HRD
Human
Rights
Defender

WHAT IS ByLock?

V3.0

1. WHAT IS "BYLOCK" ?

A – Bylock is a Messenger application which existed in virtual stores like Google Play and ITUNES between December 2013 and April 2016.

This application was active in Apple store between April 2014 and September 2014[1] and was active in Google Play store between 11th April 2014 and 3rd April 2016.[2] The communication service is provided by end-to-end encryption as it is provided in other messenger applications such as WhatsApp. No reference or confirmation is needed to register to the application. This application which is open for everyone can be initiated by adding other people (just like in Yandex Mail). It is clearly understood that Bylock was active in Google Play Store in July 2014,[3] the last entry for the Bylock in Google Play Store was in 22nd March 2015 and it was downloaded by approximately 500.000 people.[4] All the rights concerning ByLock belongs to a person named David Keynes. Another evidence that shows that Bylock is an application that was launched in Google Play Store and Apple store is the interview with David Keynes made by Ismail Saymaz from the newspaper "Hurriyet". In the interview, it is emphasized that the application was downloaded approximately 500.000 times in Google Play Store and 100.000 times in Apple Store. [5] The fact that the application "ByLock" was downloaded 500.000 times from the website (https://downloadatoz.com/) verifies David Keynes' words.[6] According to David Keynes, the users are generally from Turkey, Saudi Arabia and Iran.

B – The Information Regarding This Issue in the Report of the Tech Specialist, Daniel Walter

"It is understood from the AppAnnie data that ByLock application was among the first 100 applications in 12 countries and among the first 500 in 47 countries in Social Networking area in Apple store. It was also among the first 100 applications in 5 countries and was among the first 500 applications in 41 countries."[7] " Today, many firms and applications started to use end-to-end encryption technology. Whatsapp, Viber, Facetime, iMessage, KakaoTalk, Blackberry Messenger, Line, Ipgmail, Jitsi, Privatoria, Mailvelope, Adium, Pidgin, Retroshare, Signal, Wickr, Threema, Ceerus, Pryvate, Cyphr, Cyber Dust, Telegram, Nxtty, Silent Phone, Silent Text, Textsecure, Confide, Bleep, Surespot, Sicher, Clipchat, Chatsecure, Tigertext, AMD Secure Chat, AMES Messenger, Babble Messenger, Biocoded, Chat Bots,

---

[1] www.appannie.com/apps/ios/app/bylock/app-ranking/#type=best-ranks

[2] www.appbrain.com/app/bylock%3A-secure-chat-talk/net.client.by.lock

[3] web.archive.org/web/20140818062556/https://play.google.com/store/apps/details?id=net.client.by.lock

[4] web.archive.org/web/20150322201135/https://play.google.com/store/apps/details?id=net.client.by.lock

[5] www.hurriyet.com.tr/iste-by-lock-david-keynes-40257030

[6] m.downloadatoz.com/bylock-secure-chat-talk/net.client.by.lock/

[7] www.bylockreality.com/index.php/technical-reports/an-independent-technical-report-by-daniel-walter-about-bylock-application /

Chiffy Messenger, Confide, Cryptox, Hoccer, Imperium Messenger, Schmoose, SecEms, Secure MMX, Sicher, Squre Messenger, İCrypt, V Pal Messenger, Vigilant Secure, Cashew Messenger, Cellcrypt, Chatsecure, Nod CoCo, GData, Onechat Messenger, Rokacom, SIMSme, Snap Messenger, Wakachat, Sumrando, Wire etc. are among the applications that use end-to-end encryption technology."

"Shortly, if someone uses a communication application in his mobile phone or computer, it means that he is using an encrypted communication application regardless of his expectations and wants. Some of these applications have a strong encryption, some of them do not. Because of the users' expectations and technological possibilities, all the communication applications became encrypted. Under these conditions, the term "encrypted communication application" which is constantly emphasized and used to describe Bylock doesn't mean anything but the term "automobile with steering."[1]

2. THE MYSTERY OF NATIONAL INTELLIGENCE AGENCY OF CAPTURING THE SERVER OF BYLOCK

As the details will be examined further, there is no clear information regarding how the Bylock data was acquired. In the official court reports, it is noted that the National Intelligence Agency acquired/bought them by using "unique techniques".

Official Statements

A. In the Technical Report of NIA about Bylock, it is said that "The data is acquired by using tools, techniques and practices that are unique for the Agency."[2]

B. It is noted in the justification of the verdict of conviction that was given by 15th Heavy Penal Court of Ankara for the 2017/13 , 2017/21 Bylock case that the NIA has bought the Bylock servers. The concerned parts of the verdict states: "It is clear that the server of the application, the data on the servers of Bylock and IP addresses are bought, various data is acquired such as the content of the mail addresses and the technical analysis report and digital materials are sent to the Public Prosecutor of Ankara and General Directorate Of Security by using "unique techniques" and intelligence tools and services by the National Intelligence Agency." [3]

C. Penal Department No. 9 Of The Supreme Court's verdict no. 2015/3 E. 2017/3 also states that the data was bought: "It is clear that the server of the application, the

[1] www.bylockreality.com/index.php/technical-reports/an-independent-technical-report-by-daniel-walter-about-bylock-application

[2] Technical Report of NIA about Bylock, 3.1 Basis and Technique, page: 12

[3] www.adaletbiz.com/m/ceza-hukuku/mit-bylock-server-ini-satin-almis-h168456.html

data on the servers of Bylock and IP addresses are bought, various data is acquired such as the content of the mail addresses and the technical analysis report and digital materials are sent to the Public Prosecutor of Ankara and General Directorate Of Security by using "unique techniques" and intelligence tools and services by the National Intelligence Agency." [1]

D. In the investigation reports against the Baltic Server in Lithuania, it is stated that the personal information of users on Bylock servers were stolen by another user after the usage of application is over.

News in the Media

A. The Department of Cybersecurity of Police Department demanded the previously used mobile accounts and IP addresses that are used after 14.08.2014 from all the Internet service providers (Avea, Turkcell, Vodafone, TTnet). The IP's were examined one-by-one and the IP's that connected to the Bylock services were determined. By these detections, it is determined that the users of those IP's used Bylock.

As it can be seen in the article "Police Department denied the NIA" in the website Ozguruz.org, the Turkish Police Department and National Intelligence Agency denied each other regarding the techniques used in capturing the Bylock data. "Whereas the NIA stated in the report of 88 pages that the server in Lithuania was hacked and the message histories were captured."[2]

B. In a news report in the Newspaper "Aydınlık", it is stated that "the NIA sent its operatives to Lithuania after they found out that the servers are stored in Lithuania. They contacted with the administrators of the firm and demanded a copy of the database. They refused this request. Afterwards, some time before the coup attempt in 15th of July, the NIA paid 13 million dollars and bought the firm."

C. In a news report in the newspaper "Sözcü" which is literally a public speaker for the government, it is said that the data was acquired by a team which secretly infiltrated to the server building in Lithuania. "The team which flew to the Lithuania with a private jet firstly observed the main server building in Vilnius. After the necessary arrangements are made in a week, the infiltration operation was undertaken two months ago. The team which quietly entered the server room broke the code thanks to the technological equipment they brought."[3]

D. In the book (Fetö'nün Dijital "İni" ByLock'a Böyle Girildi: Kod Adı Baybay' , *This Is How They Entered The Digital "Lair" Of Feto: Operation Baybay In English*) which was

[1] selihandiclesimsek.av.tr/tag/yargitay-16-ceza-dairesi-bylock-karari/

[2] ozguruz.org/tr/2017/06/05/emniyet-miti-yalanladi/

[3] www.sabah.com.tr/gundem/2017/01/30/son-dakika-haberi-bylockun-ana-serveri-ele-gecirildi

published by a firm that is known to have ties with the government, it is told that the server was breached "somehow" , 18 million messages were copied and after the server found this out, the security breach was repaired.[1] As it can be observed in the official statements and news reports, the techniques which NIA used while capturing the Bylock data can be the following:

a. By getting the data from the service operators (Vodafone, Turkcell, Avea)

b. By purchasing the Baltic Server in Lithuania

c. By hacking the personal user data of Bylock

d. By infiltrating and stealing the server data in Lithuania by a specially assigned team

e. By purchasing the firm of Baltic Server by National Intelligence Agency

Although there are many speculations about how the Agency captured the personal user data of Bylock, the truth is unknown.

3. THE STATEMENTS OF THE LITHUANIAN GOVERNMENT AND CHERRY-SERVER IN WHICH BYLOCK OPERATED

A. The applications that were made to the Baltic Server firm by the people whose names are on the illegitimate lists mentioned above were responded as following:

" Chery Servers is a Bare-Metal servers provider, which means that we do not manage servers, we do not monitor their incoming/outgoing traffic, nor we store such data. Our clients are solely responsible for their server security and, unfortunately, we would not be surprised if someone has broken into one of our client's servers, as cybercrime attempts are not uncommon these days. What concerns personal information, we do not collaborate with third party institutions, nor we can reveal any kind of information associated with our clients to such institutions. As our company is registered in Lithuania, we are only accountable to local law enforcement agencies in Lithuania and can only reveal information to them when obliged to do so by local law or when a Lithuanian court order is received.

Public Relations, Mantas Levinas "

Also, some of the victims went for a court to the Baltic Server firm in Lithuania. In the case in 19.06.2017, Vilnius City District Court (Prosecutor Regimantas Zukauskas) made the following verdict:

[1] Kod Adı Baybay; Turkuvaz Publishing, İstanbul, July 2017

The company does not have possession of the data about possibly completed unauthorized (illegal) actions in the above-mentioned server. UAB "Cherry servers" provided the data, following the order of art. 97 of CPC of the Republic of Lithuania, that their client John Dash was using the IP address 46.166.164.181 from 08.08.2014. He was the first to start using this IP address in their system; he used it until 02.03.2016. During registration he indicated his contact (telephone) data in the USA, the country of registration – Germany. All the logins to the self-service system of UAB "Cherry servers" were performed via the IP addresses of the providers of the services of the Internet in Germany, the USA, Great Britain, Turkey, Honk Kong, Panama, France, the Netherlands, Norway, Australia. From 10.03.2016 to 27.09.2016 Claudia R Martins was using the service of the web hosting of the dedicated service. She is not the client due to the false payments for the services. During registration she indicated contact in Brazil. She performed logins to the self-service system on the 10th and 11th March 2016 via the IP address 158.69.127.69, which is administered by the USA company OVH Hosting, Inc. The company does not have possession of the data about logins directly to the server and actions completed in it. This data is recorded in the files in the server itself, and when the client stops using the services and having cleaned the server, the data remains. Considering the circumstances indicated and the fact that following the provisions of part 2 of art. 65, part 6 of art. 66 of the law on Electronic Communications of the Republic of Lithuania, the data of electronic communications is stored for 6 months from the date of communications, it is to be stated that at the moment there is no possibility to receive objective data about the illegal logins, having possibly occurred, to the servers of UAB "Cherry servers" rented by the app ByLock in 2016 (i. e. more than 6 months ago), as well as the taking over and use of the non-public electronic data in them and in this way to confirm or deny the statements of the complaint that the National Intelligence Organization of Turkey received the data of the users of the app ByLock (also including the Claimant's) namely in the way and under the circumstances indicated by the claimant (possibly illegally hacking the server rented by UAB "Cherry servers", having forged the data of the client of UAB "Cherry servers" and having applied due to the providing of new access (password) or with UAB "Cherry servers" itself revealing this data).

