Lithuania's responsibility on the intensive, long-term and extensive violations of rights that emerged regarding the Bylock messaging app within the context of IT law

1. Introduction

Bylock is the name of a messaging application which is claimed to be used as an in-group communication tool within a certain period of time by the people who are close to the religious community which is known as "Gülen Community ("cemaat") or "Hizmet Movement[1]" in countries where democracy and rule of law are applied, but named as "FETÖ" by the authorities and institutions of today's Republic of Turkey.

Essentially, **Bylock** is a less popular version of the other global messaging apps such as WhatsApp and KakaoTalk which are produced for means of communication. In other words, it can be described as nothing but a less common version of various messaging apps - during the time it was used -. Of course, given that Bylock has similar features as the other popular messaging apps just like in all similar products produced for the same functions, it also has unique and different technical aspects and functions.[2]

Bylock had two versions. The 1.1.7 sub-version of the first version could be accessed and it is understood that Bylock version 1 was discontinued in December 2014. Later, Bylock++ (series 2) was published and made available for download on Google Play. [3] Later again in March 2016, the application was removed as the costs of the servers of the application which kept the data and ran the application were not paid.[4]

In this text, the legal responsibilities of the State of Lithuania arising from national and international regulations and to what degree Lithuania has fulfilled those responsibilities will be examined as the cloud IT services that are provided globally are liable to Lithuanian regulations and the database and physical locations of the Bylock servers are located in Lithuania and thus, it is within their field of sovereignty.

While the responsibilities of Lithuania arising from national and international IT laws regarding Bylock will be underlined, the topic will be examined within the context of the directives of the European Convention of Human Rights, International Covenant on Civil and Political Rights, Convention on Cybercrime, European Union Information security and other related legal acquis on

---

[1] https://de.wikipedia.org/wiki/G%C3%BClen-Bewegung (15.04.2021)

[2] Bylock Application Technical Report, p. 11; https://foxitsecurity.files.wordpress.com/2017/09/bylock-mit-technical-report-turkish.pdf (Accessed: 13.05.2021)

[3] Bylock Application Technical Report, p. 10, 19, 19; https://foxitsecurity.files.wordpress.com/2017/09/bylock-mit-technical-report-turkish.pdf (Accessed: 13.05.2021)

[4] A Summary of an 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 Messaging Application as Evidence of Membership of a Terrorist Organisation, Thomas K. Moore, paragraph 28.

legal regulations and taking technical precautions that are imposed on member states, which were in effect and binding within the period that Bylock was used and finally, within the context of the directive nr. 95/43/EC which was also in effect and binding within the period that Bylock was used that was within the legal acquis of European Union for the member states in the context of the Law on the Protection of Personal Data.

2. Lithuania's responsibility in terms of the European Convention on Human Rights and European Court of Human Rights

After the coup attempt in 15th of July, 2016 in Turkey, the personal data of hundreds of thousands of people which are stored in the servers located in Lithuania were acquired by the Republic of Turkey and those data were used widely in an illegal way in courts and investigations which were processed illegally and by ignoring the fundamental rights and freedoms of people. Within this context, it is clear and beyond dispute that the IT services regarding Bylock application were provided by the IT systems located in the servers in Lithuania which are owned by Cherry Servers LTD and the data of hundreds of thousands of people from Turkey were kept and processed in those servers. Later on, because of the reasons such as both Lithuanian government and related persons and institutions not taking necessary safety precautions and Lithuanian government not fulfilling their positive obligations from national and international regulations, those illegally-acquired data were and still are used intensively and illegally in Turkey after 15 July 2016 as digital evidence during investigations and prosecutions.

Lithuania is a country which signed the European Convention on Human Rights and the UN International Covenant on Civil and Political Rights and therefore, obliged to fulfill its positive obligations. The personal data are addressed and protected within the protection of private life in accordance with the article 8 of the ECHR.

Hence, in the I. v. FINLAND case decision[5], the question in what context the written positive obligations in those Conventions should be addressed by the signee states is answered. [6]

In the event that is subject to the case I. v. FINLAND, after the application regarding the health data of the applicant who was carrying HIV virus being open for access not only for the health personnel working in that branch but for all the personnel in the hospital, the hospital management restricted access to those records, allowing only the related unit to access them. But the ECHR decided that the art.8 of the ECHR was violated, underlining that the aforementioned precaution is a delayed

[5] Application nr: 20511/03, Date of Decision: 17.07.2008

[6] Atak, S.; The Fundamental Assurances of European Council in terms of Personal Data ("Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler"), p, 117, 188;
http://tbbdergisi.barobirlik.org.tr/m2010-87-606 (Accessed: 13.05.2021) .

precaution and the Finnish legal regulations cannot provide the necessary reassurance in terms of the art. 8 of the ECHR which is about the compensation of the probable losses as a result of revealing personal data and the state did not fulfill its positive obligations in terms of protecting the private data.

