REPUBLIC OF TURKEY
MINISTRY OF JUSTICE
DEPARTMENT OF HUMAN RIGHTS

Tel. : + 90 312 549 59 06
Fax : + 90 312 549 59 27
E-mail : inhak@adalet.gov.tr

OBSERVATIONS OF THE GOVERNMENT OF THE REPUBLIC OF TURKEY ON THE ADMISSIBILITY AND MERITS CONCERNING THE APPLICATION

No. 42883/19 and other 6 applications

ÇAMURŞEN and other 6 applicants v. TURKEY

BEFORE THE EUROPEAN COURT OF HUMAN RIGHTS

Annexes: Relevant Documents

Date: ... October 2021

1. By the letter from the European Court of Human Rights ("the Court") dated 12 April 2021, the observations of the Government of the Republic of Turkey ("the Turkish Government" or "the Government") have been sought on the admissibility and merits of the applications ***Çamurşen and other 6 applications v. Turkey*** **no.42883/19 and 6 other applications.**

2. In this regard, the Government has the honour to submit to the Court the following observations.

I. THE FACTS

3. In the present applications, criminal proceedings were brought against each applicant on the charges of membership of the Fethullahist Terrorist Organisation/Parallel State Structure (FETÖ/PDY) or of attempting to overthrow the constitutional order. In the context of the criminal proceedings in question, the domestic courts requested the CGNAT data[1](internet traffic information) belonging to the telephone numbers used by the applicants from the Information Technologies and Communication Authority ("BTK" or "Authority") in order to identify as to whether the applicants had connected to the IP addresses belonging to the ByLock application established as being exclusively used by the members of FETÖ/PDY armed terrorist organisation for intra-organisational communication. In the present applications, the applicants complain that this CGNAT data, indicating when and how long they connected to IP address belonging to a server through the phones they used, have been retained by the BTK and access providers. The applicants allege that their right to respect for private life have been violated on the ground that this data have been retained by the BTK and access providers in a manner such as to exceed the time-limit prescribed by the legislation.

4. In this regard, before proceeding to the particular circumstances of the present case, the Government would like to provide the following general

[1]*CGNAT (Carrier Grade NAT):* The information on when, how many times and from which address the IP addresses of the ByLock server (target) are connected to. By means of matching the General IP and Private IP addresses which are available in the CGNAT records and assigned to the user by the GSM operator, it is possible to establish the time frame of the user's access to the target IP (namely, the time frame of the session) and the dates on which the user accessed the target IP. In other words, CGNAT data are the records including the information that how many times it was connected to IP addresses belonging to ByLock server.

information to the Court's attention for a better understanding of its observations regarding the applicants' complaints.

A) Background Information

1. The Coup Attempt dated 15 July 2016

5. On the night of 15 July 2016, in Turkey, a group organised within the Turkish Armed Forces who are the members of the Fetullahist Terrorist Organisation/Parallel State Structure (FETÖ/PDY) (hereinafter "FETÖ/PDY"), attempted to overthrow the democratic constitutional order with the use of force and violence together with civilian executives (imam) of the organisation as well as members of FETÖ/PDY who infiltrated into the police, gendarmerie and other public institutions.

6. Those who staged the coup attempt used fighter jets, helicopters, ships, tanks and heavy artillery. It was noted in the statement of the General Staff that according to the first findings, more than 8.000 military personnel were involved in the coup attempt, that 35 air crafts including fighter jets, 3 ships, 37 helicopters, 246 armoured vehicles including 74 tanks, and approximately 4.000 light arms were used in the course of the attempt.

7. During the coup attempt, bombs and armed attacks were carried out against a large number of critical places having strategic importance, including the Presidential compound, the Grand National Assembly of Turkey, the premises of the General Staff, the Ankara Police Special Operations Centre, the premises of the National Intelligence Organisation and the Ankara Police Department. The Bosphorus and Fatih Sultan Mehmet Bridges and İstanbul Atatürk Airport were occupied by means of tanks and armoured vehicles and many public institutions were occupied by armed forces of the FETÖ/PDY.

8. The plotters of the coup also attempted to assassinate the President of the Republic of Turkey at the hotel where he was staying. During the coup attempt the Chief of General Staff and numerous high-ranking generals were taken as hostages. The coup plotters targeted at the civilians who were on the streets in order to oppose against the coup and to prevent it. During that night people were shot randomly by coup plotters, the crowds were bombed and shot from the fighter jets and helicopters and tanks.

9. The coup plotters also occupied the Turkish Radio and Television Corporation (TRT), and announced a statement on behalf of the "Peace at Home Council (Yurtta Sulh Konseyi)" by means of television broadcast. The issues included in the "martial law directive" were mentioned in this statement. In the course of the coup attempt, attacks were carried out against relevant institutions and organisations including the Turkish Satellite Communications and Cable TV Operations Company (TURKSAT) in order to cut off television broadcasting and internet access throughout the country.

10. The 15 July armed coup attempt demonstrated FETO's determination to unwaveringly use terror, alongside other crimes, as a means to achieve its ultimate aim. With this act, FETÖ/PDY clearly showed itself to the world as one of the most dangerous terrorist groups. As a result of attacks of the coup plotters 251 people including civilians lost their lives and 2.194 people were injured. Several key institutions representing the will of the Turkish people, first and foremost, the Parliament, were heavily assaulted.

11. As it is revealed in the confidential correspondences of the organisation members, and those who attempted the coup confessed in their statements that they had been instructed by the ring leader of the FETÖ/PDY terrorist organisation. At the end of the proceedings conducted against the member of the FETÖ/PDY following the coup attempt, these points were also established by the judicial decisions (for detailed explanations and the judicial decisions see below). In addition, it was established in the judgments of the Constitutional Court (see *Aydın Yavuz and the others* (no: 2016/22169, 20/6/2017[2]; *Ferhat Kara [GK],* B. No: 2018/15231, 4/6/2020[3]) that the treacherous coup attempt was staged by the FETÖ/PDY armed terrorist organisation.

2. Declaration of state of emergency

12. In order to protect the Turkish democracy and the fundamental rights and freedoms of the Turkish people, and to find and bring the perpetrators of the

[2]See, the judgment in Turkish, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2016/22169
See, the judgment in English, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2016/22169?Dil=en
[3]See, the judgment in Turkish,
https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/15231?Dil=tr
See, the judgment in English, https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/15231?Dil=en

coup attempt before the justice, to completely eliminate probable future threats, and to eliminate the risk threatening the existence of the nation and to restore the damaged public order, it is State's duty to take immediate action. It is also crucial and inevitable for the State to apply exceptional measures to overcome possible dysfunctionalities of its democratic institutions due to attempted coup and to deal with ineffectiveness of the ordinary measures.

13. Faced with such a situation threatening the constitutional order, a nationwide State of Emergency was declared as of 21 July 2016 by the Council of Ministers in line with the National Security Council's recommendation and based on Articles 119-122 of the Constitution and Article 3/1-b of the Law no: 2935. The decision ruling the state of emergency was upheld by the Turkish Grand National Assembly. Considering those groups infiltrated into key state institutions as well as the dysfunctionalities and ineffectiveness that would be caused by them it is of vital importance for Turkey to declare state of emergency and accordingly notify its derogation from the Convention with a view to taking proportionate and exceptional measures.

14. After having been extended several times by the decisions taken by the Council of Ministers every three months, the state of emergency ended on Thursday, 18 July 2018 at 00:00 a.m.

3. Derogation from the European Convention on Human Rights

a. Notification of Derogation

15. Following the declaration of the state of emergency, in accordance with Article 15 of the Convention, Turkey resorted to the right of derogation from the Convention by notifying the Secretary General of the Council of Europe on 21 July 2016[4] . The decisions issued for the prolongation of the state of emergency were also submitted to Secretary General of the Council of Europe. Pursuant to Article 4 of the International Covenant on Civil and Political Rights (hereinafter "the ICCPR"), a similar notification was submitted to the Secretariat of the United Nations.

[4]Derogation of 21 July 2016, available at: https://rm.coe.int/090000168069496b

b. Public emergency threatening the life of the Turkish nation

16. The whole population of Turkey has experienced an exceptional threat because of the terrorist coup attempt occurred on 15 July 2016. This threat endangered the organised life of the community of which the State is composed in a democratic structure. The threat caused by the coup attempt was of actual nature as mentioned in the Court's case-laws and also it was of imminent nature in respect of having possibility to reoccur.

17. Taking into account the evidently violent coup attempt and the bloody casualties of the people resisting, the severity of threat facing the whole nation is apparent. As emphasized by the Constitutional Court in its judgment of *Aydın Yavuz and Others* (no: 2016/22169, 20 June 2017) in assessing the magnitude of the threat posed by the coup attempt against the democratic constitutional order, it is not sufficient to take into consideration the damage caused by this prevented attempt alone. In addition to this, the threat the whole nation might face and the possible prolongation of the clashes if the coup attempt had not been prevented in a short time or if the coup had occurred must also be assessed.

18. Accordingly, there is no doubt that the declaration of the state of emergency in the aftermath of the 15 July coup attempt by the FETÖ/PDY fell within the scope of Article 15 of the Convention.

c. Measures during the state of emergency

19. During the state of emergency all necessary measures have been taken in order to fight against terrorism and to overcome the consequences of the treacherous coup attempt within the framework of Article 15 of the Turkish Constitution. All measures taken during the state of emergency by the Decree Laws were regularly notified to the Secretariat General of the Council of Europe[5].

---

[5]For detailed information regarding notifications see:
- Decree with Force of Law No. 667, dated 22 July 2016, on the measures to be taken under the state of emergency, available at: https://rm.coe.int/09000016806969b0
-Decree with Force of Law No. 668, dated 27 July 2016, on the measures to be taken under the state of emergency, available at:https://rm.coe.int/090000168069792d
-Decrees with Force of Law Nos. 670 and 671, dated 17 August 2016, on measures to be taken under the state of emergency, available at: https://rm.coe.int/090000168069f414

d. Proportionality and Consistency of Measures during the state of emergency

20. The measures taken through Decree Laws issued within the scope of the state of emergency were in compliance with the principle of proportionality and strictly required by the exigencies of the situation derived from the large scale bloody coup attempt. All measures were for the legitimate aim of protection of national security. In terms of parliamentary oversight, in accordance with Article 119 of the Constitution, Decree Laws issued during the state of emergency were submitted for approval to the Parliament on the same day they were published in the Official Gazette, and all of them finally adopted and enacted by the Parliament.

21. The measures taken during the derogation period are consistent with the other obligations of Turkey under international law. In this connection, the Government would like to draw the Court's attention to the fact that the Government also communicated the notification of derogation to the UN authorities in accordance with Article 4 of ICCPR, following its declaration of the state of emergency.

22. Throughout the state of emergency Turkey acted in line with its international human rights obligations and observed the principles of necessity, proportionality and legality. Turkey has also maintained its cooperation with international organisations, in particular the UN and the Council of Europe.

-Decrees with Force of Law Nos. 672, 673 and 674, dated 1 September 2016, on the measures to be taken under the state of emergency, available at: https://rm.coe.int/09000016806a2ef7
-Decrees with Force of Law Nos. 675 and 676, dated 29 October 2016, on the measures to be taken under the state of emergency, available at:https://rm.coe.int/09000016806b93b9
-Decrees with Force of Law Nos. 677 and 678, dated 22 November 2016, on the measures to be taken under the state of emergency, available at: https://rm.coe.int/09000016806cd21a
- Decrees with Force of Law Nos. 679, 680 and 685 on the measures to be taken under the state of emergency, available at: https://rm.coe.int/09000016806ee865
- Decrees with Force of Law Nos. 682, 683, 684, 686 and 687 on the measures to be taken under the state of emergency, available at: https://rm.coe.int/09000016806fa1f7
- Decree with Force of Law No. 690 dated 29 April 2017 on the measures under the state of emergency, available at: https://rm.coe.int/090000168072abda,
- Decree with Force of Law No. 691 dated 22 June 2017 on the measures under the state of emergency, available at: https://rm.coe.int/090000168091f585
- the Decree with Force of Law No. 692 dated 14 July 2017 on the measures under the state of emergency, available at: https://rm.coe.int/090000168091f587
- Decree with Force of Law No. 696 dated 24 December 2017 on the measures under the state of emergency, available at: https://rm.coe.int/090000168077fa4d
- Decree with Force of Law No. 701 dated 8 July 2018 on the measures under the state of emergency, available at: https://rm.coe.int/09000016808ccc04

Several UN Special rapporteurs and Council of Europe's monitoring bodies visited Turkey during that period (see Turkish Constitutional Court's judgment of *Aydın Yavuz and Others* cited above §§ 161-162). The fact that Turkey facilitated these visits is a clear demonstration of its commitment to maintaining its cooperation with the international organisations and the conformity of the measures taken during the state of emergency with its international obligations.

23. The Government further notes that it has provided detailed explanations as to each question on the necessity and proportionality of the measures taken during the state of emergency.

e. Conclusion

24. Within the scope of the similar applications, the Constitutional Court examined the measures implemented after the coup attempt of 15 July under Article 15 of the Constitution (see *Aydın Yavuz and Others*, cited above; and *Orhan Patarya* [Plenary], no. 2019/42695, 20 May 2021).

25. The ECtHR also has concluded that notice of derogation by Turkey, indicating that a state of emergency was declared in order to tackle with the threat posed to the life of the nation by the severe dangers resulting from attempted military coup of 15 July and other terrorist acts, has been satisfied the formal requirements laid down in Article 15 § 3 of the Convention (see *Alpay v. Turkey*, no. 16538/17, § 73, 20 March 2018; *Mehmet Hasan Altan v. Turkey*, no. 13237/17, § 89, 20 March 2018; *Alparslan Altan v. Turkey*, 12778/17, § 72, 16 April 2019).

26. In the light of the foregoing, the Government respectfully invite the Court to examine the present applications as regards the Article 8 of the Convention in the scope of the Article 15 of the Convention.

4. General Characteristics of ByLock

27. The Government would like to state that ByLock application is an encrypted communication application, which is exclusively used by the members of the FETÖ/PDY armed terrorist organisation. In terms of general findings regarding the Bylock application, the Government would like to bring to the Court's attention the decisions of the Constitutional Court in the applications of

Ferhat Kara and Bestami Eroğlu and of the General Assembly of the Court of Cassation in Criminal Matters dated 26 June 2019 (see Annex 1).

28. As mentioned in the decision of the General Assembly of the Court of Cassation in Criminal Matters dated 26 June 2019 and the decision of the Constitutional Court in the Ferhat Kara application, there are different ways to detect whether people use the Bylock application (see Ferhat Kara § 96).

