DGI - Directorate General of Human Rights and Rule of Law Department for the Execution of Judgments of the ECHR
67075 Strasbourg Cedex France
E-mail: dgI-execution@coe.int

Cc: President of the Ministers' Deputies
Her Excellency Ragnhildur Arnljótsdóttir
Permanent Representative of Iceland to the Council of Europe
E-mail: ragnhildur.arnljotsdottir@utn.is

Re: Submission by The Italian Federation for Human Rights and The Arrested Lawyers Initiative pursuant to Rule 9.2 of the Committee of Ministers' Rules for the Supervision of the Execution of Judgments, Initial Observations on the Implementation of Akgün v. Türkiye (no. 19699/18) final judgment

I. Introduction

1- In line with Rule 9.2 of the Rules of the Committee of Ministers for the supervision of the execution of judgments and of the terms of friendly settlements, The Italian Federation for Human Rights[1] and the Arrested Lawyers Initiative[2] hereby present this joint communication regarding the execution of the European Court of Human Rights (hereafter "the Court" or "ECtHR") judgment in the case of Akgün v. Türkiye (no. 19699/18).

2- Our communication aims at providing updated relevant information and explanations to the Committee of Ministers concerning the individual and general measures reported by

[1] The Italian Federation for Human Rights - Italian Helsinki Committee (under the acronym, FIDU) is an organization of the Third Sector, i.e. a non-profit civil society organization. FIDU is based in Rome and operates throughout Italy and worldwide; carries out its activities through its national and local bodies, and achieves its goals in compliance with international and EU standards, as well as with the Italian Constitution and laws; it is non-profit-making and pursues civic, solidarity and social utility purposes by carrying out activities of general interest; can join international federations and networks of associations that pursue the same ends with the same methods; it can bring together other associations with a federation pact.

[2] The Arrested Lawyers Initiative (TALI) a Brussels-based rights group consists of lawyers making advocacy to ensure lawyers and human rights defenders perform their duty without fear of intimidation, reprisal and judicial harassment. TALI is a member of the International Observatory for Lawyers.

the Turkish Government for the execution of ECtHR judgment in the case of Akgün v. Türkiye (no. 19699/18).

3- As pointed out below in detail, the action report submitted by the Turkish Government on 13 October 2022 does not provide any meaningful and tangible information directly related to the actions that have been taken or are planned to be taken by the Government in order to prevent the occurrence of similar violations. Moreover, many people are still being detained, arrested and remanded in custody on the basis of Bylock data, which lacks legal and technical credibility.

II. Case Description

4- The case concerns the violation of the right to liberty and security on account of the unlawfulness of the applicant's detention and the lack of reasonable suspicion at the time of his pre-trial detention that he had committed an offence (Article 5 § 1 of the European Convention on Human Rights, hereinafter "the Convention"). The Court also concluded that there had been a violation of Article 5 § 3 with regard to the alleged lack of relevant reasons to justify pre-trial detention in the absence of reasonable grounds for suspecting the applicant; and a violation of Article 5 § 4, since neither the applicant nor his lawyer had had sufficient knowledge of the content of the red list of ByLock users, available exclusively to the prosecution, which had been of crucial importance for challenging the detention in issue.

III. Individual Measures

5- On 11 January 2018 (before the European Court of Human Rights gives its judgment on 20.07.2021), the applicant was released subject to judicial supervision. According to the Action Report, the proceeding against the applicant is still pending before the Ankara 22nd Assize Court.

6- As stated above, first of all the ECtHR found the violation of Article 5 § 1 of the Convention on account of the lack of reasonable suspicion, at the time of the applicant's initial pre-trial detention, that he had committed an offence. Although the applicant has been released, it is understood from the Action Report submitted by the Government that there is a possibility that he may be sentenced for the same offense based on the same evidence and sent to prison. As such, there is a possibility that he may be sent back to prison on the basis of a conviction on a matter which is clearly recognized by the ECHR that there is no reasonable doubt, which is legally unjustifiable.

