



Algorithmic persecution and unfair trials in Turkey

UN Universal Periodic Review submission for Turkey's Fourth UPR Cycle

For the UPR session on Turkey scheduled for the 49th session of the UN Human Rights Council (April – May 2025).

About Statewatch

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards. We began operating in 1991 and are based in London.

Contact details

Chris Jones (Executive Director): chris@statewatch.org

Web address: <https://statewatch.org>

Phone: +44 203 393 8366

Postal address: MayDay Rooms
 88 Fleet Street
 London
 EC4Y 1DH
 UK

About Arrested Lawyers Initiative

The Arrested Lawyers Initiative (TALI) began its activities in 2016, in Brussels, Belgium. Since then, it has been constantly monitoring the situation surrounding lawyers and human rights defenders in Türkiye and publishing bulletins and legal reports. TALI circulates these reports through numerous bar associations in Europe. TALI is also submitting such reports to international human rights bodies such as the Office of the UN Human Rights Commissioner and UN Special Rapporteurs. TALI publishes its reports in English, Italian and Spanish. TALI is a member of the International Observatory for Lawyers.

Contact details

Web address: <https://arrestedlawyers.org/>

Overview

1. This submission for the Universal Periodic Review (UPR) of Turkey addresses the significant human rights concerns arising from the prosecution of individuals based on their alleged use of ByLock, an encrypted messaging application similar to Signal and Telegram; and algorithmic persecution in Turkey's post-coup crackdown, specifically through the application of an algorithmic system known as the "FETÖ-Meter".

Unfair trials: Introduction

2. Since the 2016 attempted coup in Turkey, over 90,000 individuals, including public servants, police officers, academics, judges, prosecutors, businesspeople and even university students and housewives have been purged or arrested for their alleged use of ByLock. In the immediate aftermath of the 2016 attempted coup, the Turkish authorities claimed that this app had been created exclusively for the 'Gülen Movement (GM)' – a religious organization designated as the FETÖ/PDY (Fetullahist Terrorist Organisation/Parallel State Structure) due to their alleged involvement in organising the abortive coup.
3. Since the post-coup emergency rule, the Turkish domestic courts, including the Turkish Court of Cassation and the Turkish Constitutional Court, have consistently regarded involvement in the ByLock network as sufficient grounds for convicting someone of membership in an armed terrorist organisation under Article 314(2) of the Turkish Penal Code, even in the absence of other evidence. In turn, those caught in the 'ByLock' dragnet have been frantically attempting to vindicate themselves, arguing that they either never downloaded the app or, if they did, never used it for criminal or terrorist activities.
4. The case of *Yalçınkaya v Türkiye*, decided by the Grand Chamber of the European Court of Human Rights (ECtHR) on 26 September 2023, represents a significant milestone in the evolving discourse surrounding the use of ByLock. As explained below, this landmark case has spotlighted the systemic nature of human rights violations arising from domestic prosecutions and convictions related to the use of ByLock, particularly in the context of fair trial rights, freedom of expression, and freedom of assembly under the European Convention on Human Rights (ECHR).
5. Despite this decision binding Turkish courts under Article 46 of the European Convention on Human Rights (ECHR), which Türkiye is bound to as per Article 90 of its constitution, the Kayseri 2nd Assize Court reaffirmed the conviction of Mr. Yüksel Yalçınkaya on 12 September 2024. The Kayseri Court stated that its previous judgment, that the ECtHR found had breached articles 6, 7 and 11 of the ECHR, in conformity with the law.¹
6. This submission aims to highlight the urgent need for Turkey to address these systemic human rights violations and take concrete steps towards reforming its legal framework and judicial practices to prevent further miscarriages of justice and safeguard the rights of all individuals, including those accused of ByLock-related offenses.