> -The first source consists of forensic IT examination held on telephones or electronic devices belonging to the user.
>
> -The second source is the raw log information including information, including user-IDs, messages, emails, voice calls and the log records pertaining to this information, which were obtained by the MİT from ByLock servers. This raw data does not comprise the entire server data but a fraction of it.
>
> -The third source concerns the internet traffic created by individuals on their devices. In other words, this is the CGNAT data pertaining to the internet traffic reports demonstrating accesses from Turkey to ByLock IPs.

29. Accordingly, one of the legal ways establishing as to whether there is an access to the said application is to examine the internet traffic information carried out by the persons over their devices and to identify as to whether they connected to one of 9 IP addresses assigned to ByLock application. As the CGNAT data can be characterised as the data that is not possible to change and impair its integrity, it is admitted as data in the investigations conducted as to whether the persons are members of the FETÖ/PDY armed terrorist organisation.

B) Processes in respect of the Applicants

1. The Applicant Metin Çamurşen

30. An investigation was launched against the applicant Metin Çamurşen in July 2016 on charges of membership of the FETÖ/PDY terrorist organization. As a result of the relevant investigation, on 29 March 2017 an indictment was issued in respect of the applicant Metin Çamurşen for the offence of membership

of an armed terrorist organisation. The applicant Metin Çamurşen was tried for this offence before the Tekirdağ 2nd Assize Court.

31. While the proceedings against the applicant were still ongoing, on 14 September 2017 the Tekirdağ 2nd Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet traffic between the two sources. The BTK submitted the requested CGNAT data to the Assize court.

32. At the end of the criminal proceedings against him, on 29 March 2018 the applicant was sentenced to 9 years of imprisonment for the offence of membership of the FETÖ/PDY armed terrorist organisation pursuant to Article 314 § 2 of the Turkish Criminal Code (Law no. 5237). In delivering a decision on conviction in respect of the applicant, the Assize Court relied on the applicant's Bylock record, the testimonies of witnesses, and the finding of residual files relating to the FETÖ/PDY terrorist organization on his phone. On 3 July 2019 the 16th Criminal Chamber of the Court of Cassation upheld the applicant's imprisonment sentence and this sentence became final.

33. On 28 June 2018 the applicant Metin Çamurşen filed a criminal complaint against the BTK and access provider Avea (Türk Telekom) requesting a criminal investigation for the offence of failure to destroy data under Article 138 of the Turkish Criminal Code (Law no. 5237) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

34. Upon the criminal complaint filed by the applicant, the Ankara Chief Public Prosecutor's Office conducted a criminal investigation. At the end of the investigation, on 10 July 2018 it was decided not to process the criminal complaint in question with a final decision. In its decision, the Ankara Chief Public Prosecutor's Office stated that the allegations of the applicant were in the nature of defence submissions in the criminal case in which he was tried and that the assessment of evidence was at the discretion of the trial court. In this context, the Ankara Chief Public Prosecutor's Office decided that there was no criminal

act in the material incident (see Annex 2). However, the name of the applicant Metin Çamurşen was miswritten by mistake in the relevant decision. Upon the applicant's request for the correction of this mistake, on 6 August 2018 the relevant mistake was corrected and the applicant's name was rewritten.

35. On 7 August 2018 the applicant lodged an individual application with the Constitutional Court and alleged that his right to respect for private life, freedom of communication and the right to an effective remedy in the domestic law violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

36. By its decision dated 21 June 2019, the Third Commission of the First Section of the Constitutional Court held that the application had been lodged without exhausting the available administrative and judicial remedies in the law system. In that connection, the Constitutional Court declared the application inadmissible for failure to exhaust the remedies in relation to the applicant's allegations that his right to respect for private life, freedom of communication had been violated (see Annex 3).

2. The Applicant Serkan Uslu

37. An investigation was initiated against the applicant, Serkan Uslu, on charges of membership of the FETÖ/PDY terrorist organization in October 2016. As a result of the relevant investigation, An indictment was issued in respect of the applicant Serkan Uslu on 21 February 2017 for the offence of membership of an armed terrorist organisation. The applicant Serkan Uslu was tried for this offence before the Edirne 2nd Assize Court.

38. While the proceedings against the applicant were still ongoing, on 7 November 2017 the Edirne 2nd Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet traffic between the two sources. On 6 December 2017 the BTK submitted the requested CGNAT data to the Assize court.

39. At the end of proceedings against him, on 1 February 2018 the applicant was sentenced to 7 years and 6 months of imprisonment for the offence of membership of the FETÖ/PDY armed terrorist organisation pursuant to Article 314 § 2 of the Turkish Criminal Code (Law no. 5237). In delivering a decision on conviction against the applicant, the Assize Court relied on the fact that the applicant was a Bylock user, had an account at Bank Asya, had participated in the activities carried out upon the instructions of the FETÖ/PDY terrorist organization. On 23 February 2021 the 16th Criminal Chamber of the Court of Cassation upheld the applicant's imprisonment sentence and this sentence became final.

40. On 6 May 2019 the applicant Serkan Uslu filed a criminal complaint against the BTK and access providers Avea (Türk Telekom), Vodafone and Turkcell requesting a criminal investigation for the offence of failure to destroy data under Article 138 of the Turkish Criminal Code (Law no. 5237) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit.

41. Upon the criminal complaint filed by the applicant, the Ankara Chief Public Prosecutor's Office conducted an investigation. At the end of the investigation, on 22 May 2019 it was decided not to process the criminal complaint filed against the BTK and the decision of non-prosecution was issued in respect of access providers. In its decision, the Ankara Chief Public Prosecutor's Office especially pointed out that the data was not sent to the relevant court by the access provider and stated that it cannot be said that the access provider stored the CGNAT in violation of Article 6 of the Law No. 5651. In this regard, the Chief Public Prosecutor's Office relied on the fact that the data was sent to the court by the BTK, not by the access provider. Regarding the storing of the said data by the ICTA, a detailed research was carried out in terms of the right to respect for private life regulated in Article 8 of the Convention. The Prosecutor's Office held that the storing of the data in question had the legitimate aims of protecting public order and preventing crime within the meaning of Article 8 § 2 of the Convention. (see Annex 4). On 13 June 2019 the applicant filed an objection against the decision of the Public Prosecutor's

Office. By its decision of 2 November 2019, the Ankara 2nd Magistrate Judgeship dismissed the objection with a final decision (see Annex 5).

42. On 14 June 2019 the applicant lodged an individual application with the Constitutional Court, alleging that his right to respect for private life, freedom of communication and the right to an effective remedy violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

43. By its decision dated 11 June 2020, the Third Commission of Second Section of the Constitutional Court held that there had not been an interference with fundamental rights and freedoms prescribed by the Constitution in the application in terms of the right to respect for private and family life and freedom of communication or that the interference had not amounted to a violation. In this connection, the Constitutional Court declared the applicant's alleged violation of the right to a fair hearing inherent in the right to a fair trial inadmissible *ratione materiae* and the alleged violation of the right to respect for private and family life and freedom of communication inadmissible for being manifestly ill-founded without examining the application in terms of the other admissibility criteria (see Annex 6).

3. The Applicant Sadık Yayla

44. An investigation was launched against the applicant Sadık Yayla in July 2016 for membership of the FETÖ/PDY terrorist organization. As a result of the investigation, on 15 August 2017 an indictment issued in respect of the applicant Sadık Yayla for the offence of membership of an armed terrorist organisation. The applicant Sadık Yayla was tried for this offence before the Şırnak 3rd Assize Court.

45. In the course of proceedings against the applicant, on 7 December 2017 the Şırnak 3rd Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet traffic between the

two sources. The BTK submitted the requested CGNAT data to the Assize court.

46. At the end of the criminal proceedings against him, on 4 June 2018 the applicant was sentenced to 8 years and 9 months of imprisonment for the offence of membership of FETÖ/PDY armed terrorist organization pursuant to Article 314 § 2 of the Law no. 5237.In delivering a decision on conviction, the Assize Court relied on the witness statements against the applicant, the fact that the applicant was a Bylock user, that he had previously worked in workplaces that had been closed due to his connections with the FETÖ/PDY armed terrorist organization, that he had deposited money in Bank Asya in line with the organization's instructions. On 26 February 2019 the 16th Criminal Chamber of the Court of Cassation upheld the applicant's imprisonment sentence and this sentence became final.

47. On 10 August 2018 the applicant Sadık Yayla filed a criminal complaint against the authorities of BTK and of access provider Turkcell requesting a criminal investigation for the offence of failure to destroy data under Article 138 of the Turkish Criminal Code (Law no. 5237) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

48. Upon the criminal complaint filed by the applicant, the Ankara Chief Public Prosecutor's Office conducted an investigation. At the end of the investigation, on 30 October 2018, by a final decision, it was decided not to process the criminal complaint in question. In its decision, the Ankara Chief Public Prosecutor's Office stated the allegations of the applicant were in the nature of defence submissions in the criminal case in which he was tried and that the authority to discuss the evidence was at the discretion of the trial court. (see Annex 7). On 12 November 2018 the applicant filed an objection against the decision of the Public Prosecutor's Office. By its decision of 26 December 2018, the Ankara 5th Magistrate Judgeship held that there was no ground for examination on account of the fact that the relevant decision could not be counted as a decision to be subject-matter of an objection (see Annex 8).

49. On 19 November 2018 the applicant lodged an individual application with the Constitutional Court, alleging that his right to respect for private life, freedom of communication and the right to an effective remedy in the domestic law violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit.

50. By its decision dated 3 December 2019, the Third Commission of Second Section of the Constitutional Court held that there had not right to an interference with fundamental rights and freedoms prescribed by the Constitution in its examination made within the scope of the right to respect for private and family life and freedom of communication or that the interference had not amounted to a violation. In this connection, the Constitutional Court declared the applicant's alleged violation of the right to a fair trial inadmissible *ratione materiae* and the alleged violation of the right to respect for private and family life and freedom of communication inadmissible for being manifestly ill-founded (see Annex 9).

4. The Applicant Hüseyin Akbulut

51. An investigation was initiated against the applicant Hüseyin Akbulut in August 2016 for membership of the FETÖ/PDY terrorist organization. As a result of the investigation, on 7 February 2017 an indictment issued in respect of the applicant Hüseyin Akbulut for the offence of membership of an armed terrorist organisation. The applicant Hüseyin Akbulut was tried for this offence before the Istanbul 22nd Assize Court.

52. In the course of proceedings against the applicant, on 25 April 2017 the Istanbul 22nd Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet traffic between the two sources. The BTK submitted the requested CGNAT data to the Assize court.

53. At the end of proceedings against him, on 7 December 2017 the applicant was sentenced to 7 years and 6 months of imprisonment for the offence

of membership of FETÖ/PDY armed terrorist organisation pursuant to Article 314 § 2 of the Law no. 5237. In delivering a decision on conviction, the Assize Court relied on the witness statements against the applicant, the fact that the applicant was a Bylock user, that he had previously worked in workplaces that had been closed due to his connections with the FETÖ/PDY armed terrorist organization.

54. By its decision of 2 July 2020, the 16th Criminal Chamber of the Court of Cassation quashed the conviction delivered against the applicant by the first-instance court. Following the quashing decision, the case-file, in which the applicant was tried, was submitted again to the first-instance court (see Annex 10). As of the date of preparation of the Government's observations, the trial against the applicant is pending before the Istanbul 22nd Assize Court.

55. On 1 October 2018 the applicant Hüseyin Akbulut filed a criminal complaint against the authorities of BTK and of access provider Avea (Türk Telekom) requesting a criminal investigation for the offences of violation of privacy of private life under Article 134 of, recording of personal data under Article 135 of, and unlawful giving and seizure of data under Article 136 of and the failure to destroy data under Article 138 of the Turkish Criminal Code (Law no. 5237) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

56. Upon the criminal complaint filed by the applicant, the Ankara Chief Public Prosecutor's Office conducted an investigation. At the end of the investigation, on 18 October 2018 it was decided not to process with a final decision. In its decision, the Ankara Chief Public Prosecutor's Office stated that the allegations of the applicant were in the nature of evidence brought forward by the defence in the criminal case in which he was tried and that the assessment of evidence was at the discretion of the trial court. In this context, the Ankara Chief Public Prosecutor's Office decided that there was no criminal act in the material incident (see Annex 11).

57. On 5 November 2018 the applicant lodged an individual application with the Constitutional Court, alleging that his right to respect for private life, freedom of communication and the right to an effective remedy in the domestic

law violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

58. By its decision dated 12 November 2019, the First Commission of First Section of the Constitutional Court held that there had not been an interference with fundamental rights and freedoms prescribed by the Constitution in the examination made within the scope of the right to respect for private and family life and freedom of communication or that the interference had not amounted to a violation. In this connection, the Constitutional Court declared the applicant's alleged violation of the right to a fair trial inadmissible for incompatibility*ratione materiae* and the alleged violation of the right to respect for private and family life and freedom of communication inadmissible for being manifestly ill-founded (see Annex 12).

5. The Applicant Gökhan Yaman

59. An investigation was launched against the applicant Gökhan Yaman on the charge of membership of the FETÖ/PDY terrorist organization in June 2016 . As a result of the investigation carried out, on 4 August 2017 an indictment issued in respect of the applicant Gökhan Yaman for the offence of membership of an armed terrorist organisation. The applicant Gökhan Yaman was tried for this offence before the Şırnak 3rd Assize Court.

60. In the course of proceedings against the applicant, on 24 November 2017 the Şırnak 3rd Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet traffic between the two sources. The BTK submitted the requested CGNAT data to the Assize court. After the said data was sent to the relevant court, the applicant did not raise any objection regarding the legal nature of the ICTA's storing of these data in the pending proceedings. Moreover, at this stage, no claim with respect to the violation of rights due to the storing of the data in question was raised by the applicant before the court where he was tried.

61. At the end of proceedings against him, on 26 September 2018 the applicant was sentenced to 6 years, 10 months and 15 days of imprisonment for the offence of membership of FETÖ/PDY armed terrorist organisation pursuant to Article 314 § 2 of the Law no. 5237. In the decision ordering the applicant's conviction, the Assize Court relied on the fact that the applicant was a Bylock user and the statements of witnesses against him. By its decision of 26 June 2019, the 16th Criminal Chamber of the Court of Cassation quashed the conviction delivered against the applicant by the first-instance court and its decision became final.

