considered the reopening of proceedings as full reparation and therefore it considered it not necessary to afford a sum for non-pecuniary damage, again it should make that clear. But, as explained above, the reopening of proceedings can in no way constitute full reparation in terms of the second requirement of Article 41. Furthermore, the reopening, as an uncertain measure, cannot constitute a factor allowing the Court to exercise its discretion so as not to award any sum for non-pecuniary damage in the present case.

37. As I have argued above, failure to award the applicant a sum in respect of non-pecuniary damage for the violation of his rights under Convention Articles 6, 7, 8 and 11, amounts, in my view, to rendering the protection of his rights illusory and fictitious. I would thus award the applicant an amount in respect of non-pecuniary damage, by way of just satisfaction under Article 41 of the Convention. As I am in the minority, however, it is not necessary for me to determine the sum that should have been awarded.

38. Since I also found that there had been a violation of Article 8 of the Convention, and since point 6 of the operative provisions of the judgment does not concern non-pecuniary damage for a violation of Article 8 (because the majority did not find such a violation), I also voted against point 8 of the operative provisions, namely, to dismiss the remainder of the applicant's claim for just satisfaction. I did so because I would also regard the violation of Article 8 as an important consideration in determining the amount to be afforded to the applicant for non-pecuniary damage. This is another reason why I have not joined the separate opinion of Judges Schembri Orland, Pastor Vilanova and Šimáčková, who decided that there was no need to examine the Article 8 complaint, and therefore their basis for determining the amount of non-pecuniary damage would be different from mine, as apart from finding a violation of Articles 6, 7 and 11, I also consider Article 8 to have been violated.

Conclusion

39. The conclusion of my opinion is that, as regards the complaints under Article 6, unlike the majority, I would first examine the complaints of a lack of an independent and impartial tribunal and find them inadmissible. Then I would find that there has been a violation of Article 6 § 1 due to the absence of the guarantees of equality of arms and adversarial proceedings, but I disagree with the majority that there was a need to examine whether there were adequate and appropriate counterbalancing safeguards, which the

majority in any event find not to have existed. Further, like the majority, I consider that since it has been established that there has been a violation of Article 6 § 1, the applicant's complaint that the guarantee under Article 6 § 3 (c) concerning his right to effective legal assistance has been breached does not need to be examined. As regards the Article 8 complaint, I disagree with the majority that there is no need to examine its admissibility and merits, and I would proceed to find it admissible and conclude that there has been a violation of Article 8. Lastly, I disagree with the majority that the finding of a violation constitutes in itself sufficient just satisfaction for non-pecuniary damage and I would proceed, if I were not in the minority, like my distinguished colleagues Judges Schembri Orland, Pastor Vilanova and Šimáčková, and the other dissenters on this issue, to award the applicant a sum under that head.

JOINT PARTLY DISSENTING OPINION OF JUDGES RAVARANI, BÅRDSEN, CHANTURIA, JELIĆ, FELICI AND YÜKSEL

I. POINTS OF AGREEMENT

1. The majority among us, the authors of this joint opinion, agree with the Court's conclusion (see paragraph 345 of the judgment) that there has been a violation of Article 6 § 1 of the Convention, since the domestic courts failed (1) to put into place appropriate safeguards *vis-à-vis* the key piece of evidence at issue to enable the applicant to challenge it effectively, (2) to address the salient issues lying at the core of the case and (3) to provide reasons justifying their decisions. Judge Yüksel, however, does not share the view on this point and also the points expressed in paragraphs 9, 12, and 13 below (see her own separate opinion).

2. We also share the majority's view that there has not been a violation of Article 7 of the Convention in this case in relation to whether the FETÖ/PDY was recognised as a terrorist organisation at the time of the acts attributed to the applicant (see paragraph 253 of the judgment).

3. Moreover, we agree with the majority that there has been a violation of Article 11 of the Convention, since the domestic courts, when convicting the applicant for the offence of membership of an armed terrorist organisation (FETÖ/PDY), took into account as corroborative evidence the fact that the applicant had been a member of Aktif Eğitim-Sen and the Kayseri Voluntary Educators Association (see paragraph 396 of the judgment).