Factual background

7. ByLock is a communications app for encrypted written and voice messages. Accessible via most online markets and app stores including the Google Play Store and Apple Store, it was in operation between 14 March 2014 and 19 February 2016. A report by FOX-IT, a Dutch forensic IT company, found that ByLock was downloaded more than 100,000 times on the Google Play Store alone.² In 2020, a pro-Turkish government media outlet reported that over 92,000 people had been identified and prosecuted for allegedly using the ByLock app,³ while the actual numbers could be higher as this practice continues unabated.⁴
8. The Turkish Government claims that ByLock was exclusively designed and developed to fulfil the communication needs of the GM (also known as the “exclusivity claim”). This claim is routinely rubber-stamped by the Turkish judiciary despite numerous expert reports refuting it. To name a few, digital forensic reports by leading firm such as Fox-IT⁵ and experts such as Jason Frankovitz⁶ and Thomas Kevin Moore⁷ have proved that this exclusivity claim is erroneous.
9. A comprehensive report released by the Italian Federation for Human Rights in July 2023 found that in 78 of the 118 indictments examined, ByLock usage has emerged as the most damning and often decisive evidence, particularly in the post-coup period, among the various criteria used to charge individuals under Article 314 of the Turkish Penal Code (TPC) for alleged membership of the GM.⁸

ByLock cases before international human rights bodies

a) UN bodies

10. In several opinions, the UN Working Group on Arbitrary Detention (UN WGAD) has consistently concluded that downloading and using ByLock represents the exercise of a person’s basic rights to freedom of opinion and expression.⁹ Indeed, they conclude that the rights to freedom of opinion and expression protect all *forms* of expression, as well as the means of their dissemination, including all forms of audio-visual, electronic and internet-based modes of expression.¹⁰ In that regard, the UN WGAD stressed that the Turkish government made detailed submissions on how ByLock had been used by individuals who were linked to the GM in general, but had failed to elaborate on how the alleged use of the ByLock application by any of the accused individuals could amount to a criminal act. Notably, the UN Working Group recalls that this pattern, which involves widespread or systematic imprisonment or other severe deprivation of liberty, in violation of the rules of international law, suggests that under certain circumstances, these may amount to crimes against humanity.
11. In a similar vein, in the case of *Ismet Ozcelik*,¹¹ where the complainant was accused of membership of an armed terrorist organisation on the basis of downloading ByLock, the UN Human Rights Committee (HRC) found that Turkey has failed to substantiate that the detention of the applicants (authors, in the jargon of the HRC) meets the criteria of reasonability and necessity and this amounted to a violation of their rights under Article 9 (1-2) of the International Convention on Civil and Political Rights.¹²

b) The European Court of Human Rights

12. To date, the ECtHR has issued several important decisions that relate to the use of ByLock. In the *Akgün* case of July 2021, in which the applicant was a former police officer held in pre-trial detention in October 2016 due to his alleged use of the ByLock app and subsequently convicted for being a member of GM,¹³ the ECtHR found that Turkey had violated Article 5(1) (the right to liberty and security), Article 5(3) (entitlement to trial within a reasonable time, or to release pending trial) and Article 5(4) (the right to a speedy decision on the lawfulness of detention). The court considered that, when ordering the applicant's pre-trial detention in October 2016, the Turkish domestic court did not have sufficient information on the nature of ByLock to conclude that this messaging application was used exclusively by members of the "FETÖ" organisation for the purposes of internal communication. The Court concluded that in the absence of other evidence or information, the mere usage of ByLock, could not, on its own, indicate that there were reasonable suspicions that would satisfy an objective observer that he had indeed used ByLock in a manner that could amount to the alleged offences.
13. In the case of *Taner Kılıç*,¹⁴ the applicant, a prominent human rights defender and a co-founder of the Turkish branch of Amnesty International, was arrested and detained based mainly on his alleged use of ByLock together with other additional contextual factors including his subscription to the Zaman newspaper, allegedly linked to FETÖ/PDY; his family connection with the newspaper through his brother-in-law, who served as an editor; and the enrolment of his children in educational institutions with purported ties to FETÖ/PDY. In its decision, the ECtHR found violations under 5(1), 5(3), 5(4), and 5(5), as well as Article 10 ECHR. Notably, in its analysis in relation to the use of ByLock, the Court initially distinguished the present case from its *Akgün* judgment as the evidence presented by the domestic authorities in the *Taner Kılıç* case extended beyond the utilization of ByLock. Importantly, the ECtHR examined the police report commonly referred to as the "ByLock Determination or Evaluation Minute" and characterized this report as a "blunt finding", noting its lack of clear indication regarding the authorities' basis for the conclusion and the absence of underlying data or information on collection methods. Building upon *Akgün*, the Court concluded that the exclusive use of an encrypted communication application could not, by itself, be considered a constituent element of a criminal offence.
14. The recent case of *Yalçınkaya v Türkiye* from 26 September 2023 stands as the most important decision regarding the criminalization of the use of ByLock given the numerous violations found by the ECtHR. In the *Yalçınkaya* judgment, the Grand Chamber made significant findings regarding the applicant's conviction based on the use of ByLock, concluding that it clearly violated fundamental principles enshrined in the ECHR, particularly Articles 6 and 7 ECHR. Specifically, the Grand Chamber emphasised that the arbitrary judicial decisions based on the alleged use of ByLock ran counter to the core objectives of Article 7 ECHR (no punishment without law) by creating a near-automatic presumption of guilt for the victims, rendering it nearly impossible for them to challenge the ByLock evidence and prove their innocence. Importantly, the *Yalçınkaya* case sheds light on the rare invocation of Article 7, a fundamental safeguard against arbitrary or unfair criminal prosecution and punishment. The *Yalçınkaya* judgment represents only the 60th violation of Article 7 in the ECHR's history of over 25,000 violations between 1959 and 2022.¹⁵