62. On 27 March 2019 the applicant Gökhan Yaman filed a criminal complaint against the authorities of BTK requesting a criminal investigation for the offences of violation of privacy of private life under Article 134 of, recording of personal data under Article 135 of, and unlawful giving and seizure of data under Article 136 of, the failure to destroy data under Article 138 of and the offence of misconduct under Article 257 of the Turkish Criminal Code (Law no. 5237) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

63. Upon the criminal complaint filed by the applicant, the Gölbaşı (Ankara) Chief Public Prosecutor's Office conducted an investigation. At the end of the investigation, on 29 March 2019 a decision of non-prosecution was issued. In its decision, the Gölbaşı Chief Public Prosecutor's Office emphasized that it is one of the duties of the ICTA to implement the interception of communication measure applied in accordance with Article 135 of the Law No. 5271. The Chief Public Prosecutor's Office stated that in order to fulfil this duty stipulated by the law, the ICTA is obliged to archive the data regarding the interception of communication during the statutory time limitations provided for in the Law No. 5237. In this context, the Chief Public Prosecutor's Office concluded that the acts subject to the criminal complaint were procedural and lawful (see Annex 13). On 19 April 2019 the applicant filed an objection against the decision of the Public Prosecutor's Office. By its decision dated 22 May 2019, the Ankara 7th Magistrate Judgeship dismissed the applicant's objection on the ground that the relevant decision complied with the law and procedure (see Annex 14).

64. On 21 June 2019 the applicant lodged an individual application with the Constitutional Court, alleging that his right to respect for private life, freedom of communication, freedom of expression, freedom to claim rights, the principle of equality, the right to receive a reasoned decision and the right to an effective remedy in the domestic law violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

65. In its decision of 10 February 2020, the First Commission of the Second Section of the Constitutional Court only examined the application within the scope of the right to a fair trial. The Constitutional Court held that the alleged violations giving rise to the application did not fall within the scope of Article 6 of the Convention, and therefore decided that it was not under the protection of the Constitution and the Convention. In this connection, as regards the alleged violation of the right to a fair trial, the Constitutional Court declared the application inadmissible for incompatibility *ratione materiae* (see Annex 15).

6. The Applicant Duran Denizci

66. An investigation was initiated against the applicant Duran Denizci in December 2015 for membership of the FETÖ/PDY terrorist organization. As a result of the investigation, on 29 June 2016 an indictment was issued in respect of the applicant Duran Denizci for the offences of attempting to overthrowing the Government of the Republic of Turkey or prevent it from performing its duties, founding or leading an armed terrorist organisation and unlawful recording of personal data. The applicant Duran Denizci was tried for this offence before the Istanbul 14th Assize Court.

67. While the proceedings against the applicant were still ongoing, on 12 July 2017 the Istanbul 14th Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet traffic between the two sources. On 25 July 2017 the BTK submitted the requested CGNAT data to the Assize court.

68. At the end of the criminal proceedings against him, on 18 March 2019 it was held that the applicant be sentenced to aggravated life imprisonment for the offence of attempting to overthrow the Government of the Republic of Turkey or prevent it from performing its duties pursuant to Article 312 § 1 of the Law no. 5237, that he be sentenced to 7 years and 6 months of imprisonment for the offence of violation of the privacy of communications pursuant to Article 132 of the Law no. 5237 and that he be sentenced to 2 years and 8 months of imprisonment for the offence of breaching the confidentiality of the investigation pursuant to Article 285 of the Law no. 5237. In its decision on conviction in respect of the applicant, the Assize Court relied on the fact that the applicant was a Bylock user and that he was an executive responsible within the organizational structure of the FETÖ/PDY armed terrorist organization established within the General Directorate for Police.

69. The appellate review of the conviction delivered against the applicant by the first-instance court pursuant to Article 312 § 1 and Article 132 of the Law no. 5237 is still pending before the Court of Cassation. As of the date of preparation of the Government's observations, the trial against the applicant is pending before the Court of Cassation.

70. On 13 October 2017 the applicant Duran Denizci filed a criminal complaint against the authorities of BTK and of access provider Avea (Türk Telekom) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

71. Upon the criminal complaint filed by the applicant, the Istanbul Chief Public Prosecutor's Office conducted an investigation. At the end of the investigation, on 26 October 2017 a decision of non-prosecution was issued in respect of the relevant criminal complaint. In its decision, the Istanbul Chief Public Prosecutor's Office noted that the relevant court could not base its decision on unlawful evidence in the criminal case in which the applicant was tried. Moreover, it also provided that it was possible to file a criminal action if an element of crime is found during the trial, if deemed necessary by the relevant court (see Annex 16). On 23 January 2018 the applicant filed an objection against the decision of the Public Prosecutor's Office. By its decision dated 30

January 2018, the Istanbul 5th Magistrate Judgeship dismissed the applicant's objection on the ground that the relevant decision complied with the law and procedure (see Annex 17).

72. On 26 June 2018 the applicant lodged an individual application with the Constitutional Court, alleging that his right to respect for private life, freedom of communication and freedom to claim rights violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

73. By its decision dated 9 July 2019, the Third Commission of the Second Section of the Constitutional Court held that there had not been an interference with fundamental rights and freedoms prescribed by the Constitution in the examination made within the scope of the right to respect for private and family life and freedom of communication or that the interference had not amounted to a violation. In this connection, the Constitutional Court declared the applicant's alleged violation of the right to a fair trial inadmissible for incompatibility *ratione materiae* and the alleged violation of the right to respect for private and family life and freedom of communication inadmissible for being manifestly ill-founded (see Annex 18).

7. The Applicant Hüsmen Koçak

74. An investigation was launched against the applicant, Hüsmen Koçak, in July 2016 on the charge of membership of the FETÖ/PDY terrorist organization. As a result of the investigation carried out, on 25 March 2017 an indictment issued in respect of the applicant Hüsmen Koçak for the offence of founding and leading an armed terrorist organisation. The applicant Hüsmen Koçak was tried for this offence before the Tekirdağ 2nd Assize Court.

75. While the proceedings against the applicant were still ongoing, on 19 September 2017 the Tekirdağ 2nd Assize Court asked the BTK as to whether the mobile phone number belonging to the applicant had connected to IP addresses of ByLock application under Article 135 of the Code of Criminal Procedure (Law no. 5271) and also requested the CGNAT data indicating the internet

traffic between the two sources. On 6 October 2017 the BTK submitted the requested CGNAT data to the Assize court.

76. At the end of proceedings against him, on 12 April 2018 the applicant was sentenced to 9 years of imprisonment for the offence of membership of FETÖ/PDY armed terrorist organisation pursuant to Article 314 § 2 of the Law no. 5237. In the decision ordering the applicant's conviction, the Assize Court relied on the fact that the applicant was a Bylock user and the statements of witnesses against him. By its decision of 12 June 2019, the 16th Criminal Chamber of the Court of Cassation upheld the conviction delivered against the applicant by the first-instance court and its decision became final.

77. On 8 February 2019 the applicant Hüsmen Koçak filed a criminal complaint against the authorities of BTK and of access provider Avea (Türk Telekom) requesting a criminal investigation for the offence of failure to destroy data under Article 138 of the Turkish Criminal Code (Law no. 5237) with the allegation that the CGNAT data in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

78. Upon the criminal complaint filed by the applicant, the Ankara Chief Public Prosecutor's Office conducted an investigation. By its decision dated 25 February 2019, the Ankara Chief Public Prosecutor's Office decided that the investigations against the authorities of the BTK and of Avea be disjoined and continued under different investigation files. At the end of the investigation against the BTK, on 25 February 2019 the Chief Public Prosecutor's Office decided not to process it with a final decision. In its decision, the Ankara Chief Public Prosecutor's Office stated that one of the duties of the ICTA is to implement the communication interception decisions issued pursuant to Article 135 of the Law No. 5271. The Chief Public Prosecutor's Office found that ICTA can archive the data within its body during the statutory time limitations stipulated in the Law No. 5237 in order to fulfil this duty. Moreover, it relied on the fact that this is one of the exceptions stipulated in Article 28 of the Law no. 6698 on the Protection of Personal Data (see Annex 19).

79. On 11 March 2019 the applicant lodged an individual application with the Constitutional Court, alleging that his right to respect for private life,

freedom of communication and freedom to claim rights violated on the ground that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit prescribed by the legislation.

80. By its decision dated 27 February 2020, the Second Commission of the Second Section of the Constitutional Court held that there had not been an interference with fundamental rights and freedoms prescribed by the Constitution in the examination within the scope of the right to respect for private and family life and freedom of communication or that the interference had not amounted to a violation. In this connection, the Constitutional Court declared the applicant's alleged violation of the right to a fair trial inadmissible for incompatibility*ratione materiae* and the alleged violation of the right to respect for private and family life and freedom of communication inadmissible for being manifestly ill-founded (see Annex 20).

81. On 18 June 2019 the applicant brought a full remedy action against the BTK before the Ankara 2nd Administrative Court. In the relevant action, the applicant alleged that the fact that the CGNAT data, which was requested in the criminal proceedings, in respect of him had been retained longer than the statutory time limit suffered him damages and he claimed TRY 150,000 in respect of non-pecuniary damage. The applicant asserted that the damages in question had been incurred due to the administrative action of the respondent BTK administration (see Annex 21).

82. On 19 December 2019 the Ankara 2 nd Administrative Court dismissed the full remedy action (see Annex 22).The Ankara 2nd Administrative Court addressed the application lodged with it in all its aspects. In its decision, the Administrative Court stated that the ICTA has the duty of fulfilling the requests for interception of communication set forth in Article 135 of the Law No. 5271. The Administrative Court noted that the ICTA can archive all kinds of information and documents obtained from providers as a requirement of this duty. As regards the ICTA's interception obligation, the Administrative Court stated that ICTA did not have any service fault and there was no indication that CGNAT data was unduly created. Having stated that no damage that require

compensation was occurred with respect to the storing these data by the ICTA, the Ankara 2nd Administrative Court dismissed the case.

83. On 5 March 2020 the applicant filed an appeal on points of facts and law against this decision. Having examined the appeal on points of facts and law, on 30 December 2020 the 7th Administrative Chamber of the Ankara Regional Administrative Court dismissed the appeal on points of facts and law on the merits with a final decision (see Annex 23). In its relevant decision, the Regional Administrative Court relied on the ground that the decision of the first-instance court had complied with the law and procedure. The relevant decision was served on the applicant on 07 April 2021 (see Annex 24).

84. In this connection, on 30 December 2020 the full remedy action brought by the applicant before the administrative court became final . Following the notification of this decision, the applicant has the right to lodge an individual application with the Constitutional Court. However, the applicant did not mention about this decision in the application form and its annexes, nor did he submit any information or document indicating that he had exhausted the remedy of individual application before the Constitutional Court.

II. THE RELEVANT LAW AND PRACTICE

A) Relevant Domestic Law

1. Constitution

85. Article 20, entitled "*Privacy and protection of private life*", of the Constitution reads as follows[6];

> "A. *Privacy of private life*
>
> *Article 20 - Everyone has the right to demand respect for his/her private and family life. Privacy of private or family life shall not be violated."*

86. Article 125, entitled "*Judicial Review*", of the Constitution reads as follows;

> "***Judicial review***
>
> *Article 125 (1) Recourse to judicial review shall be available against all actions and acts of administration. (Sentences added on 13 August 1999 by Article 2 of the*

[6] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf

Law no. 4446) In concession, conditions and contracts concerning public services and national or international arbitration may be suggested to settle the disputes arising from them. Only those disputes involving an element of foreignness may be submitted to international arbitration.

(...)

(3)(As amended on 12 September 2010 by Article 11 of the Law no. 5982) Judicial power is limited to the review of the legality of administrative actions and acts, and in no case may it be used as a review of expediency. No judicial ruling shall be passed which restricts the exercise of the executive function in accordance with the forms and principles prescribed by law, which has the quality of an administrative action and act, or which removes discretionary powers.

(...)

(6) The administration shall be liable to compensate for damages resulting from its actions and acts."

87. Article 129 of the Constitution, entitled "*Provisions concerning the public officials*", reads as follows:

"Provisions concerning the public officials

"Article 129 (4)- Actions for compensation concerning damages arising from faults committed by civil servants and other public officials in the exercise of their duties shall be filed only against the administration in accordance with the procedure and conditions prescribed by law, as long as the compensation is recoursed to them."

2. Provisions Regarding Establishment and Authorities of ICTA

88. Article 1 of "the Law no. 5397 Amending Certain Laws" is as follows[7];

ARTICLE 1

"The procedures set out in this article and the wiretapping processes to be conducted within the scope of Article 135 of the Law no. 5271 shall be carried out from a single centre established under the name of "Presidency of Telecommunication and Communication ", an entity directly affiliated to the President of the Telecommunication Authority. This Presidency shall consist of a president, and three experts, namely technical, legal and administrative experts. There shall be a representative from each of the relevant units of the National Intelligence Organization, the General Police Department, and the Gendarmerie General Command. Sufficient number of personnel shall be employed to perform the assigned tasks. The President of Telecommunication and Communication shall be appointed by the Prime Minister upon the proposal of the President of the Telecommunication Authority. The President of Telecommunication and Communication shall have the same personnel benefits as the Board members. The Ministry of Transport shall be obliged to prepare the infrastructure concerning this centre. The establishment expenses of this centre shall be covered from the revenues of the Telecommunication Authority. All kinds of purchases of goods and services and construction works related to the establishment of this centre shall be

[7] https://www.tbmm.gov.tr/kanunlar/k5397.html

exempt from the provisions of the Law no. 4734 on Public Procurement and the Law no. 4735 on Public Procurement Contracts, except for fines and prohibition from tenders."

89. Article 3, governing definitions, Article 4, governing principles, Article 15, governing destruction of records, of the Regulation Amending the Regulation on the Procedures and Principles concerning Interception, Wiretapping of Communications Made via Telecommunications, and Assessment and Recording of Signal Information and the Establishment, Duties and Powers of the Presidency of the Telecommunication and Communication, which was prepared to determine the procedures and principles concerning interception and wiretapping of communications made via telecommunications and assessment and recording of signal information and to regulate the establishment, duties and powers of the Presidency of Telecommunication and Communication, read as follows[8];

*"**ARTICLE 3** - For the purposes of this Regulation, the term*

(..)

e) Access provider: shall mean any natural or legal persons providing their users with a means of access to Internet,

Principles

***ARTICLE 4-** Privacy of communication is fundamental.*

No one may intercept or wiretap telecommunications of another person, assess signal information or record them, except in accordance with the principles and procedures defined in this Regulation.