II. WHERE WE DISAGREE WITH THE MAJORITY

4. The majority conclude that there has been a violation of Article 7 of the Convention, since the applicant's conviction for membership of an armed terrorist organisation was based to a decisive extent on his alleged use of the ByLock application and therefore contravened the requirements of Article 7, as the domestic courts effectively imputed objective liability to the users of ByLock through an expansive and unforeseeable interpretation of the domestic law (see paragraphs 214-72 of the judgment). We do not agree with this approach, for the following reasons.

5. Firstly, the domestic courts made it clear that the use of ByLock was not the *actus reus* of the crime of membership of an armed terrorist organisation as defined by Article 314 of the Criminal Code. All constituent elements of the crime as described in the law, both objective and subjective, had to be proven in accordance with the established judicial practice.

6. Secondly, it transpires from the judgment that the applicant was convicted on the basis of his use of the ByLock application in combination with the other evidence in the case file, which included his membership of

the trade union Aktif Eğitim-Sen and the Kayseri Voluntary Educators Association, and his deposit of sums proportionate to his income into an account with Bank Asya, allegedly on the instructions of the FETÖ/PDY (see paragraphs 68, 70, 88, 94 and 384 of the judgment). One may disagree with the relevance of the domestic courts' reliance on this other evidence. But there can nevertheless be no doubt that what the domestic courts were dealing with were questions of evidence and the establishing of facts. Indeed, one of the main questions in the domestic proceedings, in the applicant's case and more generally, was to determine the evidential value of ByLock-related evidence.

7. Thirdly, the Court's ample case-law on Article 7 shows that the purpose of this provision consists in enabling a person to reasonably foresee whether an act or omission on his or her part is criminal, thus making the legal consequences of the behaviour foreseeable and protecting him or her against arbitrary prosecution (see paragraphs 238-39 of the judgment). Questions of evidence – notably regarding the assessment of evidence and of what can reasonably be deduced from the evidence – do not concern the foreseeability of the legal consequences of an act or omission, but the probability of being convicted for it (see, for example, *Del Río Prada v. Spain* [GC], no. 42750/09, ECHR 2013; *Khodorkovskiy and Lebedev v. Russia*, nos. 11082/06 and 13772/05, 25 July 2013; *Vasiliauskas v. Lithuania* [GC], no. 35343/05, ECHR 2015; *Žaja v. Croatia*, no. 37462/09, 4 October 2016; and *Pantalon v. Croatia*, no. 2953/14, 19 November 2020). We also consider that a proper reading of *Korbely v. Hungary* ([GC], no. 9174/02, ECHR 2008) and *Navalnyye v. Russia* (no. 101/15, 17 October 2017) provides little support for the majority's proposition (see paragraph 260 of the judgment) that, as an integral part of an assessment under Article 7 of the Convention, it "falls to the Court to verify whether the relevant constituent elements, and in particular the subjective, or mental, element, were duly established in the applicant's respect, in keeping with the requirements of the domestic law".

8. Fourthly, and as a consequence, the majority's unusual approach may create the impression that the Court is now departing from the established rationale and scope of Article 7, thereby also structurally blurring the inherent distinction between law and fact.

III. THE DOMESTIC COURTS' RELIANCE ON THE APPLICANT'S USE OF BYLOCK IN VIEW OF THE REQUIREMENTS OF ARTICLE 6 § 1

9. We share the majority's assessment that the applicant's rights under the Convention were violated because of the domestic court's reliance on his use of ByLock. However, in our view, the more organic, coherent and safe route would have been the one already followed by the Court under Article 6 § 1 of the Convention on minimum requirements regarding the assessment of evidence, i.e., the proviso that the Court will have to intervene if the assessment of evidence by the domestic courts is arbitrary or manifestly unreasonable (see, among other authorities, *Moreira Ferreira v. Portugal (no. 2)* [GC], no. 19867/12, § 85, 11 July 2017).

10. As explained by the Constitutional Court in its judgment of 15 April 2021 (see paragraph 184 of the judgment), a conviction for membership of an armed terrorist organisation would only follow where the courts could establish the accused's "organic" link with the organisation (based on the continuity, diversity and intensity of his or her activities) and demonstrate that he or she had acted knowingly and willingly within the organisation's hierarchical structure.

11. We are, in this respect, prepared to accept the position of the plenary criminal divisions of the Court of Cassation (see paragraph 160 of the judgment), that where it had been established beyond reasonable doubt that a person joined the ByLock network on the instructions of the FETÖ/PDY, and that he or she used ByLock to ensure secrecy, such a finding would constitute proof of some sort of connection between the accused and the organisation.

