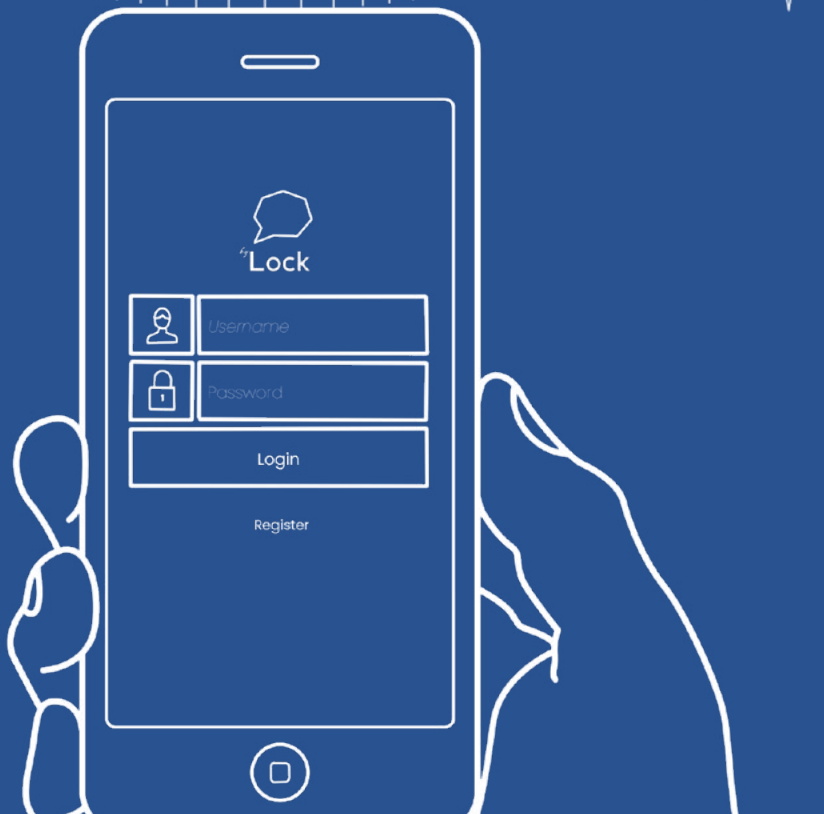
ByLock Prosecutions and the Right to Fair Trial in Turkey: The ECtHR Grand Chamber's Ruling in Yüksel Yalçınkaya v. Türkiye

Emre Turkut and Ali Yıldız



Publication information

About this report

Authors: Dr Emre Turkut and Ali Yıldız

Published by Statewatch, March 2024

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.

statewatch.org

(+44) (0) 203 393 8366

MayDay Rooms
88 Fleet Street
London EC4Y 1DH
UK

Support our work: make a donation

Scan the QR code or visit: statewatch.org/donate

Join our mailing list

statewatch.org/about/mailing-list

Registered UK charity number: 1154784

Registered UK company number: 08480724

Registered company name: The Libertarian Research & Education Trust Registered office: 88 Fleet Street, London EC4Y 1DH, UK.

Content

1. Introduction

Since the 2016 attempted coup in Turkey, over 90,000 individuals including public servants, police officers, academics, judges, prosecutors, business people and even university students and housewives have been purged or arrested for their alleged use of ByLock, an encrypted messaging app similar to Signal and Telegram. 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. 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.

The case of *Yalçınkaya v Turkiye*, 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. In the *Yalçınkaya* decision, the Grand Chamber found that the applicant's conviction based on the use of ByLock violated several important articles under the European Convention on Human Rights (ECHR), including Article 7 (no punishment without law), Article 6(1) (right to a fair trial) and Article 11 (freedom of assembly and association). More importantly, the Grand Chamber underscored that the problems leading to these human rights violations based on the vicious ByLock prosecutions were of a "systemic nature" and ordered the Turkish government to take appropriate general measures to address the issues, particularly regarding the Turkish judiciary's handling of ByLock evidence.

This report provides a comprehensive analysis of the ECtHR Grand Chamber judgment in the *Yalçınkaya* case, and the prosecutions related to the use of the ByLock app in Turkey. The clarity and non-disputed nature of the Grand Chamber's findings in *Yalçınkaya* under Article 7 of the ECHR are undeniably of paramount importance. However, we contend that the court left certain crucial questions unaddressed concerning the intersection of digital evidence and the right to a fair trial under Article 6 of the ECHR. Consequently, after conducting a thorough analysis of the *Yalçınkaya* judgment, we provide a nuanced examination of the Grand Chamber's findings under Article 6 ECHR.

Given the systemic problems caused by the ByLock app and the measures that Turkey must take to address these issues, the full implementation of the *Yalçınkaya* case may have wide-ranging implications. It could set a precedent for

thousands of similar cases in Turkey, where ByLock evidence played a decisive role in convictions and prosecutions during the post-coup period. It is clear that this decision will serve as a pivotal reference point in discussions on Turkey's application (or misuse) of terrorism provisions, digital and fair trial rights, ByLock usage, and the delicate balance between security concerns and individual liberties.

Despite its high precedential value for Turkey and potentially for several other countries grappling with the misuse of terrorism charges for contentious and controversial purposes, the *Yalçınkaya* case offers only limited normative guidance in the largely unchartered territory of digital evidence and human rights, particularly concerning electronic evidence derived from encrypted communications. In recent years, there has been a growing reliance on digital evidence in criminal proceedings, exemplified by SkyECC and EncroChat operations.[1]

These encrypted tools, widely utilized by organized crime groups, have resulted in thousands of arrests across Europe. The criminal proceedings related to SkyECC and EncroChat in various European countries have ignited intense debates surrounding the legality and integrity of digital encrypted data, the reliability of expert evidence, the neglect of fundamental criminal principles such as the equality of arms between the defence and prosecution, and notably, the lack of binding digital forensics standards – issues that give rise to concerns regarding compliance with fair trial requirements under Article 6 ECHR.[2]

In this regard, the *Yalçınkaya* case could have been an opportunity for the ECtHR to lay down normative standards regarding the human rights-compliant use of digital evidence obtained through encrypted communications, particularly given two pending EncroChat cases at the time of writing this report. Unfortunately, the ECtHR missed this opportunity, leaving important questions surrounding the intersection of digital evidence, human rights, and encrypted communications unresolved and unaddressed.

This analysis on the intersection of the use of digital evidence and the right to a fair trial under Article 6 of the ECHR can serve as a valuable reference for those engaged in the examination of other contemporary cases, *inter alia*, SkyECC and EncroChat. Primarily, however, it serves as a reminder for the Turkish authorities and policymakers to give full implementation to the *Yalçınkaya* judgment, and as a valuable source for lawyers and practitioners to tap into its huge potential. The use of digital evidence in criminal proceedings is increasing rapidly, and it is incumbent upon governments, judiciaries and legal practitioners to ensure that the changes this brings to criminal proceedings do not undermine human rights standards.

1 Fair Trials, 'EncroChat and SkyECC hacks' 8 November 2022, https://www.fairtrials.org/articles/news/encrochat-and-skyecc-hacks-germany-latest-eu-country-to-question-legality-of-evidence/.

2 Radina Stoykova, 'Encrochat: The hacker with a warrant and fair trials?' (2023) 46 *Forensic Science International: Digital Investigation*, 1-14 and Georgios Sagittea, 'On the lawfulness of the EncroChat and Sky ECC operations' (2023) 14.3 *New Journal of European Criminal Law*, 273-293.

2. Factual background

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 100,00 times on the Google Play Store alone.[3] 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,[4] while the actual numbers could be higher as this practice continues unabated.[5]

The Turkish government claims that ByLock was exclusively designed and developed to fulfil the communication needs of the Gülen Movement (GM) (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 companies such as the Fox-IT[6], and experts such as Jason Frankovitz[7] and Thomas Kevin Moore[8], have proved that this 'exclusivity claim' is erroneous.

Among the various criteria used to charge individuals under Article 314 of the Turkish Penal Code (TPC) for alleged membership in the GM, ByLock usage has emerged as the most damning and often decisive evidence, particularly in the post-coup period. A comprehensive report released by the Italian Federation for Human Rights in July 2023 confirms this finding. In a total of 78 of the 118 indictments examined, the report finds that "ByLock is used as incriminating evidence against suspects in order to establish their alleged membership of an armed terrorist organization."[9] The report also highlights that in none of these indictments were Turkish prosecutors able to present the content of communications allegedly made through the ByLock app. Instead, they appear to have grounded their allegations solely on the government's "exclusivity claim". It is noteworthy here that there is no concrete information as to how the ByLock data was acquired. Turkey's National Intelligence Organisation (*Millî İstihbarat Teşkilatı*, MIT hereafter) has said that its services came across the ByLock app "through using the methods, tools and techniques of technical intelligence that are unique to the Agency [*MIT*]"[10] which would normally diverge from standard legal safeguards. This assertion corroborates the reports that an MIT team had cracked the main ByLock servers, which were located in Lithuania.[11]

3 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

4 '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.