15. More importantly, the Grand Chamber underscored that the problems leading to these violations were of a “systemic nature”. Currently, there are approximately 8,500 pending applications before the court that involve similar complaints under Articles 6 and/or 7 of the Convention. Given that the authorities had identified around 100,000 ByLock users, it is likely that many more such applications could be submitted. Therefore, the systemic nature of the issues became evident. In accordance with Article 46 ECHR, the court ruled that Turkey must take appropriate general measures to address these systemic problems, particularly regarding the Turkish judiciary’s handling of ByLock evidence.
16. Moreover, there were notable procedural deficiencies in the criminal proceedings against the applicant, particularly in relation to his access to the ByLock evidence specific to his case and his ability to effectively contest it. These shortcomings amounted to a breach of his right to a fair trial as guaranteed by Article 6 ECHR. However, it should be stressed that the Court left several important questions unaddressed concerning the use of ByLock in Turkey that lie at the intersection of digital evidence and the right to a fair trial including admissibility of evidence, quality of evidence, requirement of an adversarial proceeding, and entitlement of disclosure. A detailed analysis on the important issues is provided in a recent comprehensive report published by Statewatch in March 2024, attached in appendix.¹⁶
17. The Grand Chamber also found a violation of Article 11 (freedom of assembly and association), as the domestic courts had interpreted Article 314(2) TPC in a broad, extensive and unforeseeable manner so as to include the applicant’s membership of a trade union and an association (Aktif Eğitim-Sen and Kayseri Voluntary Educators Association respectively) as indications of criminal conduct, such as incitement to violence or rejection of democratic society’s foundations. However, both associations had been operating lawfully before the 2016 attempted coup.¹⁷
18. In the most recent case of *Parıldak* decided on 19 March 2024, concerning the pre-trial detention of a journalist mainly based on the alleged use of ByLock, the ECtHR found violations of Articles 5(1) and 5(3) ECHR, as the applicant’s detention lacked reasonable suspicion; and Article 10, as her arbitrary detention interfered with her freedom of expression.¹⁸ In relation to the applicant’s alleged use of ByLock, the ECtHR found that the domestic decisions relating to the applicant’s detention do not contain any element relating to the use of the messaging service in question, such as, for example, the content or context of messages possibly exchanged. Consequently, the Court has reiterated and reaffirmed its precedents in the cases of *Akgun and Taner Kilic*.

Unfair trials: Recommendations

19. In line with the ECtHR Grand Chamber’s findings in the *Yalçınkaya* case and the principles set forth by the TCC, the following recommendations are proposed to the Turkish authorities for a human rights-friendly use of ByLock evidence.
 - a. **Reverse the verdict delivered by the Kayseri Court in the retrial of Yuksel Yalcinkaya.**
 - b. **Recharacterization of ByLock:** Turkish authorities should reassess the characterization of ByLock, revisiting and potentially reversing judgments

influenced by an automatic presumption of guilt. Domestic courts should apply stricter criteria for establishing membership in terrorist organizations, requiring clearer evidence of an “organic relationship” to the group.