After the collective arrests and persecution for the communication app Bylock whose servers are in Lithuania, some Human Rights Organizations examined the topic and applied to the parliament. Lithuanian Parliament examined the issue in closed session with the Law and Order of Law Committee and the Head of the Committee, Julius Sabatauskas, announced the information below officially in 19.10.2017:

"The Committee has been informed that state authorities(Ministry of Justice, Ministry of Foreign Affairs, General Prosecutor's Office, State Security Department ,Police Department) did not receive request for legal assistance from Turkish Authorities concerning the matters specified in application.[1]

[1] www.15min.lt/naujiena/aktualu/lietuva/seimo-komitetas-aiskinasi-ar-lietuva-galejo-turkijai-perduoti-bylock-vartotoju-duomenis-56-868536

It is understood from above that plenty of scenarios were created to make the Bylock records which are obtained illegally and against the domestic and International law look like lawful in Turkey and even the courts have no information regarding how the records were obtained.

4. BYLOCK IN INTERNATIONAL REPORTS

In the detailed report written by FOX-IT regarding the NIA report which is thought to be written by the information that was acquired via hacking/purchasing/stealing, it is emphasized that the information that is acquired by NIA is not transparent and reliable by saying that "*Fox-IT concludes that the MIT investigation as described in the MIT report does not adhere to the forensic principles as outlined in section 3.1 of this report and should therefore not be regarded as a forensic investigation. " ... " The investigation is fundamentally flawed due to the contradicted and unfounded findings, lack of objectivity and lack of transparency.* ***As a result, the conclusions of the investigation are questionable.*** *" .." Fox-IT recommends to conduct a forensic investigation of ByLock in a more thorough, objective and transparent manner." .." The MIT report contains very limited information on the identification of individuals."*[1]

As it is explained in detail under the title "What is Bylock?", and the European Union Data Protection Legislation are violated by accepting the usage of a the European Convention On Human Rights communication app which is widely used in 41 countries as an evidence of being a member of a terrorist organization, acquiring the personal user information of the users by intelligence service agents who don't have any authority by violating the norms of International Law and Domestic Law and by using those data as evidence in administrative and judicial investigations. Turkey and Lithuania are members of the European Council. Lithuania is also a member of the European Union. Both countries have responsibilities in front of the International law to protect the personal data.

As a result of the accession to the personal data by violating the law, it is clear that the International Regulations and Legislations are violated as following:

a. The Fair Trial Principle and the Right to Privacy, which are included in the European Convention on Human Rights and protected by the Convention are violated. This is also mentioned in the legal opinion made by William Clegg Simon Baker about the

[1] blog.fox-it.com/2017/09/13/fox-it-debunks-report-on-bylock-app-that-landed-75000-people-in-jail-in-turkey/

position in the International Law of the investigations after the July attempt in 15th July and the accepted evidence.[1] In the assesments that are made in the mentioned legal opinion, it is clearly stated that the Fair Trial Principle is violated:

" A Mysterious Report (The Report of Turkish Intelligence Service) : The authors of the report were not identified, they did not give evidence, no-one knows who they are, their qualifications and experience are unknown. No questions can be asked of the authors of the report and they cannot be asked to provide any explanation for the fact that the App has been downloaded in over 40 countries many with no connection to Turkey, nor can they be asked what evidence they relied upon to come to the belief that the downloading in countries other than Turkey was involved in the failed coup. "

" Be Sentenced in Vain With a Mysterious Report : The trial in Turkey convicted X on the basis of a technical report assessing the Bylock App. It is a fundamental principle of a fair trial that a suspect has the right " to examine or have examined witnesses against him " this is enshrined in article 6 (3) (d). The use of the technical report at trial as evidence is a clear branch of this convention right. The mechanism by which they arrived at the crucial conclusion upon which any verdict will turn is not revealed. "

Also, there are many decisions that states that the intelligence information cannot be used as evidence as it is generally collected in the absence of the concerning parties, is kept in secret, doesn't give the concerning parties the chance to object, correct and appeal to the judges:

- ECHR, BN: 9248/81, KT: 26/03/1987, Leander/Sweden, pr: 48,59
- ECHR, BN: 27798/95, KT: 16/02/2000, Amann/Switzerland, pr: 65, 69,70
- ECHR, BN: 28341/95, KT: 02/05/2000, Rotaru/Romania, pr: 43, 44;

Six months after the acquisition of the Bylock server, a verdict is made to investigate the concerning server. It was stated that even this verdict is against the law and the decision of MUSTAFA SEZGIN TANRIKULU (Application no. 27473/06), which suggests that there will be a general communication surveillance without naming any specific target, violates the 8th article of the ECHR.

The ECHR decided that the examination of the correspondence of the employee who used the online messaging application (Yahoo Messenger) of the office for his private business violates the 8th article.[2]

b- Turkey has signed the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the convention is active now.

c- The instruction number 95/46 in the European Union legislation.[3]

---

[1] www.2bedfordrow.co.uk/opinion-on-the-legality-of-the-actions-of-the-turkish-state/).

[2] (ECHR Barbulescu v. Romania, Application no: 61496/08, decision date: 05.09.2017)

[3] eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

d- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[1]

As it is mentioned above, the usage of the illegally obtadine Bylock data as evidence in investigations violated many rights and freedoms such as freedom of opinion and expression, freedom of press and media, freedom of the Internet, privacy of private and family life, privacy, confidentiality and protection of personal data. The vast majority of these are at the same time categorized as fundamental rights and freedoms.

Fundamental rights are universally protected, as they are accepted throughout the world. Those rights and freedoms are even protected against the person concerned. In other words, people cannot give up their rights and freedoms.

It is confirmed by many international reports that those rights are violated in Turkey. In the APC's letter that were sent to the Human Rights Council no. 36 which includes 56 institutions that defends the freedom of communication and thought, it is said that:

" HRC 36: Secure digital communications in Turkey are essential for human rights The Association for Progressive Communications (APC) and IFEX submitted a written statement ahead of the Human Rights Council's 36th session to express their grave concern about the growing crackdown on the use of secure digital communications, ... Ultimately, this is a failing strategy. It fails to comply with Turkey's human rights obligations by criminalising tools that are necessary for the exercise of human rights in the digital age; and it fails from a security perspective, because in the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online." [2]

In the Internet Report of Turkey of Freedom House, the arrests based on Bylock were criticized: " *In Turkey, thousands of smartphone owners were arrested simply for having downloaded the encrypted communication app ByLock, which was available publicly through Apple and Google app stores, amid allegations that the app was used by those involved in the failed July 2016 coup attempt."*[3]

5. BYLOCK DATA WAS OBTAINED ILLEGALLY AND AGAINST THE INTERNATIONAL RULES OF LAW

Turkey and Lithuania are sides in the Mutual Legal Assistance on Criminal Matters and its no. 1 Protocol.

Therefore, it is required to act accordingly when the criminal procedure requires legal aid. The methods to be used in this issue were explained by the examples in the notice of the

[1] www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[2] www.apc.org/en/pubs/hrc-36-secure-digital-communications-turkey-are-essential-human-rights

[3] freedomhouse.org/report/freedom-net/2017/turkey

General Directorate Of International Law And Foreign Relations of the Justice Department (Date 16.11.2011, no. 69/2)[1]

Thousands of penal courts applied the judicial assistance with foreign countries in accordance with this Convention and Notice. Therefore, Turkish authorities tried to illegally hack/ buy / steal instead of requesting formally. So, the International Law is also violated.

Turkey and Lithuania are among the states who signed the European Convention on Mutual Assistance In Criminal Matters. Between all the 45 states that signed the Convention, the extraditions are made in accordance with this Convention. All the details regarding the procedure of extraditions of the criminals are explained in detail at www.uhdim.adalet.gov.tr. On the same website, there is a notice with the title "The Important Things to Consider in International Rogatory Procedures"[2] which explains and exemplifies the necessary procedure. In the penal procedures, it is obligatory for the rogatory procedures to follow the instructions and tools that are determined in the concerning legislation.

Turkey and Lithuania also signed legal cooperation agreement[3] and the requests regarding legal issues must be done accordingly. Regarding Bylock issue, there is no request that is suitable to the mentioned international legal obligations.

It is not also possible for National Intelligence Agency to purchase Bylock data because it is not possible to sell those data due to the reason that they include personal correspondence and therefore secret.

6. THE ACQUISITON OF BYLOCK DATA AND ITS USAGE AS EVIDENCE VIOLATES THE CONSTITUTION, ECHR AND THE CODE OF CRIMINAL PROCEDURE

The way of obtaining the Bylock data is stated as: "It is clear that the server of the application, the data on the servers of Bylock and IP addresses are bought, various data is acquired such as the content of the mail addresses and the technical analysis report and digital materials are sent to the Public Prosecutor of Ankara and General Directorate Of Security by using "unique techniques" and intelligence tools and services by the National Intelligence Agency." In the file no. 2017/13 of 15th Heavy Penal Court of Ankara. **Downloading and using Bylock doesn't possesses any crime.** There is also no legal regulation in Turkish Penal Code about being a crime.