12. However, there is a leap from such a finding to the conclusion drawn by the domestic courts in the applicant's case, justified only by some wholly standardised phrases, that all the constituent elements of the crime as described in Article 314 of the Criminal Code were also present, the objective as well as the subjective ones. Indeed, it remains unexplained on what evidential basis the domestic courts found it proven beyond reasonable doubt that the applicant had knowledge and intent in respect of the FETÖ/PDY's alleged operations and goals related to the failed *coup d'état* in 2016. There is here a manifest evidential gap – a missing link – between the factual findings by the domestic courts on the one hand, and what could possibly be inferred from the evidence adduced on the other, in particular what could be deduced from the finding that the applicant had used the ByLock application. In our view, this amounts to a separate, additional, violation of Article 6 § 1 of the Convention.

IV. A NEED FOR GENERAL MEASURES UNDER ARTICLE 46 OF THE CONVENTION

13. Although we have, as explained, a different view from that of the majority regarding the question of applying Article 7 rather than Article 6 § 1 of the Convention, there should be no doubt that we fully share the majority's assessment that the current case forms part of a severe systemic problem in Türkiye, a problem that must be addressed by the respondent Government on a larger scale beyond the specific case, by the implementation of general measures under the guidance of the Committee of Ministers of the Council of Europe (see paragraphs 413-418 of the judgment).

PARTLY DISSENTING OPINION OF JUDGE FELICI

JUST SATISFACTION UNDER ARTICLE 41 OF THE CONVENTION: NON-PECUNIARY DAMAGE

1. I disagree with the judgment concerning point 2 of the operative provisions, holding that "there has been a violation of Article 7 of the Convention". In this respect, I have written – with Judges Ravarani, Bårdsen, Chanturia, Jelić and Yüksel – a joint separate opinion. I would like to add an additional ground of disagreement with that point. The domestic courts relied upon the applicant's membership of organisations linked with the FETÖ/PDY. This fact is accepted by the majority judgment in its analysis under Article 11 (see paragraph 384). It is difficult, if at all possible, to see how the majority can conclude in paragraph 268 that "the factual finding regarding the use of ByLock alone was considered to have made out the constituent elements of the offence of membership of an armed terrorist organisation", when the same majority also proceed with an analysis of Article 11 and find a violation of that provision on the basis that his membership of the Aktif Eğitim-Sen trade union formed part of the factual basis for his conviction. The logic of the majority, in their application of Article 7 to this case, rather seems to firmly exclude any finding of a violation of Article 11.

2. Turning now to the grounds for the present separate opinion, I wish to highlight my disagreement with the judgment concerning points 6 and 8 of the operative provisions, holding *"*that the finding of a violation constitutes in itself sufficient just satisfaction for any non-pecuniary damage sustained by the applicant", and dismissing "the remainder of the applicant's claim for just satisfaction", respectively.

3. My disagreement is thus focused on the decision not to award the applicant a sum in respect of non-pecuniary damage (see paragraphs 420-25 of the judgment and the above points of the operative provisions).

4. The applicant claimed non-pecuniary damage (50,000 euros) for suffering and distress caused by the violation of his rights – *inter alia* – under Article 6 § 1, Article 7 and Article 11 of the Convention. I confine myself, however, only to the applicant's claim under Articles 6 and 11, since I did not join the majority in finding a violation of Article 7. Unlike the majority, I accept the applicant's allegation that the unfairness of the procedure caused him suffering and distress.

5. In my view, all the requirements of Article 41 are satisfied in the present case for an award of just satisfaction: "there has been a violation" of a Convention provision, specifically Article 6; the High Contracting Party concerned allows for no or "only partial reparation"; and it is "necessary" for such an award to be granted to the applicant, who sustained suffering and distress.

6. It is my submission that Article 41 of the Convention, as worded, cannot be interpreted as meaning that "[the] finding [of] a violation of a Convention provision" can in itself constitute sufficient "just satisfaction for the injured party". This is because "the finding of a violation" is one of the prerequisites "for affording just satisfaction" and the Court cannot treat them as being on a par (see, similarly, paragraph 7 of the Joint Partly Dissenting Opinion I wrote with Judge Serghides in *Grzęda v. Poland* [GC], no. 43572/18, 15 March 2022).