5 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

6 FOX-IT report, supra footnote 3.

7 Jason Frankovitz, Expert Report on ByLock, 9 August 2017, https://drive.google.com/file/d/0B_lp_O2-rTNqWlhlQnFOUDJzSzA/view?resourcekey=0-T0xxB0IYDkeF4lkF1-OJbA

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

9 Emre Turkut and Ali Yildiz, "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

10 MIT, 'ByLock Application Technical Report', p.12, https://foxitsecurity.files.wordpress.com/2017/09/bylock-mit-technical-report-turkish.pdf

11 Murat Yetkin, 'Gülenists' Existential Fight Over A Mobile Application' HuffPost, 26 October 2016.

Forensic focus 1: MIT's ByLock technical report

In relation to investigations and prosecutions concerning ByLock, Turkish police and judicial authorities exclusively rely on the findings of the Turkish National Intelligence Agency (MIT) ByLock report entitled 'A Technical Report on the ByLock Application'. A number of digital forensic analysts have conducted extensive analysis on the ByLock app and the MIT report, and dispute the central findings it offers. Notably, a respected international digital forensics firm, Fox-IT, has identified manipulations in the MIT report. Fox-IT's report found inconsistencies in the MIT report that indicate the manipulation of results and/or screenshots by MIT. This finding raises significant questions, as it is not clear which aspects of the report stem from original data, and which information was doctored by MIT (and to what end), what part of the information available to MIT was altered before presentation, why it was altered, and what exactly was left out or changed. Overall, the Fox-IT report considers "the MIT report implicit, not well-structured and lacking in essential details" and warns that "[w]hen a report is used as a basis for serious legal consequences, the author should be thorough and concise in the report as to leave no questions regarding the investigation".

The Turkish Court of Cassation and The Turkish Constitutional Court (TCC) have also decided, contrary to previous rulings on digital evidence, that using or downloading ByLock is sufficient evidence to convict a person of membership of an armed terrorist organization, even in the absence of any other evidence. In that regard, the Plenary of the Criminal Chambers of the Turkish Court of Cassation ruled in its judgment on 26 September 2017:

> *The involvement of an individual in the ByLock App network is to be determined based on the date and number of connections of the device belonging to that individual. Besides, the content of the correspondence circulated within the ByLock network is irrelevant in this regard. The content and the parties of the correspondence would be determinative in identifying the hierarchical position of the individual concerned within the terrorist organization… Since the ByLock messaging app is a communication network, exclusively designed and developed to fulfil the communication needs of the FETÖ terrorist organization, the detection, through technical means, of the involvement of any individual within this network beyond any doubt proves the linking of the individual to the terrorist organization.*[12]

This determination is in clear contravention of the Turkish Court of Cassation's own precedents, which require that there be "continuity, diversity and intensity" and "participation within the 'hierarchical structure knowingly and wilfully" to establish membership in an armed terrorist organization.[13]

12 Turkish Court of Cassation, E. 2017/16-956, K. 2017/370.

13 Italian Federation for Human Rights, Third Party Intervention to the European Court of Human Rights https://fidu.it/wp-content/uploads/THIRD-PARTY-INTERVENTION-BY-FIDU-logo-12.10.2021.pdf

Following this precedent setting decision by the Turkish Court of Cassation, the first instance courts followed suit and relied on the ByLock evidence to convict thousands of individuals. In the ByLock app cases, almost all Turkish first instance courts have denied defendants the possibility of effectively challenging ByLock evidence and crucially have dismissed defence counsel's requests for full access to the ByLock data (entitlement of disclosure) and have refused to commission an independent expert panel to examine the integrity of digital/electronic ByLock data.[14]

Another problematic issue is that the Turkish courts do not themselves have possession of the ByLock data, so they could only ask the Turkish police for this data (partially) in relation to the defendant. The police then share with the court a document called either "ByLock Inquiry Module Minute" or "ByLock Determination or Evaluation Minute", which includes some raw data (including phone numbers and activation data) as well as very limited and often self-contradictory log data.[15] This document often includes a disclaimer saying that the information provided by the report is in the form of intelligence, and therefore does not constitute a justification for judicial proceedings.[16]

Forensic focus 2: The "ByLock Determination or Evaluation Minute" Reports by Turkish police

Based on MIT's ByLock report, Turkish prosecutors and courts have predominantly relied on a form of evidence known as the "ByLock Determination or Evaluation Minute", provided by the police, to establish whether an individual is a user of the ByLock messaging app. Since 2016, Turkish authorities also produced or commissioned several reports on ByLock based on the MIT's ByLock Technical Report. These reports include:

1. ByLock / Analysis Report on Intra-organisational Communication Application, Department of Anti-Smuggling and Organised Crime (KOM) of the General Directorate of Security, dated 4 February 2020

2. Information and Identification Guidelines on ByLock Encrypted Communication Software, Department of Combatting Cyber Crime of General Directorate of Security

3. Intra-Forensics Technical Report, dated 21 August 2020 (reference IF-17776-20)

4. A report dated 22 May 2020 prepared by the Turkish police at the request of the Ankara Public Prosecutor's Office's letter dated 21 April 2020 and numbered 220-3/7990 B.M.

14 Data integrity is a process that ensures that the information stored in a database remains complete, accurate, and reliable throughout its lifecycle – see 'Data Intergity', Glossary, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/data_integrity

15 Under Additional Article 7 of the Turkish Law on Police Duty and Authority no.2559, and Article 6 of the Turkish Law on Intelligence Services (MIT Law), the Turkish police and MİT can conduct and apply several measures to gather intelligence. These measures involve physical and digital surveillance, wiretapping, the examination of internet traffic data, and so on. These intrusive powers are of a preventive nature and are granted to these institutions for purposes such as the prevention of disorder or crime. In addition, all those measures may be applied per se under a judgeship order, and under these provisions and the established jurisprudence of the Court of Cassation, information gathered through these measures may not be used as evidence in judicial proceedings.

16 According to Additional Section of the MIT Law, information collected as part of intelligence activities cannot be requested by judicial authorities for use as evidence in criminal proceedings, with the exception of espionage cases.

According to the original MIT ByLock report and subsequent police reports, the digital investigation extracted two databases named appDb and wordpress from ByLock material, using the Data Recovery Tool for InnoDB produced by Percona LLP, and TwinDb Data Recovery. According to the police reports, the Turkish police focused on appDb as it was relevant to their investigation, and appDb contained various tables with different data types following the standard relational database structure.

The Turkish authorities state that their analysis of the ByLock database uncovered 15 tables and 32 actions/events with encrypted sections, including messages in transit. And, despite some data corruption, the police allege that they successfully recovered and decrypted approximately 162.8 million records out of 163.8 million from the tables. About 94,638 were found to be corrupt and unrecoverable. Database corruption can lead to data loss and erratic behaviour by the associated software, which in this case could have affected the ByLock application on user devices. According to these reports, each and every event should be logged by ByLock. The events correspond to actions defined in the ByLock database's action/log table and include creating a user account, adding friends, logging in, logging out, sessions expiring, sending/making or receiving text/e-mail/calls and so on.

Yet, in almost all of the ByLock Determination and Evaluation Reports sent to Turkish courts, an anomaly consistently emerges. A significant number of user activities are logged when the user was supposedly not logged in to the service, including sending and receiving chat messages, reading and deleting emails, and adding or removing friends. Although these reports attempt to show log records and consequently user activities on the ByLock service, there are significant gaps and inconsistencies in the data, particularly concerning the creation of the user account and activities logged without the user being logged in – gaps which cannot be overlooked if ByLock is to continue to hold the legal weight that it does currently.

In two important decisions in the post-coup period, namely *Ferhat Kara*[17] of 2020 and *Adnan Şen*[18] of 2021, the TCC has largely upheld this judicial ByLock practice. These two judgments concern complaints of, *inter alia*, violation of the right to a fair trial on the ground that the data regarding the use of ByLock was obtained unlawfully. In these cases, the ByLock app was relied upon as the sole or decisive evidence for conviction for membership of the FETÖ/PDY, and the relevant digital data were not brought before the trial court. The TCC however found no violation in these cases. In the case of *Ferhat Kara*, it held:

17 TCC, Individual Application, *Ferhat Kara*, B. No: 2018/15231, 04 June 2020, https://karar-larbilgibankasi.anayasa.gov.tr/BB/2018/15231?Dil=en

18 TCC, Individual Application, *Adnan Şen*, B. No: 2018/8903, 15 April 2021 https://kararlar-bilgibankasi.anayasa.gov.tr/BB/2018/8903

…the defendant was bestowed with the rights stemming from the equality of arms and adversarial proceedings and thereby [was] enabled to challenge the authenticity of the evidence concerning his ByLock app-usage… Judging from its structure, its way of deployment and its technical features, the ByLock App is an encrypted communication means that is exclusively dedicated to the organizational communication needs of the members of the FETÖ terrorist organization. The conviction of the applicant for membership of a terrorist organization, based on his usage of the ByLock App is not a violation of the right to a fair trial.[19]

The *Ferhat Kara* and *Adnan Şen* decisions mark a departure for the TCC from its own standards. In three other important judgments, namely in *Yavuz Pehlivan* (2013), *Sencer Başat* (2013) and *Yankı Bağcıoğlu* (2014), the TCC concluded that the defendant should be given an opportunity to conduct a technical examination of the relevant digital materials, and that domestic courts should commission independent expert panels to conduct such an examination, otherwise the principle of the equality of arms would be violated.[20] The TCC, however, ignored these precedents and principles in the post-coup ByLock cases, citing justification of minimal legal value including the complex nature of the FETÖ/PDY organization and the perceived significance of the ByLock app in the alleged terrorist organization's communication.