The National Intelligence Agency is not judicial police according to the article no. 164 of the verdicts of "Judicial Police and its Duties" in Turkish Penal Code and therefore is not eligible

[1] uhdigm.adalet.gov.tr/adli_yardimlasma/adli_isbirligi_ceza/cz_istinabe.html

[2] date 16.11.2011, no.69/2

[3] www.uhdigm.adalet.gov.tr/sozlesmeler/Hukuk/Litvanya.pdf

to collect evidence regarding the crime of the armed terrorist organization. The police and gendarme are judicial police according to the Penal Code, so although it didn't have the authority, the NIA acted as judicial police and collected evidence.

If the NIA purchased the data, IP addresses and the servers of Bylock, it means that it obtained the authority to intercept the data. It is clear that the NIA, which acquired the data by purchasing, would have the possibility to change the existing data and upload new data. There is no judicial interception in this phase.[1]

The NIA made a public statement on 4th of April 2017 after the huge criticizations. According to it, it is said that the data, which is claimed to be obtained in May 2016, was shared with the judicial and security authorities. It is not clear when the server and the data was obtained according to it.

Despite this statement, the judicial investigation started after the obtained data was delivered to the Office Of Chief Public Prosecutor of Ankara in 9th December 2016. After that, by the decision of 4th Criminal Court Of Peace of Ankara (date: 09.12.2016, no. 2016/6774) and by the article 134 of the Law of Criminal Procedure no. 5271 which regulates "searching, copying and seizing the computers and computer applications", the permission to "create an image file" and investigate was given.

According to this statement, **the NIA had the possibility to add, remove and correct the Bylock data by keeping the obtained data for itself for 8 months.** There isn't any judicial interference as well until 9th of December 2016.[2]

The decision by the Criminal Court of Ankara regarding the data delivered by the NIA in 9th December 2016 must have been made during the obtaining the data. The decision to examine the hard drive by the Law of Criminal Procedure doesn't change the fact that this digital data was obtained illegally and doesn't make the previous procedures legal.

The NIA prepared a secret report named Bylock Technical Explanation Report during the 8 months period in which it kept the data to itself. This report is considered as evidence now by the courts and the Court of Appeals. There is no information regarding who prepared this report, what are the professions of the ones who prepared it, why their names are not mentioned in the report and when this report was prepared. This "report" wasn't prepared according to the "expert examining" rules regulated by the 62nd and following articles of the Law of Criminal Procedure.

According to these reasons, it is not clear by who and how the Bylock data was obtained. It is kept in secret by saying: "by using "unique techniques" and intelligence tools and services by the National Intelligence Agency." It is not possible to hide the way of obtaining an evidence of a crime in a Lawful State.

---

[1] www.mit.gov.tr/basin60.html

[2] odatv.com/mitten-bylockta-nerede-hata-yaptik-itirafi-0612171200_m.html , http://aktifhaber.com/m/gundem/mit-bylock-verilerinde-hata-yapildigini-kabul-etti-h106366.html

There is no procedure of collecting evidence that was done according to Turkish Law of Criminal Procedure. **According to the Constitution, the findings that are obtained illegally cannot be used as evidence (art. 38/6).** According to the Law of Criminal Procedure, the charged crime can only be proven with legitimate evidence (art. 217/2). If the evidence is collected illegally, it should be denied (art. 206/2-a). If the verdict is based on illegally obtained evidence, it is a clear violation of law (art. 289)

As a result, as the Lawyer Hüsnü Yıldırımer stated in his article titled "BYLOCK CAN NEVER BE USED AS EVIDENCE DEFINED IN THE ARTICLE 217/2 OF THE LAW OF CRIMINAL PROCEDURE",

It is clear that the NIA's way of obtaining the data violates the articles 20, 22, 38/6 of the constitution and the article 134 of the Law of Criminal Procedure.

According to the law no. 5651 and its regulations, only the Internet data of one year can be requested by courts but the courts request the data of the years 2014-2015 now.

According to the ADDITIONAL ARTICLE 1 which is added to the Law of NIA no. 2937 (art. 11 of law no. 6532, 17.04.2014), the information, documents, data and analysis cannot be requested by legal authorities except the crimes in the 2nd book, 4th chapter, 7th period of Turkish Penal Code.

2nd book, 4th chapter (The crimes committed against the state and nation) 7th period (The crimes against the secrets of the state and the documents regarding the State security and espionage) is in the article 326-339 of the Turkish Penal Code.

But the defendants are being charged by the article 314/2. In this case, according to the "AUTHORITY OF EVALUATING THE EVIDENCE" (The charged crime can be proven by ANY EVIDENCE THAT IS OBTANIED LEGALLY) which is in the Law of Criminal Procedure article 217/2, **the data which the NIA obtained cannot be used as evidence.**

The Bylock data cannot be evidence because of the reasons mentioned above (Being against the ECHR, the Constitution and Law no. 5651 and 2937)[1]

7. THE CRITIQUE OF THE BYLOCK DECISIONS OF 16TH CRIMINAL DIVISION AND LOCAL COURTS

Penal Department no.16 of the Supreme Court is the department that deals with the appeals regarding the crimes of terror. It made a determination that the evidence are legal and Bylock is a communication application that is unique for the FETO organization in its announced decision of Bylock.[2]

[1] www.adaletbiz.com/m/ceza-hukuku/bylock-hicbir-zaman-cmk-madde-2172-anlaminda-delil-olarak-kullanilamaz-h176526.html

[2] www.adaletbiz.com/m/ceza-hukuku/16-ceza-dairesi-karari-ve-bylock-h181284.html

The statements below are the claims in the decision of the Supreme Court. The explanations starting with the letters show that these claims do not reflect the truth

1. “Bylock Application is a system which is based on sending each one of the messages with a different encrypted key to communicate via internet by using a strong encryption system.”

   a. The term “strong” is completely subjective and it is clear that the encryption in Bylock is just as the other messaging apps in the market (WhatsApp, iMessage etc.)

2. “Bylock Application is a system which is based on sending each one of the messages with a different encrypted key to communicate via internet by using a strong encryption system.”

a. The statement “each one of the messages with a different encrypted key” is completely wrong. There is no messaging app which encrypts in this way. As it was stated even in the report of the NIA, it was claimed that the encryption is made by Public-Private keys.

3. “This communication app is an application which provides the communication between the members of the organization via a special encryption that keeps them secret and which was produced as an exclusive software that only the members of the organization can use on a special server.”

a. As it is stated in the Technical Report of NIA about Bylock (Page 10 and the Attachment-2), it was clearly accepted that the app was open for everyone and can be downloaded via Google Play. Any application that is present on Google Play is absolutely not an exclusive content, it is clear that it is for public.

b. It is clear that there wasn’t any special encryption method but all the encryption is according to the industrial standards.

4. It is determined that in the Bylock communication system, the data between two users are encrypted via graphic algorithm, the graphic algorithm is a kind of open-key/ asymmetric encryption algorithm and uses two keys, one open and one secret, to encrypt and there is a security system which tries to prevent third parties to intervene and hack the communication process.

   a. The statement above is the definition of the methodology of encryption and algorithms that are used in similar applications which aims the industrial standards.

5. “It is understood that the application required exclusive installing because only the downloading is not sufficient, the registration for the app can be done by installing it via Bluetooth or USB drives, the application was only open for public for a short amount of time at the beginning of 2014 and the installation was made afterwards by memory cards, USB drives and Bluetooth as it can be understood in the correspondence between the members of the organization.”

a. None of the iOS and Android applications can be used only by downloading them. They are downloaded at first, installed and registered to the system afterwards.

b. All the Android applications fit the definition of “the registration for the app can be done by installing it via Bluetooth or USB drives”.

c. The times when the Bylock application was active in Google Play and Apple Store:

    i. Apple: April 2014-September 2014

    ii. Google Play: April 2014- April 2016

    iii. It was active not only for a short amount of time at the beginning of 2014 but approximately for 2 years.

6. “ Downloading the app is not sufficient for messaging, it is required for the second person to approve the ID number of the first one which is exclusive for the user and generated by the system automatically and otherwise, he can’t be added to the contacts list and no messaging will occur and the app requires the users to create a user name and password in the registration process. Adding new contacts is done by entering the username that was determined by the user while registering.”

a. All the messaging apps require registration (WhatsApp, Skype, Viber, Facebook Messenger etc.). It is not a special situation for Bylock.

b. All the messaging apps generate an ID for the users. For example:

    i. WhatsApp: Phone Number

    ii. Skype: Username or e-mail address

c. You have to create a password in registration for all messaging apps.

d. In some of the messaging apps, adding new contacts can be made ONLY BY ADDING THE USERNAME.

    i. Viber

    ii. WhatsApp

7. “It is not possible in the app to search by name and surname or telephone number and add new contacts with those information.”

a. It is clear that the claims regarding this are caused by the lack of information about the account management system of the applications. As it was stated, in all apps, only by the Username-ID one can add contacts. In an app which uses the phone number as the Username-ID (like WhatsApp), you can “only” add new contacts with the phone number. In an app which uses the mail address as the Username-ID (like Hangouts) you can “only” add new contacts with mail address.[1]

b. In some messaging apps, there is an option to add new contacts only by searching with the Username. For Example:

    i. Viber

    ii. WhatsApp

8. “On the other hand, the function which allows to add the contacts recorded in the phone automatically to the application and is used in the other common messaging apps doesn’t exist in Bylock.”

a. This function, which is called Phone Book Integration, is not present in many apps when they first came out, but added later. (Like Telegram Windows Phone App)

9. “For users to contact with each other via Bylock app, it Is required for the both parties to know the Username info and add each other. Shortly, due to the reason that it is required to add the ID of the person to contact with at first, it is understood that this system cannot be used by anyone at any time.”

a. In all messaging apps, it is impossible to contact with anyone without knowing the Username / code at first. For example:

    i. WhatsApp

    ii. Viber

    iii. Telegram

10. It is possible to voice call, send e-mails, send text messages and send files via the application. Therefore, it is understood that the users fulfill their need to communicate with the members of the organization without the need of using any other app, the system is designed in a way that it deletes all the correspondence and message history automatically even if the user forgets to take the necessary

[1] http://na-copywriting.com/2017/05/the-bylock-report page 24

precautions, therefore the Bylock system is designed in a way that it will prevent the access to all the previous correspondence and information about the contacts in a case of the confiscation of the device for a legal procedure and keeping the server and communication info encrypted in the database of the system is a security precaution to make sure that the detection of the users is impossible and the communication is secure."

a. In many messaging apps, voice call, sending e-mails, sending text messages and file transfer are possible. For example:

    i. Whatsapp

    ii. Viber

    iii. Facebook Messenger

    iv. Skype

b. The feature of deleting the messages without a manual process is a very important feature and the Snapchat Messaging App, which has 178 million users worldwide, has the same feature as well.

c. "keeping the server and communication info encrypted in the database of the system" is completely for protecting the user to make sure that even the employees of the software firms cannot access to the personal data of the users. It is also used in all situations that include personal data.

