

REPORT ON THE LEGAL AND TECHNICAL ISSUES AROUND TURKEY'S MALICIOUS BYLOCK PROSECUTIONS



Copyright © 2021 Arrested Lawyers Initiative All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in reviews and certain other non-commercial uses permitted by copyright law.

November 2021



TABLE OF CONTENTS

I. INTRODUCTION	4
II. FACTUAL BACKGROUND	4
1. What is the Bylock App?	4
2. When was the Bylock app in service?	4
3. The Turkish judiciary's opinion regarding Bylock	5
III. THE EVERCHANGING FIGURES	6
1. 2016 August – 2017 February The Number of Bylock App users is 215,000	6
2. March, 2017 The Number of Bylock App users is 122,000	6
3. June, 2017: The Number of Bylock App users is 102,000	7
4. 27th December, 2017 11,480 People were mistakenly prosecuted; 90,500 Bylock users remain.	7
5. 3rd January, 2018 Milliyet Daily: Turkish Intel, MiT is reinspecting the Bylock App users' list for a possible 30,000 misleading findings	8
IV. THE EVERCHANGING CRITERIA	8
1. August, 2016 Three-Colour Categorisation: Red, Blue, Orange Users	8
2. 2017 April The Three-Colour Categorization was abolished	9
3. July, 2017 Criterion for at-least three logins was implemented	9
V. EVALUATION OF THE TURKISH AUTHORITIES' CLAIMS, MiT'S BYLOCK REPORT AND BYLOCK DATA AS EVIDENCE	11
1. Meaning of the ambivalence around the Bylock users' figures and the criteria under digital forensics' standards	11
2. The fragility of the findings and digital forensic technics in MiT's Bylock Technical Report	12
3. Lack of substantivity of the 'exclusive usage' claim	12
VI. OTHER PROBLEMS CASTING DOUBT ON THE ACCURACY OF THE BYLOCK DATA PRESENTED BY THE TURKISH AUTHORITIES	14
1. IP Convergence (updated)	14
2. Assignment of random dynamic IP-Port numbers to customers	15
3. IP Routing	15
4. Discrepancies between the records from MiT and BTK	16
VII. CORRUPTION OF DATA IN THE MiT BYLOCK TECHNICAL REPORT	17
VIII. NON-COMPLIANCE WITH THE CODE OF CRIMINAL PROCEDURES	20
1. Relevant Facts	20
2. Breach of Article 160 of the Code of Criminal Procedures	22
3. Breach of Article 134 of the Code of Criminal Procedures	23
4. Evaluation of the Bylock case under the law around the seizure of digital devices	24
5. Breach of Article 135 of the Code of Criminal Procedures	25
6. Breach of the law governing data retention	25
7. Breach of the law governing intelligence activities	26
IX. CASES CONCERNING THE BYLOCK APP THAT ARE BEFORE SUPRANATIONAL MECHANISMS	28
1. Opinions by the UN Bodies on the Bylock App	28
2. Cases before the ECtHR	29
3. The Akgün judgment by the ECtHR	30
4. The problem of equality of arms	32
X. CONCLUSION	34

I. INTRODUCTION

The unprecedented mass arrest campaign which started immediately after 2016's failed coup attempt continues unabated. According to the Minister of the Interior's statement, dated 20th February, 2021, 622,646 people have been subjected to criminal investigations as a result of their alleged links to the Gülen Movement, thus being accused of membership of an armed terrorist organisation, and 301,932 of them have been arrested by the police (*gözetli* in Turkish).¹ Bylock, an encrypted online messaging application, has emerged as the Turkish government's favorite tool for justifying these mass arrests. So, at least 92,769 individuals have been identified as being users of the Bylock App² and have accordingly been subjected to criminal investigation, and arrested or detained.

According to Turkey's AKP government, Bylock App has exclusively been used by members of the Gülen Movement as a secret communication tool. The government claims that anybody who may have downloaded it is, in fact, a "terrorist." This claim has been rubber-stamped by the Turkish judiciary, without observing the defendants' right to a fair trial and giving heed to independent expert reports that are available to public.

II. FACTUAL BACKGROUND

1. What is the Bylock App?

Bylock is an encrypted i-message app that provides written and voice communication between its users. It was downloadable via Google Play Store and also the Apple Store, as apk-dl.com, apkpure.com, downloadatoz.com. According to a report prepared by FOX-IT, a prominent Netherlands based forensic IT company, from the Play Store alone, Bylock was downloaded more than a hundred thousand times.³

Date	Total installs
22 April 2014	50+
24 April 2014	100+
4 May 2014	1,000+
20 May 2014	5,000+
1 June 2014	10,000+
24 Aug 2014	50,000+
19 Jan 2015	100,000+

*Google Play Store
installation statistics on
Bylock App⁴*

2. When was the Bylock app in service?

According to the Fox-IT report, Bylock was in service between 14th March, 2014, and 19th February, 2016⁵, and this technical determination has been agreed upon by all of the experts and reports.

¹ Anadolu News Agency, <https://www.aa.com.tr/tr/turkiye/icisleri-bakani-soylu-garaya-giden-hdpli-vekili-acikladi/2151784>

² Yenisafak Daily, <https://www.yenisafak.com/gundem/fetoden-612-bin-kisiye-islem-3587006>

³ FOX-IT, Expert Witness Report on Bylock Investigation, <https://foxitsecurity.files.wordpress.com/2017/09/Bylock-fox-it-expert-witness-report-english.pdf>

⁴ FOX-IT, Expert Witness Report on Bylock Investigation.

⁵ Ibid.

Although it was claimed by AKP government officials⁶, as well as the pro-government media that the coup-plotters communicated over the Bylock App during the coup attempt⁷, this claim is therefore totally false, as the application was shut down in March, 2016, four months before the coup attempt.

3. The Turkish judiciary's opinion regarding Bylock

Since the first arrest in August, 2016, Bylock has been the primary evidence used in relation to dismissing, arresting and convicting those who do not agree with the AKP's rhetoric. The Turkish Constitutional Court and the Court of Cassation have also decided, contrary to their previous decisions on digital evidence, that using or downloading Bylock was 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 Court of Cassation ruled, in its judgment, pronounced on 26.09.2017:

"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 fulfill 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."⁸

This determination is in contravention of the Court of Cassation's own precedents, which require that there be 'continuity, diversity and intensity' and 'participation within the "hierarchical structure" knowingly and willfully' to establish membership in an armed terrorist organization.⁹ However, in Bylock cases: i. downloading the Bylock App without either the defendant's or any others' action, or any other evidence showing the defendant's link with the organization in question, suffices, so that the accused can be convicted. This is in contravention of the criteria of diversity; ii. again, downloading the Bylock App. or using it for a very short period of time (i.e., a few days) suffices for the accused to be convicted, and this is in contravention of the criteria of density and continuity.¹⁰

In line with the foregoing judgment, the Constitutional Court endorses the afore-cited conclusions of the Court of Cassation with no further inquiry, ruling:

"... 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." (Ferhat Kara, B. No: 2018/15231)

⁶ Reuters, <https://www.reuters.com/article/us-turkey-security-app-idUSKCN10E1UP>

⁷ Haber 7 news website, <https://www.haber7.com/guncel/haber/2144267-darbeciler-Bylocktan-bu-mesaji-gonderdi>

NTV news website, <https://www.ntv.com.tr/turkiye/darbeciler-tango-by-lock-ve-eagle-kullanmis,BFHNT8xvE-pw1TjN737g>

⁸ Court of Cassation, E. 2017/16-956, K. 2017/370.

⁹ 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>

¹⁰ Ibid

That being said, the legality, legitimacy and technical accuracy of the findings on which these judgments are predicated have been evaluated in the following sections.

III. THE EVERCHANGING FIGURES

1. 2016 August – 2017 February | The Number of Bylock App users is 215,000

In September, 2016, Faruk Özlü, the then Minister of Science and Technology, said that there were 215,000 Bylock users,¹¹ and in October, 2016, Veysi Kaynak, the then Deputy Prime Minister, said that 18 million messages were obtained, and that the process of decrypting each and every one of these messages was underway.¹²

2. March, 2017 | The Number of Bylock App users is 122,000

On 1st March, 2017, Hürriyet Daily News reported that: "Turkey's National Intelligence Agency (MİT) has sent a list of a total of 122,000 alleged users of the Bylock smartphone app to the Ankara Chief Public Prosecutor's Office. MİT also deciphered the contents of some 18 million messages sent through Bylock, ... and sent them to the prosecutor's office, which then transferred the lists to the Department of Anti-Smuggling and Organized Crime ... In order not to make any mistakes in the list, MİT reportedly conducted meticulous efforts and concluded that there were around 122,000 Bylock users in Turkey. The Department of Anti-Smuggling and Organized Crime transferred the list to its own database, with police in the provinces being able to check the list with a password that was given to them."¹³

On 7th April, 2017, Karar, a pro-government daily, published a story which said that:

- i) MİT, the Turkish intelligence agency, had created a new and sensitive inquiry screen,
- ii) by a double confirmation system, any incorrect findings had been eliminated
- iii) an investigation had been launched by the Ankara Prosecutorial Office to establish the identities of those who were responsible for the incorrect findings in question.¹⁴

FETÖ'cülerini ByLock üzerinden tespit eden MİT, sıfır hatayla sorgulama için veri tabanını güncelledi. Yanlış sonuçlar yeni ekrandan tek tek aykırıldı. Ankara Başsavcılığı da itiraz üzerine ByLock kullanmadığı belirlenen ancak ismi listede yer alanlarla ilgili soruşturma başlattı.

HATALAR GİDERİLDİ

Kullanıcı olmadığı halde ByLock listelerinde adı bulunanların itirazları ve KOM Daire Başkanlığı'nın "Sorgulamalarda hata çıkıyor" uyarısı üzerine MİT, ByLock kullanıcılarının isim listesinin yer aldığı veritabanında güncelleme yaptı. Bu kapsamda daha hassas sorgulama yapılabilmesi için yeni bir ekran oluşturuldu. 'KOMBS FETO-PDY Yeni Bylock Sorgusu' adı verilen ekranda yapılan sorgulamalar hataları giderdi.

ÇİFTE TEYİT YÖNTEMİ

Aık adım İzmir'deki darbe davasında atıldı. Mahkemenin yeniden sorgulama talebi üzerine KOM'un gönderdiği raporda daha önce programı kullandığı belirtilen bazı sanıklarda ByLock bulunmadığı bilgisine yer verildi. Ankara Başsavcılığı'nın da mağduriyetleri önlemek için ByLock'ta çifte teyit yöntemini uyguladığı ortaya çıktı. MİT listesinde ismi olduğu halde bazı isimler için ikinci inceleme başlatıldı. 57



**BYLOCK'A
HASSAS
SORGU
EKRANI**

KÖZEL **KENAN BUTAKIN** **MİLAL ÖZTÜRK**

11 Habertürk Daily, <https://www.haberturk.com/ekonomi/teknoloji/haber/1294035-faruk-ozlu-by-locku-tubitaktaki-fetoculer-gelistirdi>

12 Yeniçağ Daily, <https://www.yenicaggazetesi.com.tr/bakan-veysi-kaynak-18-milyon-bylock-mesaj-var-tek-tek-inceleniyor-147602h.htm>

13 Hürriyet Daily News, <https://www.hurriyetdailynews.com/turkeys-intel-agency-sends-list-of-122000-bylock-users-to-prosecutors-office-110317>

14 Karar Daily, <https://www.karar.com/Bylocka-hatasiz-sorgu-guncellemesi-441447>

3. June, 2017: The Number of Bylock App users is 102,000

On 26th June, 2017, Hürriyet Daily News reported from Ömer Fatih Sayan, the Head of the BTK (Information Technologies Agency), that a list of 102,000 people who are Bylock users had been sent by BTK to the judicial authorities. Sayan said "We have prepared reports and met the demands of the courts one by one, whichever court has the investigation files of these people on the list. ... We have confirmed that they have used Bylock. Those on the Bylock list therefore have no excuse left. By getting detailed records of their correspondences, we have once again determined that they have used Bylock."¹⁵

102,000 suspects accused of Gülen links are ByLock users, Turkish communication authority says

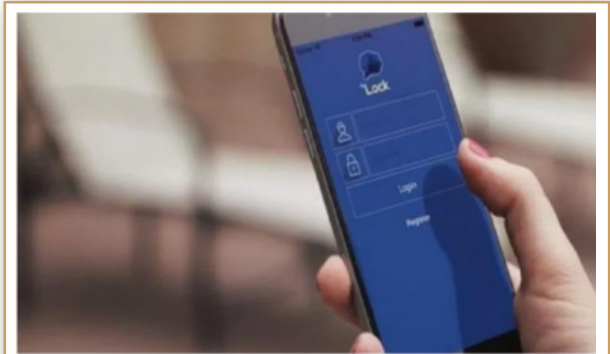
ANKARA



4. 27th December, 2017 | 11,480 People were mistakenly prosecuted; 90,500 Bylock users remain.