Records and information obtained within the scope of the activities carried out in accordance with the provisions of this Regulation shall not be used for the purposes and in line with the procedure other than those specified in this Regulation and in Additional Article 7 of the Law no. 2559 dated 4 July 1934, Additional Article 5 of the Law no. 2803 dated 10 March 1983, Article 6 of the Law no. 2937 dated 1 November 1983 and Article 135 of the Law no. 5271 dated 4 December 2004.

Privacy is fundamental in the storage and protection of information, documents and records obtained."

Destruction of records

ARTICLE 15 - (First paragraph amended by the Official Gazette no. 26572 dated 4 July 2007)(1) In the event that a decision of non-prosecution is delivered in respect of the suspect in the course of the implementation of the decision or that the judge decides otherwise regarding the decisions taken by the public prosecutor in cases where delay would be detrimental; the Presidency [of Telecommunication and Communication] shall be immediately notified by the public prosecutor, or by the

[8] https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=9596&MevzuatTur=7&MevzuatTertip=5

law enforcement, upon instruction of the public prosecutor, that the measure has been lifted.

If the decision made by the public prosecutor is not approved by the judge and sent to the Presidency within the time-limit, the Presidency shall immediately terminate the implementation of the decision.

***(Third paragraph amended by the Official Gazette no. 26572 dated 4 July 2007)**[1] Records concerning interception or wiretapping carried out in cases set out in the first and second paragraphs as well as the second paragraph of Article 12 shall be destroyed within a maximum period of ten days under the supervision of the public prosecutor at the court having competence and jurisdiction set out in Article 26, and this shall be recorded in a report.*

90. Article 22 of the Decree-law no. 671 on Regulating Some Institutions and Organisations under the State of Emergency provides as follows[9];

***ARTICLE 22**-The following additional article was added to the Law no.5651.*

"ADDITIONAL ARTICLE 3-(1) The Presidency of Telecommunication and Communication was closed.

(2) The references made to the Presidency of Telecommunication and Communication in the other legislation shall be considered as references to the Information and Communication Technologies Authority, and the references made to the President of Telecommunication and Communication shall be considered as references to the President of Information and Communication Technologies Authority."

91. Article 6, entitled "Duties and powers of the Authority", governing the duties and powers of the BTK of "the Electronic Communications Law" numbered 5809, which was enacted to create effective competition, to ensure the protection of consumer rights, to promote the deployment of services throughout the country, to ensure efficient and effective use of the resources, to promote the new investments and technological developments in communication infrastructure, network and services through regulations and inspections in electronic communication sector and to determine relevant principles and procedures thereto, provide as follows[10]:

"Duties and powers of the Authority

ARTICLE 6-(1) Duties and powers of the Authority are as follows:

(...)

c) to make necessary arrangements and supervisions pertaining to the rights of subscribers, users, consumers and end users as well as processing of personal data and protection of privacy,

(...)

[9] https://www.resmigazete.gov.tr/eskiler/2016/08/20160817-18..htm
[10] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf

ı) to obtain any kind of information and documents from the operators, public institutions and organisations, natural persons and legal entities, deemed necessary, pertaining to electronic communications, and to keep the necessary records, to submit those needed by the Ministry upon request in determination of the strategies and policies towards electronic communications sector."

92. Article 14, entitled "Periods of data retention by the operators", of the Former Regulation on Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector provides as follows:

"Periods of data retention by the operators

Article 14:

(1) The data categories defined under Article 13 shall be retained for a period of one year as from the communication, and the records concerning the failed calls shall be retained for a period of three months.

(2) Personal data, which is the subject-matter of the investigation, review, inspection or dispute, shall be retained until the related process is completed.

(3) The procedure records concerning the access to personal data or other related systems shall be retained for a period of four years."

3. Provisions Regarding the Protection of Personal Data

93. Article 28, entitled "Exceptions", of the "Law no. 6698 on the Protection of Personal Data" , which was enacted to protect fundamental rights and freedoms of individuals, particularly the right to privacy, with regard to the processing of personal data, and to regulate the obligations of natural and legal persons processing personal data, and the procedures and principles which shall be binding upon them, provides as follows[11]:

"Exceptions

ARTICLE 28-(1) The provisions of this Law shall not be applicable in the following circumstances:

(...)

ç) processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organisations duly authorised and assigned by law to maintain national defence, national security, public safety, public order or economic security."

4. Provisions Regarding Action for Compensation

94. Article 24, entitled "Basic Principle", of the Turkish Civil Code (Law no. 4721) dated 22 November 2001 reads as follows:

[11] https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1&MevzuatTertip=5

"Any person subject to an unlawful attack on his/her personal rights may claim protection from the judge against the individuals who made the attack.

Any such attack against personality rights shall be deemed unlawful, unless it is justified by the consent given by the person, whose personality rights were infringed, by a superior private or public interest, or by the use of power conferred by the law."

95. Relevant part of Article 25 , entitled "Lawsuits", of the Law no. 4721 provides as follows:

"The claimant may request the judge to order prevention the threat of attack, termination the ongoing attack, and the establishment of the unlawfulness of the attack whose effects still remain even though it has ended.

In addition, the claimant may also request publication or notification of the text of correction or the decision to the third parties.

The right of the claimant to claim compensation for pecuniary and non-pecuniary damage and to request that the gains obtained by way of the publication be paid to him/her under the provisions on acting without authority shall be reserved."

Claim for compensation of non-pecuniary damage shall not be transferred unless it is accepted by the other party; also, it shall not be transferred to the heirs by way inheritance unless it is expressly declared by the testator.

The claimant may file an action before the court located at the place of his/her residence or at the place of the defendant's residence for the protection of his/her rights.

96. Article 58, entitled "Damage to personality rights", of the Turkish Code of Obligations (Law no. 6098) provides as follows :

"Damage to personality rights

ARTICLE 58 - Any person, who alleges that his personality rights have been unlawfully damaged, may claim compensation for non-pecuniary damage. The judge may decide that another form of remedy should be used instead of payment of this damage or should be ordered in addition to this payment; especially the judge may render a condemning decision and may rule that this decision be promulgated."

97. Article 12, titled "Actions for annulment and full remedy actions", of the Code of Administrative Procedure (Law no. 2577) provides as follows:

"Actions for annulment and full remedy actions:

Article 12 – Those who sustain damage as a result of an administrative act may directly

bring an action for a full remedy or a joint action for annulment and full remedy

before the Supreme Administrative Court or Administrative and Tax Courts.

They may also first bring an action for annulment and then, upon its conclusion, bring an action for a full remedy, within the required time-limits, as from the

> ***notification of the judgment delivered in the action for annulment or the judgment to be delivered after the possible use of any judicial remedies in this regard. A full remedy action for the damages resulting from the execution of an act may also be brought in due time as from the execution of such act." In that case, the rights of the concerned persons to lodge an application with the administration in accordance with Article 11 shall be reserved."***

98. To avoid repetition, the Government would like to state that the other domestic provisions that are the subject matter of the applications in question are incorporated into the Government's observations and respectfully invites the Court to take into account the other domestic law provisions contained in the Government's observations.

B) Relevant Practices of the Constitutional Court

99. The Government would like to draw the Court's attention to a recent decision of the Constitutional Court, which set forth the domestic remedies that must be exhausted in regard to the complaints similar to those of the applicants. In its decision on the individual application of *Ertan Erçıktı,* dated 30 June 2021, filed with the same complaint as that of the applicants in the present application, the Constitutional Court held that the domestic remedy that must be exhausted prior to lodging an individual application before it was the remedy of compensation before the administrative courts or civil courts (see the decision of *Ertan Erçıktı (3),* no. 2018/14040, 30 June 2021[12]).

100. The Government would like to state that the Constitutional Court underlined in the said decision that the legal remedy exhausted prior to lodging an individual application before it must be a remedy having a prospect of success in line with the applicant's aim. In this connection, the Constitutional Court noted that the failure to destroy the internet traffic data within the scope of personal data at the end of the time-limit set out in the legislation and its unlawful use were acts against the personal rights in the circumstances of the present case. The Constitutional Court found that it was possible for those allegedly sustained damage due to the impairment of their personal rights as a result of this situation to have recourse to the remedy of compensation in accordance with the relevant legislation (see *Ertan Erçıktı (3)*, §§ 47-48).

---

[12]https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/14040?BasvuruAdi=ertan+er%C3%A7%C4%B1kt%C4%B1

101. The Constitutional Court pointed out that it was possible for the administrative and civil courts to conduct an inquiry into the alleged unlawfulness of the acts carried out in respect of the applicant and the alleged violation of his right to protection of personal data and thus, into the merits of the complaint, and to find any unlawfulness and violation of right (if any). Moreover, the Constitutional Court drew attention to the fact that in the event of the finding of an unlawful act, compensation for non-pecuniary damages might be awarded in order to redress the personal damages. In addition, the Constitutional Court noted that unlike the criminal proceedings, both individual and institutional liability might be relied on in the remedy of compensation, and that within the framework of general provisions, additional redress and measure might be ordered by the judge, along with the compensation for the violation of a right established. In the light of these findings, the Constitutional Court held that there was an effective legal remedy before the civil and administrative courts in regard to the applicant's allegations (see *Ertan Erçıktı (3)*, §§52-54).

102. The Constitutional Court ruled that in the context of finding a violation of the right to protection of personal data and providing a redress thereof, the actions for compensation were capable of offering more appropriate and reasonable prospect of success in line with the applicant's aim than the criminal proceedings. Furthermore, the Constitutional Court stated that the applicant did not raise an allegation, on the basis of concrete data, that the remedy of compensation was not an effective legal remedy. In this case, in view of the applicant's allegations of violation, the Constitutional Court concluded that the examination of the application filed without having exhausted the remedy of compensation-which appeared to be *prima facie* accessible and capable of offering prospect of success and providing sufficient redress in respect of the allegations of violation-would not be compatible with the subsidiary nature of the individual application, and declared the individual application inadmissible.

III. THE SUBJECT MATTER OF THE CASE

103. The subject matter of the case as drawn up by the Registry of the Court is as follows:

"Les requêtes concernent le rejet des plaintes pénales initiées par les requérants contre l'Autorité des technologies de communication et d'information (« Bilgi Teknolojileri ve Iletişim Kurulu », « BTK ») et certains fournisseurs d'accès à Internet pour avoir communiqué, au cours de leur procès pénal pour appartenance à une organisation terroriste, des données de trafic Internet (tels qu'informations GPRS de connexion Internet, adresses IP, données de communications etc.), conservés selon eux au-delà des délais légaux prescrits pour ce faire.

Invoquant l'article 8 de la Convention, les requérants allèguent que la conservation de telles données au-delà des délais légaux prescrits à cet égard et la publicité faite de ces données par le biais de leur communication au cours de leur procès pénal a porté atteinte à leur droit au respect de la vie privée. Se fondant sur l'article 13 de la Convention, ils allèguent avoir été privé d'une voie de recours effective."

IV. THE LAW

104. The Turkish Government has been asked to address the following questions:

Concernant toutes les requêtes:

1. Les requérants ont-t-il épuisé les voies de recours internes, comme l'exige l'article 35 § 1 de la Convention?

En particulier, le recours initié devant le procureur de la République constituait-il un recours effectif au sens de cette disposition pour le grief fondé par les requérants sur l'article 8 de la Convention?

Au vu des décisions de la Cour constitutionnelle ayant conclu dans certaines des présentes affaires au non-épuisement des recours disponibles, faute pour les requérants d'avoir saisi les instances administratives et/ou judiciaires, le Gouvernement est invité à apporter des précisions sur ces recours et à étayer leur effectivité par des exemples concrets.

2. À supposer que les voies recours internes aient été épuisées, la conservation par l'Autorité des technologies de communication et d'information (« BTK ») et/ou des fournisseurs d'accès à internet des informations relatives aux données liées au trafic Internet des requérants et leur communication au cours des procédures pénales initiées à leur encontre, peuvent-elles s'entendre comme étant constitutive d'une ingérence dans leur droit au respect de la vie privée, au sens de l'article 8 § 1 de la Convention (Benedik c. Slovénie, no 62357/14, §§ 100-106 et 117-118, 24 avril 2018)?

Dans l'affirmative, cette ingérence était-elle prévue par la loi et nécessaire au sens de l'article 8 § 2 de la Convention ?

3. Quels sont les conditions et délais de conservation des données de trafic Internet tant par les fournisseurs d'accès à Internet que par le BTK en vertu du droit interne pertinent? Ceux-ci satisfont-ils aux exigences de garanties procédurales adéquates et suffisantes ?

Concernant les requêtes nos 42883/19, 16165/20, 16296/20, 22308/20, 23143/20 et 34236/20

> *4. Les requérants avaient-ils à leur disposition, comme l'exige l'article 13 de la Convention, un recours interne effectif au travers duquel ils auraient pu faire valoir leurs griefs tirés de la méconnaissance de l'article 8 de la Convention ?*

In this regard, the observations of the Government concerning the above-mentioned questions are as follows:

ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

A. Preliminary Objection

1. Absence of a Represantative

105. First of all, the Government would like to underline that the Rule 36 §§ 2 and 4 (a) of the Rules of the Court, provides in so far as relevant:

> *"... Following notification of the application to the respondent Contracting Party under Rule 54 § 2 (b), the applicant should be represented in accordance with paragraph 4 of this Rule, unless the President of the Chamber decides otherwise.*
>
> *... 4. (a) The representative acting on behalf of the applicant pursuant to paragraphs 2 and 3 of this Rule shall be an advocate authorised to practise in any of the Contracting Parties and resident in the territory of one of them, or any other person approved by the President of the Chamber."*

106. When the applications form and its annexes are examined, it is observed that the applicants Sadık Yayla, Gökhan Yaman and Hüseyin Akbulut did not enclose any document showing that they are represented by a lawyer, and that among the documents communicated to the Government, there is no decision in which the Court authorised above mentioned applicants to pursue their own cases.