11. "It is seen that Bylock application operates on the server with the IP address 46.166.160.137. It is determined that the administrator of the server purchased 8 additional IP addresses (46.166.164.176, 46.166.164.177, 46.166.164.178, 46.166.164.179, 46.166.164.180, 46.166.164.181, 46.166.164.182, 46.166.164.183) to make it difficult to determine the users of the application

a. The usage of more than one IP address can have many different reasons in the IT world. As it can be seen on https://www.quora.com/Why-do-servers-need-more-than-1-IP-address ,

    i. Using more than one website

    ii. Providing more than one service (DNS, VPN)

    iii. The fact that the same app has different versions

    iv. To hide the server IP addresses

All the technic details of the issues mentioned above can be reached in the report that was prepared by Daniel Walter, Digital Forensics Specialist in Winthrop University.[1]

The Analysis of The Decision Of 16th Criminal Department in A Legal Perspective

The 16th Criminal Department of the Supreme Court has reached a decision about the Bylock Application that was hacked by the National Intelligence Agency

16th Criminal Department decided (2015/3 E 2017/3K) by evaluating about the articles 4 and 6 and additional article 1 of the NIA law no. 2937

The NIA is obliged to send all information, documentation, data and records that are obtained by their authority during the intelligence missions to the administrative institutions that are defined in the article 4 of the NIA law.

The authorities that they can use are defined in the article 6 of the NIA law. The additional article 1 of the NIA law is the one that should be examined deeply. According to this article**, "the information, documents, data and analysis that are in the possession of the NIA cannot be requested by legal authorities except the crimes in the 2nd book, 4th chapter, 7th period of Turkish Penal Code."**

As it is seen, the additional article is clear and concise and the crimes in the 7th period are the crimes against the State secrets and espionage. Legal authorities (The Court and the Prosecution) can only request evidence from the NIA regarding those crimes as it is stated clearly in the additional article 1.

Despite this, the Supreme Court decided that the legal authorities can act against the additional article 1 of the NIA law. Supreme Court ignored the principle of lawful state as well as violating the principle of lawfulness in the article 13 of the Constitution and the restrictions about obtaining evidence illegally which are stated in the article 38/6 of the Constitution.

It is a clear violation of law. The Supreme Court also emphasized in its decision that the search, copy, seize and evaluation of the information and evidence that are in the server or the memory of the computers should be done in accordance with the article 134 of the Law of Criminal Procedure. But this rule was also ignored while the defendants were put into legal action.

The Supreme Court, for the first time in its history, chose to form a legal precedent which is clearly against the law. The decision of the Supreme Court accepted using Bylock as a crime which is against the laws and Constitution

Lawyer Feyzi Çelik told these about this situation: "The 16th Criminal Department of the Supreme Court acted as if the Bylock is a lawful evidence while making its decision. As it can

[1] www.bylockreality.com/index.php/technical-reports/an-independent-technical-report-by-daniel-walter-about-bylock-application

be understood in the decision, the Bylock system is obtained by the espionage acts of the NIA. The verdicts about the inspection of communication in the Law of Criminal Procedure were violated. The verdict in the article 6/c about the limits of authority of NIA, "It can access to all kinds of information and documentation regarding the investigations and prosecutions regarding the crimes in the 2nd book, 4th chapter, 7th period of Turkish Penal Code (except the articles 318, 319, 324, 324 and 332), is not about the access of the legal authorities to the NIA but the access of the NIA to the data in the possession of the legal authorities.

The NIA was granted the authority to access freely to the information regarding the mentioned crimes from the concerning legal authority. The justification of this verdict to the decision is not lawful.

The verdict in the Additional Article 1 (17/4/2014-6532/11) of the law of NIA, "the information, documents, data and analysis that are in the possession of the NIA cannot be requested by legal authorities except the crimes in the 2nd book, 4th chapter, 7th period of Turkish Penal Code." Is clear and concise.

According to this verdict, "The intelligence information of the NIA can only be used by the legal authorities because of the crimes related to espionage. It can't be used except these crimes. The legal authorities cannot request any information from the NIA as well as the NIA is not obliged to report these information to the legal authorities, except the information related to espionage.

The alleged crime is not related to espionage, so it is clear that the Bylock records which are obtained via espionage acts are not legitimate evidence in accordance with the Law of Criminal Procedure[1]

8. THE PRESSURE OF POLITICS AND THE SUPREME COUNCIL OF JUDGES AND PUBLIC PROSECUTORS UPON THE BYLOCK DECISIONS

A - Supreme Council of Judges and Public Prosecutors

1-) The political power used the Supreme Council of Judges and Public Prosecutors as a pressure tool to make the judiciary accept Bylock as a crime. According to the ECHR, one of the most crucial aspects of the independence of a court is the impossibility to dismiss the assigned judges without their request or the expiration of their duty, except the situation when they are elected for the higher court. (Campbell and Fell v. The United Kingdom, para. 80 - Lauko/Slovakia, para. 63).

[1] www.adaletbiz.com/m/ceza-hukuku/bylock-kayitlarinin-hukukiligi-uzerine-h177189.html

The vice president of the Supreme Council of Judges and Public Prosecutors, Mehmet Yılmaz, made these statements about Bylock although it is an issue which the judiciary should with and although he was obliged to ensure the independence and neutrality of the judiciary: "Our biggest evidence is the clear fact that the Bylock is not an application that can be used by anyone but the members of the organization." [1]

2-) The 2nd Heavy Penal Court of Hatay started an investigation about the chief judge and members after the indictment regarding "the usage of the communication app Bylock is not an evidence itself, the content of the correspondence and the identities of the users are also should be determined" was declined (2016/225)[2]

3-) The Antalya Regional Court of Justice 2nd Penal Chamber reversed a 6-year-3-month prison sentence issued by the Denizli Assize Court on 04.04.2017 on the grounds that the investigation into the application called ByLock was insufficient. Pro-government daily newspaper Yeni Asır published news on 26.04.2017 about Şenol Demir, the chief judge of the Antalya Regional Court of Justice 2nd Penal Chamber, that vilified him for his decision. On 08.05.2017 the judge Şenol Demir was assigned by the HSYK to Konya province as a judge of first instance only after having been the chief judge of the penal chamber for 9 months and 18 days. A judge assigned to courts of second instance normally have a tenure of at least four years.[3]

4-) The Adana 11th Assize Court sentenced a deputy police chief on 20.01.2017 for being a member of a terrorist organization on the grounds that he 'used the mobile phone application called ByLock, sent his son to Işık Preparatory School between 2013-2015 and had an account in the bank called Bank Asya'. The Gaziantep Regional Court of Justice 3rd Penal Chamber reverted this decision by a majority voting on 20.04.2017 on the grounds that, 'a sentence for membership to a terrorist organization cannot be based on ByLock records, the contents of which are not known (2017/286E – 2017/573K). After this reversal, the chief judge of the 3rd Penal Chamber Zafer Yarar was assigned by the HSK to the Kayseri Courthouse on 26.05.2017 as a judge of the first instance. Mustafa Tosun, a member of the 3rd Penal Chamber who voted like the chief judge, was assigned by the same HSK decision to the Istanbul Anadolu Courthouse as a judge of first instance. Bayram Korkmaz, the member who opposed the decision about ByLock, was rewarded and made the chief judge of the 3rd Penal Chamber. Hence, the two judges in Courts of Appeal, who reversed decisions in favour of defendants sentenced for their alleged links to the organization called FETÖ/PDY, were relieved of their duty in the Regional Assize Courts without their consent 10 months and 6 days into their four-year tenure and demoted to judges of first instance.[4]

5-) Judge Fatih Mehmet Aksoy, who had previously arrested the 39 prosecutor without any evidence and jailed them, blurted out in a trial:" I can not bear it anymore, I will set all of them free." Upon this, the case prosecutor threatened the judge:"If you do that, I will have

[1] www.timeturk.com/bylock-orgutun-iletisim-yazilimi-ve-en-guclu-delilimiz/haber-317394-m

[2] www.ntv.com.tr/turkiye/feto-iddianamesini-iade-eden-hakimlere-inceleme,vvGCbLy6YE6qg14QwaGCXQ

[3] www.platformpj.org/report-non-independence-non-impartiality-turkish-judiciary

[4] www.platformpj.org/report-non-independence-non-impartiality-turkish-judiciary/

you arrested in two hours for using ByLock."After the attempts of the Police Chief of Kırşehir Province Veysel Murat Tuğrul, the judge was suspended in less than two hours. In the same province a judge was unseated during an ongoing trial by a mere telephone call. Both judges were detained on the charge of using ByLock.[1]

B- The Pressure of Politics and Partisan Media

Some of the media organs in Turkey that are called "Partisan Media" create news that will affect the political will positively and in accordance with the instructions of the political power. Therefore, they fulfill the duty to direct and manipulate the society towards the demands of the rulership.

This media group called partisan media creates news in accordance with the demands and instructions of the authority even it's wrong instead of being objective and reliable. The Erdogan regime, which uses this media power that is derived from all the communication tools like television, newspapers and magazines both misled people about Bylock and threatened and targeted the members of the judiciary who questioned the truth and the state of evidence of Bylock.

1-) In his article on the 4th of April 2017 titled, "Judges and Prosecutors who lack credence in Bylock", pro-government newspaper Akşam journalist Murat Kelkitoğlu noted this: *"At this juncture, I will share something with you. As you know, the National Intelligence Agency (MIT) came up with a lengthy list of ByLock users (..) MIT didn't laze about, it sent groups to courthouses and debriefed judges and prosecutors about ByLock and its users (..) Yet, some judges and prosecutors kept voicing their concerns, "we still haven't connected the dots between the ByLock App and FETÖ; that is why, it cannot be considered as evidence (..) so, that is how all the release verdicts are issued. Oh, friends! Didn't these traitors communicate through this program and attempt to occupy the country? Could there be any greater evidence?*

2-) On the 6th of June 2017, the pro-government daily newspaper Sabah ran with a headline that overtly affirms the undermining of judicial independence: "If there is no evidence, freedom with judicial control."The news reads as follows: "A new criteria has been introduced for ByLock detentions in FETÖ cases. Criminal courts of peace can release farmers, workers, tradesmen and housewives whose case file consists only of ByLock as evidence, with the condition of judicial control. If the suspects are civil servants and charged with the same ByLock evidence, they can apply to the newly-issued law with the stipulation that they make concrete confessions about FETÖ in line with the effective remorse law. When drawing up the legal documents, the Democratic Union Party-PYD terrorist organization will be removed from the official documents; yet, FETÖ will be preserved. Thus, the emphasis on the terrorist organization will be highlighted. This initiative taken by the Ankara Office of the Chief Public Prosecutor aims to curb unjust suffering and victimization.