According to the State-run Anadolu News Agency, the Ankara Chief Public Prosecutor's Office, on 27th December, 2017, stated that 11,480 GSM users had been found to have been involuntarily directed to the mobile phone application: Bylock.¹⁶

The Prosecutor's Office said that "the legal status of the 11,480 mobile phone users would be re-evaluated". Yüksel Kocaman, Ankara's Chief Public Prosecutor, said; "Nearly a thousand people, who were found to have been directed to Bylock through the Mor Beyin application, have been in jail in different provinces ," and added; "They will be released unless there is other evidence against them."



Turkish Prosecutors Say 11,500 Mistakenly Investigated For ByLock Use

It thus became clear that 11,480 of the 102,000 people who had been included in a list that was sent to the judicial authorities by the BTK and MIT in June, 2017, were not Bylock users after all.

After 11,480 were eliminated from the list of 102,000 people, 90,500 alleged Bylock users remained.

¹⁵ Hürriyet Daily News, <https://www.hurriyetdailynews.com/102000-suspects-accused-of-gulen-links-are-Bylock-users-turkish-communication-authority-says-114783>

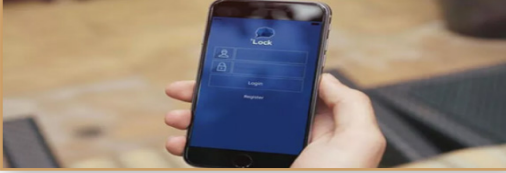
¹⁶ Stockholm Center for Freedom, <https://stockholmcf.org/turkish-prosecutors-say-11500-mistakenly-investigated-for-Bylock-use/>

5. 3rd January, 2018 | Milliyet Daily: Turkish Intel, MİT is reinspecting the Bylock App users' list for a possible 30,000 misleading findings

ByLock'ta mağdur sayısı ile ilgili flaş iddia!

ByLock tuzağını ortaya çıkaran Avukat Ali Aktaş'tan dikkat çeken açıklamalar geldi. Aktaş mağdur sayısının daha fazla olabileceğini öne sürerek "Mağdur sayısı 11 bin 480 rakamıyla sınırlı kalmayacak" dedi.

03.01.2018 - 09:18 | Güncelleme: 03.01.2018 - 09:28 | İSTANBUL (İHA)



"MAĞDUR SAYISI 11 BIN 480 RAKAMIYLA KALMAYACAK"

Mağdur sayısının 11 bin 480 kişiyle sınırlı kalmayacağını öngördüğünü belirten Aktaş, "102 bin ByLock kullanıcısı MİT tarafından tespit edilmişti. 11 bin 480 kişi düştü şuanda 60 bin üzerinde Bylock kullanıcı en az bir defa mesaj atmış veya göndermiş kişi var. 40 bin civarında da şüpheli var Milli İstihbarat Teşkilatı en az 30 bin kişiyi daha yeni baştan inceliyor. Bunların içerisinde de muhtemelen IP kayıtları, operatör hataları ve başka hatalar nedeniyle yanlışlıkla Bylock havuzuna dahil edilen kişiler varsa bunları da çıkaracak. Mağdur sayısı 11 bin 480 rakamıyla kalmayacak" ifadelerini kullandı.

3rd January, 2018, Milliyet Daily: Findings about 40,000 people are doubtful, 11,480 of them were eliminated from the Bylock list. Reinspection continues for the remaining.

In the light of the new information, Turkish intelligence has started reinvestigating at least 30,000 people who it formerly believed to have been accessing a mobile messaging application called Bylock, the pro-government newspaper Milliyet said.¹⁷

IV. THE EVERCHANGING CRITERIA

1. August, 2016 | Three-Colour Categorisation: Red, Blue, Orange Users

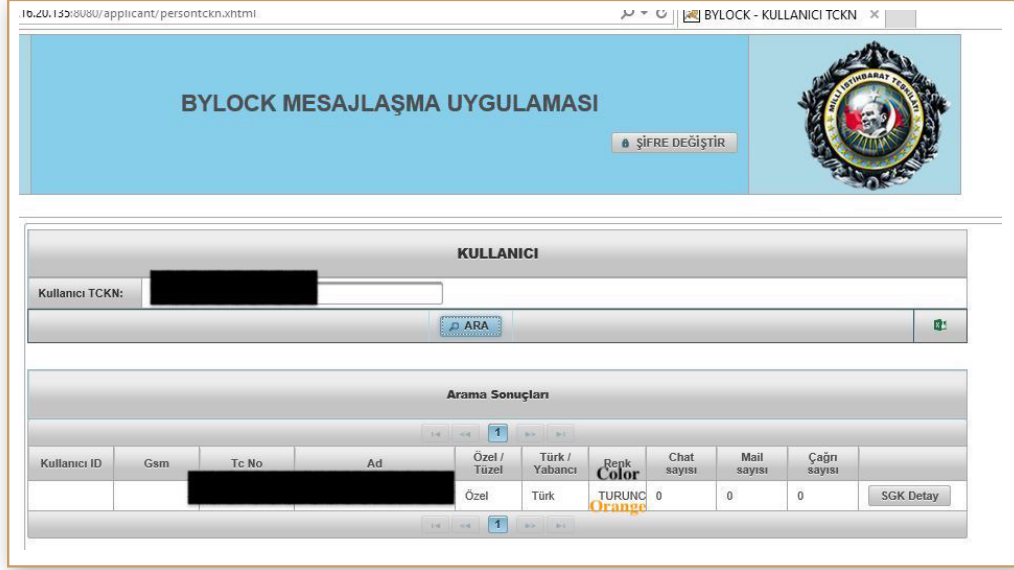
Between August, 2016, and April, 2017, Turkish intelligence, the police, and the judiciary used a "three-colour categorization system", which was devised by MİT. According to a news item that was entitled 'The Intelligence sorted FETO-members into three colours'¹⁸, Bylock users were sorted into categories as being either red, blue or orange:

- Red: User and their user id has been established, the margin of error is between 0.1 and 1 per cent.
- Orange: Although the identity of the user has been determined, his user id could not be
- Blue: Possible user, actual usage can neither be confirmed nor ruled out.

A memo, below, that was sent by the MİT to the judicial authorities concerning a certain individual, confirms the above-mentioned three colours categorization, as well as MİT's direct involvement in criminal proceedings, which is unlawful, as we will explain below.

¹⁷ Milliyet Daily, <https://www.milliyet.com.tr/gundem/Bylockta-magdur-sayisi-ile-igili-flas-iddia-2584227>

¹⁸ Sputnik news website, <https://tr.sputniknews.com/20160828/istihbarat-feto-renk-Bylock-1024591235.html>



A memo sent by the MiT to the judicial authorities concerning a certain individual

2. 2017 April | The Three-Colour Categorization was abolished

Bylock'ta renklendirme kaldırıldı

FETÖ/PDY'nin kriptolu haberleşme programı olan 'ByLock'u kullanan 122 bin şüphelinin kimliğinin belirlenmesinin ardından, kullanıcıların 'kırmızı, turuncu, mavi' olarak sınıflandırılmayacağı, tüm şüpheliler için gözaltı olacağı ve yargılama sırasında mesajın içeriğine bakılacağı öğrenildi

Kaynak : Habertürk

Eklenme : 10 Nisan 2017 17:22

10th April, 2017; The Colouring (three-colour) Criteria was abolished.

In April, 2017, the Pro-government media claimed that, "the Three-color categorization" was abandoned. An amended, the Bylock users' list, including 122,000 people, had been sent to judicial bodies.¹⁹

3. July, 2017 | Criterion for at-least three logins was implemented

FETÖ'nün kriptolu haberleşme programı ByLock'u indirip en az 3 kez kullanmış olmak suç delili sayılacak. Böylece 'Programı indirdim ama kullanmadım' bahanesinin de önüne geçilecek

FETÖ davalarının dayanaklarının başında gelen, örgütün kriptolu haberleşme programı ByLock ile ilgili yeni bir adım atıldı. Daha önce kırmızı, turuncu ve mavi kategorilere göre yapılan değerlendirmede farklı bir metot geliştirildi. Şüphelilerin programı telefon ya da tablete indirip en az 3 kez kullanmış olmaları yeterli sayılacak. Böylece, "Programı indirdim ama kullanmadım" bahanesinin de önüne geçilecek.

¹⁹ Memurlar Net news website, <https://www.memurlar.net/haber/659834/Bylock-ta-renklendirme-kaldirildi.html>

On 6th July, 2017, Sabah reported that anyone who had logged in three times to the Bylock server would be considered to be a Bylock user. With the implementation of this criterion, the number of Bylock users was updated as being 102,000.^{20 21 22}

kullanıldığı değerlendirilen abonelik bilgilerine ulaşılmıştır. Söz konusu uygulamaya, farklı en az üç günde erişen abonelikler listeye dahil edilmiştir. Bu kapsamda 102.192 farklı kimlik numarasına (ki bazı kimlik numaralarının yanlış ve sahte olduğu görülmektedir.) ait 123.115 GSM aboneliği ve 6748 ADSL aboneliği listesi Ek-1'de sunulmuştur. GSM aboneliklerine ait kayıt bilgilerinde yer alan kimlik bilgileri ile söz konusu GSM numarasının gerçek kullanıcısının bazı durumlarda farklılık arz edebileceğinin, ADSL aboneliklerinde ise aynı abonelik üzerinden birden fazla kişi tarafından bağlantı sağlanmış olabileceğinin göz önüne alınmasına ihtiyaç bulunmaktadır.

In its memo, above, sent to the Ankara Chief Public Prosecutor's Office, MİT said: "At this stage, by taking into account the operator's data, and making use of confirmation/verification methods that are within the bounds of possibility, details of [mobile network] subscriptions on which the application in question had been used have been identified. Subscriptions through which access to the application in question had occurred on at least 3 different days have been included in the list. In this regard, a list of 123,115 GSM and 6,748 ADSL subscriptions, belonging to 102,192 different ID numbers (some of which are either wrong or fake) is attached as Appendix-1."

Actually, this memo is attached to a formal letter from MİT dated 9th December, 2016, and addressed to the Ankara Chief Public Prosecutor's Office, however, the implementation of the criterion of there being at least three logins began in July, 2017.