107. Regarding the abovementioned applicants' application considering Article 37 § 1 (c) of the Convention, the Government invites the Court to strike this case out of its list of cases as it is clear that it is no longer justified to continue the examination of the above metioned applications. (see *Grimaylo v Ukraine*, no. 69364/01, 7 February 2006)

2. Admissibility

a. Non-exhaustion of Domestic Remedies

108. The Court asked the Government whether domestic remedies had been exhausted in respect of the present applications and also requested from the Government to demonstrate the effectiveness of the domestic remedies in question. In this context, the Government has been invited to address the following question:

> ***"Les requérants ont-t-il épuisé les voies de recours internes, comme l'exige l'article 35 § 1 de la Convention?***
>
> ***En particulier, le recours initié devant le procureur de la République constituait-il un recours effectif au sens de cette disposition pour le grief fondé par les requérants sur l'article 8 de la Convention ?***
>
> ***Au vu des décisions de la Cour constitutionnelle ayant conclu dans certaines des présentes affaires au non-épuisement des recours disponibles, faute pour les requérants d'avoir saisi les instances administratives et/ou judiciaires, le Gouvernement est invité à apporter des précisions sur ces recours et à étayer leur effectivité par des exemples concrets.***
>
> ***Les requérants avaient-ils à leur disposition, comme l'exige l'article 13 de la Convention, un recours interne effectif au travers duquel ils auraient pu faire valoir leurs griefs tirés de la méconnaissance de l'article 8 de la Convention ? ".***

109. In the light of its explanations below, the Government would like to point out that the applicants had lodged the present applications before the Court without exhausting domestic remedies.

i. Non-exhaustion of the Remedies of Action for Compensation before Administrative Courts and Civil Courts

110. In the present applications, the applicants, Metin Çamurşen, Serkan Uslu, Sadık Yayla, Hüseyin Akbulut, Gökhan Yaman, Duran Denizci and Hüsmen Koçak, complain that the CGNAT data was requested from the BTK, in the course of the ongoing proceedings against them on various charges related to the FETÖ/PDY armed terrorist organisation, in order to establish whether they had connected to the Bylock application. The applicants allege that the BTK and the access providers retained the said data for a period longer than the time-limit prescribed in the legislation. In the framework of these allegations, the applicants filed criminal complaints with various Chief Public Prosecutor's Offices.

Following the decision of non-prosecution as a result of the criminal complaints, the applicants lodged an individual application before the Constitutional Court. After the Constitutional Court had rendered inadmissibility decisions, the applicants filed the present applications with the Court. In this scope, the Government would like to point out that the applicants, with the exception of Hüsmen Koçak, had only exhausted the remedy of criminal investigation before filing the present applications.

111. Hükümet ilk olarak BTK'nın Devlet idari teşkilatı içerisinde kalan bir kamu tüzel kişisi olduğunu belirtmek ister. Bu nedenle de BTK'nın gerçekleştridiği her türlü işlem idari işlem niteliğindedir. Bu sebeple BTK'nın herhangi bir idari bir işleminden zarar gören kişiler, bu işleme karşı idare mahkemeleri önünde iptal davası açarak işleme son verilmesini isteyebileceği gibi, yine idare mahkemeleri önünde tam yargı davası açarak işlemden ötürü uğradığı zararın giderilmesini isteyebilir. Ancak Hükümet başvuranların erişilebilir ve başarı imkanı sunan idare mahkemeleri önündeki dava yollarını tüketmeden Mahkeme önündeki mevcut başvurları gerçekletirmiş olduklarını belirtmek ister.

1. Action for Annulment and Full Remedy Before the Administrative Judiciary

112. The Government would like to point out at the outset that ICTA is a public legal personality within the administrative structure. For this reason, a person who has been damaged by an administrative act carried out by the ICTA may file an action for annulment against this act and request the termination of the act in question. Similarly, this person may request the compensation of the damage caused by the act by means of filing a full remedy action. However, the Government would like to state that the applicants had lodged the present applications with the Court without exhausting this domestic remedy available to them.

113. In this scope, the Government, at the outset, would like to draw the Court's attention to the following information on the duties of the BTK and its position within the State administration:

114. In Article 1 of the Law no. 5397 Amending Certain Laws, it was indicated that the measures of interception of communication regulated in Article 135 of the Law no.5271 shall be carried from a single centre by the Presidency of Telecommunication and Communication (TİB). In accordance with the provisions of the State of Emergency Decree-law no. 671, the TİB was closed and all its powers were transferred to the BTK. For this reason, the BTK is tasked with implementing the measures of interception of communication regulated in Article 135 of the Law no. 5271 from a single centre.

115. The BTK has a public legal personality, and administrative and financial autonomy. Therefore, the applicants' complaint directly concerns an act and activity falling within the field of duty of a public law legal entity. The remedy which the applicants-who allegedly suffered damage due to the activity of a public law legal entity-was to bring an action for annulment or full-remedy action before the administrative judiciary against the administration (i.e. against the relevant public institution). However, there is no information or document in the application forms or annexes thereto indicating that they brought a annulment or full remedy action before the administrative judiciary.

116. Article 125 of the Constitution stipulates that recourse to judicial review shall be available against all actions and acts of the administration and the last paragraph of the said article sets forth that the administration shall be liable to compensate for damages resulting from its own actions and acts. In addition, Article 129 of the Constitution provides that compensation suits concerning damages arising from faults committed by public servants and other public officials in the exercise of their duties shall be filed only against the administration in accordance with the procedure and conditions prescribed by law, as long as the compensation is recoursed to them.

117. The applicants, who allege that the act of the ICTA, which is a body within the administrative structure, violated their right to respect for private life, if this process is still continuous, should have filed action for annulment before administrative courts in accordance with Article 12 of the Code of Administrative Procedure (Law No. 2577) in the first place. After the filing of such an action, the applicants would be able to file a full remedy action for the

compensation of the damage they claimed to have suffered, or they would also be able to file a full remedy action for the compensation of the damages, depending on the outcome of the action for annulment.

118. Following this information, the Government would like to draw the Court's attention to the information below as to the fact that the remedy ofannulment or full remedy action before the administrative courts, to which the applicants should have had recourse as regards their complaints, is accessible and capable of providing redress in the context of Article 13 of the Convention.

119. In the present application, in the proceedings conducted against the applicants for the offences of membership of a terrorist organization or of attempting to overthrow the constitutional order, the BTK was asked whether the applicants' mobile phone numbers had connected to the IP addresses established to belong to the Bylock communication application, and in this scope, the CGNAT data of the applicants were requested. The BTK considered that the requests in question qualified as a measure of interception of communication ordered under Article 135 of the Law no. 5271. Accordingly, the BTK, which is tasked with implementing measures of interception of communication ordered under Article 135 of the Law no. 5271 from a single centre, performed its legal duty and sent the said data only to the relevant courts which requested it. Therefore, the applicants' complaint is not related to the misuse or abuse of duty by a certain public official, but to the BTK's fulfilment of its legal duty.

120. In this connection, the applicants, who allegedly had suffered damage due to an administrative act, had the opportunity to bring a full remedy action before the administrative judiciary and thus, to have their alleged damages redressed in accordance with Article 125 of the Constitution. In other words, the most effective remedy which was capable of inquiring whether the applicants' internet traffic data were retained for a period longer than the time-limits set out in the legislation, and if so, of redressing the pecuniary and non-pecuniary damage arising from this act was the full remedy action to be brought before the administrative courts against the BTK. However, there is no information or document in the application form or its annexes thereto showing that the applicants exhausted this remedy.

121. The applicants also have the opportunity to lodge an individual application before the Constitutional Court after having exhausted the remedy of administrative judiciary if they consider that their damages have not been redressed. At this juncture, the Government would like to note that the decisions of the Constitutional Court on the individual applications filed by the applicants after having exhausted the remedy of criminal investigation will not prevent them from filing a new individual application after having exhausted the remedy of administrative judiciary.

122. If the applicants bring a full remedy action, the administrative courts will be able to review the administrative act carried out by the BTK in terms of legality and power. Accordingly, the administrative courts will be able to establish whether the applicants have sustained any damage and also award compensation to the applicants. The applicants, in any case, have the opportunity to have it determined whether the act of the BTK has constituted a violation of any right by lodging an individual application with the Constitutional Court against the decisions of the administrative courts.

123. **At this point, in order to demonstrate that the remedy of bringing a full remedy action is an effective remedy capable of offering prospect of success in regard to the applicants' complaint, the Government would like to draw the Court's attention to the decisions of the administrative courts in the full remedy actions brought before the administrative courts** (see Annex 25). In those actions, the administrative courts directly examined the administrative acts of the BTK. Moreover, the administrative courts also discussed whether the acts (the alleged retention of the CGNAT data for a period longer than the time-limit prescribed in the legislation)-which also gave rise to the present application- carried out by the BTK constituted a service fault. The Government would like to bring to the attention of the Court the 8 different full remedy action cases, which were filed with the allegation that the ICTA stored internet traffic information longer than the statutory time limitations stipulated in the legislation, and were examined on the merits and adjudicated by the administrative courts. The decisions in question demonstrate that the remedies before the administrative courts

constitute an effective domestic remedy with a prospect of success in respect of the applicants' complaints (see Annex 25).

124. In addition, the Government would like to submit to the Court's attention to the Constitutional Court's decision of *Ertan Erçıktı(3)* concerning a similar complaint[13] (see §§ 99-102 above).In its decision of *Ertan Erçıktı(3),* the Constitutional Court examined the alleged retention of the CGNAT data by the BTK and access providers for a period longer than the time-limits prescribed in the legislation in the context of Article 8 of the Convention.

125. The Constitutional Court pointed out that within the scope of compensation proceedings, the administrative courts and civil courts might establish whether there had been a violation of right by examining the said complaint on the merits. Therefore, the Constitutional Court held that the actions for compensation were capable of offering a more appropriate and reasonable prospect of success in line with the applicant's aim, as compared to the criminal proceedings. In view of the applicant's allegations of violation, the Constitutional Court concluded that the examination of the application filed without having exhausted the remedy of compensation-which appeared to be *prima facie* accessible and capable of offering prospect of success and providing sufficient redress in respect of the allegations of violation- would not be compatible with the subsidiary nature of the individual application, and declared the individual application inadmissible (see *Erkan Erçıktı (3)*, §§ 52-54).

126. For these reasons, the Government invites the Court to declare the present applications inadmissible for non-exhaustion of domestic remedies within the meaning of Article 35 §§ 1 and 4 of the Convention.

2. Action for Compensation Before Civil Courts

127. The applicants also filed a criminal complaint against the access provider companies, along with the BTK, with the same complaint. In the light of its explanations above, the Government would like to state that with regard to the access provider companies, the effective remedy is not the remedy of criminal investigation, but of action for compensation before the civil courts.

[13] https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/14040?BasvuruAdi=ertan

128. Indeed, the obtainment of the CGNAT records directly from the access provider companies was not the case here. Despite the foregoing, the applicants filed criminal complaints against the access provider companies, which were private law legal entities. It was possible for the applicants to have recourse to the remedy of bringing an action for compensation before the civil courts with regard to their allegations that the access provider companies, which were private law legal entities, had unlawfully retained data. In that case, the civil courts would have the opportunity to examine the fault and strict liability status of the said companies within the scope of the provisions of tortious act. If the civil courts deemed it necessary, they might also award compensation to the applicants in order to redress their alleged damages.

129. Under the Articles 24 and 25 of the Turkish Civil Code (Law no. 4721) and Article 58 of the Code of Obligations (Law no. 6098) apart from actions of pecuniary and non-pecuniary compensation to be brought by those whose personal rights were attacked against the offenders within the meaning of civil law, it is also provided that they may file a request for prevention of attack risk, termination of on-going attack and finding of unlawfulness of the attack the effects of which were on-going even if it ended. It is also stipulated that the victim may file a request for notification of the correction or decision to the third parties or its publication(see §§ 94-97 above).

130. The Government would like to point out that the remedy of compensation in question was also exhausted by other persons with the same complaint as the applicants, and that the civil court carried out an examination, on the merits, in respect of the lawfulness of the impugned act (see Annex 26). Accordingly, with regard to the finalized case-files before the civil courts, plaintiffs always have the opportunity to file an individual application with the Constitutional Court. In the present applications, the applicants have not submitted any information or document that they exhausted the remedy of compensation before the civil courts in respect of their complaints against access providers and then exhausted the individual application remedy before the Constitutional Court. In this context, the Government would like to reiterate that the effective remedy for the alleged retention by the access providers of the internet traffic data for a period longer than the time-limits stipulated in the

legislation is not the remedy of criminal investigation, but of action for compensation before the civil courts.

131. The Government would also like to recall that the findings of the Constitutional Court in the application of Ertan Erçıktı (3) may also be applied to existing applications with regard to complaints against access providers (see §§ 99-102 above).Having also regard to the fact that the complaint is the same in terms of the present applications, the Government considers that there are no circumstances requiring departure from the above-mentioned acceptances of the Constitutional Court in regard to the determination of effective remedies. For these reasons, the Government invites the Court to declare the present applications inadmissible for non-exhaustion of domestic remedies within the meaning of Article 35 §§ 1 and 4 of the Convention.

3. Non-Exhaustion of the Remedy of Individual Application after the Delivery of the Decision of the Administrative Court in the Application no. 16165/20

132. Another point the Government would like to indicate under this heading is that the applicant Hüsmen Koçak in the application no. 16165/20 brought a full remedy action before administrative courts regarding his complaint (see § 74-84 above).

133. On 18 June 2019 the applicant Hüsmen Koçak brought a full remedy action before the Ankara 2nd Administrative Court in relation to his complaint giving rise to his application. By its decision of 19 December 2019, the Ankara 2nd Administrative Court dismissed the action. The applicant Hüsmen Koçak filed an appeal on points of facts and law (*istinaf*) against the relevant decision. Having examined the relevant appeal, on 30 December 2020 the 7th Administrative Chamber of the Ankara Regional Administrative Court definitively dismissed the applicant's appeal on points of facts and law (see § 84 above).

134. The Government considers that the applicant Hüsmen Koçak's recourse to the administrative law remedy shows that he implicitly accepted the effectiveness of this remedy. The applicant lodged the present application with the Court before the conclusion of the administrative law remedy, the

effectiveness of which was accepted by the applicant. Moreover, in his application form or its annexes, the applicant did not provide any information that he had resorted to this remedy.

135. The applicant Hüsmen Koçak had the opportunity to lodge a new individual application with the Constitutional Court in relation to his complaint after the delivery of the Ankara Regional Administrative Court's decision dated 30 December 2020. However, in the application form or its annexes, the applicant did not submit any document showing that he had lodged an individual application. Accordingly, it is considered that even though the applicant Hüsmen Koçak brought an action before the administrative court, he did not lodge an individual application with the Constitutional Court, thereby failing to duly exhaust this effective remedy.