19 TCC, Ferhat Kara, supra footnote 17, para 159.

20 TCC, Individual Applications, *Yavuz Pehlivan and others*, App No. 2013/2312, 04 June 2015, *Yankı Bağcıoğlu and others*, App No. 2014/253, 09 January 2015, *Sencer Başat and others*, App No. 2013/7800, 18 June 2014.

3. ByLock cases before international human rights bodies

a. UN bodies

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.[21] 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.[22]

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. In parallel to what the ECtHR has established, the Working Group opines that the criminal nature or context of the correspondence via the ByLock App must be given regard when assessing the evidential value of the use of that app to establish terrorist membership.

Furthermore, the WGAD notes numerous cases involving the arrest and prosecution of individuals on the basis of their alleged use of ByLock, where such use is considered to be the key manifestation of an alleged criminal activity. In referring to those cases, along with those that are under scrutiny, the WGAD also concludes that, in the absence of a specific explanation of how the mere use of ByLock constitutes a criminal act, the detention of those accused was arbitrary. The Working Group goes on to find that even if any of the suspected individuals had used ByLock, this use would constitute merely the exercise of their freedom of expression, a right that is protected under Article 19 of the International Covenant on Civil and Political Rights: the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers… through any media of choice."

Having expressed its regrets that its opinions have not been respected by the Turkish authorities, and that the cases in question follow the same pattern, the 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 are crimes against humanity. A report by the NGO *instituDE* examines in detail the widespread or systematic commission of the crime of the arbitrary deprivation of liberty on the pretext of, amongst other things, the use of ByLock, and its potential qualification as a crime against humanity.[23]

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

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

23 *Institude*, Human Rights Violations in Turkey rising to the level of Crimes against Humanity : The Case of Gülen Group, 13 August 2021, https://institude.org/report/human-rights-violations-in-turkey-rising-to-the-level-of-crimes-against-humanity-case-of-Gülen-group.

In a similar vein, in the case of *Ismet Ozcelik*,[24] where the complainant was accused of membership of an armed terrorist organisation on the basis of downloading ByLock, the UN Human Rights Committee (HRC) said:

> *… the only evidence held against İsmet Özçelik is the use of the ByLock application and the deposit of funds in Bank Asya. In these circumstances, the Committee considers that the State party has not established that the authors were promptly informed of the charges against them and the reason for their arrest, nor was it substantiated that their detention meets the criteria of reasonability and necessity. It recalls that a derogation under Article 4 cannot justify a deprivation of liberty that is unreasonable or unnecessary. The Committee therefore finds that the authors' detention amounted to a violation of their rights under Article 9 (1-2) of the Covenant.*[25]

In its decision, the HRC refers to the report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression, who visited Turkey in November 2016, and who recorded numerous cases of arrests that were based solely on the presence of ByLock on the accused person's computer and on ambiguous evidence. In reference to this, the HRC notes the dangerous pattern being established by these cases. Finally, the Committee holds that the detention of the individuals concerned, on the mere ground of the use of ByLock, fails to meet the twin criteria of reasonableness and necessity.

b. The European Court of Human Rights

To date, the ECtHR has issued several important decisions that relate to the use of ByLock. Arguably, the recent case of *Yalçınkaya v Türkiye* from 26 September 2023 stands as the most important decision given the numerous violations the Court found in this application. However, before delving further into the *Yalçınkaya* case and its precursor case of *Akgün v Turkiye*, developments leading up to the ruling will be analysed.

The first decision communicated to Turkey on the use of ByLock was *Akgun v Türkiye*,[26] on 2 April 2019. Given the particularities of the *Akgün* case, the ECtHR's questions were limited mainly to detention standards including reasonable suspicion and relevant safeguards to challenge detention under Article 5 ECHR. In this regard, they did not raise novel issues with regard to the ByLock evidence, and thus the Court's approach was rather modest.

A more critical and in-depth approach was taken in the subsequent group of communicated cases, including the case of *Yalçınkaya.* This case was communicated to Turkey on 19 February 2021.[27] In its communication, the ECtHR posed several critical questions to the Turkish government, covering important issues including the process of acquisition and analysis of the ByLock data under the law governing data retention; the evidentiary value of the ByLock evidence; and the reliability, accuracy, authenticity and integrity of the ByLock data on which the allegations of ByLock use are predicated.

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

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

26 ECtHR, *Tekin Akgün v Turkey* App No 19699/18, 20 July 2021 (see below section 3).

27 The ECtHR's communication to Turkey is available at: http://hudoc.echr.coe.int/eng?i=001-208743

It is important to stress that the ECtHR formulated these questions in such a way as to delve into the technical aspects of the ByLock investigations to uncover whether basic principles of digital forensics were complied with throughout the domestic processes. More specifically, the ECtHR requested that the Turkish government explain what the raw data obtained by the MIT report involved, and how MIT processed that data in order to identify the individual users of ByLock, including the applicant, before handing the relevant data over to the prosecuting authorities.[28] Importantly, these critical questions mainly relate to a core principle of criminal proceedings: equality of arms. As the ECtHR has consistently held in its case law, the proceedings must be adversarial and parties must be given an opportunity to comprehensively challenge the basis of the allegations against them.

At its core, the ECtHR was sceptical that ByLock meets such important standards. Many individuals whose detentions and convictions were based on the alleged use of ByLock in Turkey were denied access, which then prevented them from challenging the lawfulness of their detentions and convictions.

i. The Akgün judgment

The applicant in this case was a former police officer put into pre-trial detention in October 2016 due to his alleged use of the ByLock app. He was subsequently convicted for being a member of a terrorist organization, referred to by the Turkish authorities as FETO/PDY. After exhausting domestic remedies, the applicant lodged an application before the ECtHR with regard to his placement in pre-trial detention. 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 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 FETO/PDY organisation for the purposes of internal communication. In the absence of other evidence or information, the document in question, stating merely that the applicant was a user 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.

In its defence, Turkey employed two expert reports, which basically reiterate the conclusions of the official ByLock Technical Report produced by MIT. It appears from the way in which the authors of these reports drew conclusions that they had also not been granted access to the raw ByLock data. As such, they had to base their conclusions on the findings of the MIT report, thus considerably impairing their credibility, objectivity and accuracy. That the Turkish government did not even grant the forensic experts that it hired access to the original, unpro-

28 See also a blog post summarizing the *Yalçınkaya* case and scrutinizing the questions posed by the ECtHR within the context of this case, from both the legal and technical perspectives: Yasir Gökçe, Admissibility of ByLock related data as evidence is now under the scrutiny of the European Court, https://strasbourgobservers.com/2021/07/07/admissibility-of-ByLock-related-data-as-evidence-is-now-under-the-scrutiny-of-the-european-court/

cessed ByLock data, reveals the extent to which MIT had deviated, in its ByLock investigation, from the most basic principles of digital forensics.

Related to this, the ECtHR established that neither the applicant nor his lawyer had sufficient knowledge of the substance of the ByLock data. In other words, the applicant was not aware of the variety of evidence underlying the allegation that he had used ByLock and had therefore not been sufficiently and equally empowered to challenge the accusations that were put against him. As such, he was deprived of his right, stemming from the equality of arms and adversarial proceedings, leading to a violation of Article 5(4) of the Convention.

The European Court also found that the domestic court had not been sufficiently informed of the substance of the evidence, when ordering the applicant's pre-trial detention in October 2016. More precisely, the domestic court did not possess sufficient information on the nature of ByLock to conclude that the messaging app was used exclusively by members of the GM for the purposes of internal communication.

The court also ruled that "as a matter of principle, the mere fact of downloading or using a means of encrypted communication, or indeed the use of any other method of safeguarding the private nature of exchanged messages, could not in itself amount to evidence capable of satisfying an objective observer that an illegal or criminal activity was being engaged in." In other words, the ECtHR considers that, in principle, the use of Bylock is part of an enjoyment of the right to privacy, as well as of the right to respect for one's private life. According to the European Court, the domestic court should have paid attention to the way in which ByLock was employed by Mr Akgün. In the absence of other evidence or information, an official report, stating merely that the applicant was a user of ByLock, could not, taken alone, indicate that there were reasonable grounds for suspicion that could satisfy an objective observer that the defendant had indeed used ByLock in a manner that might amount to evidence of membership of a terrorist organisation.

Furthermore, the ECtHR found that the predication of suspicion based merely on digital evidence is problematic because the nature of the procedure and the technology used to collect digital evidence is complex and may therefore diminish the ability of national judges to establish its authenticity, accuracy and integrity. Where such evidence is the sole or exclusive basis for suspicion about a suspect, the national judge must seek further information before examining its potential evidentiary value under domestic law. It was only where the use of an encrypted communication tool was supported by other evidence about that use, such as, for example, the content of the exchanged messages or the context of such exchanges, that one is able to speak of evidence that may satisfy an objective observer that there were reasonable grounds to suspect the individual who was using that communication tool of being a member of a criminal organization.