20 Yenisafak Daily, <https://www.yenisafak.com/gundem/Bylockta-3-kez-kullanma-kriteri-2749035>

21

22 Sabah Daily, <https://www.sabah.com.tr/gundem/2017/07/06/Bylockta-3-kez-kullanma-kriteri>

V. EVALUATION OF THE TURKISH AUTHORITIES' CLAIMS, MİT'S BYLOCK REPORT AND BYLOCK DATA AS EVIDENCE

1. Meaning of the ambivalence around the Bylock users' figures and the criteria under digital forensics' standards

It is fair to expect that the digital investigation concerning the Bylock App should rely on accurate, stable, as well as well-documented and well-protected data, especially when compared to the grave consequences that the investigation bears, *vis-à-vis* those individuals who have allegedly downloaded and/or used the messaging app. However, the everchanging figures and criteria around the use of the Bylock App cast a haunting shadow over the integrity and authenticity of the messaging app, as well as its subsequent admissibility as evidence before a court of law.

In light of the aforesaid, and having applied the framework of the Harmonized Model for Digital Evidence Admissibility Assessment (HM-DEAA), which encapsulates the essential requirements that determine evidence admissibility, it would be pertinent to assert that certain technical requirements ensuring the admissibility of digital evidence in a court of law have not been met in the Bylock investigations. First and foremost, modifications of digital evidence cannot be explained merely by a statement that "the erroneous and incorrect findings have been remedied", especially when those modifications point to a margin of error of more than 100%, and one in every two individuals was falsely 'accused of' having used the Bylock App. The authorities who are competent to handle the Bylock raw data must extend this necessity along with the justification that obliges them to rectify their conclusions only after being authorized by a court of law to perform those modifications. Besides, they must comply with a standard of proof, and furnish a proof of compliance, for maintaining the data's integrity and authenticity as they carry out the modifications on the Bylock metadata. In other words, they must prove that there has been a proper chain of custody which logs and justifies those steps that they have taken to "correct their previous erroneous findings". Lastly, the suspect/defendant must be empowered to confirm the integrity and authenticity of the Bylock evidence, as well as the modifications thereon, by acquiring the right of access to (a virtual clone of) the Bylock data, as well as the right to conduct an independent forensic analysis.

All in all, the reduction in the number of individuals who allegedly used and/or downloaded the Bylock App, from 225,000, to 122,000, then to 102,000 and, finally, down to 90,500, must be associated with a compelling case, made by competent authorities, as to the necessity and imperative for such modifications, must also be forfeited as a result of technical integrity-assuring measures. Neither of the legal and technical safeguards that will be explained above was put forward by the MİT. The digital forensic analysis that was conducted by the MİT is fraught, with a marginal error of more than 100 percent, in terms of the number of false positives and inconclusive criteria, as well as having a lack of integrity- and authenticity-assuring measures, such as cryptographic hash functions or sequence documentation. As such, it is safe put forward the view that the Bylock data has forfeited its legal character of being admissible evidence during legal proceedings.²³

²³ 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/>

2. The fragility of the findings and digital forensic technics in MiT's Bylock Technical Report

Generally, the Turkish police and judicial authorities exclusively rely on the findings of the Turkish National Intelligence Agency (MiT) in relation to investigations and prosecutions concerning Bylock, relying upon MiT's report 'A Technical Report on the Bylock Application'²⁴. A number of digital forensic analysts have conducted extensive analysis on the Bylock App and on MiT's report, and have disputed the findings and analysis of the MiT Bylock Technical Report.

FOX-IT, a leading Netherlands-based, digital forensic company concluded that:

"Fox-IT encountered inconsistencies in the MiT report that indicate the manipulation of results and/or screenshots by MiT. This is very problematic, since it is not clear which of the information in the report stems from original data, and which information was modified by MiT (and to what end). This raises questions as to what part of the information available to MiT was altered before presentation, why it was altered, and what exactly was left out or changed. When presenting information as evidence, transparency is crucial in differentiating between original data (the actual evidence) and data added or modified by the analyst. Furthermore, Fox-IT finds the MiT report implicit, not well-structured and lacking in essential details. Bad reporting is not merely a formatting issue. Writing an unreadable report that omits essential details reduces the ability of the reader to scrutinize the investigation that lead to the conclusions. When a report is used as a basis for serious legal consequences, the author should be thorough and concise in the report so as to leave no questions regarding the investigation. Fox-IT has read and written many digital investigation reports over the last 15 years. Based on this experience, Fox-IT finds the quality of the MiT report very low, especially when weighed against the consequences of the conclusions."²⁵

Likewise, an expert report prepared by two Turkish digital forensic experts, Koray Peksayar and Levent Mazılıgüney, concluded that; (i) the Data obtained by MiT from Bylock's server is corrupted; (ii) Understanding the reason for the inconsistencies found would only be possible through provision of the *original* evidence, the uncorrupted digital data itself, and by the examination of such by all of the parties in the criminal case; (iii) Corrupted digital data cannot provide acceptable, admissible evidence for criminal cases.^{26 27}

The expert digital forensic analysts find the argumentation of the MiT report seriously flawed, incorrect and questionable. They set forth several inconsistencies in the MiT report that indicate manipulation of the data. They also advance that the MiT report was written in such a biased manner as to vindicate the pre-determined findings and outcomes that the MiT had championed. The most noteworthy ones of these inconsistencies and discrepancies are brought to the reader's attention below.

3. Lack of substantivity of the 'exclusive usage' claim

Based on the MiT Bylock Technical Report, the Court of Cassation has ruled that the 'Bylock messaging App is a communication network, *exclusively* designed by, and developed to fulfill, the communication needs of the FETÖ terrorist organization'^{28 29}, and therefore downloading

²⁴ Expert Witness Report on Bylock Investigation by FOX-IT.

²⁵ Ibid.

²⁶ Levent Mazılıgüney and Koray Peksayar, Expert Opinion on the Accuracy and Reliability of the Digital Data Obtained from the Bylock Server in Lithuania, <https://www.patreon.com/posts/accuracy-and-of-54329745>.

²⁷ 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>

²⁸ Court of Cassation, E. 2017/16-956, K. 2017/370.

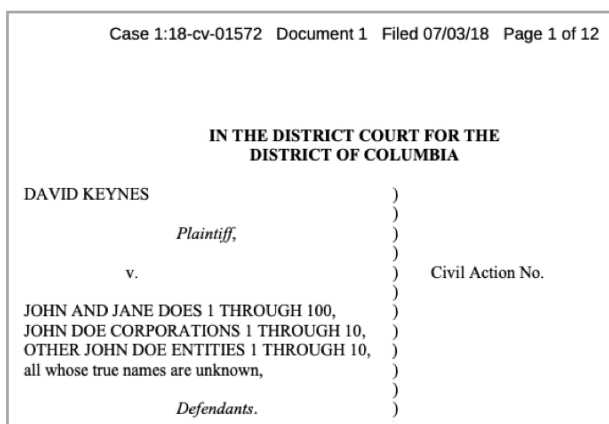
²⁹ The Constitutional Court endorses the conclusion of the Court of Cassation (Ferhat Kara, B. No: 2018/15231).

or using this app equals being a member of an armed terrorist organization. However, this has been shown to be incorrect by international expert reports. Three separate digital forensic reports, by FOX-IT, Jason Frankovitz and Thomas Kevin Moore, have established the 'exclusivity claim' to be factually incorrect. These verifiable reports include:

"... Bylock was available on the Google Play and Apple App stores... the Bylock App was ranked in the top 100 applications in 12 countries, and in the top 500 apps in 47 countries. This would seem to demolish the claim that only those who were members of FETO/PDY were users of the App... It is ridiculous to suggest that all those users were members of the Gülen Movement."³⁰

"Examples of the platforms that hosted Bylock are the Google Play Store, Apple Store, apk-dl.com, apkpure.com and downloadatoz.com. ... MIT considers the Bylock application to have been unknown to the public before 15th July, 2016. Fox-IT has attempted to verify this statement with the statistics that are available. ... Historical download and install statistics from the Google Play store indicate that there were Bylock installations from at least April, 2014, and these reached 100,000 installations on 19th January, 2015. These observations suggest that the public had actually known and used, Bylock in the years leading up to 15th July, 2016."³¹

"During the time the Bylock Application was available on Google Play, it could have been downloaded by anyone with an Android device and a Google account. After an App is removed from its App marketplace, it is still possible to download and install the app from other websites that have a copy... Not only can the Bylock App be downloaded by anyone, but once it has been downloaded, the person who downloaded it could create their own Bylock account and start sending messages to other users... I found nothing in my examination of the Bylock App indicating that the App was able to enforce a specific group membership as a condition of use."³²



<https://storage.courtlistener.com/recap/gov.uscourts.dcd.198259/gov.uscourts.dcd.198259.1.0.pdf>

More importantly, according the recently surfaced official court document, David Keynes who offered Bylock app for use of public via Google Play Store and Apple iTunes Store told a US Federal Court that he was the owner of Bylock app, that the application was created to be presented to technology companies in Silicon Valley for eventual development, that the Bylock app was available for download via the Google Play Store and via the Apple iTunes Store.

Mr Keynes also states in his petition followings: “.. the Application has been downloaded by 500,000 to 1,000,000 people,

mostly from Turkey, Sweden, Azerbaijan, and Cyprus, with over 500,000 downloading the App on the Google Play Store and the rest downloading it on the Apple Store. During the years 2015 and 2016, the Defendants hacked Bylock by accessing its server and application, and at a minimum downloading personal and identifying information of Bylock’s users. It then held this information for future use against political dissidents.”

³⁰ Enjoined expert witness reports by UK lawyers William Clegg Q.C. and Simon Baker, and the forensic expert Thomas Kevin Moore.

³¹ Expert Witness Report on Bylock Investigation by FOX-IT.

³² Expert Report of Jason Frankovitz dated 9/8/2017.

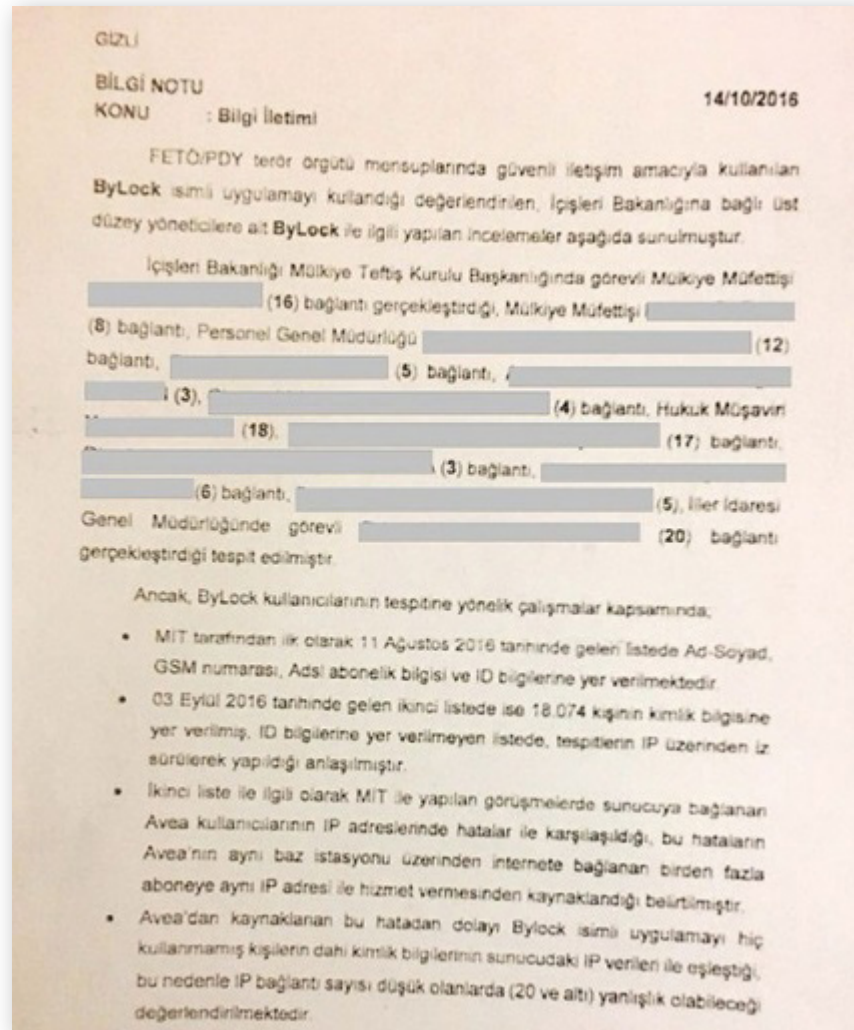
VI. OTHER PROBLEMS CASTING DOUBT ON THE ACCURACY OF THE BYLOCK DATA PRESENTED BY THE TURKISH AUTHORITIES

1. IP Convergence (updated)

The main method employed in the MIT Bylock Technical Report, and through which Bylock users are identified, is the monitoring of the respective IP traffic of suspects. If a suspect is found to have accessed any of the Bylock servers, he is defined as a Bylock user, and is charged and subsequently indicted for being a member of an armed terrorist organisation.