IV. Importance of the case

7- The Turkish government often states that in order to be convicted for membership in an armed terrorist organization; the Court of Cassation adopted a criteria of *'continuity, diversity and intensity'* and *'participation within the "hierarchical structure" knowingly and willfully'*.[3]

8- The Plenary of Criminal Chambers of the Court of Cassation ruled on 26.09.2017, that: *"Since the Bylock messaging app is a communication network, exclusively designed and developed to fulfil the communication needs of the FETÖ terrorist organisation, the detection, through technical means, of the involvement of any individual within this network proves, beyond any doubt, the link between the individual and the terrorist*

[3] Ibid.

organisation." and "… the content of the correspondence circulated within the Bylock network is irrelevant in this regard."[4] [5]

9- With regard to Bylock, the Court of Cassation held that if someone is Bylock user, he/she shall be convicted regardless of whether the criteria of "continuity, diversity and intensity" is met "However, the perpetrators of crimes that can only be committed by members of the organization, even if they do not have the characteristics of continuity, diversity and intensity in terms of their nature, the way they are committed, the gravity of the damage and danger caused, and their contribution to the purpose and interests of the organization, should also be accepted as members of the organization." (3rd Criminal Chamber of the Court of Cassation E. 2021/2112, 16th Criminal Chamber of of the Court of Cassation E. 2019/2397)

V. General Measures

10- The Turkish Government, in its Action Report, have provided information on the evidentiary role of the Bylock application, on the judicial practice concerning the examination of the Bylock evidence and on other measures taken and envisaged with a view to further safeguard the right to liberty and security in its general context.

11- In the Action Report submitted by the Government, it was stated that the Bylock application was exclusively used by the members of the FETO/PDY organization, and this was supported by a large number of judicial decisions and expert reports (Action Report, §14).

12- In this sense, all courts in Turkey can convict people on the grounds of using the Bylock app, citing the April 24, 2017, decision of the 16th Criminal Chamber of the Court of Cassation, which was upheld by the Plenary Criminal Chambers of Court of Cassation on September 26, 2017. The use or download of the Bylock application is still seen as evidence of membership of the Gulen movement.[6] But the information given by the Government does not correspond to the real situation.

13- It is a very clear fact that the Bylock application had not been exclusively used by a particular group. Below, we will explain the reasons why the government's claim on the use of Block exclusively by a group is not true and baseless.

14- First of all, we would like to draw the Committee of Minister's attention to the fact that the Bylock was put into use on 3 December 2013. It was a messaging and voice calling application, which could be downloaded from Google Play[7] until 3 April 2016 and from Apple Store until 7 September 2014, whose updated versions has remained in use until the first months of 2016,[8] which, during the period of its use, has been downloaded and used by a total of at least six hundred thousand (600,000) people, including five hundred thousand from Google Play and one hundred thousand from the Apple Store.

15- Similar statements can be found in the Technical Report prepared by the MİT (Turkey's Intelligence Organization). According to the Technical Report, Bylock had 215,092 users and was downloaded mainly in Turkey, Saudi-Arabia and Iran.[9] In this context, According to AppAnnie report, Bylock was ranked top 100 in 12 countries and top 500 in 47 countries among social media tools in App Store between the dates of May-Sep 2014. In the period of June 2014-December 2015, it was ranked top 100 in 5 countries and top 500 in 41 countries among different categories in Google Play. When looking at the list

[4] Court of Cassation, E. 2017/16-956, K. 2017/370.

[5] The Constitutional Court endorses the conclusion of the Court of Cassation without any further inquiry. (Ferhat Kara, B. No: 2018/15231).

[6] https://www.memurlar.net/haber/1057902/bylock-kullanan-5-feto-uyesinden-4-u-tutuklandi.html
[7] https://www.appbrain.com/app/bylock%3a-secure-chat-talk/net.client.by.lock
[8] https://www.appannie.com/apps/ios/app/bylock/app-ranking/#type=best-ranks
[9] MIT Technical Report, p.15

carefully it is seen that there are African countries such as Tanzania and Madagascar, European countries such as Romania and Belgium, Asian countries such as Turkmenistan and Uzbekistan, American countries such as Venezuela and Panama; shortly, it was used in many countries from all corners of the world. Those ranks are set by using the number of app downloaded from App Store in related country. Thereby, Bylock is popular due to download numbers and times across countries.