7. In this case, the Court has decided not to award any amount for such damage, explaining – in particular – its approach in paragraph 425 of its judgment as follows:

> "As regards non-pecuniary damage, the Court acknowledges that the applicant may have suffered some distress and anxiety on account of the violations that have been found. However, it also notes, as indicated in the framework of its findings under Article 46, that the applicant has the possibility under Article 311 § 1 (f) of the CCP to have the domestic proceedings reopened following the delivery of the present judgment, and that the reopening of the proceedings in accordance with the requirements of the Convention provisions at issue in the present case would in principle constitute the most appropriate form of redress, should he so request."

8. I reiterate in full the considerations made in the above-cited separate opinion. With regard to the specific approach indicated in the previous paragraph – namely the fact that in paragraph 425 of the judgment the Court states that the reopening of the proceedings "would in principle constitute the most appropriate form of redress, should [the applicant] so request" – I would underline that reopening is an uncertain measure (see the term used here, "possibility"); in the present case, as the Court has decided both on the merits and on the non-pecuniary damage, it will not have the possibility of supervising the outcome of the possible reopening of the proceedings at national level; moreover, reopening cannot be seen as appropriate or as providing full reparation.

9. Failure to award the applicant a sum in respect of non-pecuniary damage for the violation of his Article 6 and Article 11 rights amounts, in my view, to rendering the protection of his rights illusory and fictitious. This runs counter to the Court's case-law to the effect that the protection of human rights must be practical and effective and not theoretical and illusory, as required by the principle of effectiveness which is inherent in the Convention (see *Artico v. Italy*, 13 May 1980, §§ 33, 47-48, Series A no. 37).

10. I would thus award the applicant an amount in respect of non-pecuniary damage, by way of just satisfaction under Article 41 of the Convention.

PARTLY DISSENTING, PARTLY CONCURRING OPINION OF JUDGE YÜKSEL

A. AS REGARDS ARTICLE 6 OF THE CONVENTION

I am unable to agree with the majority's conclusion that there has been a violation of Article 6 § 1 of the Convention in this case. There are three main reasons for this disagreement. First, the analysis of the domestic courts' decisions does not seem to be consistent with the Court's case-law. Second, I am not convinced that the majority have given adequate consideration to the novel issue of electronic evidence and its role in the applicant's case. Third, I believe that insufficient consideration has been given to how Türkiye's derogation under Article 15 impacts the analysis under Article 6 § 1 of the Convention.

- 1 -

First, I am not convinced that the majority's analysis of the domestic courts' decisions is consistent with the Court's case-law. Under its case-law, the Court takes "into account the 'proceedings as a whole' before deciding whether or not there has been a violation of the Convention" (see *Mirilashvili v. Russia*, no. 6293/04, § 164, 11 December 2008, and *Edwards v. the United Kingdom*, 16 December 1992, § 34, Series A no. 247-B). The majority, however, seem to focus merely on five isolated alleged shortcomings without assessing the proceedings as a whole (see paragraphs 331-341). I am not convinced that these alleged shortcomings are sufficient, individually or collectively, to lead to the conclusion that there has been a violation in this case.

(a) With regard to the first alleged shortcoming, namely that the domestic authorities did not explain why they could not hand over the raw data (see paragraph 331), it seems that the majority overlook the role that the raw data played in the applicant's case. (i) It is notable that the majority even "accept that there may have been legitimate reasons for not sharing the raw data with the applicant in the present case" and that "it is not the role of this Court to decide whether or not such non-disclosure was strictly necessary since, as a general rule it is for the national courts to assess the evidence before them" (see paragraph 329; see also *Rowe and Davis v. the United Kingdom* [GC], no. 28901/95, § 62, ECHR 2000-II). It seems to be somewhat inconsistent to accept that it may not be possible to share the relevant electronic evidence with the applicant, while at the same time placing significant emphasis on the domestic authorities' alleged lack of reasoning as to the sharing of the raw data. (ii) It is apparent from a supplementary report drawn up on 22 May 2020 that it was not possible to sort the raw data on a user-ID basis without first processing them, and that it was not otherwise possible to share the raw data in their entirety with any particular suspect, as that data contained information