- c. **Retrial and objective effect of the *Yalçınkaya* judgment:** Turkish courts must consider the objective impact of the *Yalçınkaya* judgment, prioritizing retrials for individuals convicted based on ByLock allegations to ensure justice in line with Turkey’s international obligations.
- d. **Access to complete ByLock dataset:** Defendants should have access to the complete ByLock dataset relevant to their cases to uphold the principle of equality of arms. Any restrictions on disclosure must be justified and determined impartially, with defendants receiving at least a digital copy of their own ByLock data.
- e. **Examination of exculpatory evidence:** Courts must investigate potential exclusion of exculpatory evidence from ByLock material to prevent miscarriages of justice, ensuring the integrity of digital evidence.
- f. **Addressing gaps in ByLock material:** Turkish courts should probe missing time periods within ByLock material to maintain the fairness of proceedings, ensuring the continuity of digital records.
- g. **Scrutiny of the Turkish intelligence agency’s handling of data:** Courts should examine the Turkish intelligence agency’s processing of ByLock data without judicial supervision to safeguard the chain of custody and procedural integrity of digital evidence.
- h. **Oversight and review of ByLock data:** Establishing an independent expert panel to scrutinize the quality, reliability, and integrity of ByLock evidence is crucial. This panel should investigate any technical issues and have full access to relevant materials to ensure a transparent examination.
- i. **Legal and judicial reforms:** Undertake comprehensive reforms to ensure the collection, use, and evaluation of digital evidence, such as ByLock data, comply with international human rights standards, particularly those relating to privacy, due process, and fair trial.

Algorithmic persecution: Introduction

20. Developed and implemented in the aftermath of the failed coup attempt on 15 July 2016, the “FETÖ-Meter” has been used to identify, dismiss, detain, and otherwise persecute individuals within the Turkish Armed Forces (TAF) and other parts of the public sector on the grounds of alleged affiliations with the Gülen Movement, designated by the Turkish government as the Fethullahist Terrorist Organization (FETÖ).
21. Following the 2016 attempted coup, the Turkish government undertook widespread purges within the military and public services, affecting over 150,000 individuals. The “FETÖ-Meter”, an Excel-based algorithm, played a significant role in this process by profiling military officers and others based on a broad range of criteria, many unrelated to any criminal activity. This submission highlights the concerns over the legal basis, methodology, and impact of the FETÖ-Meter on the rights of individuals.

The FETÖ-Meter system in Turkey

22. The FETÖ-Meter is a Microsoft Excel-based algorithm designed by Rear Admiral Cihat Yaycı to profile all active and retired military officers. According to Yaycı, it is a “decision support program” that helps the decision makers to uncover the “crypto” Gülenist soldiers.¹⁹ According to the state-run Anatolian News Agency, at least 810,000 individuals have been subjected to this profiling algorithm.²⁰ It has been used by a special unit called ‘The Office of Judicial Proceedings and Administrative Action’ (ATİİİŞ), within the Personnel Department of the Turkish Naval Forces (TNF).
23. The set of criteria deployed in order to try to identify so-called “crypto” Gülenist soldiers were first published by pro-government journalist Nedim Şener in his book titled *Hero Traitors*.²¹ The book, published on 15 May 2018, includes a document titled Personnel Criterion Point Card.²² On 11 September 2018, the state-run Anadolu Agency (AA) published an article that included screenshots of the Personnel Criterion Point Card.²³ Cihat Yaycı himself later gave interviews to several news platforms and explained the criteria and the workings of FETÖ-Meter in detail.²⁴ In these interviews, Yaycı also confirmed the authenticity of the card which Şener had published.
24. According to Şener and Yaycı, each individual is grouped into four categories based on the score they were given by the algorithm:
- (i) 0.00– 0.999 point: to be monitored,
 - (ii) 1.000 – 1.999 point: to be subjected to a thorough investigation,
 - (iii) 2.000 – 2.999: to be suspended or dismissed from the post,
 - (iv) 3.000 and above: shall be dismissed.²⁵
25. The FETÖ-Meter criteria which were published by Şener and confirmed by Yaycı may be grouped in four categories, namely (i) those directly about the core of private life of the profiled person; (ii) those about the professional life (starting from the military school) of the profiled person; (iii) those about social circle and affiliation of the profiled person; (iv) those about the relatives of the profiled person.