16- On the other hand, David Keynes, the licensee of the application in question, gave testimonies in the case that he had instituted to claim damages in the lawsuit against Turkey in the USA on account of the seizure of Bylock, contrary to his statements featured in the government's opinion. He also stated that ByLock had been a free messaging app that anyone could download from the Google Play app stores and that his aim had been to develop an application with a view to selling it to techno companies in Silicon Valley. He also stressed that Bylock had end-to-end encryption just like other most frequently used messaging apps. (Annex 1)

17- In the testimony he gave in Turkey, Keynes said, "I am seemingly the licensee of the program, but you can think of me as Mehmet as a tea-maker in a company. I didn't use it and I don't know about whether other people outside the Gülen Group used it". However, in the lawsuit he filed in the USA, he had stated that he had financed the application completely. As is understood, the claim that Bylock is exclusively used by a certain group has been denied by the licensee himself.

18- In the third-party opinion (Annex 2) submitted by the Italian Federation for Human Rights to the case of Saglam v Turkey, wrongness of this so-called exclusivity claim was explained in detail:

> **50. International Reports:** Three separate digital forensic reports, by Fox IT, Jason Frankovitz and Thomas Kevin Moore, have established the 'exclusivity claim' to be factually incorrect. (**Annex 3, 4, and 5**). These verifiable reports, attached to this submission, are commended to the Court and 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.'
>
> "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 installation 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."
>
> "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.'

19- Similarly, Digital Forensics Experts T. Koray PEKSAYAR and Dr. Levent MAZILIGÜNEY prepared the Expert Opinion titled "Evaluation of the Argument that the Bylock Application has been Used Exclusively" and published on 1 September 2021 (Annex 6 -7)

20- At the end of that Expert Opinion (p. 7), the experts concluded that "there is no widely used mobile communication application that does not use encryption. If a communication application is encrypted, this does not prove that the application in question is for exclusive use. It was possible to use the ByLock application by downloading it from mobile app stores during the period when it was available on mobile app stores. Any reference from any third party was not needed to download and use the ByLock

application (other than the user and the application). There was no obstacle or restriction to users' downloading and using the ByLock application from mobile app stores. A portion of the matters cited as proof of exclusiveness of the ByLock application stems from the preferences of application developers or admins. It is possible to find numerous communication applications having similar features. If several or all features specified are found in a communication application, this does not prove beyond reasonable doubt from a technical perspective that the application in question is for exclusive use. It is considered that an application that can be downloaded, installed and used from mobile app stores and that can be used without a third party's reference cannot be for exclusive use".

21- For these reasons, the statement "exclusively used by the members of the FETO/PDY organization" in the action report submitted by the Government does not reflect the truth. Of course, the issue of "courts" making the determination of "exclusively used by the members of the FETO/PDY organization" is also important.

22- *The government's Action Report stated that the domestic courts had established a well-established case law (See §11).* This information submitted to the Committee of Ministers is however incorrect. Because in order to speak of "a well-established case law" there must be an independent and impartial judiciary. It should also be emphasised that this "established case-law", as expressed by the Turkish authorities, has been condemned by the Court as a violation of the Convention in the case of Akgün v. Türkiye (no. 19699/18)