Lastly, it is worth noting that the ECtHR puts emphasis on supporting evidence which particularly points to the existence of an "illegal" and/or "criminal"

activity that furthers the objectives of a "criminal" organization, such as the illegal or criminal nature of the content of messages. When considering the vagueness and ambiguity of the criteria for terrorist membership in Turkey, the European Court appears to promote the redefinition or reinterpretation of "terrorist membership" around these terms.

ii. The Taner Kılıç judgment

In the case of *Taner Kılıç*,[29] the applicant was a prominent human rights defender and a co-founder of the Turkish branch of Amnesty International. In June 2017, his residence and workplace underwent a search, leading to his arrest based on allegations related to his purported affiliation with an armed terrorist organization, namely FETÖ/PDY. He was subsequently detained by a Turkish magistrate judge, who made reference to his download and use of ByLock. Additionally, contextual factors contributing to the detention included 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. The pre-trial detention was subject to multiple extensions, culminating in the applicant's conviction for membership in an armed terrorist organization, resulting in a sentence of six years and three months' imprisonment.

In its decision, the ECtHR conducted a comprehensive examination of the case under Articles 5(1), 5(3), 5(4), and 5(5), as well as Article 10 ECHR. Notably, the court's findings concerning Article 5 are significant with regard to the use of ByLock. Under this part of the judgment, the Court initially distinguished the present case from its *Akgün* judgment, wherein the Turkish government was found to have breached Article 5(1), (3), and (4) by solely grounding the applicant's arrest and pre-trial detention on the alleged use of ByLock. In contrast, the evidence presented by the domestic authorities in this 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. As such, the circumstantial evidence initially relied upon by the authorities was deemed insufficient to ground reasonable suspicion that the charges against the applicant constituted a criminal offence at the relevant time. The court observed that, based on the case records, the use of ByLock emerged as the decisive factor supporting the charges. Building upon *Akgün*, the Court highlighted that the exclusive use of an encrypted communication application could not, by itself, be considered a constituent element of a criminal offence. This inadequacy left an objective observer without elements reasonably convincing them that a criminal offence had occurred.[30]

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

30 Para. 106 of *Taner Kılıç* judgment.

Forensic focus 3: An Example of 'ByLock Determination or Evaluation Minute'

For the purposes of the present report, the authors have conducted a detailed examination of a 'ByLock Determination or Evaluation Minute' report. In the said report, there are:

- 107 instances of user 1XXXXX logging in while already logged in;
- 14 instances of user 1XXXXX logging out when already logged out;
- 107 instances where a session timed out without any active session.

These discrepancies suggest that the logout event, which should follow a login event, and session expiry, which should follow an active session, are not logically consistent within the data. The above-mentioned ByLock determination report also shows significant delays in message delivery which indicates data processing errors:

- 11 messages lack a "received" time;
- one message has a "received" time dated January 9th, 1900;
- 2,854 messages were delayed by more than six hours;
- one message was marked as "received" more than 86 hours after being sent.

Regarding messages user 1XXXXXX exchanged, there are several problems:

- four messages with no 'sender' account number;
- one message with no 'recipient' account number;
- 11 messages with no 'received' date;
- 996 blank messages.

More than 190 messages contained text indicating they could not be decrypted.

In summary, the log data contains a number of anomalies that raise questions about the integrity and accuracy of the recorded data. These include illogical session events, significant message delivery delays, and issues with the message content records.

It is noted that each sent message should correspond to an event '13' in the ByLock log data. However, upon cross-referencing these messages with the log data, several discrepancies are found. For instance:

- on a particular day in September 2015, the log entries indicate that

user 1XXXXXX exchanged several messages with user 7XXXXX, but there are no records of exchanged messages on this date;

- there is no recorded activity for user 1XXXXXX on a particular day in November 2015, although several messages are listed as sent on this date;
- on a particular day in December 2015, there are log entries for five messages sent to user 7XXXX, but none match the indicated timestamp.

In conclusion, listed messages and event logs largely do not match. This discrepancy raises concerns about the integrity of the log data and the accuracy of the messaging records.

MIT's ByLock report indicates that a user must be logged in order to access the application's functionality. The log data presented in the ByLock Determination and Evaluation Report that we examined, however, shows that user 1XXXXX apparently sent and received messages, amended "friend" associations, and so forth, on 2,782 distinct occasions without being logged in. On the one hand, this could indicate that there are fundamental errors in the log data. Alternatively, it could demonstrate that there is no requirement for a user to be logged in to make use of the ByLock services. This latter possibility would, of course, throw into serious doubt the attribution of actions to a particular user.

Log data contains chronologically nonsensical log data in the form of logging in whilst already logged in, logging out whilst already logged out or having a user session expire, despite apparently not having logged in. The substantial number of inconsistencies in the log data, along with the fact that these have apparently neither been detected nor resolved is problematic from a forensic perspective.

Moreover, multiple expert reports conclusively demonstrated that Mr Kılıç had never utilized the ByLock system. Remarkably, these reports were only taken into consideration in January 2019, when the Istanbul Assize (Heavy Panel) Court[31] ordered the termination of the applicant's pre-trial detention "in light of the evidence."[32] These factors led the court to find violations of Article 5(1) and (3) ECHR with respect to the applicant's detention, which was unlawful and arbitrary.[33] The court also found that the applicant did not possess an effective remedy for these violations which amounted to a violation of Article 5(5) ECHR.[34] Finally, the ECtHR observed that the pre-trial detention of the applicant was intricately tied to his role as a human rights defender, potentially exerting a "chilling effect" on such activities,[35] leading to a conclusion that there had been a violation of Article 10 ECHR (freedom of expression).

31 Assize (heavy penal) courts in Turkey deal with serious crimes including crimes against the security of the state and constitutional order as other cases that require a sentence of more than ten years of imprisonment including life imprisonment – see the Turkish Justice System Booklet, Turkish Justice Academy, https://taa.gov.tr/yuklenenler/dosyalar/0e03c8d1-c1be-4c7f-ada0-97ba13291f65-turk-yargi-sistemi-brosur-son-28.08.2020-eng2.pdf

32 Para. 36 of *Taner Kılıç* judgment.

33 Paras. 116 and 120 of *Taner Kılıç* judgment.

34 Para. 128 of *Taner Kılıç* judgment.

35 Para. 144 of *Taner Kılıç* judgment.

4. The European Court of Human Rights judgment in Yalçınkaya

a. Factual background

The *Yalçınkaya* case (15669/20) concerns an application lodged on 17 March 2020 by a teacher who was dismissed from public service through a coercive state of emergency decree issued on 1 September 2016, during the post-2016 coup period in Turkey.[36] In his application to the ECtHR, the applicant challenged his trial and conviction under Article 314(2) of the TPC for alleged membership in a terrorist organisation, the GM, which the Turkish authorities designated as the FETÖ/PDY due to their alleged involvement in organising the 2016 attempted coup.

On 6 September 2016, the applicant was arrested on suspicion of membership of the GM. He was interrogated by the police on 8 September 2016, mainly on the allegation that he used the ByLock app. On 9 September 2016, he was placed in pre-trial detention. On 6 January 2017, the Kayseri public prosecutor filed a bill of indictment against the applicant with the Kayseri Heavy Penal Court. At the first hearing held on 21 March that year, the Kayseri Court convicted the applicant and sentenced him to six years and three months imprisonment. The crucial evidence leading to the applicant's conviction was the use of ByLock. The Kayseri Court also took into account other evidence including the applicant's membership of a trade union and an association which were closed down under state of emergency rule over their alleged links with FETÖ/PDY, and his February 2014 deposit of 3,110 Turkish lira (approximately €1,000 at the time) in Bank Asya, which was closed down on alleged GM charges during the Turkish post-coup emergency period.

On 9 October 2017, the Ankara Regional Appeals Court dismissed the applicant's appeal request. To substantiate the evidence, especially the ByLock use claim, the Turkish Information and Communication Technologies Agency (*Bilgi Teknolojileri ve İletişim Kurumu*, BTK[37]) provided the Court with a report dated 29 June 2017. This was prepared by a digital forensics expert and indicated that the applicant had connected to the ByLock server's IP address a total of 380 times, on six different days between 3 and 23 October 2015

On 30 October 2018, the Turkish Court of Cassation upheld the applicant's conviction, and on 26 November 2019, the TCC summarily dismissed the applicant's individual application as manifestly ill-founded. As noted above, the *Yalçınkaya* case was communicated to the Turkish Government on 19 February 2021. On 3 May 2022, the Grand Chamber of the ECtHR was granted jurisdiction over the case, and following a hearing on 18 January 2023, delivered its decision some eight months later, on 26 September. In its decision, the Grand Chamber found that the applicant's conviction based on the use of ByLock violated several important articles under the ECHR, including Article 7 (no punishment without

36 Decree No. 672 of 1 September 2016, available at https://rm.coe.int/16806a2e17.

37 The BTK is responsible for the regulation of telecommunications services and providers.

law), Article 6(1) (right to a fair trial) and Article 11 (freedom of assembly and association).

b. Findings under Articles 7 and 11

As noted above, the Turkish domestic courts, including the Turkish Court of Cassation and the TCC, have consistently regarded the downloading or use of ByLock as sufficient grounds for convicting someone of membership in an armed terrorist organisation, even in the absence of other evidence. To the Grand Chamber, these 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 out of over 25,000 violations between 1959 and 2022.[38]

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.[39]

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.

c. Findings under Article 6

The Grand Chamber thoroughly analysed the applicant's complaints under Article 6 ECHR (right to a fair trial), issuing crucial findings. However, it also 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. In what follows, we will delve into the key components of a fair trial including admissibility of evidence, quality of evidence, requirement of an adversarial proceeding, and entitlement of disclosure.