Legal analysis of the FETÖ-Meter system:

26. There is little doubt that the application of the FETÖ-Meter system in Turkey has severely intruded on some of the most fundamental principles of the democratic society governed by rule of law. As explained above, the ATİİİŞ unit obtained sweeping personal information about at least 810,000 individuals from various official bodies and the resulting mass data collection was used to target hundreds of thousands of people via such measures as dismissal, detention, and prosecution for terrorism-related charges.²⁶
27. The established case law of the two most important international human rights mechanisms, namely the European Court of Human Rights (ECtHR)²⁷ and the UN Human Rights Committee (HRC),²⁸ clearly acknowledges that the protection of personal data is of fundamental importance to a person’s enjoyment of his or her right to privacy. Similarly, the Turkish Constitution explicitly protects personal data under its Article 20(3).²⁹ In the case of *Ekimdzhiiev and Others*,³⁰ for example, the ECtHR explained that “mere storing of data relating to someone’s private life” and

“general retention of data” may likely violate the right to respect for private life in the absence of adequate safeguards. In its jurisprudence, the HRC also affirmed that relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted and effectively ensure that “information concerning a person’s private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible” with the ICCPR.³¹ In a similar vein, the Turkish Constitutional Court (TCC) has consistently held that “it is not sufficient that a legal regulation to limit the right to request the protection of personal data exists in form, but the legal rules must be in the character of specific, accessible and foreseeable regulations that do not allow arbitrariness.”³²

28. Despite all these unequivocal principles arising out of the relevant international and domestic jurisprudence, neither Yaycı himself nor the ATİİİŞ unit, however, have been legally vested with such wide authority to carry out any of the activities explained above. Accordingly, there seems to exist no legal basis to lawfully obtain and process the personal data of hundreds of thousands of individuals. Nor has the unit ever sought a warrant from a competent judicial authority to obtain and process the data in question. All those operations were carried out solely pursuant to an order issued by the then Commander of the TNF who had no authority to delegate such power to his staff to perform the operations carried out by the ATİİİŞ.
29. There is also little doubt that the activities of ATİİİŞ constitute “automatic processing” and fit the definition of “high-risk profiling” under Article 2 of Council of Europe Convention 108, to which Turkey is a party.³³ Such automatic processing of personal data may constitute serious interferences with a broad spectrum of human rights. Fundamentally, Convention 108 requires state parties to obtain and process data fairly and lawfully in a manner that respects a broad spectrum of human rights, including rights to privacy, peaceful assembly, and expression.
30. A comprehensive report published by *Statewatch* in November 2021 finds that the FETÖ-Meter was indiscriminately used in post-coup dismissals particularly from the Turkish army, and that those dismissed had been subjected to “the depths of the persecution, mistreatment, torture humiliation and victimization in the aftermath of the 15 July 2016 failed coup.”³⁴
31. The findings of the report in relation to the “collective guilt” standard are worth quoting *in extenso*: “...the FETÖ-Meter list essentially illustrates the expanding practice of criminalising normal and everyday activities as terrorist crimes. It establishes a pattern for the application of punitive measures towards not only primary suspects, but also those people who associate with them, particularly their family members, colleagues, neighbours, and even social media contacts who they did not necessarily know. In the vast majority of cases, the evidence gathered through the application of the ‘FETÖ-Meter’ list, allegedly linking Turkish citizens to disparate terrorist organizations, gives rise to a dangerous standard of ‘guilt by association’ or ‘collective guilt’ which, inter alia, violates the principles of individual legal responsibility, fairness and legal certainty.”³⁵ The report concludes the application of the FETÖ-Meter has clearly violated many fundamental human rights and basic tenets of criminal law, including individual legal responsibility, legal certainty, the right to a fair trial, the right to privacy and the right to data protection.

32. Against this backdrop, the FETÖ-Meter and other similar algorithms have become powerful tools to demonize, target and suppress initially the Gülenists, then Kurdish and leftist groups and finally virtually all dissent based, in many cases, on a tenuous or very remote connection with the *raison d'être* of the 2016 attempted coup and the resulting state of emergency. More strikingly, this harsh crackdown and severe repression utilized an approach characterised by guilt by association, or collective responsibility.