23- The Council of Judges and Prosecutors ('HSK') which is under control of the executive branch has been exerting pressure on the judges not to question exclusivity claim and reliability of Bylock data. According to the 16th Criminal Chamber of the Court of Cassation, ByLock data and its content was accessed and evaluated for the first time after the Ankara 4th Criminal peace judgeship decision rendered on 9 December 2016. However, Vice President of the Supreme Council of Judges and Public Prosecutors (HSYK, transformed into HSK in 2017) Mehmet Yılmaz announced on 6 October 2016 that "Bylock is the software of the organization and our most important evidence; It is clear that ByLock is a program that cannot be used by people other than members of the organization". Before the data was examined and it was not determined who used the application, and when the content of the messages and emails were unknown, vice president of the HSYK declared that it was exclusively used by Gülenists and the data were the strongest evidence. The HSK (then HSYK) is an administrative body supervising the judges and prosecutors of the first and second instance courts and declarations of its vice-president have huge influence on the judges. Assessment of evidence is a judicial function and exclusively belongs to the judges; administrative bodies such as HSK do not have any competence to assess evidence. Declaration of ByLock as the strongest evidence of membership to a terrorist organization by the Vice-President of the Council of Judges and Public Prosecutors may constitute an instruction for the judges and courts and it is completely in contradiction with the independence of judiciary.

24- In addition, the members of the judiciary who granted the defendant's requests to probe into Bylock data by observing the principle of equality of arms were punished in ways such as being assigned to another place and stripping of their titles or starting a disciplinary investigation against them. This scheme causes a chilling effect within the judiciary:

A) Antalya Regional Appeal Court of Justice, 2nd Penal Chamber reversed an aggravated imprisonment sentence for six years and three months pronounced by the Assize court in Denizli on 4 April 2017 on the grounds that the investigation into ByLock application was insufficient. On 26 April 2017, Şenol Demir, the Chief Justice of the Antalya Regional Court of Justice, 2nd Criminal Chamber was vilified by pro-

government daily Yeni Asır because of his decision. [10] On 8 May 2017, Judge Demir was assigned by the HSK to Konya as a judge of the first instance after only 9 months and 18 days serving as judge of second instance court. [11] Judges of the second instance normally have a term of at least four years.

B) A similar incident occurred at the Regional Appeal Court of Justice in Gaziantep. The Adana 11th Assize Court convicted a deputy police chief on 20 January 2017 for being a member of a terrorist organization on the grounds that he 'used the ByLock App, sent his son to Işık Preparatory School between 2013 and 2015 and had an account in Bank Asya'. The Gaziantep Regional Appeal Court of Justice, 3rd Criminal Chamber reversed this decision with a majority vote on 20 April 2017 holding that, 'a conviction for membership to a terrorist organization cannot be based on Bylock records, the contents of which are not known' was unlawful (2017/286E – 2017/573K). After this reversal, the Chief Justice of the 3rd Criminal Chamber Zafer Yarar was assigned by the HSK to the Kayseri Province on 26 May 2017 as a judge of the first instance. Mustafa Tosun, a member of the 3rd Criminal Chamber who voted with the chief justice, was assigned with the same HSK decree to Istanbul as a judge of the first instance. Bayram Korkmaz, the member who voted against the reversal of the conviction, was promoted to chief justice of the 3rd Criminal Chamber. [12]

C) During a hearing held on 1 February 2017 in Kırşehir Assize Court, Chief Judge Fatih Mehmet Aksoy, in regard to 39 detained suspects who were pending trial without any shred of evidence, blurted out, "I cannot bear it anymore; I will set all of them free." Upon hearing this remark, the case prosecutor threatened the Chief Judge: "If you do that, I will have you arrested in two hours for using ByLock". [13] Under the initiative of the Police Chief of Kırşehir Province, Veysel Murat Tuğrul, who had been observing the court proceedings, the judge was suspended in less than two hours on the allegation that he used ByLock.[14] This incident demonstrates how the judicial independence is usurped and how vulnerable the judges are. It also shows how a judge can be unseated during an ongoing hearing from his office by a mere telephone call made by the police chief to the Capital, which shatters any notion of inremovability of judges and of judicial independence. As for Chief Judge Fatih Mehmet Aksoy, he was detained later that afternoon on charge of using ByLock[15] and was then arrested. [16] He was then suspended on 2 February 2017 on the grounds of using ByLock, and it was not until 31 December 2017 that he was reinstated after having been ascertained that he was not a ByLock user. [17]