[1] www.platformpj.org/report-non-independence-non-impartiality-turkish-judiciary/

Suspects' confessions taken within the new judicial control, freedom to decode the structure of the FETÖ organization are stipulated to be congruous. "Obviously, the source of the news is the Ankara Office of Chief Public Prosecutor which dictates which evidence will be accepted and how it will be utilized in case proceedings. In the aftermath of the 15th of July 2016 coup, some judges confessed that they have issued arrest decisions at the behest of the chief public prosecutor; and, therefore, this information corroborates the claim that arrest orders are issued to the courts. If the assessment of evidence is handed over to the Office of Chief Public Prosecutor and if the judges wield the power of justice by following the orders, it is literally a travesty of justice.[1]

As mentioned here the responsibility of lawful evidence gathering for legal proceedings or assessing the pertinence of evidence for the case at hand was taken over by the state-institution intelligence agency which fulfils the mandates and orders of the executive body. It is impossible to talk about the security and immunity of judges in a system where the ruling body have a vice-like grip over the lawful gathering, production and integrity of the assessment of the evidence. The above-mentioned shows a direct interference in the judicial structure and also shows the undermining of judicial security and impartiality.

9. TRAGICOMIC BYLOCK INVESTIGATIONS

As it is seen in the examples, in the user lists of Bylock which is created by the NIA somehow, there are many people who even didn't use smart phones and this is one of the most important reasons why the lists are not true.

1- A Stallholder Auntie,

The stallholder auntie who was claimed to be a ByLock user was detained in a marketplace while selling vegetables in Aksaray. The woman who has no information about what ByLock is and has a very old model of mobile phone was thrown into detention room.[2]

2- An elderly with chronic illness,

Uncle Rustem, an elderly with chronic illnesses such as cardiac and high blood pressure was detained over using ByLock. The old man admitted that he used ByLock for two years because he thought the judge was referring to Beloc which was a medicine he is using for the heart disease. He has been using it for years. Also, he has a Nokia 5310, an old model regular cell phone, which is not possible to download a smartphone application.[3]

---

[1] www.platformpj.org/report-non-independence-non-impartiality-turkish-judiciary/

[2] www.cumhuriyet.com.tr/m/foto/foto_galeri/798713/1/
Semt_pazarinda_ByLock_operasyonu..._Gozaltina_alinan_pazarci_teyze_serbest_birakildi.html

[3] www.cumhuriyet.com.tr/m/haber/turkiye/
841472/60_yasindaki__Rustem_dedeye__tutuklama_talebi__ByLock_u_kalp_ilaci_sandi.html

3- A Truckdriver,

A truckdriver denied loading ByLock to his truck. He has heard ByLock for the first time in his life and he thought it was a kind of cargo. He showed the invoices to prove not to carry ByLock.[1]

10. TECHNICAL DILEMMAS

According to the NIA Law no. 2937, the NIA can only use the authority as judicial police regarding the crimes related to espionage. That's why the NIA must report any evidence which it finds by coincidence without waiting.

But the NIA didn't take the necessary action in legal terms although it found the Bylock data in May 2016.

The NIA kept this data in its possession and made examinations for 6 months although it wasn't its duty and it wasn't assigned to do so and prepared a technical report. There isn't any assignments for it according to the Law of Criminal Procedure and its Bylock list and technical analysis report have no meaning legally according to the articles 73 and 134 of the Law of Criminal Procedure. It is not possible for Bylock to be legal evidence as the legal procedure haven't been followed. That's why the Bylock list and the analysis report should be declared null and void legally.

Despite all these, tens of thousands of people are being arrested with these illegal lists. The NIA presented the list ann the LOG records of Bylock which he prepared to the Office of Chief Public Prosecutor of Ankara in 9 December 2016 and in the same day, the examination decision was made by Criminal Court of Peace. It means that this court decision about the Bylock lists and examination is not real.

Because all the examination was made before this decision. All the disinformation and changes are made before the LOG records were delivered to the legal authorities, which are not obtained in legal ways. Even after this phase, there wasn't any objective expert examination and the legal procedures were made by the report of the intelligence unit.

After the voices became heard about how the right to fair trial is violated and local and international regulations don't allow this, the courts started to demand the internet traffic information of the users from the concerning institution.

But the parts in the articles 4 and 6 of the law of coping with the cybercrimes (no. 5651) which allows the people's internet information to be surveilled and delivered to the legal authorities were cancelled by the decision of the Constitutional Court in 2015. Although this

[1] www.cumhuriyet.com.tr/m/haber/turkiye/
842992Kamyoncu__isci__ogrenci__ev_hanimi..._26_kisiye_ByLock_operasyonu.html

is known, the Constitutional rights of communication and its privacy is being violated and the opposition is being pressured.

- In the decision of the ECHR of Turkey - Mustafa Sezgin Tanrıkulu (18 July 2017), it is stated that "The intelligence services are not directed to the crimes but to the collection and evaluation of the information systematically and regularly for the elimination of the threats to the superiority of law and national security within the regulations that form them."
- The Supreme Court stated regarding the court decision which allows the Gendarme to be able to intercept the communication of everyone in Turkey in 4 June 2008 (E.2008 / 874 and K.2008 / 7160) that: "A permission in country-scale which defines everyone in Turkey as suspects will not be given to any institution in a democratic state.

So it concluded that the decision of inspection of communication for the general populace is a violation of the article 8 of the Convention.

Also, the NIA confessed that even after the Bylock data was sent to the legal authority, they made changes on them and this was a subject of official correspondence.[1]

For a digital data, there is no "**update and correcting"** , there is no legislation in either Turkish Law or any democratic lawful system. Digital detection method is regulated in the article 134 of the Law of Criminal Procedure.

The hash value of the data is included in the records. Any changes after this point will result in changes in the hash value and the digital data to lose its status of evidence.

The NIA officially confessed that they "updated and corrected" the Bylock lists.

The NIA's "update and correction" after they sent the data to the legal authority means that they may have done lot more before they delivered the data.

The digital footprint may be fictionalized as well. The Wi-fi passwords may be broken, any correspondence may be one without the notice of the owners.

Turk Telekom was revealed to bought an application to hack the internet passwords of people just at the same time when the claims of Bylock were in the agenda.[2]

Turk Telekom ordered a software to control all the Internet traffic in Turkey, detect the identities of the users and hack their passwords.[3]

NIA's capabilities and possibilities should also be examined after it was revealed that they can make "updates and corrections" on the data which was sent to the legal authorities.

---

[1] http://odatv.com/mitten-bylockta-nerede-hata-yaptik-itirafi-0612171200.html

[2] http://www.webmasto.com/turk-telekom-procera-networks-internet-gozetimi-yazilimi

[3] www.cumhuriyet.com.tr/m/haber/dunya/621344/Muthis_iddia__Turk_Telekom_dan_musterilerine_karsi_casus_yazilim_siparisi.html

Is it possible to make correspondence by third parties with the mobile phones of the people as if the real user was making it without his notice?

How it is possible to make this correspondence via the Service Providers without the notice of the user? Does the NIA has a capability like this? The NIA owns a professional IMSI catcher device which it bought it from both Israeli and Turkish firm. (https://eksisozluk.com/imsi-catcher--1608021 http://www.trsecurity.net/sahada-cep-telefonu-dinleme-sistemlerine-bir-bakis/)

With the device IMSI Catcher, you can send a message to anyone via any mobile number and use the internet traffic of any device. It means that someone can create a WhatsApp account by using your phone number and use your number to verify that account. After that, he can write messages in your name via any mobile connection or Wi-fi. The second parties would think that you sent them those messages. By this method, Bylock accounts can also be created.

The applications like WhatsApp creates accounts by sending a verification to your number at only the beginning and don't require your phone number afterwards. In Bylock, even this verification is not necessary. It is possible for them to write messages via WhatsApp, Bylock or any other communication app after they activate the account with IMSI Catcher without your notice.

The lists were updated and correct many times before they were delivered to the legal authorities. It is not clear that how many people were the victims and who wrote the artificial correspondence.

TECHNICAL PARADOX

1. **VPN**

This was also stated in the legal opinion made by William Clegg Simon Baker about the position in the International Law of the investigations after the July attempt in 15th July and the accepted evidence.

In the mentioned legal opinion under the title "There Are A Number Of Assertions Contained In The MIT Report Which Are Fundamentally Contradictory", it was stated that : "The MIT Report asserts at paragraphs 3.5.1 to 3.5.5 that IP blocking was used to force users to use a VPN (virtual proxy network) to access the ByLock App. At 3.6 however, it is suggested that IP addresses were used to identify ByLock users. These two assertions are mutually incompatible, since the IP addresses would not have been able to be used to identify users if VPNs were being used"

2. CGNAT PROBLEM

CGNAT: Carrier Grade Network Address Translation.

IP: The identity of every user on the Internet just like the mobile phone number. All the computers, smartphones, tablets, TV's, surveillance cameras etc. use IP addresses. In the IPv4 that is used now, there are 4,294,967,296 IP addresses. IPv6 is created because there isn't enough IP addresses in IPv4 but using it is very expensive for the Service Providers

There are 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses on the IPv6. The Service Providers prefer to use cheaper CGNAT instead of using the IPv6

In the places that use CGNAT, the devices that connect to the Internet require real IPs. We can think the real IP as the phone number and virtual IP as the paid phone. There is a standard in using, registering, reporting the real IP but such standard doesn't exist in using virtual IP's.