Recommendations

33. It is highly recommended that the Turkish government should immediately and unconditionally:

- a. Call for the immediate suspension of the FETÖ-Meter system until a thorough and transparent review of its legal basis, methodology, and impact on human rights is conducted.
- b. Conduct a comprehensive human rights impact assessment of the FETÖ-Meter and similar algorithms to evaluate their impact on the rights of individuals, including the right to privacy, freedom of expression, and the right to a fair trial.
- c. Ensure transparency and accountability in the use of algorithmic systems, including the disclosure of criteria, methodologies, and decision-making processes, as well as accountability mechanisms for abuses.
- d. Establish oversight mechanisms and additional safeguards to ensure that the use of algorithmic systems like the FETÖ-Meter is subject to scrutiny and review by independent courts.
- e. Strengthen its data protection laws to align with international standards, ensuring that individuals have control over their personal data and that it is processed fairly and lawfully.
- f. Provide technical assistance and capacity-building support to domestic authorities to ensure that they have the knowledge and skills necessary to develop and implement algorithmic systems in compliance with human rights standards.
- g. Engage meaningfully with civil society organizations, including human rights defenders, activists, and legal experts, in the development, implementation, and oversight of algorithmic systems to safeguard against abuses and ensure respect for human rights
- h. Undertake legislative and constitutional reforms to ensure that any algorithmic systems used for profiling individuals or making decisions affecting their rights are in compliance with international human rights standards, including the right to privacy and data protection.

Appendix 1

'ByLock Prosecutions and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in *Yüksel Yalçınkaya v. Türkiye*', *Statewatch*, March 2024

Appendix 2

'Algorithmic persecution in Turkey's post-coup crackdown: The FETÖ-Meter system', *Statewatch*, November 2021

¹ Turkish court ignores landmark ECHR ruling in retrial,

<https://arrestedlawyers.org/2024/09/15/turkish-court-ignores-landmark-echr-ruling-in-retrial/>

² Fox-IT, 'Expert Witness Report on ByLock Investigation' 13 September 2017 <https://blog.fox-it.com/wp-content/uploads/2017/09/bylock-fox-it-expert-witness-report-english.pdf>

³ 'FETÖ'den 612 bin kişiye işlem' (612,000 people were processed for FETÖ), *Yeni Safak*, 27.11.2020, <https://www.yenisafak.com/gundem/fetoden-612-bin-kisiye-islem-3587006>.

⁴ See, for instance, the announcement by the Turkish Minister of Interior regarding new arrests over ByLock usage on 23 January 2024: <https://x.com/AliYerlikaya/status/1749793685527498788>

⁵ FOX-IT report, supra footnote 1.

⁶ Jason Frankovitz, Expert Report on ByLock, 9 August 2017, https://drive.google.com/file/d/0B_Ip_O2-rTNqWlhlQnFOUDJzSZA/view?resourcekey=0-T0xxB0lYDkeF4IkF1-OJbA

⁷ 'Opinion on the reliance on use of the ByLock messaging application as evidence of membership of a terrorist organisation' enjoined reports by William Clegg Qc and Simon Baker and Thomas Moore, 24-25 July 2017, <https://www.2bedfordrow.co.uk/opinion-on-the-legality-of-the-actions-of-the-turkish-state/>

⁸ Emre Turkut and Ali Yıldız, "Perils of Unconstrained Prosecutorial Discretion: Prosecuting Terrorism Offences in Post-Coup Turkey" *The Italian Federation for Human Rights*, July 2023, <https://fidu.it/wp-content/uploads/FIDU-Report-Turkut-Dent-Yildiz.pdf>

⁹ UN WGAD, *Faruk Serdar Köse vs Turkey, Kahraman Demirez et. al v. Turkey and Kosovo, Nermin Yasar v. Turkey*, WGAD/2020/30,47,74.

¹⁰ UN Human Rights Committee, General Comment No. 34, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

¹¹ The UN Human Rights Committee, *İsmet Özçelik et. al.*, CCPR/C/125/D/2980/2017, 26 March 2019

¹² For a similar conclusion in another application, see: UN Human Rights Committee, *Mukadder Alakus*, CCPR/C/135/D/3736/2020, 1 March 2023.