38 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.

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

i. Admissibility/Reliability of ByLock evidence

Relying on Article 38 of the Turkish Constitution[40] and Additional Section 1 of the *MIT Law*,[41] the applicant argued that ByLock data was inadmissible evidence.

The court first clarified its role in determining the admissibility of a piece of evidence or reviewing its assessment by national courts. It noted that, while Article 6 ECHR guarantees the right to a fair trial, "it does not lay down any rules on the admissibility of evidence or the way in which evidence should be assessed, these being primarily matters for regulation by national law and the national courts."[42] It is therefore not for the court "to pronounce on whether and in what circumstances and format intelligence information may be admitted in criminal proceedings as evidence," given the limits of the court's power as regards the admissibility and assessment of evidence, which is a matter that primarily remains within the discretion of national courts and other competent authorities."[43] Accordingly, the court's task is to review "whether the proceedings as a whole, including the way in which the evidence was obtained, were fair," and importantly, "whether the applicant was given the opportunity to challenge the evidence and to oppose its use."[44]

The ECtHR observed that the applicant's conviction for membership of an armed terrorist organisation rested decisively on the finding that he had used the ByLock application, a finding primarily based on the data obtained by the MIT report. In such circumstances, as the court held, the quality of the evidence in question and the applicant's ability to effectively challenge it in proceedings that complied with the guarantees of Article 6(1) (entitlement to a fair and public hearing) were all the more important.

In this connection, the ECtHR clearly observed that "sections 4(1) and 6(1) of the [*MIT Law*], invoked by the domestic courts and the Government as the legal basis for the MIT's conduct, do not envisage procedural safeguards akin to those set out under Article 134 of the CCP [referring to the Turkish Code of Criminal Procedure] with respect to the collection of electronic evidence, including independent authorisation or oversight." The court went on to acknowledge that in cases where the collection or processing of such information is not subject to prior independent authorisation or supervision or a *post factum* (retrospective) judicial review, or where it is not accompanied by other procedural safeguards or corroborated by other evidence, its reliability may be more likely to be called into question.[45]

ii. Quality of the ByLock evidence

The Court also highlighted that ByLock data is electronic evidence and as such its collection, securing, processing and analysis requires special technologies, and raises distinct reliability issues as it is inherently more prone to destruction, damage, alteration or manipulation.[46]

40 Article 38 stipulates that "findings obtained through illegal methods shall not be considered evidence". See: The Constitution of Turkey, https://www.anayasa.gov.tr/media/7258/anayasa_eng.pdf

41 On the content of this provision, see, supra footnote 16.

42 Para. 302 of *Yalçınkaya* judgment.

43 Para. 314 of *Yalçınkaya* judgment.

44 Para. 303 of *Yalçınkaya* judgment.

45 Para. 314 of *Yalçınkaya* judgment.

46 Para. 312 of *Yalçınkaya* judgment.

The European Court notes that the MIT had apparently retained the ByLock data for many months prior to their submission to the judicial authorities, and the Ankara Fourth Magistrate's Court's subsequent order for the examination of the ByLock data pursuant to Article 134 of the Turkish Code of Criminal Procedures (TCCP) cannot entail a *post factum* judicial review of the MİT's data collection activity. Thus, the Court concludes that the applicant's doubts regarding the reliability of the ByLock data were not abstract or baseless, and thus may not be readily dismissed.[47]

The ECtHR recognises that the circumstances in which the ByLock data was retrieved by the MIT raised *prima facie* doubts as to their "quality" in the absence of specific procedural safeguards geared to ensuring their integrity until the handover to the judicial authorities.[48] The Court goes on to say that given the absence of any concrete information in the case file to suggest that the data in question had at any point been subjected to examination for verification of their integrity, whether at the time of their submission to the judicial authorities in December 2016 or subsequently, the Court considers that the applicant had a legitimate interest in seeking their examination by independent experts and that the courts had the duty to properly respond to him.[49]

The European Court notes, however, that the domestic courts did not address the matter of how the integrity of the data obtained from the server had been ensured in all respects particularly in the period prior to their transmission to the judicial authorities on 9 December 2016. More specifically, they did not account for the fact that between their collection by the MIT and the magistrate's court's subsequent order for their examination, the ByLock data had already been processed and used not only for intelligence purposes, but as criminal evidence to initiate investigations and arrest suspects, including the applicant.[50]

The Court further observes that, while ByLock data combined with internet traffic and location data could potentially identify an individual as a ByLock user, the Turkish Government's claim that the ByLock app was exclusively used by alleged members of the FETÖ/PDY for organizational purposes adds heightened significance to the maintenance and validity of the raw ByLock data. Despite this increased importance, the ECtHR points out that the judgments of the Turkish domestic courts, including the Court of Cassation, relied primarily on extrajudicial findings by the MIT regarding the alleged exclusive and organizational nature of ByLock and did not thoroughly scrutinise those findings.

iii. Adversarial proceedings and the equality of arms

According to the ECtHR, a fundamental aspect of the right to a fair trial is that criminal proceedings should be adversarial and that there should be equality of arms between the prosecution and defence. This means both the prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party.[51]

47 para. 317 of *Yalçınkaya* judgment.

48 para. 323 of *Yalçınkaya* judgment..

49 para. 333 of *Yalçınkaya* judgment.

50 para. 334 of *Yalçınkaya* judgment.

51 Para. 306 of *Yalçınkaya* judgment.

iv. Requirement of disclosure

The ECtHR underlines that the right to an adversarial trial also requires that the prosecution authorities disclose to the defence all "material evidence" in their possession for or against the accused, and consequently vests the defence with the entitlement of disclosure. According to the Court, the term "material evidence" cannot be construed narrowly, in the sense that it cannot be confined to evidence considered as relevant by the prosecution. Rather, it covers all material in the possession of the authorities with potential relevance to the defence's case, also if not at all considered, or not considered as relevant.[52]

Given that the applicant's conviction for membership of an armed terrorist organisation rested decisively on the finding that he had used the ByLock application based on the data obtained by MIT, the European Court unequivocally noted that the applicant should have the right to seek access to the data underpinning the accusation of his being a ByLock user and having used it for the purposes of organising the GM.[53]

In this connection, the ECtHR highlighted that the applicant had available to him all the ByLock reports relied on by the domestic courts in the criminal proceedings, and that the accuracy of the ByLock data pertaining to him had been verified on the basis of data obtained from other sources. However, the Court considered that they were not determinative of the question of whether the applicant's defence rights *vis-à-vis* the ByLock evidence were duly respected in the present case.[54]

The ECtHR also highlighted that that the requirement of disclosure to the defence of "all material evidence" for or against the accused cannot be construed narrowly, in the sense that it cannot be confined to evidence considered relevant by the prosecution. Rather, it covers all material in the possession of the authorities with potential relevance for the defence, even if not at all considered, or not considered as relevant by the prosecution authorities. Accordingly, the fact that the applicant had access to all the ByLock reports included in the case file does not necessarily mean that he had no right or interest to seek access to the data from which those reports had been generated.[55] The European Court notes that the applicant was given no explanation by the domestic courts as to why, and upon whose decision, the raw data – particularly to the extent that they concerned him specifically – were kept from him. He was therefore deprived of the opportunity to challenge this restriction.[56]

v. Independent expert examination

According to the ECtHR, a review of the overall fairness of the proceedings must also incorporate an assessment as to whether the applicant was given the opportunity of challenging the evidence and of opposing its use in circumstances where the principles of adversarial proceedings and equality of arms between the prosecution and the defence were respected.[57] Taken from this perspective, a potentially signif-

52 Para. 307 of *Yalçınkaya* judgment.

53 Para. 327 of *Yalçınkaya* judgment.

54 para. 326 of *Yalçınkaya* judgment.

55 Para. 327 of *Yalçınkaya* judgment.

56 para. 331 of *Yalçınkaya* judgment.

57 para. 324 of *Yalçınkaya* judgment.

icant avenue for challenging evidence could be done through the engagement and involvement of independent experts, whose examination could serve as a crucial mechanism in ensuring the integrity and reliability of ByLock as an evidentiary foundation.