Technically, it is very difficult to determine who uses the real IP in the Service Providers that use CGNAT. In Turkey, almost all the Service Providers use CGNAT. **The Director of EUROPOL, Rob Wainwright states that the odds to determine the users are around 10 percent of the users.** The claim that the Bylock users were detected via IP addresses in Turkey in which the CGNAT is used is not realistic as it is said that maximum 10 percent of the CGNAT users can be detected.[1]

11. THE LIES ABOUT THE CONNECTION BETWEEN THE COUP ATTEMPT AND THE BYLOCK CONNECTION AND THE PARADOXES REGARDING THEM

1-Labor and Social Security Minister Mehmet Müezzinoğlu also told reporters in Bursa on Tuesday that the Turkish Intelligence Agency has determined the identity of nearly half the 180,000 users of ByLock,. It is claimed by the Justice and Development Party (AKP) that plotters of the July 15 coup attempt used it for communicating.[2]

2- After the Attempted Coup, Turkish Authorities said that the smartphone chat application may have been created by FETÖ members, so they could communicate secretly about the coup plot.10 And also it is claimed by the Justice and Development Party (AKP) that plotters of the July 15 coup attempt used it for communicating.[3]

---

[1] https://twitter.com/bylockgercegi/status/939917992330252288

[2] www.turkishminute.com/2016/09/14/turkish-minister-indicates-purges-continue-bylock-users/

[3] www.turkishminute.com/2016/09/14/turkish-minister-indicates-purges-continue-bylock-users/

3- A senior Turkish official told Reuters "The ByLock data made it possible for us to map their network -- at least a large part of it", "What I can say is that a large number of people identified via ByLock were directly involved in the coup attempt." The Turkish official also said ByLock may have been created by the Gulenists themselves so they could communicate.[1]

4- However, in the same news it was said that experts consulted by Reuters were not able to verify that ByLock may have been created by the Gulenists themselves.[2]

5 The other thing is that HSYK said in its public statement on the day of first of November 2016 (01/11/2016) 14 "…according to the information obtained from the authorities and the public open source, the application of ByLock has not been used since February 2016 by the member of organization (referring FETÖ)."[3]

6- According to the news of The Wall Street Journal senior Turkish intelligence officials said that " in the months before Turkey's failed coup, the country's spy agency penetrated online chat rooms and decoded millions of secret messages but found no mention of the plot, None of the ByLock messages referred to a coup plot."[4]

So, if this is true, how can using and downloading ByLock application be used as the most important evidence of membership of terrorist organization.[5]

7- Abdurrahman Dilipak, whose word is respected in the environments that are linked to the political power wrote that the Bylock was used in the 15th July coup attempt but the application was removed 4 months ago as it can be seen in the technical reports.[6]

12. THE EXAMPLES ABOUT THE PEOPLE WHO ARE CLAIMED TO USE BYLOCK BUT PROTECTED

Some claims were made saying that there are MP's from all political parties in the parliament who uses the application.[7]

In some of the websites, even the names of the MP's who allegedly used the application were shared.[8]

---

[1] www.reuters.com/article/us-turkey-security-app-idUSKCN10E1UP

[2] www.reuters.com/article/us-turkey-security-app-idUSKCN10E1UP

[3] www.hsyk.gov.tr/DuyuruOku/930_basin-duyurusu.aspx

[4] www.wsj.com/articles/turkeys-powerful-spy-network-never-saw-coup-coming-1469823062

[5] tsjustice.info/wordpress/2016/11/08/crime-use-bylock/

[6] www.timeturk.com/15-temmuz-da-bylock-tan-emriniz-var-mi-diye-abilerini-arayan-siyasiler-belediye-baskanlari-biliniyor/haber-303241

[7] www.yenicaggazetesi.com.tr/milletvekilleri-de-bylock-kullaniyormus-146765h

[8] www.dilekhaber.com/haber/iste-bylock-kullanan-akp-milletvekilleri-340/

a. Mithat Sancar, the MP of HDP Mardin stated that "We demanded that the list of users of Bylock among the politicians should be requested from the NIA, but it was denied."

"I was a member of the Commission of Investigating the Coup. We expressed our claims and opinion during the commission meetings. All our requests were denied about uncovering the political branch of the coup. For example, we demanded that the list of users of Bylock among the politicians should be requested from the NIA. Only the politicians, not everyone. Our demand was denied. We said "Let's see sho uses it, MPs, the Ministers, the Councilors, the Mayors. We wanted to see if there are people among us as well. But our requests weren't accepted."[1]

b. Ahmet San, the brother-in-law of Tahir Akyürek, the mayor of Konya, was detained in 22 August 2017 but released from the Police Office without being sent to the Prosecution.[2] Although this, the Police Office reported in 7 November 2017 that Ahmet Şan's mobile phone didn't have Bylock installed.[3]

c. The Former General Director of TRT and the Governor of Samsun, İbrahim Şahin, was claimed to be a user of Bylock, the communication network of FETO. According to the special news of superhaber.tv, it was detected that Şahin used FETO's secret communication network "Bylock" after the investigation made by the Office Of The Chief Prosecutor.[4]

Despite this, there wasn't any detention or arrest about him. After the investigation which is done when Abdurrahman Keskin made an indictment about İbrahim Şahin to be a member of the FETO armed terrorist organization, it was stated in the investigation file of the Prosecution that the Bylock software was found in Şahin's phone: " It was determined by the Police Office that In 5 January 2016, the Bylock software was installed via the mobile number 0532 788 63 .. but there wasn't any content such as messages, mails etc. "

d. The Former head of the Association of Judges and Prosecutors (YARSAV) , Ömer Faruk Eminağaoğlu shared the list of 66 people which was written by Nejat Kumbasar with the titled "THE FULL LIST OF THE POLITICIANS OF AKP THAT USED BYLOCK" but there is no investigation or legal procedure about any of them.[5]

[1] odatv.com/mecliste-cok-carpici-bylock-reddi-2410171200.html

[2] t24.com.tr/haber/konyaspor-baskani-bylocktan-gozaltina-alindi,423025

[3] tr.sputniknews.com/turkiye/201711071030909888-polis-rapor-eski-konyaspor-baskan-telefon/

[4] www.medyatava.com/haber/trt-eski-genel-muduru-ve-samsun-valisi-icin-bylock-iddiasi_144991

[5] twitter.com/eminagaoglu/status/914108825313189888, http://odatv.com/samil-tayyar-kime-o.-cocugu-dedi-3009171200.html

13. THE UN, EU AND BYLOCK

a- From the report of David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression :

Criminalization of encryption

Several examples were brought to the attention of the Special Rapporteur of arrests for the alleged use of an encrypted messaging app, called ByLock. The authorities have linked ByLock to the Gülen movement, claiming that it is a secret communication tool for Gulenists. The arrests take place sometimes merely on the basis of the existence of ByLock on a person's computer, and the evidence presented is often ambiguous. Reportedly, the MIT obtained a list of global ByLock users that has been used to track and detain persons. Tens of thousands of civil servants reportedly have been dismissed or arrested for using the application.[1]

b- EU Anti-Terror Chief KERCHOVE "As for FETO, we don't see it as a terrorist organisation, and I don't believe the EU is likely to change its position soon," Kerchove said, using the Turkish government's acronym for Gulen's network. You need not only circumstantial evidence - like just downloading an app - but concrete substantive data which shows that they were involved...," he told Reuters in an interview cleared for publication on Thursday.[2]

c- As noted by UN Special Rapporteur on freedom of expression in a 2015 report, "encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks." Clearly, the mere use of encryption cannot be considered a criminal behaviour.[3]

d - UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein "it is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a Government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental human rights."[4]

e-The United Nations' Working Group on Arbitrary Detention (WGAD), which works under UN Human Rights Council, has called on Turkish government to immediately release police superintendent Kürşat Çevik who are arbitrarily arrested and still kept in Şanlıurfa prison.

The verdict states that Turkey has violated Articles 9, 10 and 11 of the Universal Declaration of Human Rights and Articles 9, 10 and 14 of the International Covenant on Civil and Political Rights.

---

[1] t.co/yi0741iSoz?amp=1 page 14

[2] mobile.reuters.com/article/amp/idUSKBN1DU0DX?__twitter_impression=tr

[3] medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9

[4] medium.com/privacy-international/winning-the-debate-on-encryption-a-101-guide-for-politicians-4ff4353d427

(He was kept in jail for over six months without any formal charges and was not informed of the accusations. Only met four times with his lawyers during the nine months of his deprivation of liberty and that both he and the lawyer have had limited access to the case files to obtain samples from it)[1]

"The indictment stated that he had used a communication programme called "Bylock". The government does not at any point offer evidence that the use of encryption itself is illegal in Turkey. The applicant in this case responded to the government allegation, "The source notes that publicly available knowledge of the use and access to that software is that it has been unavailable for download on the Apple platform since July 2014. Mr. Çevik purchased his phone in the summer of 2015, so it would have been impossible for him to download it. The source notes with concern that his trial has been postponed until 4 July 2017 as the judge is believed to be awaiting further evidence that Mr. Çevik and his co-accused have used the software. In this respect, the source is concerned that such evidence may be fabricated."[2]

14. THE INTERNATIONAL SOCIETY AND THEIR OPINION ON BYLOCK

a- Danish politician from the Liberal Party Michael Aastrup Jensen, who is also the vice chairperson of Alliance of Liberals and Democrats for Europe, said: "Although, on one hand, I salute the Turkish delegation for taking up this issue, I must also say frankly that there are problems in Turkey. There are problems in a democratic country such as Turkey when the fight against terrorism is used as an excuse for labeling a lot of people terrorist sympathizers. We have seen mass arrests of ordinary people, perhaps just because they downloaded a Gülen app or something. That must not stand in a European country that calls itself democratic. That is not the way forward. That only ends up creating a breeding ground for terrorist organizations and radical views, and it must stop." Jensen highlighted an absolutely terrific point that tens of thousands of people are locked up in Turkey because they downloaded a WhatsApp-like messaging application called ByLock that was publicly available on Google Play.[3]

b- "Lumping together all ByLock users and anyone who contacts them as criminals is totally illegal," said Johann Bihr, the head of RSF's Eastern Europe and Central Asia desk. "The judicial authorities cannot accuse journalists on the basis of this app alone, without establishing a specific and individual link to criminal activities."[4]

---

[1] (Human Rights Council Working Group on Arbitrary Detention Opinion No. 38/2017 concerning Kursat Çevik (Turkey))

[2] medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9

[3] www.turkishminute.com/2017/07/03/opinion-erdogans-terrorists-in-turkey

[4] www.rsf.org/en/news/journalists-new-wave-arrests-turkey

c- Germany's best-selling Weekly Computer Magazine (434,030 Baski) was published by Computer Bild on 16.09.2017 head of Germany Association of Journalists Prof. Dr. Frank Überall :

Many people in Turkey (citizens, journalists and dissidents) face the court because of ByLock.