This method of identifying Bylock users through their respective IP addresses is not reliable, as Turkish telecommunications operators, and particularly Avea and Turk Telekom, do not provide a static IP service, which means that the same IP number can be given to different customers.

As revealed by Ahmet Takan, a Turkish journalist, this is called "IP Convergence", and when it was first noticed by the Turkish security authorities in October, 2016, a circular was promptly sent to the relevant authorities warning them of the IP Convergence issue.³³

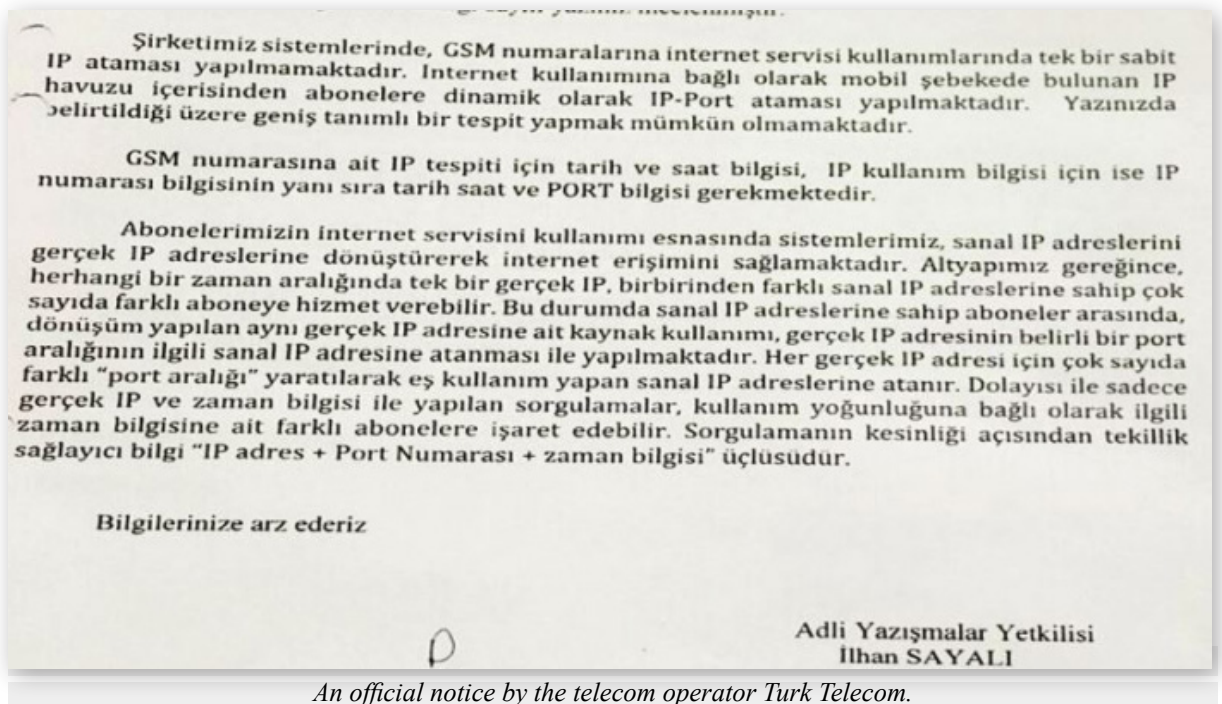


The notice (above), dated 14th October, 2016, says that:

- The MIT list, dated 3rd September, 2016, included 18,074 individuals who were identified as Bylock users through an examination of their respective IP traffic.
- The mobile phone operator AVEA gives the same IP number to each and every device which connects to the same mobile base station.
- Anybody who has accessed the Bylock server less than 20 times may therefore not be an actual Bylock user.

2. Assignment of random dynamic IP-Port numbers to customers

Turkish telecommunications operators, and particularly Avea and Turk Telekom, do not provide a static IP service to their customers, instead they assign random dynamic IP-Port numbers from the available IP pool. This consequently means that the same IP number can be assigned to different customers at different times. In an official memo, shown below, that was sent by the telecoms operator Turk Telecom to the judicial authorities, therefore said: "given the numerous customers who use the same IP address at the same time, misleading results can arise from IP address-based queries."



3. IP Routing

One technique employed in the MIT Bylock Technical Report to attribute the Bylock app to its alleged users, is that their IP addresses are being detected in the Bylock servers. However, two independent forensic experts have found that users of eight different smart phone apps were being routed to Bylock servers as a result of some random pop-up advertisement. A review of the matter has subsequently revealed that at least 11,480 individuals were routed to Bylock servers as a direct result of those 8 applications.

In December, 2017, the Ankara Chief Public Prosecutor conceded that 11,480 people, over a thousand of whom had been arrested, were wrongly prosecuted for being Bylock users.

On 3rd January, 2018, Milliyet Daily reported that although 11,480 individuals had so far been removed from the BYLOCK list, the circumstances of another 30,000 people who had been included in that same list were being reviewed.³⁴

4. Discrepancies between the records from MiT and BTK

Apart from the official Bylock Technical Report, MiT sent individual Bylock reports, prepared per user, to the judicial authorities. The courts then requested that BTK transmit to them the alleged Bylock users' internet traffic records. In the records cited in one of the academic journals that has published material on the subject, notable inconsistencies between the MiT reports and the BTK records are observed. The Figure below exemplifies how the two records, belonging to the same defendant, conflict with each other. According to the MiT report, the alleged Bylock user's IP on 18.02.2015 at 20:59:05 was 216.185.45.194 while, at the very same time, BTK records suggest that the IP was 46.166.164.177. Other examples of inconsistencies are pointed out in the Figure.³⁵

MIT REPORT		No	Hareket	Tarih	IP	Client		
		33	Login	2015-02-18 20:59:05	216.185.45.194	android		
BTK RECORDS		NUMARA	ÖZEL IP	ÖZEL PORT	GENEL IP	GENEL PORT	OTURUM BASLAMA TARİHİ	HEDEF IP
		505	10.57.102.77	41802	5.47.230.88	13527	18.02.2015 20:59:05	46.166.164.177
MIT REPORT		No	Hareket	Tarih	IP	Client		
		65	Login	2014-11-11 22:24:03	46.16.37.78	android		
BTK RECORDS		NUMARA	ÖZEL IP	ÖZEL PORT	GENEL IP	GENEL PORT	OTURUM BASLAMA TARİHİ	HEDEF IP
		505	10.58.117.178	55886	5.47.245.197	21851	11.11.2014 22:24:05	46.166.164.177
MIT REPORT		No	Hareket	Tarih	IP	Client		
		20	Login	2015-03-10 23:52:38	50.118.162.43	android		
BTK RECORDS		NUMARA	ÖZEL IP	ÖZEL PORT	GENEL IP	GENEL PORT	OTURUM BASLAMA TARİHİ	HEDEF IP
		505	10.57.131.127	51566	5.47.195.140	16391	10.03.2015 23:52:24	46.166.164.181
		505	10.57.131.127	43930	5.47.195.140	16045	10.03.2015 23:52:43	46.166.164.181

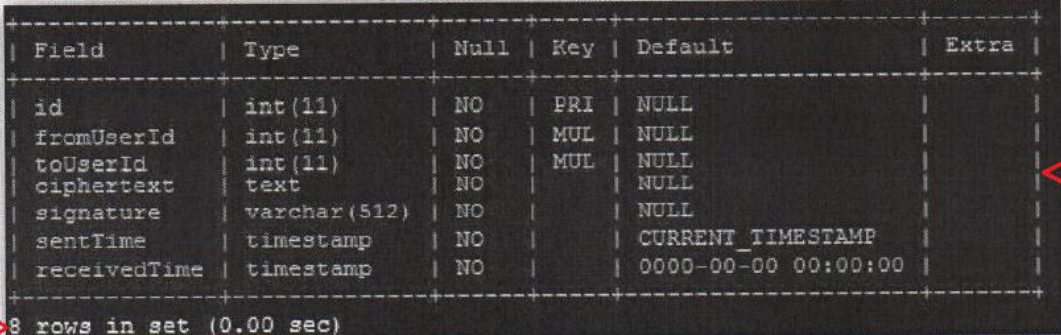
Comparison of MiT and BTK records (Personal information is blacked out for security concerns)

³⁴ Milliyet Daily, <https://www.milliyet.com.tr/gundem/Bylockta-magdur-sayisi-ile-ilgili-flas-iddia-2584227>

³⁵ Yasir Gökçe, The Bylock Fallacy, *Digital Investigation*, <https://doi.org/10.1016/j.diin.2018.06.002>

VII. CORRUPTION OF DATA IN THE MIT BYLOCK TECHNICAL REPORT

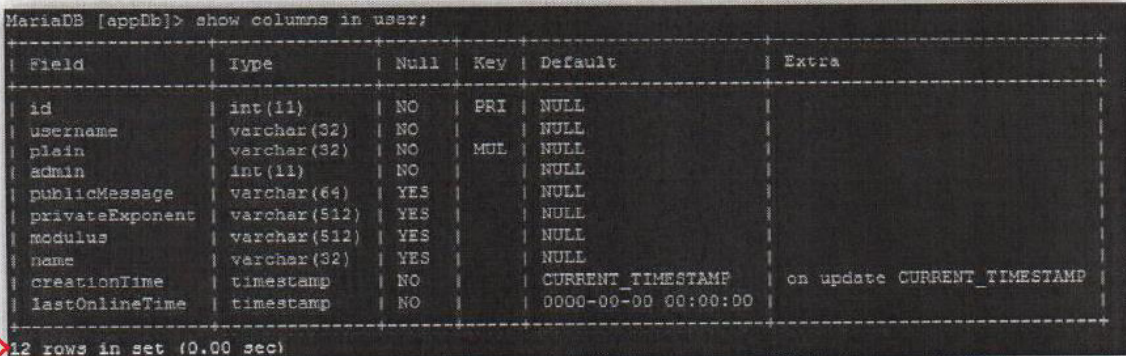
The aforesaid forensic analyses draw attention to some examples of the manipulation of data by MiT, which is evident in the screenshots in the technical report under Section 3.6.2, Section 3.6.2.4, and Section 3.6.2.15. The screenshots represent the output of an SQL query, displaying the rows and the total number of rows returned. The total number of rows indicated at the bottom of the screenshot does not match the actual number of rows. What's more, one can see the spacing differences between the rows.



Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
fromUserId	int(11)	NO	MUL	NULL	
toUserId	int(11)	NO	MUL	NULL	
ciphertext	text	NO		NULL	
signature	varchar(512)	NO		NULL	
sentTime	timestamp	NO		CURRENT_TIMESTAMP	
receivedTime	timestamp	NO		0000-00-00 00:00:00	

8 rows in set (0.00 sec)

Figure 5 at page 31 of the MIT Bylock Report



```
MariaDB [appDb]> show columns in user;
```

Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	
username	varchar(32)	NO		NULL	
plain	varchar(32)	NO	MUL	NULL	
admin	int(11)	NO		NULL	
publicMessage	varchar(64)	YES		NULL	
privateExponent	varchar(512)	YES		NULL	
modulus	varchar(512)	YES		NULL	
name	varchar(32)	YES		NULL	
creationTime	timestamp	NO		CURRENT_TIMESTAMP	on update CURRENT_TIMESTAMP
lastOnlineTime	timestamp	NO		0000-00-00 00:00:00	

12 rows in set (0.00 sec)

Figure 15 at page 48 of the MIT Bylock Report

Another corruption of data that has been exemplified by the aforesaid digital forensic analysts is the Table below, which was employed in the MiT Bylock Report. The Table is a salient example of how MiT inexplicably removed data from a command listing. It represents a command line whose output is IP tables. Although the command line prefix (`root@hst-46-166-160-137:~#`) is visible in the Table, the command itself cannot be seen, an inconsistency which is notably unexpected and which suggests manipulation by the MiT. It can be inferred that the command was intentionally removed from the listing so that an inquisitive reader cannot verify whether the depicted output is really the result of the command that has been removed.

```
root@hst-46-166-160-137:~#  
iptables -N LOGGING  
iptables -A INPUT -s 5.2.80.0/21 -j LOGGING  
iptables -A INPUT -s 5.11.128.0/17 -j LOGGING  
iptables -A INPUT -s 5.23.120.0/21 -j LOGGING  
iptables -A INPUT -s 5.24.0.0/14 -j LOGGING  
iptables -A INPUT -s 5.44.80.0/20 -j LOGGING  
iptables -A INPUT -s 5.44.144.0/20 -j LOGGING
```

Command table at page 25 of the MIT Bylock Report

Moreover, according to two forensic experts, Assistant Professor Baha Şen, and the digital forensics expert Rafet Öngöçmen, who were assigned by the Ankara Public Prosecutor's Office within the investigation no. 2016/104109, they concluded that the copy of the Bylock digital data that was given to them for examination was corrupted. Their report, dated July 12th, 2017, shows that the Bylock digital data is corrupted, and cannot therefore be opened, it may thus be opened only by using special recovery techniques.

Disk içerisinde yer alan ve **113.789.140 KB (108 GB (116.520.079.360 bayt))**'lik kapasiteye sahip "**ibdata1**" dosyasının **MySQL** veri tabanı dosyası olduğu görülmüş ve içerisindeki verilerin tablo yapısının ortaya çıkartılması için çalışmalar yapılmıştır. Ancak ilgili dosya yapısı bozuk olduğu için şema bileşenlerine erişilememiştir.

ibdata1 dosyası içerisindeki verilere erişim sağlanabilmesi ve bu verilerin tablolar halinde kurtarılması için **Linux Centos ve Debian** işletim sistemleri üzerinde "**Percona Data Recovery (percona-data-recovery-tool-for-innodb)**" <https://www.percona.com/> ve "**TwinDB Data Recovery (undrop-for-innodb)**" araçları kullanılmıştır. <https://recovery.twindb.com/>

İlgili araçlar ile yapılan işlemler sonucunda "**ibdata1**" içerisinde toplam **(28)** adet tablonun bulunduğu "**appDb**" ve "**wordpress**" isimli iki ayrı veri tabanının yer aldığı, **abDb** içerisinde toplam **(15)** adet tablonun bulunduğu, **wordpress** veri tabanında **(11)** adet tablonun yer aldığı görülmüştür. "**byLock**" veri tabanına ait "**appDb**" detaylı olarak incelenmiştir.

The "ibdata1" file located on the disk and has a capacity of 113.789.140 KB (108 GB (116.520.079.360 bytes)) has been found to be MySQL database file, and in order to reveal the table structure of the data, required works have been carried out. However, the schema components are not accessible because the corresponding file structure is corrupted.

"Percona Data Recovery tool-for-innodb" on **Linux Centos and Debian** operating systems for accessing and recovering data in **ibdata1** file <https://www.percona.com/> and **"TwinDB Data Recovery (undrop-for-innodb)"** tools were used. <https://recovery.twindb.com/>

As a result of transactions with related tools, it is observed that "ibdata1" contains a total of (28) tables, contains two separate databases, named "appDb" and "Wordpress" and abbDb contains a total of (15) tables, wordpress database contains (11) tables. The appDb "belonging to the" bylock " database was examined in detail.

This screenshot was taken from the report titled Expert Opinion on the Accuracy and Reliability of the Digital Data Obtained from the Bylock Server in Lithuania of Koray Peksayar and Levent Maziligüney³⁶

³⁶ Levent Maziligüney and Koray Peksayar, Expert Opinion on the Accuracy and Reliability of the Digital Data Obtained from the Bylock Server in Lithuania, <https://www.patreon.com/posts/accuracy-and-of-54329745>.

VIII. NON-COMPLIANCE WITH THE CODE OF CRIMINAL PROCEDURES

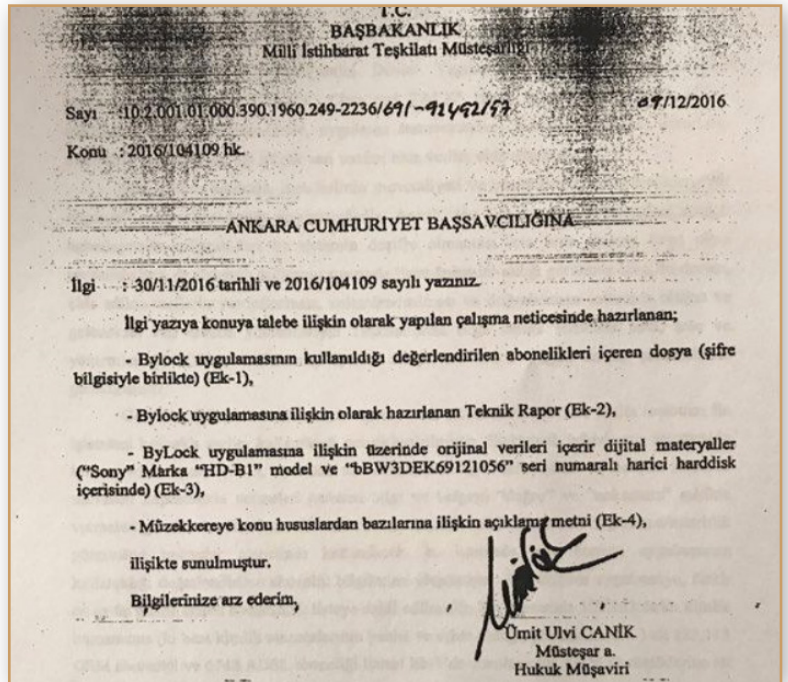
1. Relevant Facts

When did the Turkish government and the judiciary become aware of the Bylock App? When was the Bylock data handed to the judicial authorities by the Turkish National Intelligence Service (MİT)?

In its press statement, dated 6th April, 2017, MİT stated that all of the findings about Bylock, and the raw data compiled through intelligence initiatives, were shared with judicial, security and other authorities in May, 2016.³⁷ Likewise, a Turkish government official, who spoke to Agence France-Presse said that MİT began decrypting messages that had been sent on Bylock in May, 2016.³⁸ However, the Ankara Chief Public Prosecutor's Office subsequently challenged this statement, and said: "we were not given Bylock data by MİT at that time. We became aware of Bylock after July 15th [2016]."³⁹ 40

This controversy indicates an essential problem with regard to the authenticity and admissibility of Bylock as evidence. This issue will be delved into in the chapters that follow.

In September, 2016, Faruk Özlü, the then Minister of Science and Technology, said that there were 215,000 Bylock users,⁴¹ and on 6th October, 2016, Veysi Kaynak, then Deputy Prime Minister, said that 18 million messages had been obtained and the process of decrypting each and every one of these messages was underway.⁴² Further, it was reported on 11th November, 2016, that an indictment presented by the Izmir Prosecutor, Ayhan Yılmaz, to the Izmir 13th Heavy Penal Court, stated that MİT had already decrypted 17 million of the 18 million text messages, plus 2.5 million of 3.5 million e-mails.⁴³ MİT passed devices containing digital data from Bylock's servers to the judicial authorities on 9th December, 2016.



Official memo dated 9th December, 2016 of the MİT on the delivery devices containing digital data from Bylock's servers

37 Press Statement of MİT, <https://www.mit.gov.tr/basin60.html>

38 Middle East Eye, <https://www.middleeasteye.net/haber/mitin-bylock-celiskisi-717302>, <https://www.bbc.com/turkce/haberler-dunya-39513263>

39 Cumhuriyet Daily, <https://www.cumhuriyet.com.tr/haber/mitin-bylock-celiskisi-717302>

40 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>

41 Habertürk Daily News, <https://www.haberturk.com/ekonomi/teknoloji/haber/1294035-faruk-ozlu-by-locku-tubitaktaki-fetoculer-gelistirdi>

42 Yeniçag Daily News, <https://www.yenicaggazetesi.com.tr/bakan-veysi-kaynak-18-milyon-bylock-mesaj-var-tek-tek-inceleniyor-147602h.htm>

43

Anadolu News Agency, <https://www.aa.com.tr/tr/15-temmuz-darbe-girisimi/Bylock-fetoye-uyelikte-belirleyici- kabul-edildi/682560>

Accordingly, the first judicial order to authenticate (digital image taking) digital Bylock data was made on 9th December, 2016, by the Ankara 4th Criminal Peace Judgeship.⁴⁴

This order explicitly mentioned that a hard disk and a USB stick containing digital data found on Bylock were passed to the Ankara Chief Public Prosecutor's Office and, on 9th December, 2016, the Ankara Chief Public Prosecutor's Office asked for an order to authenticate the digital data and to subsequently examine these devices. ,

On 24/3/2017, another hard disk containing digital data from Bylock servers was passed by the MIT to the Ankara Chief Public Prosecutors and, subsequently, a separate image taking and forensic examination authorization order was given.⁴⁵

T.C.
ANKARA
4. SULH CEZA HÂKİMLİĞİ
DEĞİŞİK İŞ NO : 2016/6774

Aslı Gibidir
Adnan GÜNGÖR
C.Savcısı-34212

HAKİM : ABDURRAHMAN GÜN 40869
KATİP : NİHAL GÖKALAN 96444

Ankara Cumhuriyet Başsavcılığı'nın, 09/12/2016 tarih ve 2016/104109 soruşturma sayılı yazısı ile,
"Ankara Cumhuriyet Başsavcılığı tarafından FETÖ/PDY Silahlı Terör Örgütü mensuplarına yönelik yürütülen soruşturmalar kapsamında örgüt üyeleri tarafından kullanılan kapalı devre iletişim programı Bylock ile ilgili Millî İstihbarat Teşkilatından gelen;
1- 1 adet Sony marka HD-B1 model, üzerinde bBW3DEK69121056 seri numaralı ve ön yüzünde 1173d7a09195cf0274ce24fd69ede96 yazılı harddisk,
2- 1 adet Kingston marka DataTraveler, uç kısmında DTIG4/8GB 04570-700.A00LF 5V 0S7455704 yazılı flash bellek üzerinde,
CMK'nun 134. maddesi gereğince 2 adet kopya çıkarılmasına, bu kopyalardan birinin Ankara Cumhuriyet Başsavcılığı Emanetinde saklanmasına, diğer kopyanın üzerinde kayıtların çözülerek metin haline getirilmesi için bilirkişi incelemesi yaptırılmak üzere Cumhuriyet Başsavcılığımıza gönderilmesine, Millî İstihbarat Teşkilatından gönderilen yukarıda marka ve modelleri ile seri numaraları belirtilen harddisk ve flash belleğin Mahkeme Emanetinde saklanmasına" karar verilmesi talep edilmekte, evrak incelenildi;