136. For these reasons, the Government invites the Court to declare the above mentioned application inadmissible for non-exhaustion of domestic remedies within the meaning of Article 35 §§ 1 and 4 of the Convention.

ii. The failure of the applicant Gökhan Yaman in the application no. 22308/20 to raise his present complaints during his trial before the Assize Court

137. The Government would like to state that the applicant Gökhan Yaman never raised his complaint about the retention of internet data for a period longer than the statutory time-limit, during the criminal proceedings in which this data was requested. During the criminal proceedings, the applicant never alleged that retention of the data in question for a period longer than the statutory time-limit had constituted a violation of the right to respect for private life under Article 8 of the Convention and Article 20 of the Constitution, and he therefore did not give an opportunity to the Assize Court to carry out such an assessment. In this context, the Government is of the view that the applicant lodged the present application without exhausting an effective domestic remedy. In this regard, the Government would like to provide the following observations in respect of non-exhaustion of domestic remedies by the applicant:

138. The applicant had not alleged at any stage of the proceedings before the Assize Court even indirectly or in abstract terms any infringement

whatsoever of the right to respect for private and family life. The courts of instance have the power to evaluate the legality of the evidence in criminal proceedings. Therefore, the applicant, who has alleged that the BTK was requested to submit the CGNAT data for use as evidence in criminal proceedings violated his right to respect for private life, should have raised this allegation also before the courts of instance. Thus, the courts of instance would have had the opportunity to examine the nature of the relevant evidence and whether the retention of the CGNAT records constituted a breach of a right. However, since the applicant did not duly exhaust this remedy, the courts of instance were unable to carry out an assessment as regards the CGNAT data.

139. Therefore, as the applicant failed to raise before the national courts, even in substance, the complaint relating to a violation of Article 8 of the Convention or Article 20 of the Constitution, the Government kindly invites the Court to declare the abovementioned application inadmissible for non-exhaustion of domestic remedies.

iii. As regards the fact that the complaints raised in applications nos. 23143/20, 44197/19 and 34236/20 concern the ongoing domestic proceedings

140. The Government would like to reiterate once again that the applicants are entitled to raise their complaints, which constitute the subject-matter of the present application, in the ongoing criminal proceedings in domestic law, in the course of which the internet traffic data has been requested. The applicants Hüseyin Akbulut and Duran Denizci, against whom the criminal proceedings are ongoing, must first allege in the criminal proceedings against them that the retention of internet data by the BTK constituted a violation of Article 8 of the Convention and Article 20 of the Constitution. Accordingly, the courts of instance will become able to examine and assess the lawfulness of the relevant data. The Government reminds the Court that the remedy before the courts of instance is effective, and so as to avoid repetition, it would like to reiterate its explanations under the previous heading (see §§ 137-139 above).

141. In the light of the foregoing, the Government notes that as of the date when the applicants Hüseyin Akbulut, Duran Denizci and Serkan Uslu lodged an application with the Court, the proceedings, in the course of which the internet

traffic data giving rise to their complaints was requested, were still pending (see §§ 37-43 / 51-58 / 66-73 above).

142. A trial was conducted against the applicant Hüseyin Akbulut in the case-file no. E. 2017/26 by the İstanbul 22nd Assize Court on the charge of membership of the FETÖ/PDY armed terrorist organisation, and the applicant was convicted of this offence. Following this decision, the applicant filed an appeal on points of facts and law, which was dismissed on the merits by the İstanbul Regional Court of Appeal. The applicant subsequently filed an appeal against this decision. Having examined the applicant's appeal, on 2 July 2020 the 16th Criminal Chamber of the Court of Cassation quashed the decision of the first-instance court and sent the case-file back to the İstanbul 22nd Assize Court. As of the date of the preparation of the Government's observations, the criminal proceedings against the applicant are still pending in the case-file no. E. 2020/419 before the İstanbul 22nd Assize Court.

143. Criminal proceedings were brought against the applicant Duran Denizci before the İstanbul 14th Assize Court for attempting to overthrow the constitutional order. The İstanbul 14th Assize Court decided to sentence the applicant to aggravated life imprisonment for the offence in question. Following this decision, the applicant filed an appeal on points of facts and law, which was dismissed on the merits by the İstanbul Regional Court of Appeal. The applicant filed an appeal against the decision of the Regional Court of Appeal. As of the date of preparation of the Government's observations, the applicant's case-file is still pending before the Court of Cassation.

144. A trial was conducted against the applicant Serkan Uslu in the case-file no. E. 2017/34 by the Edirne 2nd Assize Court on the charge of membership of the FETÖ/PDY armed terrorist organisation, and the applicant was convicted of this offence. The applicant's conviction was upheld by the Court of Cassation and became final on 23 February 2021. However, the applicant lodged his present application with the Court on 17 July 2020 when the criminal proceedings against him were still pending. Therefore, the Government is of the view that the applicant Serkan Uslu lodged the present application with the Court

while he still had the opportunity to raise his present complaints before the domestic criminal court.

145. In this regard, the Government considers that in respect of all three applicants, the complaint giving rise to the present application should have been first raised in the pending criminal case-files. Since there are pending criminal case-files against the applicants, they also have the opportunity to raise their complaints before the courts of instance. In this respect, in accordance with the principle of subsidiarity, the applicants should have submitted their complaints to the domestic courts of instance before submitting them to an international court.

146. For these reasons, the Government invites the Court to declare inadmissible the applications of all three applicants within the meaning of Article 35 § 1 of the Convention on the grounds that the criminal proceedings are still pending in respect of the applicants Hüseyin Akbulut and Duran Denizci and the criminal proceedings were pending as of the date of introduction of the application in respect of the applicant Serkan Uslu.

b. Abuse of the right of application in respect of the application no. 16165/20

147. The Government is of the opinion that recourse to the administrative law remedy is of great importance in respect of the present application, especially for the redress of the damage alleged by the applicant. Indeed, on 18 June 2019 the applicant Hüsmen Koçak brought a full remedy action before the Ankara 2nd Administrative Court in relation to his complaint giving rise to the present application. On 19 December 2019 the Administrative Court dismissed the action. The applicant filed an appeal on points of facts and law against this decision. Having examined the relevant appeal, on 30 December 2020 the 7th Administrative Chamber of the Ankara Regional Administrative Court dismissed on the merits the applicant's appeal on points of facts and law (see § 82-84 above). Accordingly, the full remedy action brought by the applicant before the administrative court became final. The applicant had the opportunity to file an individual application with the Constitutional Court against this decision. However, the applicant did not file any information or document showing that he lodged an application with the Constitutional against the relevant decision.

148. The applicant lodged the present application before the Court on 19 March 2020, when the above-mentioned full remedy action before the administrative court was ongoing. Nonetheless, in his application form or its annexes, the applicant did not mention the existence of the relevant full remedy action he had brought or the stage reached in the relevant action.

149. If new, important developments occur during the proceedings before the Court and if - despite the express obligation on him or her under the Rules of Court - the applicant fails to disclose that information to the Court, thereby preventing it from ruling on the case in full knowledge of the facts, his or her application may be rejected as being an abuse of application (see Predescu v. Romania, no. 21447/03, §§ 25-27, 2 December 2008; Gross v. Switzerland [GC], §§ 28-37).It is therefore considered that the applicant abused his right to individual application on account of the fact that he did not inform the Court about a matter of importance to the clarification of the remedies he exhausted in domestic law and the effectiveness of these remedies.

150. In the light of these explanations, the Government invites the Court to declare inadmissible the application no. 16165/20 on the ground of abuse of the right of application.

3. Merits

151. The Court asked the Government the following questions on the merits of the present applications;

> ***"2. À supposer que les voies recours internes aient été épuisées, la conservation par l'Autorité des technologies de communication et d'information (« BTK ») et/ou des fournisseurs d'accès à internet des informations relatives aux données liées au trafic Internet des requérants et leur communication au cours des procédures pénales initiées à leur encontre, peuvent-elles s'entendre comme étant constitutive d'une ingérence dans leur droit au respect de la vie privée, au sens de l'article 8 § 1 de la Convention (Benedik c. Slovénie, no 62357/14, §§ 100-106 et 117-118, 24 avril 2018)?***
>
> ***Dans l'affirmative, cette ingérence était-elle prévue par la loi et nécessaire au sens de l'article 8 § 2 de la Convention?***
>
> ***3. Quels sont les conditions et délais de conservation des données de trafic Internet tant par les fournisseurs d'accès à Internet que par le BTK en vertu du droit interne pertinent? Ceux-ci satisfont-ils aux exigences de garanties procédurales adéquates et suffisantes?"***

152. First of all, the Government invites the Court to declare the present applications inadmissible, in the light of its admissibility objections above(see §§ 108-150 above).Where the Court rejects these objections, the Government submits to the Court the following observations in relation to the above-cited questions.

a. As regards the lack of interference

153. The Government indicates at the outset that there has been no interference with the applicants' right to respect for private life or their freedom of communication.

154. Indeed, as indicated above (see §§ 27-29 above), the ByLock was an application provided for the exclusive use of the members of the FETÖ/PDY since the beginning of 2014, when it started to be used for the first time. The members of the organisation used this application from the very beginning in order to conceal their identities and ensure organisational communication. In this context, the judicial authorities requested the BTK to submit the CGNAT data to determine whether the applicants were users of this application. However, it is out of the question that the applicants' correspondence exchanged with other persons was interfered with. Nor were the conversations made or messages exchanged between the applicants and other persons in the past retained or shared by the BTK with judicial authorities. In other words, the interception of communication under the Law no. 5271 was not an activity targeting the applicants' communications or disclosing them to judicial institutions or other persons.

155. In parallel with the above-mentioned assessment, the CGNAT data was not obtained from the applicants themselves or their computers, computer software or computer files. The CGNAT data did not contain the applicant's correspondence falling within the scope of their private life, but contained information showing that whether they had connected to IP addresses of the ByLock server. Accordingly, the applicants' communications were not directly the subject of a measure.

156. Furthermore, the applicants' actual complaint is not about an alleged interference with their private lives due to the obtaining and processing of this

data. The applicants complain about the retention of the CGNAT data for a period longer than the time-limit prescribed in the legislation.

157. For these reasons, the Government invites the Court not to make an examination under Article 8 of the Convention since there has not been any interference with the applicants' right to respect for private life. Where the Court considers otherwise, the Government would like to draw the Court's attention to the following observations:

b. As regards the alleged retention of the CGNAT data beyond the time-limits prescribed in the law

158. In their application forms and their annexes, the applicants allege that the CGNAT data was retained for a period longer than the time-limits laid down in Article 6 of the Law no. 5651 and Article 8 of the Regulation on the Procedures and Principles Regulating the Publications on the Internet.

159. At this point, the Government first notes that the allegation that the access providers retained the applicants' internet traffic data for a period longer than the time-limit lacks any factual basis. Indeed, in the present case, the judicial authorities requested the internet traffic data not from the access providers, but from the BTK under Article 135 of the Law no. 5271. Therefore, there is nothing that requires the examination of the allegation that the internet traffic data pertaining to the applicants was retained by the access providers for a period longer than the prescribed time-limit. Besides, access providers do not comply with the requests relating to internet traffic information that are directly submitted to them by the courts. As regards the allegation that the internet traffic information was retained by the BTK for a period longer than the time-limit prescribed in the legislation, the Government would like to submit the following observations to the Court.

160. The Law no. 5651 on Regulation of Publications on the Internet and Fight against Offences Committed by means of such Publication[14] (the Law no. 5651) was adopted on 4 May 2017 and entered into force upon its publication in the Official Gazette dated 23 May 2007.

[14] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

161. Article 1 of the Law no. 5651 governs the aim of this Law, which reads as follows:

> "*The aim and scope of this Law is to regulate the responsibilities and liabilities of content providers, hosting providers, access providers and mass use providers, and the principles and procedures applicable to efforts to fight, through the content, hosting and access providers, against certain offences committed in the internet environment.*"

162. As is seen, the relevant Law was introduced to regulate the obligations and responsibilities of "content providers, hosting providers, access providers and mass use providers".

163. Article 2 of the same Law contains definitions, the relevant part of which reads as follows: "*Access provider shall refer to natural or legal persons providing its users with a means of access to Internet*".

164. Article 3 of the Law no. 5651 concerns the obligation to make a notification and provides that content, hosting and access providers are obliged to present their contact details on the Internet site in such a manner as to enable users to access them.

165. Article 4 of the Law no. 5651 governs the obligations of content providers and Article 5 governs the obligations of hosting providers.

166. Article 6 § 1 (b) of the Law no. 5651 governs the obligations of access providers. The relevant part of this Article reads as follows:

> "*ARTICLE 6 - (1) The Access Provider shall be responsible for:*
>
> *(...)*
>
> *(b) Retaining traffic information concerning the services it provides, as specified by regulations, for a period of not less than six months and not more than two years, as shall be determined by regulation, and ensuring the accuracy, integrity and confidentiality of that information.*

167. As is seen, Article 6 of the Law no. 5651 governs the obligations of access providers and specifies how long the access providers should retain the internet traffic information. Accordingly, the access providers are required to retain the internet traffic data for a determined period between 6 months and 2 years. The relevant Article also states that the exact period is determined by the Regulation.

168. In this regard, in the "Regulation on the Procedures and Principles Regulating the Publications on the Internet", which was issued on the basis of the Law no. 5651 dated 4 May 2007, the obligations and responsibilities of content, hosting and access providers as well as the principles and procedures regarding the fight against certain offences committed on the Internet through the content, hosting and access providers have been regulated.

169. Article 8 § 1 (b), entitled "Obligations of access providers", of this Regulation introduced on the basis of the Law no. 5651 reads as follows: "***The access provider shall be obliged to retain the traffic information for a period of one year****, to preserve, with a time stamp, the accuracy, integrity and file integrity values of the data created as well as to ensure its confidentiality,* ***so that the Presidency [of Telecommunication and Communication] could perform its duties entrusted by the Law and other related legislation*** *regarding the services it provides.*"

170. As can be understood from the purpose and systematic of the Law no. 5651 and the relevant Regulation as well as from the titles of Articles of the Law no. 5651, the Law no. 5651 and the relevant Regulation apply solely to the *hosting providers, access providers and content providers* acting in accordance with the provisions of private law and governs their rights and obligations. Accordingly, the access providers have been placed under an obligation to retain the internet traffic data for a period of one year. Thus, it is clear that the relevant articles of the Law no. 5651 prescribe a time-limit not as regards the BTK, which is a public institution, but as regards access provides established and operating in accordance with the provisions of private law.