* ByLock: trap for dissidents *

ByLock messaging application from 2014 was for android and iOS. Especially Turkey was popular in Saudi Arabia and Iran. In Turkey, especially opponents use this encryption program because they encrypt the correspondence. In MIT 2015, the Lithuanian server hacker (serverda had a list of ByLock users- unfortunately the list on the server was unencrypted), then ByLock users were followed up by the government. Also, even if the program was deleted from the phone, the program left a mark in the user profile of the phone and could be detected again.

* ByLock users generally suspect *

Even using ByLock- no matter what the reason- is enough for people to be suspicious in Turkey. According to the news agency of the state, Anadolu News Agency, it is claimed that the users are the Teror Organization which is connected with the Gülen Movement. Turkish government to live in the USA for the 2016 coup attempt Fethullah Gulen is responsible.

*ByLock- an alternative to Skype and the like ByLock was announced by American-born American citizen David Keynes. In an interview Keynes said that the application was made so that he could communicate in an encrypted manner among the opponents on the smile sympathizers. But Turkish journalists also use this program to share information about prosecutors and security units.

* Football Star is under arrest for ByLock *

Drinking is seriously criticized. President of the German Gazetagi Union, President Frank Überall wants immediate release of arrested journalists. "In Turkey, the last remnants of the rule of law were the paranoids of the State President Erdogan and his followers," he added. Finally, National Goalkeeper Ömer Catkic has been arrested for his laughing act - allegedly using ByLock himself.[1]

d- Member of @europarl_en Co-Chair Euronest Assembly At home in Germany & Europe Rebecca Harms @RebHarms

"The report by @foxit on ByLock and the accusations in turkish trials shows how bizarr the indictments are. "[2]

"Must read: @foxit investigation of MIT report on #ByLock , the basis for detention of 75.000 people #Turkey @cumhuriyetgzt @WashingtonPoint"[3]

---

[1] romanyahaber.com/2017/10/14/computer-bild-bylock-iddialarini-inceledi-sacma-suphe/

[2] twitter.com/RebHarms/status/923574434404937729

[3] twitter.com/RebHarms/status/918085191704465408

" The new report by @FreedomHouseDC on The Freedom of the Internet in #Turkey2017 just another must read #ByLock @foxit @cumhuriyetgzt "[1]

e- Kenneth Roth Executive Director, Human Rights Watch @KenRoth

" Despite Erdogan's claims, it violates rights for Turkey to detain people for downloading a popular encryption app" . link: http://bit.ly/2fEDJqm)[2]

f- Serena Tinari Investigative Journalist // co-president @investigativ_ch // proud co-founder @serenatinari

" Jailed for 7 years, 6 months for using an encrypted App, for being followed on Twitter and for being a young journalist. Shame on you #Turkey the world biggest journos jailer. Free Parıldak. #journalismnotacrime "[3]

g- Matthew Green, teach cryptography at Johns Hopkins.
MDblog.cryptographyengineering.com @matthew_d_green

"Turkey has 100,000 people under arrest for downloading a free encrypted messenger off Google Play. Do not draw lessons from Turkey."[4]

ı- The Tor Project @torproject

"This is a major human rights breach - thousands in Turkey were arrested for downloading an encrypted messaging app" (link: https://www.theguardian.com/world/2017/sep/11/turks-detained-encrypted-bylock-messaging-app-human-rights-breached) theguardian.com/world/2017/sep… [5]

j- Angsuman Chakraborty Software Architect, Entrepreneur Founder:

@angsuman "Turkey arrested 75K citizens for downloading encrypted messaging app ByLock " [6]

k- Sejal Parmar Senior Adviser Assistant Professor of Law @ceuhungary

Vienna, Austriapeople.ceu.edu/sejal_parmar

"Turks detained for using encrypted app 'had human rights breached' #Turkey #HDIM2017"[7]

l- Sarah McLaughlin Free speech advocate with @theFIREorg.

@sarahemclaugh

---

[1] twitter.com/RebHarms/status/931084006908678144
[2] mobile.twitter.com/KenRoth/status/911076364618424320
[3] twitter.com/serenatinari/status/933079749898973185
[4] twitter.com/matthew_d_green/status/919269688852533248
[5] twitter.com/torproject/status/907677742690439171
[6] www.twitter.com/angsuman/status/907939341778935808
[7] www.twitter.com/_SejalParmar/status/907511716195569664

"Turkey is now arresting journalists for simply using an encrypted messaging app. Madness."[1]

m- Aral Balkan Cyborg rights activist (cyborgrights.eu) Desig

ner (not decorator). @aral

" People are being imprisoned as we speak in Turkey just for using an encrypted chat app called ByLock. Why we need (link: https://cyborgrights.eu) cyborgrights.eu " [2]

n-Thorsten Benner Co-Founder & Director, Global Public Policy Institute (@GPPi) Berlingppi.net/team/thorsten-…@thorstenbenner

" Turkey, where using encrypted app incriminates you: "All of suspects reportedly users of ByLock messaging app" 47 academics and civil servants detained over suspected Gülen links[3]

o- Kevin Collier BuzzFeed News cybersecurity correspondent. From West Virginia.

"Main evidence is they used an encrypted messaging app. Turkey stays two steps ahead in the slide to dystopia. " [4]

p- AlonBenMeir Professor at @NYUCGA, Fellow @WorldPolicy. @TheWorldPost, @Jerusalem_Post contributor. Analyst on Mid-East politics focusing on negotiation/conflict resolution. @AlonBenMeir

" Conspiratorial mindset is so pervasive in #Turkey even those w/ common encrypted messaging apps on their phones are at risk of being jailed " [5]

r- Lucy Purd on Policy Officer @privacyint, puzzling over the future of human rights & tech.

@LucyPurdon

@AmosToh adlı kullanıcıya yanıt olarak

" Did #Turkey mention the "proof" they have that journalists (and thousands of others) are terrorists is that they used encryption?" [6]

s- Amnesty pointed out that downloading ByLock should not of itself be a crime since the app had been downloaded over [7]

---

[1] www.twitter.com/sarahemclaugh/status/895683862319292416

[2] www.twitter.com/aral/status/891727366409551873

[3] hurriyetdailynews.com https://twitter.com/thorstenbenner/status/884831096256507904

[4] www.twitter.com/kevincollier/status/840017994780684289

[5] www.twitter.com/AlonBenMeir/status/831269308315607040

[6] www.twitter.com/LucyPurdon/status/874289708779659264

[7] www.t.co/joJgseAp3P

15. FAMOUS PEOPLE WHO ARE ARRESTED, INVESTIGATED, RECEIVED IMPRISONMENT BECAUSE OF BYLOCK

1- Doğan Holding's Ankara Administrartive representative Barbaros Muratoğlu was arrested on Dec.2016 on charges of aiding Gülen Movement. Among the main reason of his arrest was making phone calls with lawyers and civil servants who were alleged to use a free Googleplay & Apple Stores messaging application called ByLock. Because of this accusation The İstanbul Court sentenced Murat Barbarosoğlu to 2 years and 1 month.[1]

2- Judge Sefa Akay was detained and charged weirdly to be a "member of terrorist organisation" for reason of using the ByLock messaging application. According to some of the news appeared in the media, in his defence, he stated that he was a Freemason and he downloaded the application from Google Play Store after recommended by the Foreign Minister of Burkina Faso and was using it for some Masonic correspondence. Judge Aydin Sefa Akay has been sentenced to seven years and six months for membership of an alleged 'Gulenist Terrorist Organisation' (FETO) which the government insists exists. He has been provisionally released pending the outcome of his appeal process. As Akay's passport has been forfeited and banned from leaving the country as a judicial precaution, he will not be able to leave Turkey.[2]

3- "Use of ByLock was also the sole reason the Turkish police gave for the arrest of Amnesty's Turkey Chair ,Taner Kılıç" [3]

4- 35 Journalists; The Turkish police carried out a new wave of arrests this morning under a combined warrant issued today for 35 journalists and media workers suspected of installing the encrypted messaging app ByLock on their smartphones.... In practice, the judicial authorities tend to criminalize any link with ByLock users, as they have in the case of Cumhuriyet columnist Kadri Gürsel.[4]

5- TV Anchor Fatma Karaağaç was fired for downloading an encrypted messaging application possibly faces imprisonment.[5]

SOME WELLKNOWN FOOTBALLERS TAKING HIS SHARE FROM MASS ARRESTING OF ByLock

1- Bekir İrtegün, who played at famous footbal clubs such as Fenerbahce and Basaksehir, is a national footballer. İrtegün is accused of using a messaging application called ByLock that is available to anyone on Google Play and Apple Store. Ultimately, he has also became a ByLock victim by being detained.[6]

---

[1] www.milliyet.com.tr/dogan-holding-temsilcisinin-feto-gundem-2363507/

[2] www.platformpj.org/another-victim-turkeys-witch-hunt-un-judge/

[3] www.eff.org/tr/deeplinks/2017/07/global-condemnation-turkeys-detention-innocent-digital-security-trainers

[4] https://rsf.org/en/news/journalists-new-wave-arrests-turkey

[5] www.internethaber.com/unlu-spiker-bylocktan-isten-atildi-foto-galerisi-1760482.htm

[6] www.sozcu.com.tr/2017/gundem/bekir-irtegun-kimdir-neden-gozaltina-alindi-bylock-mu-kullaniyor-1950805

2- Omer Catkic, who played at plenty of famous football clubs in Turkish Super League, is an old national goalkeeper. He was arrested recently because of using a messaging application called ByLock that is available to anyone online, and paying money in Bank Asya. He is anymore a ByLock victim.[1]

3- Zafer Biryol, who played at the most famous football clubs such as Fenerbahce, is an old national footballer and a football coach now. He was newly arrested due to using a messaging application called ByLock that is available to anyone on Google Play Store and Apple Store, and paying money in Bank Asya. He is last ByLock victim from football world.[2]

4- It is not false to say the fact that Hakan Sukur is one of the most important figures in Turkish football history. Sukur gained great successes both in Galatasaray, winning UEFA cup sole club in Turkey, and in Turkish National Football Team. He was also a parliamentariar. Though, he also couldn't avoid being a ByLock victim. Jokosely, he is accused of not only using a messaging application called ByLock that is available to anyone online but also being one of whom using it maximum.[3]

16. THE TRAGEDY IN TURKEY BECAUSE OF BYLOCK

There is no official statement regarding how many of the investigations to the people that have allegedly ties with the Gulen Movement are directly associated with Bylock. But still, almost all dismissals, detainments and arrests starting from October 2016 (when the procedural acts for Bylock have been initiated) are made for using Bylock application. Because of this, the Bylock victimhood is clear to see when you look at the data of the year 2017.