25- Another issue particularly emphasised in the "Akgun case" is that it is also important for the judge to have sufficient information in terms of electronic evidence, and only in this way can the judge determine the authenticity, accuracy and integrity of the evidence. In other words, the court emphasized the authenticity, accuracy and integrity of the evidence collected within the scope of ByLock, taking into account the sensitive place of electronic evidence in criminal procedure law. As a matter of fact, it has been observed in many cases how important it is for the evidence to have these qualities. This is because there is inconsistent information even in the ByLock usage contents presented in these cases. In particular, the inconsistencies between the reports from MİT and BTK (Information

[10] http://www.yeniasir.com.tr/sürmanşet/2017/04/26/hakimden-skandal-bylockkarari
[11] https://twitter.com/aliaktas7/status/862022086059077635
http://www.adaletbiz.com/m/ceza-hukuku/bylock-kararina-bozma-h148726.html
[12] https://odatv.com/bylocktan-verilen-mahkumiyet-kararini-bozan-o-hakimler-suruldu-2705171200.html
[13] *ByLock* is a smart phone application allegedly invented and used by the members of the Gülen Movement. For more information see http://www.platformpj.org/opinionarbitrary-use-bylock-instrument-false-accusation/
[14] https://www.cnnturk.com/turkiye/fetoculeri-yargiladigi-sirada-fetoden-aciga-alindi
[15] https://www.haberturk.com/gundem/haber/1376040-hakim-fetoculeri-yargilarken-aciga-alindi
[16] http://www.kirsehirhaberturk.com/agir-ceza-mahkemesi-baskani-tutuklandi.html
[17] https://www.yenisafak.com/gundem/o-hakim-de-mor-beyin-magduru-2940916

Technologies Agency) are well known to everyone. The unlawfulness of sentencing on the basis of evidence accepted without any questioning despite the obvious inconsistencies is also seen in the Court's judgement. In addition to the need for the judge to be well-informed, the Court also requested that the digital data to be used as evidence be scrutinized for authenticity, accuracy and completeness. However, the picture that emerged during the proceedings in domestic law indicates that the opposite was the case[18].

26- Taking all these points into account, it is not possible to say that there is a well-established case law on the Bylock application, since there is no independent and impartial judiciary in Turkey. In fact, the domestic courts' "a well-established case law" is in direct conflict with the judgments of the European Court of Human Rights.

27- ***In the Action Report submitted by the Turkish authorities, it is stated that case law developments and other evidence related to the Bylock Application are available to all judicial bodies.*** **This information also does not reflect the truth.**

a) Generally, the Turkish police and judicial authorities exclusively rely on the findings of the Turkish National Intelligence Agency (MİT) in relation to investigations and prosecutions concerning Bylock, relying upon MİT's report 'A Technical Report on the Bylock Application'. FOX IT, a Netherlands-based, leading digital forensic company, however, concluded that:

"Fox-IT encountered inconsistencies in the MİT report that indicate the manipulation of results and/or screenshots by MİT. 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 MİT (and to what end). This raises questions as to what part of the information available to MİT 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 MİT 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 led 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 MİT report very low, especially when weighed against the consequences of the conclusions**."[19]

b) Likewise, an expert report prepared (Appendix:8) by two Turkish digital forensic experts KORAY Peksayar and Levent Mazılıgüney, concluded that; (i) Data obtained by MIT from ByLock's server is corrupted; (ii) Understanding the reason for 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 parties in the criminal case: (iii) Corrupted digital data cannot provide acceptable, admissible evidence for criminal cases.[20]

c) **Issues of admissibility stemming through non-compliance with procedural rules**: There are also several serious procedural defects in the obtaining of Bylock data, such that they are inadmissible in criminal proceedings.

[18] Yasir Gökçe, "The Bylock fallacy: An In-depth Analysis of the Bylock Investigations in Turkey", Digital Investigation, n°26, September 2018, pp. 81-91

[19] Expert Witness Report on Bylock Investigation by Fox IT (Appendix 5).