The ECtHR Grand Chamber, in its substantive analysis, underscores the legitimate interest of the applicant in petitioning for the examination of the raw ByLock material by impartial and independent experts. In this regard, the Turkish courts bear the onus of providing an appropriate response to such legitimate concerns, as the data under scrutiny may have undergone various phases of examination to verify its integrity, whether at the time of their submission to the judicial authorities in December 2016 or subsequently.[58]

Implicit in the ECtHR's reasoning is the recognition that the applicant's pursuit of an independent examination is not merely an exercise in procedural formality but a manifestation of the overarching commitment to uphold the principles of justice, fairness, and due process. The right to challenge evidence through the engagement of independent expertise emerges as an essential component of safeguarding the integrity of legal proceedings and ensuring that the principles of adversarial justice and equality between the prosecution and defence are steadfastly maintained.

vi. Lack of reasoning and ignored requests

The ECtHR first underlines that, in principle, the inability of the defence to have direct access to the evidence and to test its integrity and reliability firsthand places a greater onus on the domestic courts to subject those issues to the most searching scrutiny.[59] Yet, the applicant's requests (i.e. the commission of an independent expert panel, disclosure of evidence, access to ByLock material, questions about admissibility of evidence, disconnection in the chain of evidence) which were relevant and significant to his defence, were either readily dismissed or even left unanswered.[60]

The European Court concluded that the aforementioned prejudice sustained by the defence was compounded by the deficiencies in the domestic courts' reasoning *vis-à-vis* the ByLock evidence. The applicant deemed it important to access all the ByLock material to be able to contest the accuracy of the allegations made in his regard, in particular to refute the argument that the ByLock application had been used "exclusively" by the members of the FETÖ/PDY, or that he had used it for "organisational" purposes. The defendant could not challenge this claim directly on the basis of the ByLock data, because it lay at the prosecution's sole disposal. Therefore, it was crucial for the domestic courts to support them with sufficient and pertinent reasoning, and to address the applicant's objections regarding their veracity, which they failed to do.[61]

58 para. 333 of *Yalçınkaya* judgment.

59 para. 334 of *Yalçınkaya* judgment.

60 paras. 334-336 of *Yalçınkaya* judgment.

61 para. 337 of *Yalçınkaya* judgment.

vii. Conclusion

Overall, the ECtHR found that there were not enough safeguards in place to ensure that the applicant had a genuine opportunity to challenge the evidence against him and conduct his defence in an effective manner - on an equal footing with the prosecution. The domestic courts' failure to respond to the applicant's specific and pertinent requests and objections raised a legitimate doubt that they were impervious to the defence arguments and that the applicant was not truly "heard". The domestic courts' silence on vital matters that went to the heart of the case also raised well-founded concerns on the applicant's part regarding their findings and the conduct of the criminal proceedings "as a matter of form" only.[62] In light of these factors, the European Court found that Article 6(1) ECHR was breached.[63]

d. Criticism of the Yalçınkaya judgment

The *Yalçınkaya* judgment has garnered mostly positive responses. Scholars and Turkey observers have frequently commented on the case as one with the potential to have far-reaching implications, setting a precedent for thousands of similar cases in Turkey where ByLock evidence was decisively used for convictions and prosecutions in the post-coup period. Yet, as noted above, the ECtHR Grand Chamber judgment leaves some important questions unaddressed.

i. The status of Gülen Movement at the material time

One important question the Grand Chamber overlooked relates to the status of GM at the material time. It is clear that at the time of the acts attributed to the applicant, namely the use of ByLock, the GM was not proscribed as a terrorist organization and, on the contrary, enjoyed a wide and respectable presence in all sectors of Turkish society. Despite this fact, the Turkish judiciary had applied the material and mental elements of the offence retrospectively – an approach of the Grand Chamber that Dr Yasir Gokce finds "unfortunate".[64] Relatedly, he argues that "it would have been an eye-opener for the Turkish government if the court had scrutinized whether this secret communication app was used during and/or for the purpose of staging the 15 July coup attempt, which the government alleges, has been orchestrated by the Gülen Movement and due to which, by and large, the latter was declared as a terrorist organization."[65]

ii. The 'quality of law' test of Article 314 of the Turkish Penal Code

Another problematic approach of the Grand Chamber was related to the quality of law test with regard to Article 314(2) of the TPC. On this point, in the *Yalçınkaya* case, the Grand Chamber clearly found that the Turkish judiciary's interpretation of Article 314(2) TPC in ByLock related cases violated Article 7 ECHR. However, it has held that Article 314(2) was in principle foreseeable and articulated with

62 para. 341 of *Yalçınkaya* judgment.

63 para. 346 of *Yalçınkaya* judgment.

64 asir Gokce, 'Systemic Problems Unveiled: The Yalçınkaya Case and the Demise of the ByLock Digital Evidence' ECHR Blog, 25 October 2023, https://www.echrblog.com/2023/10/systemic-problems-unveiled-Yalcinkaya.html

65 Ibid.

sufficient precision to allow an individual, with suitable legal advice if necessary, to discern which actions or omissions might subject them to criminal liability. In his analysis, Ali Yildiz highlights that this approach is inconsistent with the Grand Chamber's findings in many post-coup cases, *inter alia* the case of *Selahattin Demirtas v Turkey II* of December 2020. Here, the court remarked that "national courts seem to have overlooked the principles of Article 314(2) TPC established in the case law of the Turkish Court of Cassation (namely standards of continuity, diversity and intensity)" and that Article 314(2) TPC's foreseeability is questionable in the context of Article 5 ECHR. [66]

iii. The collection and acquisition of ByLock data

The ECtHR Grand Chamber's approach to the illegally obtained ByLock evidence was also problematic. To recap what was highlighted above, in his application, the applicant argued that the ByLock evidence was seized and used in breach of the requirements laid out in domestic law, specifically Article 6(2)-(4) of the MIT Law and Articles 134-135 of the TCCP. Article 6(2) of the MIT Law stipulates that a prior court order is required for the MIT to interfere with communications performed via means of telecommunication. At the time of seizure, it seems that the MIT obtained all the data from the ByLock server without any judicial decision. Later on, the MIT examined the ByLock digital materials in the absence of any prior judicial decision, prepared a technical report, determining the users of this communication tool and shared the data on a USB stick and hard disk with the police and the chief public prosecutor's office in Ankara in May 2016 without any judicial control.

As detailed above, in an attempt to rectify these procedural errors and shortcomings, in its precedent-setting judgment on 24 April 2017, the Turkish Court of Cassation erroneously relied on Article 134 of TCCP (on "search of computers, computer programs and transcripts, copying and provisional seizure"), rather than the sole correct provision applicable in this case, namely Article 135 of the TCCP (on "interception of correspondence through telecommunication"). This gave rise to several important legality issues and the applicant, Yalçınkaya, raised these claims in relation to his right to a fair trial because his conviction was decided on illegally obtained evidence, in contradiction with the clear provisions of domestic law.

The Grand Chamber, however, took another approach in its judgment. Rather than delving into these complaints, its focus was largely limited to examining the domestic court's reasoning. It is important to note that the ECtHR has a limited role in determining the admissibility of a piece of evidence or reviewing its assessment by national courts. It has consistently held in its case law that it does not determine "whether the contested evidence was actually obtained lawfully in terms of domestic law and was admissible, or whether the domestic courts made any substantive errors in their assessment of the relevant evidence" and that its task under Article 6(1) ECHR is "rather to assess the fairness of the proceedings

66 Ali Yildiz, 'Strasburg Weighs In On Political Persecution In Turkey', Verfassungsblog, 31 October 2023, https://verfassungsblog.de/strasburg-weighs-in-on-political-persecution-in-turkey/

as a whole, taking into account the specific nature and circumstances of the case, including the way in which the evidence was taken and used, and the manner in which any objections concerning the evidence were dealt with."[67]

Viewed from this perspective, one might contend that the court's approach is justified. Yet, adopting a more uniform stance regarding the use of digital evidence in criminal proceedings — thus transcending the specifics of the *Yalçınkaya* case well beyond ByLock and Turkey — the Grand Chamber had the chance to seize an opportunity to establish some general principles, particularly addressing electronic evidence obtained from encrypted communications.

iv. The use of digital evidence in criminal proceedings

As alluded to above, the *Yalçınkaya* judgment carries immense significance for Turkey. In his analysis of the case, Dr Emre Turkut argues that "at a more general level, the Grand Chamber's message is particularly relevant to only a handful of countries that misuse terrorism charges for contentious and controversial purposes" and that "the impact of this decision could have extended well-beyond Turkey (to countries with a relatively high quality of democracy and human rights compliance) if the Grand Chamber had not seemingly 'missed out' on an 'opportunity' to address the use of electronic evidence, particularly evidence obtained through encrypted communication networks, in criminal proceedings."[68]

While the Grand Chamber did offer extensive guidance on issues related to mass surveillance in the cases of *Big Brother Watch*[69] and *Centrum För Rättvisa*[70], it did not provide the same level of clarity when it came to the digital evidence obtained through interception of telecommunications. It is important to note here, at the time of writing, that the court has two pending cases involving digital data obtained through the infiltration of EncroChat, a network similar to ByLock.[71] Against this backdrop, a more in-depth analysis could have provided much-needed clarity in the uncharted territory of digital evidence and human rights and on the intersection between digital evidence and the right to a fair trial under Article 6 of the ECHR, as well as on the principles of subsidiarity and human rights-compliant digital evidence use – issues that could have added value for the pending EncroChat cases. With the mounting reliance on digital evidence in criminal proceedings and given the escalating discourse on the weaponisation of such evidence, the *Yalçınkaya* judgment conspicuously leaves such important aspects largely unaddressed.

v. The right to privacy

In his application, the applicant also raised a claim that his right to privacy was violated. The application based his claim on the fact that the MIT and the Turkish police interfered with his right to respect for correspondence without any legal basis and that the internet traffic records were illegally stored for more than one year and subsequently used in the case. Yet, the ECtHR took another approach by addressing the issue of using a communication app as potential conduct that might

67 ECtHR, *Huseyn and Others v. Azerbaijan*, App Nos. 35485/05 and 3 others, 26 July 201, para. 199, 200

68 Emre Turkut, 'Article 7' Shockwaves, ByLock and Beyond: Unpacking the Grand Chamber's *Yalçınkaya* Judgment, Strasbourg Observers, 13 October 2023 https://strasbourgobservers.com/2023/10/13/article-7-shockwaves-bylock-and-beyond-unpacking-the-grand-chambers-yalcinkaya-judgment/

69 ECtHR Grand Chamber, *Big Brother Watch and Others v. the United Kingdom*, App Nos. 58170/13 62322/14 24960/15, 25 May 2021.