concerning many other suspects as well (see paragraph 121). Given the complexity of the electronic evidence in question, I am not sure so much weight should be placed on the fact that this report, and the explanation as to why the applicant could not be given access to the raw data, was not produced earlier. (iii) The majority seem to consider the raw ByLock data to have been critical to the applicant's case. This seems to be justification for the emphasis on the need to give reasons regarding the raw data. However, this also seems to pay insufficient regard to how the domestic courts actually reached the conclusion that the applicant had used ByLock in this case and shows a failure to engage with the way in which electronic evidence is actually used in criminal trials. The domestic courts did not rely on the raw ByLock data as such in the applicant's conviction. Rather, the Kayseri Assize Court relied on a ByLock report drawn up by the Kayseri Security Directorate during the investigation stage and the report drawn up by KOM at the trial stage (see paragraph 68). The Ankara Regional Court of Appeal, in addition to the reports just referred to, relied on the "ByLock Identification Report" produced on 3 June 2017 by the KOM and the BTK communication records (see paragraphs 78-79), and an expert report by a digital forensics expert on the basis of all the information in the case file (see paragraphs 80 and 88). This expert report examined "records obtained from [the BTK] and [the KOM] concerning the specified GSM number used by the applicant and the entire content of the case file; this report, which was submitted on 29 June 2017, [was] taken as the basis of [the court's] verdict in view of its consistency with the HTS records furnished by the BTK, the ByLock assessment and identification reports furnished by the KOM and the content of the case file, [as well as its] detailed, comparative and scrutinisable nature" (see paragraph 88). It is also apparent from the explanations in paragraph 121 of the judgment that it was not possible to sort the raw data without first processing them and that a user interface had to be developed. Consequently, I believe that the majority have overlooked the role that the raw data actually played in the applicant's case and are incorrect to identify the alleged lack of reasoning as to why they could not be shared as a shortcoming on the part of the domestic courts.

While the majority lay emphasis on the raw data and suggest that they were of "critical importance", they also identify a number of other alleged shortcomings – namely, (i) the domestic courts' failure to respond to the applicant's request for an independent examination of the data; (ii) the domestic courts' failure to respond to a number of the applicant's other arguments, particularly with regard to the reliability of the ByLock evidence; (iii) the fact that the domestic courts gave judgment without waiting for the content to be decrypted; and (iv) that there were "palpable lacunae" in the domestic courts' reasoning (see paragraphs 332-340). I have difficulty with the majority's analysis of these alleged shortcomings, as I believe that they have paid insufficient regard to a number of key principles in the Court's

case-law. For instance, I note that "Article 6 does not impose on domestic courts an obligation to order an expert opinion to be produced or any other investigative measure to be taken solely because it is sought by a party" (see *Mirilashvili*, cited above, § 189). On this point, taking into account the Court's case-law and the extensive examination of the data already carried out by the domestic courts, I am not sure that this can be used as a basis for the outcome proposed. Similarly, although the majority acknowledge that the handling of electronic evidence, particularly where it concerns data that are encrypted and/or vast in volume or scope, may present the law enforcement and judicial authorities with serious practical and procedural challenges at both the investigation and trial stages (see paragraph 312), I fail to see what impact this has had on their analysis in this case.

(b) Bearing in mind the above, it seems that all of the alleged shortcomings identified by the majority essentially boil down to the single issue that there was a lack of reasoning on the part of the domestic authorities. In this respect, it is important to consider the standards in the Court's case-law with regard to the reasoning of domestic courts. While courts are not obliged to give a detailed answer to every argument raised, it must be clear from the decision that the essential issues of the case have been addressed (see *Taxquet v. Belgium* [GC], no. 926/05, § 91, ECHR 2010). It seems that the domestic courts did address the essential issues raised by the applicant in their decisions. The applicant's main concerns, as argued before the domestic courts, seem to be (i) that the FETÖ/PDY was not designated a terrorist organisation at the time he allegedly used ByLock and was a member of the organisations linked to FETÖ/PDY (paragraph 71); (ii) that the ByLock data had been obtained unlawfully (paragraph 73); and (iii) that there had been insufficient examination of the data by experts (paragraph 75). (i) The Ankara Regional Court of Appeal indicated that under Turkish law the absence of a prior judicial ruling designating FETÖ/PDY as a terrorist organisation did not preclude criminal liability for membership of a terrorist organisation (see paragraph 84). (ii) The domestic courts also indicated that the data had been lawfully collected under Turkish law (see paragraph 85). (iii) As already explained above, the domestic courts also dealt with the issues of the verification and examination of the data (paragraphs 76-80 and 88). Accordingly, it does appear that by their actions and reasoning, the domestic courts including the appeal courts (see paragraphs 83-88 and 98), addressed the essential issues in the applicant's case.