171. Access providers are legal persons which are not part of the administration but are subject to private law. In its decision on the individual application of *Ertan Erçıktı*, the Constitutional Court drew attention to this point and held that civil and administrative courts constituted an effective remedy which had to be exhausted as regards the allegations that the access providers had stored the data for a period of time longer than prescribed or that the BTK had sent the data to the judicial authorities despite the expiry of the prescribed time-limit. Having regard to the fact that the applicants' complaint also

concerned the storage of the CGNAT data for a period of time longer than prescribed, the Government considers that there is no reason to depart from the decision of the Constitutional Court.

172. In conclusion, the Government would like to state that the applicants did not raise any complaint about any lack of legal basis for the retention of internet traffic records. Nor did they make any complaint to the effect that it was not possible for the BTK to retain such data. Moreover, the applicants did not allege that the internet traffic records pertaining to them had been obtained without a court decision. The only complaint raised by the applicants concerns the fact that the data regarding them was retained for more than one year although the legislation stipulates that the internet traffic records can be retained for a maximum period of one year. However, as stated above, the one-year time-limit mentioned by the applicants is not for the BTK but for the access providers. The Government therefore notes that there was no unlawfulness in the relevant act, namely the submission of the CGNAT data pertaining to the applicants to the relevant courts by the BTK for use as evidence in criminal proceedings.

173. Accordingly, the Government invites the Court firstly to declare this complaint inadmissible or otherwise to hold that the relevant complaint is manifestly ill-founded since the statutory time-limit applies only to access providers.

c. As regards the allegation that the BTK unlawfully obtained and disclosed the CGNAT data (Internet traffic data)

174. In Article 135 of the Criminal Procedure Code numbered 527", the measure of "Interception, Wiretapping and Recording of Communications" is regulated. The relevant Article provides as follows:

> "*(1) (Amended on 21 February 2014 by Article 12 of the Law no. 6526) 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, during an investigation or prosecution conducted in relation to an offence, there is strong suspicion that the offence has been committed and there is no other means of obtaining evidence. The public prosecutor shall submit his or her decision immediately to the judge for an approval and the judge shall render a decision within 24 hours. Upon the expiry of this period or if the judge decides to the contrary, the measure shall be lifted by the public prosecutor immediately. (Last two sentences abolished on 24 November 2016 by Article 26 of the Law no. 6763)*

(2) (Added on 21 February 2014 by Article 12 of the Law no. 6526) Any such request shall be accompanied with the document or report indicating the owner, or if known, the user of the phone line or the means of communication in respect of which a measure is to be imposed in accordance with this article.

(3) The suspect's or accused person's communications with individuals who may refrain from acting as a witness shall not be recorded. In cases where this circumstance has been revealed after the recording, the recorded material shall be destroyed immediately.

(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 on 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. The decision to impose a measure shall be valid for a period of maximum two months and this period may be extended for an additional one month. (Additional sentence: (Added on 25 May 2005 by Article 17 of the Law no. 5353) However, for offences committed within the activities of an organisation, the judge may decide to extend the period several times, each time for no longer than one month and not exceeding three months in total, if deemed necessary.

(5) For the apprehension of the suspect or the accused person, (...) the location of a mobile phone may be established upon the decision of the judge or, in cases where a delay would be detrimental, by the decision of the public prosecutor. The decision related to this matter shall state (...) the number of the mobile phone and the duration of the locating process. The locating process shall be conducted for a period of maximum two months and this period may be extended for an additional one month.

(6) (Added on 2 December 2014 by Article 42 of the Law no. 6572) 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 on 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. (Additional sentences inserted on 24 November 2016 by Article 26 of the Law no. 6763) The public prosecutor shall submit his or her decision within 24 hours to the judge for an approval and the judge shall make a decision within maximum 24 hours. Upon the expiry of this period or if the judge decides to the contrary, the records shall be destroyed immediately.

(7) Decisions rendered and actions taken in accordance with the provisions of this article shall be kept confidential for the duration of the measure.

(8) The provisions contained in this article relating to the monitoring, recording and evaluation of signal information shall only be applicable to the offences listed below: a) The following offences set out in the Turkish Criminal Code; 15, (Amended on 2 December 2014 by Article 42 of the Law no. 6572) Disruption of the unity and territorial integrity of the State (Article 302), 16. (Added on 2 December 2014 by Article 42 of the Law no. 6572) Offences against the Constitutional order and its functioning (Articles 309, 311, 312, 313, 314, 315,

> *316), 17. Offences against State secrets and espionage (Articles 328, 329, 330, 331, 333, 334, 335, 336 and 337), ...*
>
> *(9) No one may monitor or record the electronic communications of another person except in accordance with the principles and procedures defined in this Article."*

175. In the immediate aftermath of the entry into force of the Law no. 5271, the Law no. 5397 amending different laws was adopted. Article 1 of this Law introduced new paragraphs to Additional Article 7 of the Law on the Duties and Powers of the Police (Law no. 2559). Article 1 § 9 of the Law no. 5397 stipulates that "*The practices specified in this article and the interceptions to be made within the scope of Article 135 of the Law no. 5271 shall be carried out from a single center established under the name of the "Presidency of Telecommunication and Communication", which is directly affiliated to the President of the Telecommunication Authority.*" Therefore, the Law no. 5397 provides that the procedures concerning the measure laid down in Article 135 of the Law no. 5271 should be carried out from a single centre to be established under the name of Presidency of Telecommunication and Communication.

176. In this regard, "*the Regulation on Procedures and Principles Concerning Interception and Wiretapping of Communications Made via Telecommunications and Assessment and Recording of Signal Information and on Establishment, Duties and Powers of the Presidency of Telecommunication and Communication ("the Regulation") governing establishment, duties and powers of the Presidency of Telecommunication and Communication*" was adopted.

177. Article 1 of the Regulation provides that the Regulation was introduced, *inter alia*, to determine the procedures and principles concerning interception and wiretapping of communications made via telecommunications and assessment and recording of signal information and to regulate the establishment, duties and powers of the Presidency of Telecommunication and Communication within the framework determined by Articles 135 to 138 of the Law no. 5271.

178. Article 3 of the Regulation describes an operator as "*a company which provides electronic communications services and/or provides electronic communications network and operates the infrastructure within the framework of*

authorisation."

179. In addition, the duties of the Presidency of Telecommunication and Communication are specified in Article 17 of the Regulation. Accordingly, the duties of the Presidency of Telecommunication and Communication read as follows:

> "(...)
>
> *b) to carry out from a single centre the acts and procedures concerning the interception, wiretapping and recording of communications and assessment of signal data to be carried out under Article 135 of the Law no. 5271,*
>
> *c) to examine whether the requests under sub-paragraphs (a) and (b) comply with this Regulation and other relevant legislation, and to apply to the competent authorities if necessary,*
>
> *d) to submit to courts and Chief Public Prosecutor's Offices the data and information (...) obtained as a result of the procedures carried out pursuant to sub-paragraphs (a) and (b), if they request,*
>
> *e) **(Amended by the Official Gazette no. 27312 and dated 7 August 2009)** to ensure that all kinds of technical infrastructure, which will enable the interception, wiretapping, assessment and recording of signal information to be carried out within the framework of this Regulation and the performance of the duties assigned by the Law no. 5651 and other legislation, are established by public institutions and organisations, public service organisations and operators, and to initiate procedures to punish the operators who do not establish the necessary infrastructure,*
>
> *f) **(Amended by the Official Gazette no.26572 and dated 4 July 2007)** to ensure that all kinds of information, documents and records received from public institutions and organisations, public service organisations and operators regarding the activities of the Presidency are archived in accordance with information security criteria, save for Article 12 § 2 and Article 15 § 3,*
>
> *(...)*

180. The Presidency of Telecommunication and Communication ("TİB") was closed down pursuant to Article 22 of the Decree Law no. 671 of 17 August 2016. Its duties and responsibilities were transferred to the Information Technologies and Communication Authority ("BTK"), and the references to the Presidency and President of Telecommunication and Communication included in the relevant legislation were deemed as having been made to the BTK. For this reason, in order not to cause confusion, the provisions regarding the TİB will hereinafter be referred to as "BTK".

181. As a result, the BTK, is obliged to carry out the procedures for the interception, wiretapping, assessment and recording of the signal information for

legal purposes within the scope of Article 135 of Law no. 5271, in a timely manner, completely and without causing any disruption, and to carry out all these operations from a single center. One of the duties that the BTK is obliged to perform in order for it to fulfil the aforementioned duty is to archive all kinds of information, documents and records provided from the operators, as specified in sub-paragraph (f) of Article 17 § 1 of the Regulation. In this way, the requirement of archiving all kinds of information, documents and records received from public institutions and organisations, public service organisations and operators in relation to the activities of the Authority in accordance with the information security criteria was adopted as a legislative provision. The BTK obtains Internet traffic data only within the scope of the relevant criminal investigation or criminal proceedings within the framework of the decisions taken by public prosecutors or courts in accordance with the Law no. 5271, and submits the data at issue to those judicial authorities. It does not share it with any other person or institution. For example, the BTK does not share these data with the relevant courts, even if these data are requested by civil or administrative courts, since there is no criminal investigation or prosecution, that is, there cannot be a decision taken within the scope of Law no. 5271.

182. On the other hand, the Law no. 5809 on Electronic Communications Law (Law no. 5809), which was published in the Official Gazette dated 10 November 2008, includes provisions vesting the BTK with regulation and supervision authority in the electronic communications sector. The duties and powers of the BTK in respect of the activities included in this Law are set out in Article 6 of the same Law, and the duty of "making necessary arrangements and inspections in respect of the rights of subscribers, users, consumers and end users as well as the processing of personal data and protection of privacy has been entrusted to the BTK by sub-paragraph (c) of paragraph 1. Pursuant to sub-paragraph (ı) of the same Article, the BTK shall be entitled and authorised "*to request, from operators, public authorities and institutions, natural persons and legal entities, any kind of information and documents which it considers necessary in the context of electronic communications and to keep necessary records.*"

183. In addition, Article 12 of the Law no. 5809 governs the rights and obligations of the operators. According to paragraph 5 of the relevant Article, "*the operators are obliged to construct the technical infrastructure before providing electronic communications services for the satisfaction of the requests through the electronic communication systems in relation to national security and the regulations introduced by the Law nos. 5397 and 5651 and by other relevant laws. The operators which have already been providing electronic communications services are obliged to construct the specified technical infrastructure at their own expense under the same conditions within a period of time to be determined by the Authority.*"

184. In line with the above-mentioned legislative provisions and pursuant to the provisions of the Law nos. 5397, 5271 and 5809, the BTK is under a legal obligation to comply with the requests of the Chief Public Prosecutor's Offices and the courts if they request Internet traffic data within the scope of judicial investigations and proceedings. Therefore, the fulfilment of such obligation by the BTK within the framework of the relevant provisions is also a requirement for the submission of information to be requested by the judicial authorities within the scope of any investigation or criminal proceedings. In other words, the BTK is under a duty to obtain any kind of information and documents from all relevant institutions including operators and to comply with the requests of the judicial authorities within the scope of Article 135 of the Law no. 5271.

185. At this point, it must be noted that the circumstances in which this Law shall not be applicable are listed in Article 28, entitled "Exceptions", of the Law on Protection of Personal Data (Law no. 6698), which was adopted in order to protect fundamental rights and freedoms of individuals, particularly the right to privacy, during the processing of personal data and to set forth the obligations of the natural or legal persons who process personal data as well as the principles and procedures with which they must comply. Sub-paragraph (ç) of paragraph 1 of the said Article provides that the provisions of this Law shall not be applicable to the processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organisations duly authorised and assigned by law to maintain national defence, national security, public safety, public order or economic security. In view of the fact that the BTK

was also established to carry out, from a single centre, the procedures in respect of the requests of the judicial authorities within the scope of criminal investigations and that it submits Internet traffic data to the judicial authorities only upon a request within the framework of the above-mentioned provisions, it is obvious that the Law no. 6698 cannot be applied to the impugned power of the BTK.

186. Therefore, the Government would like to state that it is not unlawful for the BTK to obtain Internet traffic data within the framework of the provisions of the aforementioned legislation and to submit such data only to the judicial authorities upon judicial decisions made in accordance with the procedures.

d. As regards the existence of safeguards in legislation and in practice to prevent arbitrary interference or abuse

187. First of all, the Government would like to note that the applicants have not alleged that the Internet traffic data sent by the BTK to the judicial authorities was subject to any technical insecurities (see, in this regard, *Breyer v. Germany*, § 96). Accordingly, the Government invites the Court not to hold an examination with regard to the safeguards. Furthermore, the Government would like to draw attention to certain safeguards in the legislation on data security.

188. In this scope, it should be noted first of all that the BTK is obliged to satisfy the requirements of the request submitted by the chief public prosecutor's offices and courts under Article 135 of the Law no. 5271 in relation to interception, wiretapping and recording of communications and assessment of signal information. The BTK submits Internet traffic data to judicial authorities only upon a request by those authorities under Article 135 of the Law no. 5271. In the present case, the internet traffic data pertaining to the phone line used by the applicants was shared by the BTK in line with the decisions of the Assize Court pursuant to Article 135 of the Law no. 5271.

189. In its judgment in the case of *Karabeyoğlu v. Turkey* (no. 30083/10, 7 June 2016), the Court also examined Article 135 of the Law no. 5271 in the context of Article 8 of the Convention. In that case, the Court first established that the relevant provision constituted the legal basis for the interference with the suspects' communications. The Court also concluded that the provision in

question set out in a detailed manner the guarantees specifying the extent and modalities of the margin of appreciation afforded to the administration and had a binding force circumscribing the discretionary power of the competent authority in the application of the measures in question. In this scope, the Court attached particular importance to the provision in Article 135 of the Law no. 5271 requiring the law to detail the precautions to be taken to communicate - intact and complete - the recordings made for the purposes of possible control by the judge and by the defence, and to set out the circumstances in which the destruction of the recordings may take place in particular after a dismissal or an acquittal.

190. More importantly, the Court drew attention to Articles 4 and 27 of the Regulation on Procedures and Principles concerning Interception and Wiretapping of Communications Made via Telecommunications and Assessment and Recording of Signal Information and on Establishment, Duties and Powers of the Presidency of Telecommunication and Communication, which provide that the records and information obtained within the framework of the activities carried out in accordance with the provisions of the Regulation in question may only be used for a purpose or within the framework of a procedure as set out in Article 135 of the Code of Criminal Procedure. Accordingly, in the light of these considerations and of the detailed examination of the national legislation, the Court concluded that the interference based on Article 135 of the Law no. 5271 had been necessary in a democratic society for the protection of national security and public order and the prevention of crime within the meaning of Article 8 of the Convention (see *Karabeyoğlu v. Turkey*, §§ 78-111).