[20] Expert Opinion on the Accuracy and Reliability of the Digital Data Obtained from the Bylock Server in Lithuania (Appendix 8).

d) Procedural requirements for the obtaining / gathering, processing and examination of digital data stipulated in the Criminal Procedure Law (CMK – No:5271). 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 prosecution) as evidence; the digital data obtained from suspects (or defendants) must be collected in accordance with the technical requirements that are set by the law and must be submitted to the judicial authorities in a complete, 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 safe confiscation and examination to leave the original media to 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."[21]

e) **Application of the requirements explained above to the way that Bylock data obtained and processed:** In its press statement dated 06th April 2017 MİT stated that all of the findings about the Bylock and the raw data compiled through intelligence initiatives were shared with judicial, security and other authorities in May, 2016. [22] Likewise, a Turkish government official, who spoke to Agence France-Presse said MİT began decrypting messages sent on Bylock in May, 2016.[23] 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 15 [2016].*"[24]

f) In September, 2016, Faruk Özlü, the then Minister of Science and Technology, said that there were 215,000 Bylock users[25] and on 6th October 2016, Veysi Kaynak, then Deputy Prime Minister, said that 18 million messages had been obtained and that the process of decrypting each and every one of these messages was underway.[26] Further, it was reported on 11th November 2016 that an indictment presented by the Izmir Prosecutor Ayhan Yilmaz to the Izmir 13th Heavy Penal Court, stated that MİT had already decrypted 17 million out of 18 million text messages, plus 2.5 million out of 3,5 million e-mails.[27]

g) **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.[28]** This order explicitly mentioned that a hard disk and a USB stick containing digital data on Bylock were passed to the Ankara Chief Public Prosecutor's

[21] 16th Chamber of the Turkish Court of Cassation, 21.04.2016, 2015/4672 E., 2016/2330 K
[22] Press Statement of MİT, https://www.mit.gov.tr/basin60.html
https://www.cumhuriyet.com.tr/haber/mitin-Bylock-celiskisi-717302
https://www.bbc.com/turkce/haberler-dunya-39513263
[23] https://www.middleeasteye.net/news/turkey-tracked-thousands-Gülenists-encrypted-messages
[24] Ankara Başsavcılığı kaynakları, "O tarihte bize MİT'ten Bylock kayıtları gönderilmedi. Biz Bylock'u 15 Temmuz'dan sonra öğrendik" dedi.
https://www.cumhuriyet.com.tr/haber/mitin-Bylock-celiskisi-717302
[25] Faruk Özlü: ByLock'u TÜBİTAK'taki FETÖ'cüler geliştirdi (Habertürk),
https://www.haberturk.com/ekonomi/teknoloji/haber/1294035-faruk-ozlu-by-locku-tubitaktaki-fetoculer-gelistirdi
[26] Bakan Veysi Kaynak: '18 milyon ByLock mesaj var, tek tek inceleniyor' (Yeniçag),
https://www.yenicaggazetesi.com.tr/bakan-veysi-kaynak-18-milyon-Bylock-mesaj-var-tek-tek-inceleniyor-147602h.htm
[27] 'ByLock' FETÖ'ye üyelikte belirleyici kabul edildi
https://www.aa.com.tr/tr/15-temmuz-darbe-girisimi/bylock-fetoye-uyelikte-belirleyici-kabul-edildi/682560
[28] Ankara 4th Criminal Peace Judgeship, 9/12/2016, 2016/6774.

Office and, on 9th December 2016, the Ankara Chief Public Prosecutor's Office asked for an order to authenticate the digital data and subsequently examine these devices.