Overall, in the light of all of the above, it appears that the majority have failed to identify, by reference to the standards in the Court's case-law, how "there were not enough safeguards in place to ensure that the applicant had a genuine opportunity to challenge the evidence against him and conduct his defence" (see paragraph 341). Taking into account the proceedings as a whole, as seen in the file, the domestic courts shared the information used to convict the applicant and gave him adequate opportunity to challenge that

information. The domestic courts appear to have taken on board the applicant's concerns with regard to the adequacy of the information in the case file, leading them to request additional verification to this effect. I believe this demonstrates, in view of the Court's case-law identified above, that the domestic courts had in place adequate safeguards to protect the applicant's right to a fair trial.

- 2 -

Second, I would like to express my regret that the majority have not engaged with one of the important and novel issues raised by this case; namely, the use of electronic evidence in criminal proceedings. The Grand Chamber ought to have considered how the Article 6 § 1 analysis should be refined in this specific context. This is especially so since the case concerns "electronic evidence attesting to an individual's use of an encrypted messaging system that was allegedly designed by a terrorist organisation for the purposes of its internal communications" (see paragraph 344). In this respect, I would like to point to the Court's case-law to the effect that "Article 6 should not be applied in such a manner as to put disproportionate difficulties in the way of the police authorities in taking effective measures to counter terrorism or other serious crimes" (see *Ibrahim and Others v. the United Kingdom* [GC], nos. 50541/08 and others, § 252, 13 September 2016). Given the novel issue of electronic evidence, the Court should also not lose sight of the fundamental principle of subsidiarity. It should be borne in mind, in this connection, that the assessment of the admissibility and probative value of a particular piece of evidence, as well as the determination of whether the offence has materialised on the facts, are primarily for national courts to assess (see *Bochan v. Ukraine (no. 2)* [GC], no. 22251/08, § 61, ECHR 2015, and *Moreira Ferreira v. Portugal (no. 2)* [GC], no. 19867/12, § 83, 11 July 2017; see also *Correia de Matos v. Portugal,* [GC] no. 56402/12, § 116, 4 April 2018). Consequently, the Court's engagement with how the guarantees of Article 6 § 1 apply in the context of this case appears to be inadequate.

- 3 -

In the same way as the majority have not sufficiently engaged with the novel issue of electronic evidence in combatting terrorism, they have also not engaged with the interaction between Articles 6 § 1 and 15 of the Convention. The essential investigative and judicial actions leading to the applicant's conviction had been taken at a time when there was a derogation under Article 15 in place in respect of Türkiye. This derogation was enacted as a direct consequence of the attempted coup in July 2016 (see paragraphs 10-15). During the attempted coup, military personnel under the instigators' control bombarded several strategic State buildings, including the Parliament building and the presidential compound, attacked the hotel where

the President was staying, held the Chief of General Staff hostage, occupied television studios and fired on demonstrators. According to the submissions, more than 250 people, including civilians, were killed on the night in question and more than 2,000 people were injured (see paragraph 11). Despite these exceptional circumstances, the majority do not engage in substantive analysis as to how Türkiye's derogation under Article 15 impacts the analysis under Article 6 § 1.

In this connection, I firstly disagree with the majority's reliance on the Government's arguments in relation to Article 6 § 3 (c) of the Convention. In paragraph 354 the majority note the Government's statement made as part of their submissions under Article 6 § 3 (c) of the Convention that "the state of emergency had not been determinative in the decisions of the judicial authorities, and that the judicial activities were carried out by [their] own principles and rules". The majority, whilst acknowledging the "limited significance of this statement" nevertheless suggest that it is consistent with the "Government's observations that the criminal proceedings were conducted by the domestic courts in a manner that duly observed the applicant's procedural rights" (paragraph 354). I have difficulty with this reasoning because it implicitly suggests that the Government did not make submissions regarding the state of emergency's relevance to this case. As is apparent from the case file, this may be misleading. The sentence relied upon by the majority forms part of a broader argument and is taken out of context. Furthermore, the arguments in relation to Article 6 § 3 (c) are wholly separate from the arguments with respect to Article 6 § 1. Consequently, I do not think the majority should draw upon the submissions made within the scope of Article 6 § 3 (c) for the purposes of their analysis under Article 6 § 1.