GEREĞİ DÜŞÜNÜLDÜ:
Ankara Cumhuriyet Başsavcılığı'nın, 09/12/2016 tarih ve 2016/104109 soruşturma sayılı talebin **KABULÜ** ile;
1 adet Sony marka HD-B1 model, üzerinde bBW3DEK69121056 seri numaralı ve ön yüzünde 1173d7a09195cf0274ce24fd69ede96 yazılı harddisk ve
1 adet Kingston marka DataTraveler, uç kısmında DTIG4/8GB 04570-700.A00LF 5V 0S7455704 yazılı flash bellek üzerinde CMK'nun 134. Maddesi uyarınca inceleme yapılabilmesi için 2 kopya çıkarılmasına,
Kopya çıkarılması için Ankara İl Emniyet Müdürlüğü Siber Suçlar Şube Müdürlüğünden yeterince uzmanın görevlendirilmesi için Ankara Cumhuriyet Başsavcılığına mützekkere yazılmasına,
Kopya üzerinde FETÖ/PDY soruşturmaları kapsamında bilirkişi incelemesi yaptırılması ve metin haline getirilebilmesi için Ankara Cumhuriyet Başsavcılığına gönderilmesine,
Millî İstihbarat Teşkilatından gönderilen 1 adet Sony marka HD-B1 model, üzerinde bBW3DEK69121056 seri numaralı ve ön yüzünde 1173d7a09195cf0274ce24fd69ede96 yazılı harddisk ile 1 adet Kingston marka DataTraveler, uç kısmında DTIG4/8GB 04570-700.A00LF 5V 0S7455704 yazılı flash bellek ve birer kopyasının soruşturma süresince adli emanette muhafazasına,
Soruşturma dosyasının Ankara Cumhuriyet Başsavcılığı'na İADESİNE,
Soruşturma dosyası üzerinde yapılan inceleme sonunda kararın öğrenildiği tarihten itibaren 7 gün içerisinde Ankara 5. Sulh Ceza Hakimliği'ne itiraz yolu açık olmak üzere karar verildi.09/12/2016

Katip 96444
ASLI GİBİDİR
.....12/2016
Hakim 40869
ADM

T.C.
ANKARA
5. SULH CEZA HÂKİMLİĞİ
DEĞİŞİK İŞ NO : 2017/2056 D.İş

Adnan GÜNGÖR
C.Savcısı-34212

HAKİM : Yusuf ARSLAN 97998
KATİP : Mehmet TELLİ 94087

Ankara C. Başsavcılığı Anayasal Düzene Karşı İşlenen Suçlar Soruşturma Bürosunun 24/03/2017 gün ve 2016/180056 sayılı yazılan ile,
Cumhuriyet Başsavcılığımız tarafından FETÖ/PDY Silahlı Terör Örgütü mensuplarına yönelik yürütülen soruşturma kapsamında örgüt üyeleri tarafından kullanılan kapalı devre iletişim programı Bylock ile ilgili Millî İstihbarat Teşkilatı Müsteşarlığına Cumhuriyet Başsavcılığımıza gönderilen Datatraveler G4 marka DTIG4/8GB 04570-760B00LF 5V 0S 7575458 seri numaralı TAIWAN ibaresi bulunan dijital materyal üzerinde CMK 134.maddesi gereğince inceleme yapılmasına, kopya çıkarılmasına (imaj alma) bu kayıtların çözülerek metin haline getirilmesine karar verilmesi talep edilmiş olmakla, talep ekindeki belgeler incelenmekte,
İspat aracı olarak yararlı görüldüğünden, imaj alma talebinin kabulüne dair aşağıdaki şekilde karar verilmiştir.

GEREĞİ DÜŞÜNÜLDÜ:
Talebin **KABULÜ** ile,
Datatraveler G4 marka DTIG4/8GB 04570-760B00LF 5V 0S 7575458 seri numaralı TAIWAN ibaresi bulunan dijital materyal üzerinde CMK 134.maddesi gereğince inceleme yapılmasına, kopya çıkarılmasına (imaj alma) bu kayıtların çözülerek metin haline getirilmesine
Evrakın Ankara C. Başsavcılığı'na iadesine,
Dair, CMK'nun 268 maddesi gereğince 7 gün içerisinde Hakimliğimize verilecek bir dilekçe veya tutanağa geçirilmek koşulu ile zabıt katibine beyanda bulunulması suretiyle kararın tebliğinden itibaren Ankara 6. Sulh Ceza Hakimliği nezdinde itiraz yolu açık olmak üzere dosya üzerinde yapılan inceleme sonucunda karar verildi. 24/03/2017

Katip 94087
E imza
Hakim 97998
E imza

Order of Ankara 4th Criminal Peace Judgeship, 9/12/2016 (L) | Order of Ankara 5th Criminal Peace Judgeship, 24/3/2017(R)

However, the document, dated 17th October, 2016 (next page), shows that digital data, including the users' IDs of account holders had been processed by MIT and disseminated to the law enforcement agencies in September, 2016, without any judicial oversight, and before the judgeship order of the Ankara 4th Criminal Peace Judgeship. This document proves that the Bylock digital data, having been processed by the MIT, passed to the Turkish police, and this data was uploaded by the latter to the database of the Turkish Police's Anti-Terror Department.

44 Ankara 4th Criminal Peace Judgeship, 9/12/2016, 2016/6774.

45 Ankara 5th Criminal Peace Judgeship, 24/3/2017, 2017/2056.

Bu bağlamda Emniyet Genel Müdürlüğü Terörle Mücadele Daire Başkanlığının 01.08.2016 tarih ve 45599763/56586.(12220)1239-1036(2)/ Bilgi İletimi yazıları ile İltisaklı IV kurumundan temin edilen ve İstihbarat Daire Başkanlığı tarafından, Terörle Mücadele Daire Başkanlığına gönderilen, FETÖ/PDY üyelerinin kendi içlerindeki iletişimi sağladıkları "BYLOCK" adlı programı mobil cihazlarına yükleyerek kullandıkları değerlendirilen şahısların listesi Daire Başkanlığımızca yapılan çalışmalar sonucu; Polnet ortamında çalışan "D ŞUBE VERİLERİ PROGRAMI" isimli sorgu programı haline getirilmiştir.

Bahse konu program üzerinde "BYLOCK" kullanıcıları ile ilgili, A [REDACTED] Başsavcılığının [REDACTED] sayılı soruşturması kapsamında yakalanarak gözaltına alınan şüphelilerden D Şube Verileri Programı üzerinden yapılan sorgulamasında Bylock tespiti yapılmış, 29.09.2016 tarihinde D Şube Verileri Programı veri tabanında güncelleme yapılarak yapılan sorgulamalar sonucunda Kırmızı, Turuncu ve Mavi renk olmak üzere kategorize edilmesine istinaden veri tabanı üzerinde yeniden yapılan incelemede;

[REDACTED] 29.09.2016 tarihinde [REDACTED] Renk TURUNCU" şeklinde bilgilerin yer aldığı.



FETÖ/PDY terör örgütü üyelerinin örgütsel görüşmelerde iletişim imkânı sağlayan "BYLOCK" isimli programı kullandığının tespit edildiği, Yukarıda belirtilen Bylock modülü sorgulamasında elde edilen verilerin PVSK, Ek 7. Madde kapsamında ve istihbari mahiyette olduğu tespit edilmiş olup.

İş bu Araştırma ve Tespit Tutanağı tarafımızdan tanzimle altı birlikte imzalanmıştır.
17/10/2016

Tem Şb Gör.

Tem Şb Gör.

Tem Şb Gör.

2. Breach of Article 160 of the Code of Criminal Procedures

According to Art. 160 of the Code of Criminal Procedures, criminal investigations are administered by public prosecutors. Art. 164 of the CCP requires that judicial law enforcement departments shall act upon the instructions of the public prosecutors. Judicial law enforcement officers should therefore ask for instruction from the public prosecutors in regard to every step that they will take, and shall duly inform them about every development.

Under Articles 2/e and 161 of the Criminal Procedure Law (CMK – No:5271) and the Article of Annexe-6 of the Law in regard to the Duties and Authorities of the Police, the law enforcement agent who learns of a situation that implies that a crime was, or is, being committed, should immediately inform the Public Prosecutor and proceed with the investigation under his/her orders. Proceedings without a legal search warrant or a proper judicial order are considered illegal.⁴⁶

Firstly, it should be underlined that MİT is not a judicial law enforcement body, and therefore cannot be involved in criminal proceedings except for those involving crimes of espionage.

46 16th Chamber of the Turkish Court of Cassation, 21.04.2016, 2015/4672 E., 2016/2330 K

Second, in a case in which MiT explored a crime that was committed during its intelligence activities, it should duly inform the judicial authorities and ask for instruction, as explained above. However, on the contrary, MiT, without any judicial oversight, conducted an investigation relating to Bylock and its users for months, and did not inform the judicial authorities until July, 2016, and did not pass the digital evidence to the judicial authorities until 9th December, 2016.

3. Breach of Article 134 of the Code of Criminal Procedures

Art. 134 of the CCP stipulates that digital evidence may be acquired from electronic devices, as well as its proper authentication, preservation, processing.

The Court of Cassation has ruled on the procedural requirements in relation to digital data, such as that of Bylock, that:

"In criminal proceedings, evidence must be obtained in accordance with the law and must be obtained using methods sanctioned by the law. In order to be able to conduct a fair trial, and to be able to evaluate the findings collected during the investigation (and the prosecution) as evidence; the digital data obtained from suspects (or defendants) must be collected in accordance with the technical requirements that are set up by the law, and must be submitted to the judicial authorities in a complete, and uncorrupted state. It is the purpose of the Legislator, while enacting Art. 134 of the Criminal Procedure Law (CMK) in detail. Since the fact that external intervention in the digital evidence is technically feasible, and that it is often not possible to determine by whom the intervention was made, it is necessary for its safe confiscation and examination to leave the original media with the suspect after its image has been taken in situ... Under Articles 2/e and 161 of the Criminal Procedure Law (CMK – No:5271) and the Article of Annexe-6 of the Law in regard to the Duties and Authorities of the Police, the law enforcement agent who learns of a situation that implies that a crime was, or is, being committed, should immediately inform the Public Prosecutor and proceed with the investigation under his/her orders. Proceedings without a legal search warrant or proper judicial order are considered illegal."^{47 48}

The statement of the Deputy PM⁴⁹, the indictment of the Izmir Prosecutor,⁵⁰ the document above dated 17th October, 2016, together provide a strong inference that the data from Bylock had been examined and processed by MiT long before it was passed to the judicial authorities, as the date of first judicial order to authenticate (digital image taking) the digital Bylock data was 9th December, 2016.⁵¹

In accordance with procedure, as outlined above, MiT should have immediately passed this data and these devices to the judiciary as they were, and *without delay*, so as to enable the latter to carry out the first authentication/image taking process within the ambit of a judicial order, and then carry out an examination under the Code of Criminal Procedure. MiT does not have any authority to examine and process such data.

The processing of the data by MiT without judicial oversight, and its consequent late delivery to the authorities, raise serious questions for the Court as to the integrity and authenticity of the Bylock evidence. Likewise, another serious issue concerning the integrity of the Bylock evidence is that the disintegration of the digital evidence and the conducting of the forensic

47 16th Chamber of the Turkish Court of Cassation, 21.04.2016, 2015/4672 E., 2016/2330 K

48 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>

49 Yeniçağ Daily, <https://www.yenicaggazetesi.com.tr/bakan-veysi-kaynak-18-milyon-Bylock-mesaj-var-tek-tek-inceleliyor-147602h.htm>

50 Anadolu News Agency, <https://www.aa.com.tr/tr/15-temmuz-darbe-girisimi/Bylock-fetoye-uyelikte-belirleyici-kabul-edildi/682560>

51 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>

examination (forensic image taking), as two separate processes, took place on two separate dates, 9th December, 2016, and 24th March, 2017.⁵²

As the result of this non-compliance with procedural laws, neither the judicial authorities nor the defendants know:

How the digital data relating to BYLOCK was saved until 9th December, 2016, and 24th March, 2017?