h) The statement of the Deputy PM and the indictment of the Izmir Prosecutor together provide a strong inference that data from Bylock had been examined and processed by MİT a long time *before* it was passed to judicial authorities, as the date of first judicial order to authenticate (digital image taking) digital Bylock data was 9th December 2016.[29]
i) In accordance with procedure (as outlined above), MİT should have immediately passed this data and these devices to the judiciary as they were, *without delay* so as to enable the latter to carry out the first authentication/image taking process under the ambit of a judicial order and then carry out an examination under the Code of Criminal Procedure. MİT does not have any authority to examine and process it. Given concerns about the corruption of the data, this defect is serious rather than technical one.
j) The processing of the data by MİT without judicial oversight**,** and its consequent late delivery to the authorities, raise serious questions as to the integrity and authenticity of Bylock evidence. Likewise, another serious issue concerning the integrity of Bylock evidence is the disintegration of the digital evidence and the conducting of the forensic examination (forensic image taking) as two separate processes took place on two separate dates, 9th December, 2016, and 24th March, 2017. (Annex 9)
k) Indeed, another hard disk was passed by the MİT to the Ankara Chief Public Prosecutors and, subsequently, a separate image taking and forensic examination authorisation order was given on 24/3/2017.[30] It shows MİT did not preserve the integrity of the digital data, divided it into the parts and passed to the judicial authorities in two parts, one in December, 2016 and the latter in March 2017.
l) 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 Court the principle of the requirement for equality of arms.
m) **The Turkish Constitutional Court's (TCC) inconsistent rulings in Bylock cases**: In Bylock cases, including the Applicant's, the Turkish courts have denied defendants the possibility of effectively challenging Bylock evidence and, in particular, have dismissed defence requests that i) digital data about Bylock should be given to the defense for examination purposes and/or ii) that the Court should commission an independent panel of experts to examine the Bylock data.
n) Another problematic issue is the Courts do not themselves have possession of the Bylock data, so they can only ask for the police for this data (partially) in relation to defendant. The police respond by sending a document, which is called the *Bylock Determination and Evaluation Report*, to the Court. This documents often include a disclaimer to the effect that the police's involvement is solely limited to the printing out of the response from the Bylock database module, for which the police do not accept any liability. ()

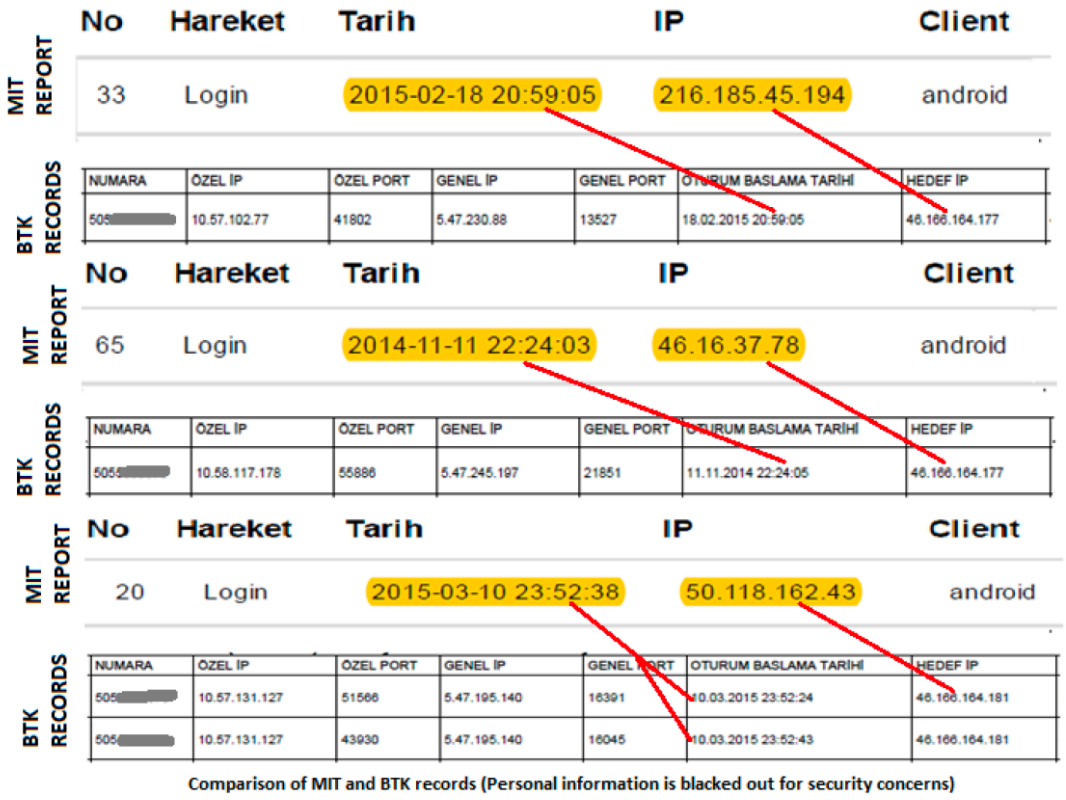
28- What is so-called "***other evidence related to the Bylock Application are available to all judicial bodies"?***

a) It is simply internet traffic data that the Court obtains from BTK (Information Technologies Agency) which is public entity.
b) These data are however often inconsistent and does not have safeguards as to ensure its reliability. (Image below is from the report at Annex 8)