¹³ ECtHR, *Tekin Akgün v Turkey* App No 19699/18, 20 July 2021

¹⁴ ECtHR, *Taner Kılıç v Turkey* App No 208/18, 31 May 2022.

¹⁵ The statistical data on violations found by the ECtHR in CoE member states between 1959-2022 is available at https://www.echr.coe.int/documents/d/echr/stats_violation_1959_2022_eng.

¹⁶ *Statewatch*, 'ByLock Prosecutions and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in *Yüksel Yalçınkaya v. Türkiye*' co-authored by Dr. Emre Turkut and Ali Yıldız, March 2024, available at: <https://www.statewatch.org/media/4200/sw-echr-yalcinkaya-bylock-report.pdf>

¹⁷ Both entities were shut down immediately after the declaration of the state of emergency under the Government's emergency powers.

¹⁸ ECtHR, *Parıldak v Türkiye*, App No 66375/17, 19 March 2024.

¹⁹ See two interviews by Cihat Yaycı: (1) 'FETÖMETRE Nasıl Çalışıyor? Cihat Yaycı İlk Kez Anlatıyor (How does Fetometre work? Cihat Yaycı explains for the first time)', available at: <https://www.youtube.com/watch?v=my0keJf5png>, and (2) 'Cuneyt Özdemir'in Cihat Yaycı Röportajı Fetö'cülerini Çılgına Çevirdi!' available at: <https://www.youtube.com/watch?v=7FPaOGbqu6o>

²⁰ 'Turkish navy algorithm detects allegedly 4,500 Gülen-linked officers among 800,000 profiled' *Turkish Minute*, 11 September 2018 <https://www.turkishminute.com/2018/09/11/turkish-navy-algorithm-detects-allegedly-4500-gulen-linked-officers-among-800000-profiled/>

²¹ Nedim Şener, *Karaman Hainler: Türk Silahlı Kuvvetleri'nde Fetö'nün Kriptoları*, (Destek Publishing, 2018) 376 pp.

²² Nedim Şener describes the Personnel Criterion Point Card as 'Table Regarding the Criteria Used to Determine Feto/Pdy Members within the Turkish Armed Forces, known as the Fetometer in the General Public. (Point Card)'.

²³ 'FETÖ metre' ile kriptolar deşifre ediliyor' Anadolu Agency, 11 September 2018 <https://www.aa.com.tr/tr/15-temmuz-darbe-girisimi/feto-metre-ile-kriptolar-desifre-ediliyor/1251818>

²⁴ See Yayci's interviews, footnote (n 1)

²⁵ See Şener (n 3) p. 225

²⁶ The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and the Turkish Personal Data Protection Law similarly define 'personal data' as any information relating to an identified or identifiable individual ('data subject').

²⁷ ECtHR, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, judgment of 27 June 2017, Application no. 931/13, [GC], para 137.

²⁸ ICCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, paras 1-10 <https://www.refworld.org/docid/453883f922.html>

²⁹ Official translation of the Turkish Constitution is available at: <https://www.anayasa.gov.tr/en/legislation/turkish-constitution/>

³⁰ ECtHR, *Ekimdzhev and Others v. Bulgaria*, judgment of 11 January 2022, Application no. 70078/12, paras 379-381 and para 418

³¹ ICCPR General Comment No. 16 (supra footnote n 10), paras 1,3,4,8,10

³² TCC, Doc No: 2022/33, Decision No: 2022/67, 1 June 2022, para 9 and Doc No: 2021/42, Decision No: 2022/45, 21 April 2022, para 13

³³ Protection Of Individuals With Regard To Automatic Processing Of Personal Data In The Context Of Profiling Recommendation, CM/Rec(2021)8 adopted by the Committee of Ministers of the Council of Europe on 21 November 2020, <https://edoc.coe.int/en/international-law/10670-protection-of-individuals-with-regard-to-automatic-processing-of-personal-data-in-the-context-of-profiling-recommendation-cmrec20218.html>

³⁴ Statewatch, 'Algorithmic persecution in Turkey's post-coup crackdown: The FETÖ-Meter system' co-authored by Dr. Emre Turkut and Ali Yildiz, pp. 20-28 <https://www.statewatch.org/media/2943/algorithmic-persecution-in-turkey-fetometer-report.pdf>

³⁵ Ibid, pp. 8-9.