Secondly, the main reason adduced by the majority for not engaging with the interaction between Article 6 § 1 and Article 15 seems to be that the "Government have not adduced any detailed reasons" regarding how the measures taken in the applicant's case were necessitated by the state of emergency (see paragraph 355). (i) I am not convinced this is an adequate justification for not engaging with the question of how Articles 6 § 1 and 15 interact. This is a question of principle that the Court is addressing for the first time in such context; consequently, it is not satisfactory for the Court to limit its analysis to the arguments of the domestic authorities. (ii) In any event, I do not think that the majority adequately engage with the arguments as to the relevance of the state of emergency. It is apparent from the case file and the arguments of the national authorities, including the national judiciary, that the state of emergency is the fundamental underlying context of this case. In this regard, I disagree with the suggestion that there was no indication that the "'exclusivity' argument at issue had been developed by reason of the special circumstances of the state of emergency" (see paragraph 353). In my view, the Court of Cassation's finding that ByLock was exclusively used by FETÖ/PDY (see paragraphs 158-160) cannot be divorced from the post-*coup*

d'état circumstances, considering the purpose of declaring the state of emergency and the complexity of the challenged posed by FETÖ/PDY. Further, it is not a novelty under the Court's case-law to take into account the context of a derogation and the difficulties facing Türkiye in the aftermath of the attempted military coup of 15 July 2016 when interpreting and applying Article 15 of the Convention (*Baş v. Turkey*, no. 66448/17, § 221, 3 March 2020). Indeed, from a survey of the case-law, it seems that Article 15 has been deployed in different contexts: the first, where there is a relatively isolated event that is understood to threaten the life of the nation (for instance, *A. and Others v. the United Kingdom* [GC], nos. 3455/05 and others, 19 February 2009); and second, where there is a "particularly far-reaching and acute danger for the territorial integrity of [a Contracting State], the institutions of the [State] and the lives of the province's inhabitants" (*Ireland v. the United Kingdom,* 18 January 1978, § 212, Series A no. 25). I wonder if, in these different types of public emergencies, Article 15 may be interpreted and applied in a way that is tailored to the specific context of the threat to the life of the nation. As seen in the case-law, where a derogation is triggered by a "far-reaching and acute danger" as opposed to a relatively isolated event, greater consideration may need to be given to this general context when assessing if the measures were necessary in relation to the exigencies of the situation. Consequently, taking into account the far-reaching impact of the state of emergency on the institutional apparatus of the state (see paragraphs 10-16) and the fact that the domestic judiciary were dealing with the "use of an encrypted messaging system that was allegedly designed by a terrorist organisation for the purposes of its internal communications" (see paragraph 344), I do not believe that the majority have given adequate consideration as to how the derogation context should impact the analysis in the present case.

In the light of the foregoing and the case-law of the Court, I believe that the reasoning of the majority does not provide sufficient elements to conclude that there has been a violation of Article 6 § 1 in this case. Under the standards set in the Court's case law, the domestic courts should make clear from the decision that the essential issues of the case have been addressed (*Taxquet*, cited above, § 91), and the Court should assess the fairness of the proceedings as a whole (*Mirilashvili*, cited above, § 164, and *Edwards*, cited above, § 34). What appears from the domestic courts' decisions as a whole is that they did address the essential issues in the applicant's case. Consequently, bearing in mind the reasoning of the domestic courts, the role and particularities of the electronic evidence and the state of emergency, I am unable to agree with the conclusion that there has been a violation of Article 6 § 1 in the circumstances of this case.

B. AS REGARDS ARTICLES 11 AND 46 OF THE CONVENTION

Regarding the applicant's complaint under Article 11 of the Convention, although I agree with the conclusion that, in the particular circumstances of the present case, there has been a violation, I am unable to subscribe to the entirety of the majority's reasoning. I agree that there has been a violation of this provision on account of a lack of explanation by the domestic courts on the issues noted in the judgment. However, I am unable to agree with the reasoning as regards "lawfulness" since the majority place reliance on *Selahattin Demirtaş v. Turkey (no. 2)* (no. 14305/17, 22 December 2020) and I maintain my legal view expressed in that case.

Considering my view that there has been no violation of Article 6 § 1 or of Article 7 in the present case, I am also unable to support the inclusion of an Article 46 indication in the judgment.