191. Moreover, the requests in court decisions submitted to the BTK - regarding whether there was a connection between the IP of a GSM line used by an accused or a suspect and another target IP between two specific dates, namely whether there was communication between these two IP addresses- are considered within the scope of the concept of interception of communications regulated in Article 135 of the Code of Criminal Procedure, and only the requests that meet the conditions in the relevant Article are complied with by the BTK. It is understood that where there is a connection between the indicated IP addresses, this means that there was communication between the relevant IP

addresses and therefore this issue falls within the scope of the concept of interception of communications laid down in Article 135 of the Code of Criminal Procedure. In the relevant requests, all Internet traffic data pertaining to an individual is not provided or an inquiry is not carried out in terms of all target IP addresses; rather, it is established, limited to the request, whether an individual communicated with a specific IP address over a GSM line used by him/her. The suspect or accused person has the opportunity to express his objections and reservations about the authenticity of this data at every stage of the investigation or prosecution.

192. Furthermore, the BTK does not unconditionally and unexceptionally comply with the requests made by the prosecutor's offices or courts; it assesses whether the requests meet the conditions specified in Article 135 of the Law no. 5271. In this context, where the BTK establishes that the requests are contrary to the Law no. 5271, the BTK does not comply with these requests. Indeed, sub-paragraph (b) of Article 17 of the Regulation on Procedures and Principles Concerning Interception and Wiretapping of Communications Made via Telecommunications and Assessment and Recording of Signal Information and on Establishment, Duties and Powers of the Presidency of Telecommunication and Communication entrusts the BTK with the task of carrying out acts and actions under Article 135 of the Law no. 5271 regarding the interception, wiretapping and recording of communications and assessment of signal data from a single centre. Sub-paragraph (c) of the same Article authorises the BTK to examine whether the request under sub-paragraphs (a) and (b) comply with this Regulation and other relevant legislation, and to apply to the competent authorities if necessary.

193. In other words, sub-paragraph (c) of the relevant Article provides the BTK with the opportunity to examine compliance with the relevant legislation and to apply to the competent authorities if necessary. The opinion no. 33597 dated 15 May 2014 and the opinion no. 27362 dated 21 April 2015 submitted by the Directorate General for Criminal Affairs at the Ministry of Justice noted that the BTK was required to apply to the judicial organs for the requests considered to be unlawful, and that following such an application, an action had to be carried out in accordance with the judicial decisions delivered (see Annex 28).

194. Accordingly, in case of a request that does not meet the conditions specified in Article 135 of the Law no. 5271, the BTK files an objection with another judicial authority seeking not to comply with such a request, and if the relevant objection is found to be justified, the BTK does not comply with the request at issue.

195. Article 4 of the Regulation governing establishment, duties and powers of the BTK contains general principles to be applied in the performance of activities within the scope of this Regulation. This Article provides as follows:

> *"**Principles***
>
> ***ARTICLE 4**: Privacy of communication is fundamental.*
>
> *No one may intercept or wiretap communications of another person, assess signal information or record them through telecommunication, except in accordance with the principles and procedures defined in this Regulation.*
>
> *Records and information obtained within the scope of the activities carried out in accordance with the provisions of this Regulation shall not be used for the purposes and in line with the procedure other than those specified in this Regulation and in Additional Article 7 of the Law no. 2559 dated 4 July 1934, Additional Article 5 of the Law no. 2803 dated 10 March 1983, Article 6 of the Law no. 2937 dated 1 November 1983 and Article 135 of the Law no. 5271 dated 4 December 2004.*
>
> *Privacy is fundamental in the storage and protection of information, documents and records obtained."*

196. The above-cited provision of the Regulation indicates that the information to be obtained within the scope of the activities carried out can only be used for the purposes specified in the laws on which the purpose of obtaining is based, and thus the limit of use of this data has been determined. It is further stated that privacy is fundamental in the retention and protection of data.

197. Article 15 of the Regulation governs the destruction of data shared with judicial authorities. The relevant Article provides as follows:

> *"**Destruction of records***
>
> ***ARTICLE 15 - (First paragraph amended by the Official Gazette no. 26572 dated 4 July 2007)**[1] In the event that a decision of non-prosecution is delivered in respect of the suspect in the course of the implementation of the decision or that the judge decides otherwise regarding the decisions taken by the public prosecutor in cases where delay would be detrimental; the Presidency [of Telecommunication and Communication] shall be immediately notified by the public prosecutor or by the law enforcement, upon instruction of the public prosecutor, that the measure has been lifted.*
>
> *If the decision made by the public prosecutor is not approved by the judge and sent*

> *to the Presidency within the time-limit, the Presidency shall immediately terminate the execution of the decision.*
>
> ***(Third paragraph amended by the Official Gazette no. 26572 dated 4 July 2007)***[(1)] *Records concerning the processes of interception or wiretapping carried out in cases specified in the first and second paragraphs as well as the second paragraph of Article 12 shall be destroyed within a period of maximum ten days under the supervision of the public prosecutor at the court having competence and jurisdiction specified in Article 26, and this shall be recorded in a report."*

198. As is seen, the data shared with the judicial authorities pursuant to Article 135 of the Law no. 5271 is immediately destroyed if the investigation is terminated by a decision of non-prosecution or the decision made by the public prosecutor is not approved by the court.

199. Article 51 of the Law on Electronic Communications (Law no. 5809)[15], titled "Processing of personal data and protection of privacy", reads, in so far as relevant, as follows:

> *"(1) In the processing of personal data, the principles of being in compliance with the law and the rules of good faith, being accurate and up-to-date when necessary, being processed for certain, clear and legitimate purposes, being relevant, limited and proportionate to the purpose for which it is processed, and being kept for the period required for the purpose for which it is processed shall be complied with.*
>
> *(2) Confidentiality of electronic communication and the related traffic information shall be fundamental, and it shall be forbidden to wiretap, record, store, cut off or monitor the communication without the consent of all parties to the communication, except for the cases stipulated by the relevant legislation and judicial decisions.*
>
> ...
>
> *(10) As regards the services provided under this law,*
>
> *a) Personal data, which is the subject-matter of the investigation, review, inspection or dispute shall be retained until the related process is completed;*
>
> *b) Procedure records relating to access to personal data and other related systems shall be retained for two years;*
>
> *c) Records showing the consent of subscribers/users for the processing of personal data shall be retained at least for the duration of the subscription."*

200. After mentioning these legal provisions, the Government would like to indicate the processes of procuring data from access providers, retention of them and sharing of them with judicial authorities pursuant to Article 135 of Law no. 5271 as well as the guarantees at these stages.

201. Internet traffic data is transferred to the BTK data centre systems at

[15] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf

the highest security level through the closed circuit technical infrastructure (point-to-point physical cable line established only for this purpose), which has been installed between the Access Providers and the BTK, which does not have Internet output and which is controlled by end-to-end security devices. Internet traffic data transferred to the data centre via the secure technical infrastructure between the operators and the Authority is sent to the archive servers without any intervention, and stored in the archive servers, again without any process, within the framework of criteria of information security, pursuant to sub-paragraph (f) of Article 17, entitled "Duties of the Presidency" of the Regulation on Procedures and Principles Concerning Interception and Wiretapping of Communications Made via Telecommunications and Assessment and Recording of Signal Information and on Establishment, Duties and Powers of the Presidency of Telecommunication and Communication". There is technically no way to access this data; however, if a request is made under Article 135 of the Law no. 5271, a procedure is carried out by the personnel in charge of this task as required by the request. Not every personnel working in the BTK can make such a query, and only authorised personnel can make queries. Therefore, these data can be accessed only by a limited number of people and if only requested by judicial authorities (see in this regard *Breyer v. Germany*, § 97).

202. Logs of the queries made by the personnel in charge are kept in the system, and in case of a possible abuse, it can be established which query has been made by the personnel on the basis of which court decision. Moreover, while making a query, an authorised staff member can only see the results relating to the criteria he/she enters and the points specified in the judgeship's decision, and he/she cannot see any other data.

203. **Article 27, entitled "Criminal provisions"**, of the Regulation reads as follows: "*Information obtained within the scope of the activities carried out in accordance with the provisions of this Regulation shall not be used for purposes and procedure other than those specified in the laws that serve as the basis of this Regulation. The principle of privacy shall be respected in the retention and protection of the information, documents and records obtained. Public prosecutors shall directly conduct an investigation against those acting contrary to the provisions of this paragraph, even if such an act has been committed in the*

course of or in connection with official duties." Thus, the most important obligation which the BTK must comply with in the performance of the duties with which it is entrusted is always privacy. Furthermore, any personnel who cause data to be corrupted or be obtained by unauthorised third parties or who lead to an unauthorised action to be taken in violation of the right to respect for private life of an individual will be directly subject to an investigation without the need for a permission for an investigation.

204. Furthermore, the BTK is a public legal entity which was established with a view to conducting requests under Article 135 of the Law no. 5271 from a single centre. In other words, the legislator envisioned that the BTK, which has a public legal personality, would meet the demands of judicial authorities with regard to such data single-handedly, instead of the practice in which each of the different access providers, which are private companies, shared the data with judicial authorities separately (see in the same vein *Breyer v. Germany,* § 98). Therefore, public prosecutors or courts request these data from the BTK, not from the access providers. Indeed, in the present case, the Assize Courts procured the internet traffic data belonging to the applicants' telephone lines from the BTK by virtue of Article 135 of the Law no. 5271 (see § 26-100 above).

205. It is clear that the aim of the alleged interference with the applicants' right to respect for private life was closely related to ensuring national security and preventing crime. The Government would like to draw the Court's attention to the fact that the alleged interference, which was based on the aims of protecting national security and preventing crime, was based on legitimate aims set out in Article 8 § 2 of the Convention. Therefore, it is undoubted that the interference in the present case was of the nature that necessitated an exception to the special safeguards inherent in the right to respect for private life. It is one of the fundamental duties of the State to identify and prevent acts of terrorism targeting the Republic of Turkey. From this standpoint, detecting terrorist organisations and their activities and, in this context, limiting the right to respect for private life for the purpose of prevention of crime clearly pursues a legitimate aim.

206. Furthermore, there is no information showing that the interference, namely the submission of the CGNAT data by the BTK to the case-files pertaining to the applicants, went beyond the aim of uncovering the activities and identifying the members of the said organisation and ultimately bringing down the organisation. Nor did the applicants raise a complaint to the effect that this data was not used within the limits of the aims for which they were acquired. The CGNAT data in question was used only in criminal proceedings conducted on charges relating to the relevant organisation.

207. The Government considers that the State struck a fair balance between, on the one hand, the prevention of crime and protection of national security and, on the other, the applicants' interests in the context of the protection of the right to respect for private life. Indeed, all internet data of the applicants was not requested in the present case. The courts conducting trials against the applicants requested the internet traffic information between the IP addresses established to be used by the ByLock application and the phone numbers, which the applicants admitted to have used. These pieces of data were requested from the BTK, which was legally obliged to comply with such requests under Article 135 of the Law no. 5271. At this point, the Government brings to the Court's attention that the request concerned contact information relating to specific IP addresses and covering a limited period of time.

208. In conclusion, the Government would like to emphasise that there are, in the practice and the legislation, sufficient safeguards against arbitrary interference and abuse of internet traffic data.

e. Conclusion

209. In the light of all these explanations, the Government kindly invites the Court to hold that there has been no interference or violation of the applicants' right to respect for their private life, their right to protection of personal data or freedom of communication.

CONCLUSION

210. Firstly, the Government of the Republic of Turkey kindly requests the Court to make an assessment on the applicants' complaints regarding Article 8 of the Convention under Article 15 of the Convention.

211. In the second place, in the light of the observations and explanations made above, the Government of the Republic of Turkey firstly invites the Court to dismiss the present applications for not meeting the admissibility criteria for the legal grounds stated above.

212. Where the Court rejects those objections, the Turkish Government respectfully invites the Court to hold that there has been no violation of the Convention provisions as regards the relevant complaints in the present applications.

06. October 2021

Dr. Hacı Ali AÇIKGÜL

Co-Agent of the Government of the Republic of Turkey

ANNEXES

1- Decision no. E.2017/16.MD-956, K.2017/370 of the Plenary of the Court of Cassation in Criminal Matters, dated 26 September 2017, Decision no. E.2018/16-418, K.2019/513 of the Plenary of the Court of Cassation in Criminal Matters, dated 26 June 2019

2- Decision not to process the criminal complaint filed by Metin Çamurşen

3- Decision of the Constitutional Court in respect of Metin Çamurşen, dated 21 June 2019

4- Decision not to process and not to prosecute, delivered following the criminal complaint filed by Serkan Uslu

5- Decision delivered following the objection filed by Serkan Uslu against the decision not to process and not to prosecute

6- Decision of the Constitutional Court in respect of Serkan Uslu, dated 11 June 2020

7- Decision not to process the criminal complaint filed by Sadık Yayla

8- Decision delivered following the objection filed by Sadık Yayla against the decision not to process

9- Decision of the Constitutional Court in respect of Sadık Yayla, dated 3 December 2019

10- Quashing Decision of the 16th Criminal Chamber of the Court of Cassation, dated 2 July 2020

11- Decision not to process the criminal complaint filed by Hüseyin Akbulut

12- Decision of the Constitutional Court in respect of Hüseyin Akbulut, dated 12 November 2019

13- Decision not to prosecute, delivered following the criminal complaint filed by Gökhan Yaman

14- Decision delivered following the objection filed by Gökhan Yaman against the decision not to prosecute

15- Decision of the Constitutional Court in respect of Gökhan Yaman, dated 10 February 2020

16- Decision not to prosecute, delivered following the criminal complaint filed by Duran Denizci

17- Decision delivered following the objection filed by Duran Denizci against the decision not to prosecute

18- Decision of the Constitutional Court in respect of Duran Denizci, dated 9 July 2019

19- Decision not to process the criminal complaint filed by Hüsmen Koçak

20- Decision of the Constitutional Court in respect of Hüsmen Koçak, dated 27 February 2020

21- Petition for a full remedy action before the administrative court, filed by Hüsmen Koçak

22- Decision of the Ankara 2nd Administrative Court, dated 19 December 2019

23- Decision of the 7th Administrative Chamber of the Ankara Regional Administrative Court, dated 30 December 2020

24- Notification report of 7 April 2021 pertaining to Hüsmen Koçak

25- Decisions of administrative courts relating to similar complaints

26- Decisions of civil courts relating to similar complaints

27- Opinions of the Directorate General for Criminal Affairs, dated 15 May 2014 and 21 April 2015