70 ECtHR, Grand Chamber, *Centrum För Rättvisa v. Sweden,* App No. 35252/08, 25 May 2021.

71 ECtHR. Fact Sheet on Mass Surveillance available at: https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng.

form the basis of the constituent elements of the offence of terrorism, rather than as an interference of a mere enjoyment of the right to private life. Thus, the Court ignored valid Article 8 ECHR claims raised by the applicant.

However, given the disproportionate nature of MIT's ByLock operation, allowing them to gather the data of hundreds of thousands of individuals and considering that ByLock was accessible to anyone and thus not exclusively used by members of the GM, a more rights-oriented approach would have been welcome. As noted above, such an approach has been taken in the various opinions of the UN WGAD concerning ByLock.

5. Roadmap for the future: what steps must Turkish authorities take to fully implement the Yalçınkaya judgment?

At the outset, it must be stressed that compliance with the ECtHR's judgments is a shared responsibility of all national authorities under Article 46 ECHR.[72] The Grand Chamber's findings in the *Yalçınkaya* case, particularly those under Articles 6 and 7 ECHR, entail clear obligations on Turkish national authorities to take appropriate measures to remedy these infringements of the applicant's rights. To this end, the reopening of the criminal proceedings would be the most appropriate way of putting an end to the violations found in the present case, and the new trial should be compatible with the conclusions and spirit of the *Yalçınkaya* judgment.[73] Despite the seeming simplicity of this solution, Turkey's diminishing commitment to implement ECtHR rulings over the past decade as exemplified – at the time of writing – by the backlog of 126 leading judgments (i.e. those that identify serious or structural problems) awaiting action,[74] including such high-profile cases as *Selahattin Demirtaş*[75] and *Osman Kavala*[76] raises concerns about the forthcoming implementation of the *Yalçınkaya* case.

Beyond these individual measures, in relation to its finding under Article 7 ECHR, the Grand Chamber unequivocally highlighted that the problems leading to these violations were of a "systemic nature". Therefore, in accordance with Article 46 ECHR, the court called on Turkey to take general measures to address these systemic problems, particularly regarding the Turkish judiciary's handling of ByLock evidence. Importantly, the Grand Chamber emphasized that Article 46 ECHR holds the force of a constitutional rule in Turkey, according to Article 90(5) of the Turkish Constitution, which grants international human rights treaties preferential treatment over domestic law.

The clarity and non-disputed nature of the Grand Chamber's findings in the *Yalçınkaya* case under Article 7 of the ECHR are undeniably of paramount importance. However, as we detailed above, under Article 6 ECHR, the Court left certain crucial questions unaddressed concerning the intersection of digital evidence and the right to a fair trial under Article 6 of the ECHR. These questions essentially leave wide discretion for the Turkish domestic authorities. Before proposing recommendations to the Turkish authorities to fully implement the *Yalçınkaya* judgement, it must be emphasized that the three important decisions by the TCC from 2014 and 2015 provide a distinct framework and guidance for lower courts for how to address and remedy the fair trial deficiencies identified in the *Yalçınkaya* judgment. As also briefly noted above, in the judgments of *Yavuz Pehlivan, Yankı Bağcıoğlu* and *Sencer Başat*, the TCC concluded that the defendants should be given the opportunity to conduct a technical examination of the digital materials, otherwise the principle of the equality of arms would be violated**.** The

72 See, CoE Committee of Ministers, 1475th meeting, 19-21 September 2023, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680ac9e79

73 para. 412

74 See the 'Country Factsheet: Türkiye', Department for the Execution of Judgments of the ECtHR, https://www.coe.int/en/web/execution/turkey

75 ECtHR Grand Chamber, *Selahattin Demirtas v Turkey (no.2)* App No. 14305/17, 22 December 2020

76 ECtHR *Osman Kavala v Turkey*, App No. 28749/19, 10 December 2019. In 2022, the Committee of Ministers of the CoE decided to launch infringement proceedings against Turkey due to its refusal to implement the *Kavala* judgment. See: See, 'CoE's Committee of Ministers refers the *Kavala v. Turkey* case to the ECHR', Media Release, Ref. DC 013(2022) 02 February 2022 and Interim Resolution CM/ResDH(2021)432 'Execution of the judgment of the European Court of Human Rights Kavala against Turkey', 2 December 2021, available at https://rm.coe.int/0900001680a4b3d4.

TCC's findings in relation to the admissibility and reliability of digital evidence, which are of utmost importance for the ByLock cases in these instances, merit quoting *in extenso.*

In the *Yavuz Pehlivan* application, the TCC held that:

> *In the present case, the evidence which was shown as the basis for the crimes that the applicants were charged with is not the evidence seized from the applicants, but digital materials seized from third parties and it is seen that the judicial authorities did not let the applicants who were tried under detention examine this evidence and conduct a technical examination of it... It is concluded that the applicants did not have sufficient information regarding the content of the digital materials and documents… and did not have the opportunity of conducting a technical examination of the relevant digital materials either, and therefore, the principle of the equality of arms was violated.*[77]

In the *Yankı Bağcıoğlu* application, the TCC elaborated on the principle of equality of arms in criminal proceedings:

> *Faced with the allegation of the applicant that the documents contained within the digital evidence had not been created and procured by himself, it is necessary that an access that would allow an effective defence to be made pertaining to these allegations be provided or that an examination fitting this purpose be conducted by the trial instance… The failure to grant the opportunity of access and examination in such a manner as to result in the defence pertaining to the evidence constituting the basis for the accusations becoming ineffective causes the main function of the criminal trial not to be fulfilled… In the present case, the applicants were sentenced by relying on the information and documents contained within the digital evidence… The request of the applicants that an expert examination be commissioned on this evidence in order to investigate their allegations that the digital data did not reflect the reality was dismissed… The fact that the evidence was thus kept confidential by the Court, especially that the evidence was not made available to and examined by the defence due to the pretext of state secret made it impossible for the applicants to fully bring forward their allegations as to the soundness of the digital evidence. However, the Court delivered its judgment of conviction by making an assessment based on this digital evidence and the judgment was upheld by the Court of Cassation for the same reasons. It is clear that the procedure and method pursued by the Court under these kinds of circumstances are not in compliance with the principle of the equality of arms and do not contain a guarantee that sufficiently protects the applicant's interests. … [therefore] the principle of the "equality of arms" of the criminal trial aimed at ascertaining the material fact was violated.*[78]

In the *Sencer Başat* application, the TCC similarly highlighted:

> *…in terms of the complaints as regards the evaluation of the digital data, as the*

77 TCC, *Yavuz Pehlivan*, supra footnote 20, para. 80.

78 TCC, *Yankı Bağcıoğlu*, supra footnote 20, para. 74-77.

fact that the expert reports and expert opinions that the applicants presented were not accepted by the Court of First Instance and dismissal of their requests from the court to have the expert examination made about these issues with insufficient justifications were contrary to "the right to a reasoned decision" and the principle of "equality of arms", the right to a fair trial enshrined in Article 36 of the Constitution was violated."[79]

a. Measures to be taken with regard to breaches of Article 7

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.

i. Recharacterization of ByLock

At the outset, it is imperative for Turkish authorities to reconsider their characterization of ByLock. Specifically, the Turkish Court of Cassation's three pivotal precedents have significantly influenced the trajectory of all criminal proceedings involving ByLock usage and resulted in the establishment of an almost automatic presumption of guilt based solely on ByLock use.[80] In these judgments, the Turkish Court of Cassation confirmed that the collection and processing of the ByLock data had been carried out in compliance with the relevant legal framework largely mirroring the findings that had been made by the MIT in its ByLock report. As a first step, these judgments by the Turkish Court of Cassation should be revisited and reversed in line with the findings and principles set forth in the *Yalçınkaya* judgment. Additionally, the domestic courts in Turkey should rigorously apply the established criteria, as articulated in the case law of the Turkish Court of Cassation, for establishing membership in an armed terrorist organization. This entails demonstrating, with greater stringency, the defendant's "organic relationship" to the organization through the "continuity, diversity and intensity" of the attributed acts. Furthermore, the prosecution must establish that the defendant acted "knowingly and willingly" within the "hierarchical structure" of the organization.[81]

ii. Retrial and objective effect of the Yalçınkaya judgment

Turkish courts should take into consideration the objective effect of the *Yalçınkaya* judgment in line with the TCC's *Ibrahim Er* judgment.[82] In the *Ibrahim Er* judgment, the TCC clearly highlighted that the objective function/nature of its decisions (precedent value and/or *stare decisis*), which generally manifests itself in the form of interpreting the Turkish constitution, takes precedence over its subjective function of justice in a specific case:

An individual application may be lodged if it is alleged that these authorities have failed to provide protection in accordance with the Constitution in a particular matter. The Constitutional Court then interprets the Constitution in relation to that matter and renders a judgment. Thereafter, in their examina-

79 TCC, *Sencer Başat*, supra footnote 20, para. 72

80 Turkish Court of Cassation, 16th Criminal Division, E.2015/3, K.2017/3, 24 April 2017; the Plenary of Criminal Divisions, E. 2017/16-956, K. 2017/370 26 September 2017, and the Plenary of Criminal Divisions, E.2018/16-418, K.2019/513, 27 June 2019.