- Why has the digital evidence been disintegrated?
- Was the digital data corrupted by Turkish İNTEL (MİT)?
- What measures were taken to preserve the authenticity of the digital evidence while MİT processed it?
- Why was the forensic image taking not carried out as soon as the data was obtained from the Bylock servers?

All in all, as pointed out here⁵³, the MİT seems to have failed to adhere to very basic principles of digital forensics throughout the handling of the Bylock data, from its acquisition to its analysis, modification and preservation. The foremost of such failures is the lack of documentation during the analysis. The MİT has failed to record, and thereby to provide transparency for, the sequence of steps it took during its analysis, a deficiency which notably impairs the chain of custody in relation to the digital evidence. Besides, the MİT apparently neglected to apply cryptographic hash functions to the clusters of Bylock data which were to be subjected to digital forensics. Without such cryptographic procedures, the data's integrity cannot be guaranteed by the analysts, because they would lack the hashed values that act as the anchors and which enable them to prove that the data has not been corrupted, either by them or by third parties. Moreover, the results of the Bylock Technical Report are not replicable nor are they independently verifiable, as suspects have never been provided with an exact bit-by-bit copy, or a forensic image of the digital evidence against them. Lastly, neither in the Technical Report nor afterwards has the MİT specified how the security of either the original or the processed Bylock data is ensured, or what measures are carried out to preserve its integrity, e.g., access controls, encryption, logging, etc.⁵⁴

MİT's failure to comply with the law, and the Ankara Chief Public Prosecutor's Office's ignorance of this failure, warrants an independent expert's forensic examination of all of the digital data and devices relating to Bylock. However, without exception, defendants have been denied this by the Turkish Courts, which raises, for the European Court of Human Rights and other international tribunal, the principle of the requirement for equality of arms.⁵⁵

4. Evaluation of the Bylock case under the law around the seizure of digital devices

Should one assume the accuracy of the official narrative: that the MİT purchased the Bylock servers from the Lithuania-based company 'Baltic/Cherry Servers', the MİT can then be claimed to have relied on Article 134 of the Code of Criminal Procedure, which necessitates a judge's decision for the seizure of electronic devices. In that regard, the warrant issued by the

⁵² Ibid

⁵³ 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/>

⁵⁴ Ibid.

⁵⁵ 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>

Ankara 4th Peace Judge to allow the hard drives containing the Bylock data to be seized and searched, has frequently been cited in an attempt to allude to the legality of the procedure of data acquisition under Article 134 of the TCPC. Although this gives the impression of the involvement of a judge prior to the acquisition of Bylock, it fails to capture the fact that, by the time the Ankara 4th Peace Judge decided on a seizure order, the MiT had already acquired, processed and analysed the Bylock data, and had prepared the Bylock user lists based on them.

5. Breach of Article 135 of the Code of Criminal Procedures

In order for an interception of private communication not to violate the right to a private life, and to be presented before a court as evidence, the following criteria are envisaged in Article 135 of the Code of Criminal Procedure, and they must be fulfilled:

- An investigation or prosecution must already have been launched.
- There must be strong grounds for suspicion, indicating that the crime has been committed.
- There must be no other possibility to obtain evidence.
- On the condition that the three criteria mentioned above are met, a judge may decide to intercept or wiretap the private communications of suspects.

According to the official figures in the MiT's Bylock Technical Report, the number of people whose metadata was obtained by the MiT is 225,000. However, one cannot document the investigations that had been launched against those 215,000 individuals by the time that the Bylock data were obtained. The Bylock Technical Report, or the subsequently-produced reports, have not cited any tangible evidence that underpins a strong suspicion of crime. They have also failed to evaluate whether there is another possibility through which to obtain evidence. Last, but not least, there is no judicial decision ordering the interception of the Bylock communications that allegedly belong to those 225,000 suspects.

6. Breach of the law governing data retention

The way in which the Bylock metadata was gathered also has legal implications in terms of the Turkish law on data retention. In its Bylock Technical Report, the MiT asserts that entries in the log tables of the Bylock database have been used to identify individuals. These entries involve the IP addresses of Bylock users during login and registration. An IP address is linked to an individual by matching it with the log data that are retained by internet service providers. The period within which internet service providers are allowed to retain metadata sheds light on the problematic aspect of the attribution of IP addresses to individuals by the MiT.

Under the Turkish Personal Data Protection Law, personal data shall not be processed without obtaining the explicit consent of the data subject, unless it is expressly permitted by any law. The Regulation on the Processing, Storage and Preservation of Personal Data legislates that the exact retention period of communications data is *one year*. Put differently, internet service providers cannot retain log data for more than one year, otherwise the criminal offence of a failure to destroy the data despite the expiry of the legally prescribed period would apply.

It is observed that the great majority of the Bylock metadata is dated in late 2014. If applying the one-year data retention period, the internet service providers had to destroy the internet traffic data as of the end of 2015. In 2016, therefore, at the time that the Bylock investigations

began, internet traffic data from 2014 should have been deleted. However, on 26th June, 2017, Hürriyet Daily News reported from Ömer Fatih Sayan, the Head of the BTK (Information Technologies Agency) as saying that a list of 102,000 people who are Bylock users was sent by BTK to the judicial authorities. Sayan said: "We have prepared reports and met the demands of the courts one by one, whichever court has the investigation files of these people on the list. ... We have confirmed that they have used Bylock. Those on the Bylock list therefore have no excuse left. By getting detailed records of their correspondence, we have once again determined that they have used Bylock."⁵⁶ This statement shows that the Turkish authorities retained the internet traffic data of individuals for more than one year, thus being in a clear breach of the aforementioned legal provision.

7. Breach of the law governing intelligence activities

Under Additional Article 7 of the Law on Police Duty and Authority no.2559, and Article 6 of the Law Founding the MiT no. 2937, Article 6 of the Law Founding the MiT no. 2937, the Turkish police and MiT 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.

Bylock data acquired by MiT may not be used as evidence because:

- a) *MiT shall use its powers therein as a preventive measure,*
- b) *MiT should have obtained a judgeship order before conducting intelligence activities in relation to the Bylock App and its users,*
- c) *However, MiT carried out intelligence operations which involve digital surveillance and the examination of internet traffic data without a judgeship order authorizing them to do so,*
- d) *The data acquired by MiT is intelligence information, and it may not be used in judicial proceedings.*

⁵⁶ Hürriyet Daily News, <https://www.hurriyetdailynews.com/102000-suspects-accused-of-gulen-links-are-Bylock-users-turkish-communication-authority-says-114783>

IX. CASES CONCERNING THE BYLOCK APP THAT ARE BEFORE SUPRANATIONAL MECHANISMS

1. Opinions by the UN Bodies on the Bylock App

The UN Working Group on Arbitrary Detention have consistently concluded that downloading and using Bylock represents the exercise of a person's basic rights to freedom of opinion and expression.⁵⁷ 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.⁵⁸

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 Gülen movement, in general, but had failed to elaborate on how the alleged use of the Bylock application by any of the accused individuals could be equated with a criminal act. In parallel to what the ECtHR has established, the UN Working Group opines that the criminal nature or context of the correspondence via the Bylock App must be given regard when assessing the evidentiary value of the use of that App for terrorist membership.

Furthermore, the UN Working Group notes numerous cases involving the arrest and prosecution of individuals on the basis of their alleged use of the Bylock App, 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 UN Working Group also concludes that, in the absence of a specific explanation of how the mere use of Bylock constituted a criminal act, the detention of those accused was arbitrary. The UN Working Group goes on to conclude that even if any of the suspected individuals had used the Bylock App, 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, namely, the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, ... through any media of choice."

After 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 UN Working Group recalls that this pattern, which involves widespread or systematic imprisonment or other severe deprivation of liberty, in violation of the rules of international law, suggests that under certain circumstances, these are crimes against humanity. The widespread or systematic commission of the crime of the arbitrary deprivation of liberty on the pretext of, amongst others, the use of Bylock, and its potential qualification as being a crime against humanity, have been covered in great depth in the linked report.⁵⁹

In a similar vein, where the complainant was accused of membership of an armed terrorist organisation on the basis of downloading Bylock, the Human Rights Committee said: "... the only evidence held against İsmet Özçelik is the use of the Bylock application and the deposition of funds in the 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

⁵⁷ Faruk Serdar Köse vs Turkey, Kahraman Demirez et. al v. Turkey and Kosovo, Nermin Yasar v. Turkey, WGAD/2020/30,47,74.

⁵⁸ Human Rights Committee, General comment No. 34, <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

⁵⁹ Institute, <https://institute.org/report/human-rights-violations-in-turkey-rising-to-the-level-of-crimes-against-humanity-case-of-gulen-group>

that the authors' detention amounted to a violation of their rights under Article 9 (1-2) of the Covenant." ⁶⁰

In its decision, the UN Human Rights Committee 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 Human Rights Committee connotes the existence of the dangerous pattern that is being established by all these cases. Last, the Committee holds that the detention of the individuals concerned, on the mere ground of the use of Bylock, fails to meet the criteria of reasonableness and necessity.

2. Cases before the ECtHR

In the case of *Saglam v. Turkey*, an individual who was convicted of membership of an armed terrorist organisation ("FETÖ") for using Bylock, the European Court of Human Rights (ECtHR) posed⁶¹ a series of questions to the Turkish government about the Bylock messaging app. These questions had been asked by defendants, such as Mr. Saglam, since day one of the accusations, but had so far fallen on deaf ears in relation to the Turkish judiciary. Almost the same questions have been directed in the case of *Yalcinkaya v. Turkey*, which is pending before the ECtHR.⁶²

That being said, the foremost of these questions are cited below, along with the respective sections of the present report that satisfactorily addresses them.

The following question from the ECtHR aims to examine whether the Bylock data was obtained lawfully, and whether the Bylock app is of an evidentiary nature, which merits the qualification of being legal and legitimate evidence that is admissible before a court of law. This question was extensively addressed under Subsections XIII.1-4 of the report.

Did the domestic authorities comply with the statutory provisions under Turkish law regulating the collection, examination and use of evidence, including electronic and digital evidence, in so far as the Bylock evidence is concerned?

In the question below, the ECtHR scrutinizes the process of the acquisition and analysis of the Bylock data under the law governing data retention. To that end, it highlights various provisions of the Turkish regulations on data retention, and asks whether the Bylock data were obtained and retained having due regard to these provisions. The report covers this topic in depth under its Subsection XIII.6.

Was the evidence concerning the applicant's use of Bylock obtained lawfully, having regard to the allegation that the internet traffic information provided by the Information and Communication Technologies Authority (Bilgi Teknolojileri ve İletişim Kurumu, 'BTK') was not retained and disclosed lawfully, as it included information that predated the maximum time-limit set out in the law for the retention of such data?

Last, but not least, the following question boils down to the reliability, accuracy, authenticity and integrity of the Bylock data on which the allegations of Bylock use are predicated. The ECtHR aims to delve into the technical aspects of the Bylock investigations in order to uncover whether basic principles of digital forensics have been complied with throughout. This question was addressed in great depth under Sections III-IV-V-VI and VII of the report.

⁶⁰ The UN Human Rights Committee, *İsmet Özçelik et. al.*, CCPR/C/125/D/2980/2017.