According to the official numbers of July 2017, 142.648 people were dismissed from public service after the coup attempt in July 15th 2016. 33.506 of them were returned to their duties but 109.142 people lost their jobs after the coup.[4]

The Minister for Internal Affairs, Süleyman Soylu, announced that 48.305 people were arrested at the end of the FETO operations in 2017 in the press conference in 09.01.2017. [5]

In the statement of the Ju stice Department in 22.10.2017 , it is stated that totally 49.697 people are in jail, 8.997 people have been issued a warrant and 738 people are in custody.[6]

---

[1] www.fanatik.com.tr/2017/08/28/eski-milli-kaleci-omer-catkic-tutuklandi-1315742

[2] www.hurriyet.com.tr/gundem/son-dakika-unlu-futbolcu-fetoden-tutuklandi-40670012

[3] www.yeniakit.com.tr/haber/hakan-sukur-bylocku-en-cok-kullanan-fetocu-224621.html

[4] www.diken.com.tr/feto-bilancosu-50-bin-tutuklu-105-bin-sanik-9-bin-firari-109-bin-issiz/

[5] www.haberler.com/genel-guvenlik-ve-uyusturucuyla-mucadele-10436262-haberi

[6] www.memurlar.net/haber/702257/adalet-bakanligi-ndan-feto-operasyonlari-bilancosu.html

The number of the users is 265 thousands according to the Ministers of Erdogan. In the first indictment prepared by the Office of Chief Public Prosecutor of Istanbul, the number of registered users of Bylock was stated as 215.92.[1]

The number was decreased to 91 thousand people on December 2017 without knowing how and why. According to the data stated, **it can be accepted that approximately 50 thousand people are in jail and 41 thousand people haven't been investigated yet.** Among those prisoners, there are 17 thousand women who allegedly used Bylock and 624 babies who are in need of nursing by the date 11.01.2018. Even the women who recently gave birth are being taken into custody even before being discharged from the hospital.[2] Arrests continue in July 2018.

It was stated that there are more than 50 suicide cases among the police, officers, judges and prosecutors who are dismissed from their duties because of the claims of using Bylock.[3]

The cases of suicide in jails have reached the number of 40 since 15.07.2016 according to the MP from CHP, Barış Yarkadaş.[4]

Although Bylock is a free communication app that could be found on Google Play Store and Applestore, 50 thousand people got arrested without any additional investigations by the judiciary of Erdogan. The lives of tens of thousands of people who never heard of Bylock became destroyed because the list of the NIA is considered as true and clear evidence. **The list of NIA was updated a few times and the number of the people was decreased to 91 thousand by removing 11.480 people from the list on December 2017. It was later understood that 4 people who were among those 11.480 people killed themselves.[5]**

Hüseyin Maden, who was a 40-years-old Physics teacher , Nur Maden (36), his wife who was a kindergarten teacher, their children Nadire (13), Nur (10) and Feridun (7) got drowned in the Aegean Sea while trying to escape from the country to the Greece because of this unjust persecution.[6] Also the teachers Ugur Abdurrezzak, his wife Ayşe and their children Münir (3) and Enes (11) died similarly when they were sought in Turkey because of Bylock.

Mehmet Safi Ceter was arrested for 16 months while he was serving as an officer because of being a user of Bylock while he never used it. The Prosecution stated that he didn't use it but he wasn't returned to duty still.

Emre Öztürk was first dismissed and then arrested while he was serving as a Music teacher. He was under arrest for 6 months and then released without any explanation.

---

[1] www.hurriyet.com.tr/bylock-icin-ilk-iddianame-215-bin-92-kullanici-var-40342896

[2] www.tr724.com/hastanede-oda-basan-polis-yeni-dogum-yapan-anneyi-yataga-kelepceledi/

[3] www.khkliplatformu.com/khklilarda-50den-fazla-intihar-vakasi.html

[4] www.evrensel.net/haber/335711/yarkadas-ohalde-en-az-kirk-kisi-cezaevinde-intihar-etti.

[5] www.haberdar.com/gundem/hatali-bylock-listesinde-adi-olan-4-kisi-daha-once-intihar-etti-h74216.html

[6] www.shaber3.com/maden-ailesinin-huzunlu-hikayesi-haberi/1293247/

Only one example is enough to picture how great is the victimhood in fact; Şükrü Önder, a former MP from AKP was arrested in 02.06.2017 and sentenced for imprisonment in 29.11.2017 for 6 years and 3 months. He was then released on December 2017.

There are thousands of people now who say that they were left to starvation, dismissed from their jobs, kept apart from their family for months and announced as traitors and terrorists and then were apologized just like nothing happened. It shouldn't be that easy.[1]

In conclusion, more than 100 thousand people became unemployed because a simple communication app is considered as absolute evidence for being a member of a terrorist organization and they were left to starvation by blocking any way that they can find a job. There are 50 thousand arrests and probably 40 thousand more in the future just for using Bylock and they got sentenced for imprisonment between 7.5 and 15 years.

17. THE LIST OF RESPECTED ANALYSIS AND REPORTS ABOUT BYLOCK

A- TECHNICAL REPORTS

1- An Independent technical report by Daniel Walter about ByLock application http://na-copywriting.com/2017/05/the-bylock-report/

2- An Independent technical report by a Forensic Company about ByLock application http://bylockreality.com/index.php/technical-reports/an-independent-technical-report-by-a-forensic-company-about-bylock-application

3- Dutch IT firm debunks Turkish intel report on ByLock that put 75K Turks behind bars https://blog.fox-it.com/2017/09/13/fox-it-debunks-report-on-bylock-app-that-landed-75000-people-in-jail-in-turkey/amp/

B- THE NEWS

1- Scandal answer from the judge

http://bylockreality.com/index.php/news/108-news/269-scandal-answer-from-the-judge

2- An overview about illegality of using ByLock application as evidence in trials https://t.co/8gBQgUlGeZ

3- AKP set up fake ByLock content produce team

[1] www.memurlar.net/haber/722421/darbeden-sonra-ilk-besteyi-yapmisti.html

http://bylockreality.com/index.php/news/108-news/272-akp-set-up-fake-bylock-content-produce-team

4- "No doubt that Turkey has breached the Convention rights of those arrested and detained since the failed coup.." https://t.co/ThuS3EG1cO

5- Turks detained for using app 'had human rights breached'

https://amp.theguardian.com/world/2017/sep/11/turks-detained-encrypted-byloc

k-messaging-app-human-rights-breached

6- ".. cannot accuse journos on the basis of this app alone, without establishing a specific and individual link to criminal activities."

https://rsf.org/en/news/journalists-new-wave-arrests-turkey

7- International Documents Medya Les journalistes turcs visés par une nouvelle vague d'arrestation

http://bylockreality.com/index.php/news/108-news/276-international-documentsmedya-les-journalistes-turcs-vises-par-une-nouvelle-vague-d-arrestation

8- The Erdogan regime is using ByLock app to sweep away its oppponents like Amnesty Turkey Chair Kiliç @UN Judge Akay ..etc https://t.co/qP5V4nQfZB

9- HRC 36: Secure digital communications in Turkey are essential for human rights https://www.apc.org/en/pubs/hrc-36-secure-digital-communications-turkey-are-essential-human-rights

10- The guardian Tens of thousands of people have been arrested or dismissed from officein a wide-ranging crackdown since the coup https://t.co/wXLoNL8eJF

11- The Erdoğan Government has jailed over 50,000 people on trumped-up terror charges in the last 11 months alone.

https://t.co/s0FYIWoiAv

12- http://www.informationsecuritybuzz.com/expert-comments/amnestys-turkish-chair-trial-post-coup-crackdown-allegations-downloaded-bylock-app/

13- in Turkey, thousands of smartphone owners were arrested simply for having downloaded the encrypted communication app ByLock, which was available publicly through Apple and Google app stores, amid allegations that the app was used by those involved in the failed July 2016 coup attempt. https://freedomhouse.org/report/freedom-net/2017/turkey

C- LEGAL OPINIONS

1- Turkish Police Say No Basis To Arrest People Over ByLock App

http://bylockreality.com/index.php/legal-opinions/109-legal-opinions/279-turkish-police-say-no-basis-to-arrest-people-over-bylock-app

2- Opinion on the Legality of the Actions of the Turkish State in the aftermath of the failed coup attempt in 2016 and the Reliance on Use of the ByLock App as evidence of membership of a terrorist organisation

https://www.2bedfordrow.co.uk/opinion-on-the-legality-of-the-actions-of-the-turkish-state/

3- UN Judge Akay has been sentenced to 7,5 years imprisonment on the grounds of using this comm. app.

http://www.platformpj.org/opinion-observations-bylock-app-arrest-un-judge-sefa-akay/

4- "Use of ByLock was also the sole reason the Turkish police gave for the arrest of @amnesty ' s Chair ,T.Kılıç" https://www.eff.org/tr/deeplinks/2017/07/global-condemnation-turkeys-detention-innocent-digital-security-trainers

5- An article via Justice at Swiss Supreme Court Thomas Stadelmann about @BylockReality http://tsjustice.info/wordpress/2016/11/08/crime-use-bylock/

6- The legal opinion submitted by By W. Clegg QC & S.Baker That ByLock Arrests Are Farce that ByLock Arrests Are Farce http://www.platformpj.org/report-legal-opinion-published-uk-argues-bylock-arrests-farce/

7- Being arrested for using encryption like being arrested for locking your front door or owning a safe. https://medium.com/@privacyint/encryption-at-the-centre-of-mass-arrests-one-year-on-from-turkeys-failed-coup-e6ecd0ef77c9

8- Sad Story of Independence and Objectivity of the 16th Penal Chamber of the Court of Cassation www.platformpj.org/opinion-sad-story-independence-objectivity-16th-penal-chamber-court-cassation/

9- Understanding ByLock reality

http://www.platformpj.org/opinion-arbitrary-use-bylock-instrument-false-accusation/