81 For a similar recommendation made by the CoE's Venice Commission see: Opinion on Articles 216, 299, 301 and 314 of the Penal Code of Turkey, CDL-AD(2016)002, 15 March 2016, para. 106, https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)002-e

82 TCC, *İbrahim Er et al* [GC], B. No: 2019/33281, 26/1/2023 (for similar assessments, see K.V., para. 53; F.N.G., para. 38).

tion of the same matter, the public authorities and the courts of first instance must take into account the Constitutional Court's decisions on the application and interpretation of the Constitution, the determination of the scope and limits of fundamental rights, and the cases where human rights require it, and consider the conclusions reached through the interpretation of the provisions of the Constitution. To do otherwise would result in all disputes concerning the same issue being brought before the Constitutional Court. It is impossible to maintain an individual application procedure that functions in this way. The Constitutional Court's interpretation of the Constitution is of critical importance for the continued functioning of this procedure. The best fulfilment of this function depends on the Constitutional Court focusing on issues where it has not interpreted the Constitution before, rather than ensuring justice in each application.

As outlined above, the objective nature and precedent value of the *Yalçınkaya* is unquestionable. Consequently, it remains a clear international obligation on the part of the Turkish authorities, particularly courts, to consider affording retrials to individuals previously convicted based on allegations related to their purported ByLock usage. The objective impact of the *Yalçınkaya* decision should serve as a guiding principle for Turkish authorities in their efforts to ensure justice.

b. Measures to be taken with regard to breaches of Article 6

i. Access to complete ByLock dataset

The principles of the equality of arms must be preserved in ByLock cases. Defendants should have access to the complete ByLock dataset and records relevant to their cases in accordance with the right to disclosure set forth in the *Yalçınkaya* judgment as well as the TCC precedents mentioned above. If there are valid and justifiable reasons that prevent the sharing of the complete dataset, these should be articulated through a decision-making process that involves the defendants effectively. The scope and justification for any restrictions on the right to disclosure must be clearly outlined and determined by an impartial judiciary. Regardless of these limitations, defendants should, at a minimum, receive a digital copy of all the ByLock data specific to their own accounts to enable adequate time for preparation of their defence.

ii. Examination of exculpatory evidence

Turkish domestic courts must investigate whether potential exculpatory evidence was deleted or excluded from the ByLock material, preventing any miscarriage of justice. The integrity of digital evidence is paramount, and any such omissions could constitute a miscarriage of justice.

iii. Addressing gaps in ByLock material

Turkish courts should also investigate the reasons behind the missing time periods within the ByLock material, to determine if these gaps have undermined the fairness of the proceedings against the defendants. The continuity of digital records is essential for establishing a comprehensive and truthful representation of the evidence. The reasons behind missing time periods within the ByLock material should be probed, to ensure the continuity of digital records for a comprehensive and truthful representation of the evidence.

iv. Scrutiny of the Turkish intelligence agency's handling of data

Turkish domestic courts should investigate the actions of the MIT in processing ByLock data without judicial supervision, ensuring the chain of custody and procedural integrity of digital evidence. This examination should ensure that the chain of custody was maintained and that the procedural integrity of the digital evidence was not compromised.

v. Oversight and review of ByLock data

In an effort to ensure that there are safeguards to counterbalance the lack of equality of arms and adversarial proceedings, and thus ensuring the overall fairness of the criminal proceedings, Turkish courts should engage an independent expert panel. This panel would be tasked with scrutinizing the quality, reliability, authenticity, and digital forensic integrity of the ByLock evidence and implementing safeguards to counterbalance existing disparities. Moreover, it should meticulously investigate any technical issues regarding potential manipulation, alteration, or deletion of the ByLock data subsequent to its acquisition by the MIT as detailed in Forensic Focus (1, 2, 3 and 4). Against this backdrop, all relevant materials should be fully accessible to the independent expert panel with a view to ensuring an unimpeded and transparent examination and the panel's investigation must be exhaustive.

Forensic focus 4: Discussions with forensic experts and our conclusions

In preparation for this report, the authors held discussions with several forensic experts who have published reports on the ByLock app and who had interacted with individuals accused of downloading and using ByLock.[83] These discussions complemented our detailed analysis. Through these consultations and examinations, we have reached the following conclusions:

- The Turkish Police report states that to access the database, they used two third-party data recovery tools designed for the MySQL/InnoDB databases: Data Recovery Tool for InnoDB by Percona

83 Given the confidential nature of our discussions, we will maintain anonymity regarding the names involved.

LLP, and TwinDb Data Recovery. However, there is no mention of attempts to access the database through its native application environment using official MySQL and InnoDB software. The use of these tools would be reasonable if the database was found to be corrupt; however, these tools are not officially endorsed by Oracle Corporation, the developer of MySQL and InnoDB.

- In addition, the tools used are open-source projects and do not seem to have official endorsement from Oracle Corporation. Without verification data, the reliability of the recovered data using these tools cannot be ascertained. The report does not explain why the database provided to the Police was in a corrupted or damaged state.
- The Turkish authorities' own report raises legitimate concerns about the integrity of the data extracted from the ByLock database and the methods used for recovery, suggesting that the results obtained might be questionable. Without access to the native application environment or endorsement from official developers of the database management systems, there are uncertainties surrounding the accuracy of the data analysis presented in the Turkish Police's report.
- In the reports of Turkish authorities, there are various references to the ByLock data having been obtained from a "server" or "database". This being the case, there would have been at least three logical steps involved in producing the reports of Turkish authorities:
    - seizure and forensic preservation of the server equipment from which the ByLock data was subsequently extracted; this would typically involve the creation of one or more forensic images, comprising a tamper-proof and verifiable representation of the data stored on this equipment;
    - extraction of the raw data using forensically-sound hardware and software tools and techniques;
    - analysis and processing of the extracted data to produce a meaningful report for submission in evidence or use as intelligence.
- Without contemporaneous notes or statements detailing how the digital evidence was seized, extracted, analysed and interpreted, there can be no independent verification of the techniques and processes used and therefore little confidence in the ultimate evidential product.

- To check the quality of the evidence, a forensically certified copy of the material provided to the Turkish police by MIT is required, along with relevant documentation and technical evidence to identify its original source and the steps taken to preserve its integrity both during acquisition and throughout any subsequent analysis.

6. Conclusion

The ECtHR Grand Chamber's judgment in *Yalçınkaya* marks a pivotal moment in the ongoing discourse surrounding the use of ByLock in Turkey. This report aimed to comprehensively navigate through the nuances of this landmark judgment, shedding light on its potential implications that reverberate beyond the immediate legal context. The Grand Chamber's clear emphasis on the systemic problems inherent in ByLock prosecutions and its explicit call on the Turkish government to institute appropriate general measures underscore the imperative for a comprehensive re-evaluation of the entire landscape, not only in addressing ByLock-related prosecutions but also in safeguarding the independence of the Turkish judiciary at large.

The report offers a series of recommendations for the Turkish authorities to fully implement *Yalçınkaya* judgment. These recommendations span a spectrum of important areas, including the need to recharacterize the ByLock evidence in legal proceedings, taking into account the objective nature of the *Yalçınkaya* decision, upholding the principle of equality of arms in the realm of digital evidence, scrutinizing the Turkish intelligence agency's handling of sensitive information, examining potentially exculpatory evidence, and addressing of any gaps within the ByLock material. Each of these issues occupies a position of paramount importance in shaping the trajectory of Turkish judicial practices concerning ByLock usage.

This report is not merely a call to action for the Turkish authorities; it also stands as a resource for legal practitioners, underscoring the shared responsibility to diligently adhere to ECtHR judgments. The full implementation of the *Yalçınkaya* case harbours the potential to establish a clear precedent, which may influence the trajectory of thousands of similar cases. Moreover, it is poised to play a pivotal role in recalibrating the intricate balance between security imperatives and the protection of individual liberties across the Turkish legal landscape.

In conclusion, the *Yalçınkaya* case presents an opportunity for Turkish authorities to reflect on their actions and consider the merits of a meaningful reform within the Turkish judiciary. Our assessment underlines that implementing the recommendations in this report offers the potential to help build a fairer and more rights-respecting legal system in Turkey.

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