⁶¹ ECtHR, <http://hudoc.echr.coe.int/eng?i=001-208741>

⁶² ECtHR, <http://hudoc.echr.coe.int/eng?i=001-208743>

Was the evidence concerning the applicant's use of Bylock sufficiently reliable? In particular;

- (i) To what extent was the digital evidence obtained regarding the applicant a reliable indicator of his use of Bylock, from a technical point of view? Did the domestic courts sufficiently assess the reliability of the digital evidence presented to it by the prosecution and did they respond to the applicant's concerns regarding the reliability of that data?
- (ii) What safeguards were available in domestic law to protect the integrity and authenticity of the Bylock data obtained by the MiT during the period preceding its submission to the prosecution authorities, given that the relevant procedural safeguards envisaged under the Criminal Code of Procedure were not found by the domestic courts to have any application during that initial period?

Finally, it is worthwhile here to highlight a piece which summarizes the *Yalcinkaya* case and scrutinizes the questions posed by the ECtHR within the context of this case, from both the legal and technical perspectives.⁶³

3. The Akgün judgment by the ECtHR

Mr. Akgün, a former police officer, was put into pre-trial detention in October, 2016, due to his alleged use of the Bylock App, and he was convicted for being a member of a terrorist organization. After exhausting the domestic remedies, Mr. Akgün lodged an application before the ECtHR.

The ECtHR held that Turkey was:

- in violation of Article 5 § 1 (the right to liberty and security) of the European Convention on Human Rights;
- in violation of Article 5 § 3 (entitlement to trial within a reasonable time, or to release pending trial), and
- in violation of Article 5 § 4 (the right to a speedy decision on the lawfulness of detention).

The case concerned the applicant's being placed in pre-trial detention on suspicion of being a member of an organisation that is referred to by the Turkish authorities as "FETÖ". The European Court considered that, when ordering the applicant's pre-trial detention, in October, 2016, the domestic court had not had sufficient information on the nature of Bylock to conclude that this messaging application was used exclusively by members of the "FETÖ" organisation for the purposes of internal communication. In the absence of other evidence or information, the document in question, stating merely that the applicant was a user of Bylock, could not, in itself, indicate that there were reasonable suspicions that would satisfy an objective observer that he had indeed used the Bylock App in a manner that could amount to the alleged offences.

In her defense, Turkey employed two expert reports, which basically reiterate the conclusions of the official Bylock Technical Report of the MiT (paras. 57 & 60). It appears from the way in which the authors of these reports drew conclusions that they had not also been granted access to the rough Bylock data, and that they had to base their conclusions on the already

⁶³ 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/>

established findings of the MIT report, a phenomenon which considerably impairs the credibility, objectivity and accuracy of the expert reports. That the Turkish government has not granted even the forensic experts that it had itself hired access to the original, unprocessed Bylock data, reveals the extent to which the MIT had deviated, in its Bylock investigation, from the most basic principles of digital forensics.

Related to this, the ECtHR has established that neither the applicant nor his lawyer had sufficient knowledge of the substance of the Bylock data. In other words, Mr. Akgün was not aware of the variety of evidence underlying the allegation that he had used the Bylock App, and had therefore not been sufficiently and equally empowered to challenge the accusations that were put against him. That means, he was deprived of his right, stemming from the equality of arms and adversarial proceedings, and this led to the violation of Article 5 § 4 of the Convention.

Another finding of the European Court that prompted it to rule against Turkey is 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 Gülen movement for the purposes of internal communication.

Yet another finding of the European Court which merits attention, is 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 the Bylock App as an enjoyment of the right to privacy, as well as of the right to respect for one's private life. According to the Court, the domestic court should have paid attention to the way in which the Bylock App 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, in itself, indicate that there were reasonable grounds for suspicion that could satisfy an objective observer that he had indeed used Bylock in a manner that might amount to the fact that he was a member of a terrorist organisation.

Furthermore, the ECtHR finds the predication of suspicion that is based merely on digital evidence 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. However, where such evidence is the sole or exclusive basis for a 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 worthwhile 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 the exchanged messages via the Bylock App. 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.

4. The problem of equality of arms

In the cases of *Saglam v. Turkey*⁶⁴ and *Yalcinkaya v. Turkey*⁶⁵, both cases pending before the Court, the ECtHR has requested that the Turkish Government explain what the raw data obtained by the MİT involved, and how the MİT 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.

The Court continued "in view of the applicant's allegation that he could not obtain a copy of the Bylock data, was the applicant provided with a real and effective opportunity (i) to have knowledge of and comment on all digital evidence adduced, or of the observations filed by the prosecution in that respect with the domestic courts; (ii) to review all of the material evidence in the possession of the prosecution for or against him/her; and (iii) to challenge the authenticity and reliability of the digital evidence used against him/her and to oppose its use, as required by the principles of equality of arms and adversarial proceedings (see, for instance, *Rook v. Germany*, no. 1586/15, §§ 56-59, 25th July, 2019)? In this connection;

- (i) What information and documents did the applicant have available to him in the case file as proof of his use of Bylock? Was that information available prior to his conviction by the Court of First-Instance, or was some of the material evidence corroborating his use of Bylock added to the file at the appeal stage?
- (ii) Did the domestic legal framework and case-law provide for the right to obtain a copy of the digital data that was in the possession of the prosecution? If so, was it complied with on the facts of the present case? Moreover, is there a right under Turkish law to examine and take a copy of the relevant digital evidence when such evidence forms part of criminal proceedings other than those against the applicant?
- (iii) In this context, did the applicant's alleged inability to review the evidence handed over by the MİT to the prosecuting authorities put the defence at a disadvantage *vis-à-vis* the prosecution? If so, were the alleged difficulties that were caused to the defence sufficiently counterbalanced by the procedures followed by the judicial authorities (see, *mutatis mutandis*, *Rowe and Davis v. the United Kingdom* [GC], no. 28901/95, §-61, ECHR 2000II; *Sigurður Einarsson and Others v. Iceland*, no. 39757/15, §§ 90 and 91, 4th June, 2019; *Rook*, cited above, §§-67 and 72)?

ECtHR's above mentioned, and very to the point questions are mainly related to the principle of equality of arms. Before starting to examine the Turkish courts' way of dealing with Bylock cases, the Turkish Constitutional Court's three precedents, which are very relevant to this problem are worth mentioning. In three separate judgments (*Yavuz Pehlivan and others* [GK], B. No: 2013/2312, *Yankı Bağcıoğlu and others* [GK], B. No: 2014/253, *Sencer Başat and others* [GK], B. No: 2013/7800), the TCC concluded that the defendant should be given an opportunity to conduct a technical examination of the relevant digital materials, otherwise the principle of the equality of arms would be violated:

"In the present case, the evidence which was given as the basis for the crimes for which the Applicants were charged is not evidence that was seized from the Applicants, but digital materials that were seized from third parties, and it has been demonstrated that the judicial authorities did not let the Applicants, who were tried while under detention, examine this evidence and conduct a technical examination of them. ... It is concluded, therefore, that the Applicants did not have sufficient information regarding the content

⁶⁴ ECtHR, <http://hudoc.echr.coe.int/eng?i=001-208741>

⁶⁵ ECtHR, <http://hudoc.echr.coe.int/eng?i=001-208743>

of the digital materials and documents, and did not have the opportunity to conduct a technical examination of the relevant digital materials either, and therefore, the principle of the equality of arms was violated. [Yavuz Pehlivan and others [GK], B. No: 2013/2312, 4/6/2015, § 80]⁶⁶

In the present case, the Applicants were sentenced as a result of relying on the information and documents that were 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, or that their images be submitted, was dismissed. ... the Court delivered its judgment to convict the Applicants by making an assessment that was based on this digital evidence, and the judgment was upheld by the Court of Cassation for the same reasons. ... It is clear that the procedures and methods 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" ... was violated. [Yankı Bağcıoğlu and others [GK], B. No: 2014/253, 9/1/2015, § 74-77]⁶⁷

In terms of the complaints in relation to the evaluation of the digital data, since the fact that the expert reports and expert opinions that the Applicants presented were not accepted by the Court of First Instance, and the dismissal of their requests to have an expert examination undertaken on these issues, by the Court, and with insufficient justifications, were contrary to "the right to a reasoned decision" and to the principle of "equality of arms; the right to a fair trial ... was violated. [Sencer Başat and others [GK], B. No: 2013/7800, 18/6/2014, § 72]"⁶⁸

However, in the Bylock cases, the Turkish courts have denied defendants the possibility of effectively challenging Bylock evidence and, in particular, have dismissed the defense's requests that:

- i) digital data about Bylock should be given to the defense for examination purposes, and/or that
- ii) the Court should commission an independent panel of experts to examine the Bylock data.⁶⁹

In contradiction to its above-mentioned rulings, the TCC have also found no violations in Bylock cases.

Another problematic issue is that the Turkish Courts do not themselves have possession of the Bylock data, so they can only ask the police for this data (partially) in relation to the defendant. The police respond by sending a document, which is called the *Bylock Determination and Evaluation Report*, to the Court. 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.⁷⁰

Under the TCC's precedents, the procedures and methods used by the Turkish courts in Bylock cases are not in compliance with the principle of the equality of arms, and/or do not contain a guarantee that sufficiently protects any applicant's rights to a fair trial.⁷¹

⁶⁶ 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>

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Ibid.

⁷⁰ Ibid.

⁷¹ Ibid.

X. CONCLUSION

In relation to the above-mentioned facts, it can fairly be asserted, without hesitation:

- i. *That there are everchanging figures and criteria on the side of the Turkish authorities around the use of the Bylock App (Section III-IV),*
- ii. *The Turkish authorities claim on the exclusive usage is proven to be wrong (Section V.3),*
- iii. *That there is evidence of delayed and disintegrated forensic authentication of the digital data related to Bylock (Section VII),*
- iv. *That there is poor employment of the basic digital forensic principles, as well as traces of inconsistencies and data manipulation in the official Bylock Technical Report by MIT (Section V-VI-VII)*
- v. *That the digital data / evidence related to the Bylock App has been obtained without the order and oversight of a judicial authority (Section VIII),*
- vi. *That the digital data / evidence that is related to the Bylock App was processed before forensic authentication (under a judge's warrant) (Section VIII.1-5),*
- vii. *That there was illegal use of Bylock related data obtained through administrative investigations in judicial proceedings (Section VIII.7),*
- viii. *That the Bylock related internet traffic metadata was retained for longer than the legally prescribed period (Section VIII.6),*
- ix. *That there is validation and substantiation of many of these findings in the proceedings of supranational mechanisms, such as ECtHR and the UN Human Rights bodies, (Section IX),*

And these make data about Bylock usage at the least unlawfully obtained evidence, and casts the shades of notable doubts in relation to the evidence's integrity, authenticity, reliability, and accuracy, thereby depriving it of qualification as legal evidence.

The unsettled narrative about how Bylock data was acquired, processed and considered, and the shifting claims about the facts relating to the evidence, such as ever-changing criteria and the number of individuals who allegedly used the App; the judicial authorities' decisions that deny the defense the possibility of obtaining and examining Bylock evidence against the defendant, together with the law enforcement agency's warning that the data cannot be the basis for judicial procedures, all create doubts in regard to the fabrication, alteration or corruption of the data.

Furthermore, also, withholding the copy of the digital data/evidence that is related to the Bylock App from both the defendants and their counsel casts a thick and reasonable shadow over the evidence and constitutes the violation of the right to a fair trial.

In conclusion, one can say that Bylock is not lawful and admissible evidence but is a tool of malicious prosecution given to the Turkish Judiciary by the National Intelligence Agency. The only possible remedy for tens of thousands malicious prosecutions would be the quashing of all of the convictions which were even partly based on the Bylock App, and then giving all those who have been so convicted a fair trial where the above-mentioned ECtHR and the UN decisions will be taken into account.