[29] Ibid.
[30] Ankara 5th Criminal Peace Judgeship, 24/3/2017, 2017/2056.

4. Discrepancies between the records from MİT and BTK

Apart from the official Bylock Technical Report, MİT 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 MİT 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 MİT 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 İP	ÖZEL PORT	GENEL İP	GENEL PORT	OTURUM BASLAMA TARİHİ	HEDEF İP
505[redacted]	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 İP	ÖZEL PORT	GENEL İP	GENEL PORT	OTURUM BASLAMA TARİHİ	HEDEF İP
505[redacted]	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 İP	ÖZEL PORT	GENEL İP	GENEL PORT	OTURUM BASLAMA TARİHİ	HEDEF İP
505[redacted]	10.57.131.127	51566	5.47.195.140	16391	10.03.2015 23:52:24	46.166.164.181
505[redacted]	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)

VI. Recommendations to Committee of Ministers on individual and general measures

29- Consequently, the Action Report submitted by the Turkish Government in reply to the ECtHR's Akgun case demonstrates that the necessary measures have not been taken to abide by the judgment, except the payment of just satisfaction awarded.

30- No action plan was prepared for the elimination of the practices that led to the European Court of Human Rights judgement of violation in Akgun v. Turkey. Instead, an action report was prepared claiming that all violations cited by the European Court of Human Rights had been eliminated.

31- The points made by the Government in the Action Report do not reflect the reality as stated above. It is also a clear indication of the Government's lack of political will, any plan or project for the proper implementation of the said judgment of the Court. Indeed, it is a clear indication of this that the higher courts, including the Constitutional Court, have never referred to the Akgun v. Turkey judgment in their judgments. Contrary to the findings of the European Court of Human Rights, many people are still being detained and arrested on the grounds of Bylock Application.

32- First of all, the submitters kindly invite the Council of Ministers to examine the implementation of the Akgün v. Turkey judgment under debated meetings and keep the monitoring of this case in the agenda of every DH meeting and request to consider the following recommendations:

a) Monitor the applicant's proceedings, which is currently (According to the Action Report) pending before the Ankara 22nd Aggravated Criminal Court,
b) Ask whether domestic courts have access to all data and evidence related to the Bylock application, including Bylock digital data, as stated in the Government's Action Report,
c) Amend broad and vaguely worded articles of the Turkish Penal Code and the Law No. 3713 on Prevention of Terrorism such as “being member of an armed terrorist organization” and other offenses categorized as “crimes against the state” to meet the requirements of the principle of no punishment without law, to make them precisely defined and foreseeable and, where relevant, explicitly linked to the commission of violent acts,
d) Ensure the criminal law is strictly applied and restrictively interpreted particularly in ‘crimes against state’ cases,
e) Monitor all court decisions ordering detention and prosecutors’ request for detention to ensure that they rest on sufficient facts establishing the existence of reasonable suspicion of criminal activity and that detention is a measure of last resort not pursued for ulterior purposes,
f) Emphasize that it is imperative that government and state officials, including those occupying high office, desist from all forms of interference in the administration of justice in order to uphold the independence of the judiciary and the impartiality of judicial decision making,
g) Take measures to uphold the independence of the judiciary by introducing constitutional amendments, reversing those passed in April 2017, to reform the Council of Judges and Prosecutors to establish it as a body structurally independent of the executive whose decisions are open to full judicial review.

Sincerely submitted for your consideration

On behalf of the co-submitters

Italian Federation for Human Rights