Positive obligations are described as ensuring the effectiveness of human rights in social reality, preventing the fundamental rights to be violated by third parties and the necessary precautions that need to be taken by the state in order to effectively benefit from the rights by Harris O'Boyle and Warbrick. Malinverni differentiates between the positive obligations that directly arise from the Convention and the positive obligations that are derived by legal opinion from the qualities of the rights in the Convention and the principles of equality and effectiveness. On the contrary, Schutter explains positive obligations as any kinds of obligations which, in the case of a violation, will not only damage the applicant or a small group but a wide sect and even the whole society. Sudre makes a distinction regarding the positive obligations whether the state failed to act in an event of a violation of rights or whether the state allowed for violation of fundamental rights caused by private persons. In the German literature, the positive obligations are defined and accepted as the fundamental rights that ensure benefiting from the state services or the responsibility to do what is necessary. [7]

In summary, no matter whichever description and opinion is accepted for the case of acquiring Bylock data by Turkey, the chain of actions mean both that Turkey actively and severely violated the ECHR and Lithuania acted passively in violation to the positive obligations of protection imposed by the Convention by not taking precautions and not protecting the personal data stored in its field of sovereignty and fields of private life enough both technically and legally. Therefore, in the case of acquiring Bylock data by Turkey, it did not fulfill its positive obligations imposed particularly by the art. 8 of the ECHR because the European Court of Human Rights did not find it sufficient to only regulate for the protection of private data and requested that the necessary security precautions should be taken within the rules for not causing uncertainties in terms of the officials and asked for the implementation of the aforementioned precautions personally and concretely.

Moreover, the facts that the Law that is regulated by Lithuania to protect personal data was insufficient and it excluded the personal data on Bylock databases were reflected in the decisions of Lithuanian Prosecution Offices. [8]

---

[7] Metin, Y.; The Positive Obligations Regarding Protection of Life and Health Imposed on Signee Countries by European Convention of Human Rights ("Avrupa İnsan Hakları Sözleşmesinin Yaşamın ve Sağlığın Korunması ile İlgili Olarak Taraf Devletlere Yüklediği Pozitif Yükümlülükler"); p. 113; https://dergipark.org.tr/tr/download/article-file/540079 (Accessed: 14.03.2021)

[8] For example, the Decision of Dismissal of Charges with the date 30.05.2017 of Lithuanian Judicial Police Bureau, Important and Organized Crimes Investigation Branch, 5th Committee, 3rd Department and Refusal of Objection Decision of Lithuanian Attorney General's Office with the date 19.06.2017.

On the other hand, Lithuania could not offer evidence regarding having taken the necessary security precautions for protection of private data and implementing them during the related prosecutions.

Similarly, in the decision of Benedict v. Slovenia case, the ECHR decided that the signee states must provide the necessary protection of private data legally and even decided that preparing only legal regulation for this subject is not enough to fulfill this responsibility but those laws must provide clear and sufficient protection.[9] In the same decision, the ECHR reached a court decision that the IP addresses are considered as personal data (Paragraph 108), the police making identification and starting investigations by collecting IP addresses and subscription data without court warrants violates the art. 8 of the Convention (paragraphs 128, 130, 133) as the restrictions do not bear the condition of "lawfulness". In the light of this decision, it can be said that the Lithuanian government cannot leave the responsibility to Cherry Servers LTD and Turkish Authorities and be free of any obligations.

3. In terms of the UN International Covenant on Civil and Political Rights and Decisions of the UN Organizations

According to the UN International Covenant on Civil and Political Rights, art. 17, provision 1, *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."* According to provision 2, *"Everyone has the right to the protection of the law against such interference or attacks."*

This article of the UN International Covenant on Civil and Political Rights makes it as an obligation for the signee states, especially everyone within their field of sovereignty, to provide legal protection against the interventions and violations against their private lives and private data.

Hence, for the purpose of providing guidance to fulfill those obligations, the UN started to prepare the Guidelines for the Regulation of Computerized Personal Data Files in 1976 and later, this document was published on 14 December 1990. [10]

When the case of illegal acquiring of data from Bylock servers is examined, it is understood that Lithuania did not take any effective legal precautions within the Guidelines for the Regulation of Computerized Personal Data Files nr. 45/95 and the personal data of hundreds of thousands of people were not both legally and technically protected as they should be according to the related articles of the UN International Covenant on Civil and Political Rights.

---

[9] https://ciftci.com.tr/wp-content/uploads/2018/05/AI%CC%87HM-Karar%C4%B1.pdf Especially the part between paragraphs 130-135 include significant evaluations regarding this subject.

[10] Akçalı Gür, B.; Transferring Personal Data Abroad in terms of International and European Law ("Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması"), p. 853; https://dergipark.org.tr/en/download/article-file/902576 (Accessed: 14.05.2021)

Those violations of rights related to Bylock which arose from Lithuania not providing sufficient legal and technical protection were also reflected in various organs of the UN. [11]

4. In terms of Lithuanian Constitution and Penal Law

The article 22 of Lithuanian Constitution regulates the immunity of private life. Within this context, the messaging, phone calls, telegraph notifications and all other kinds of communication are immune. The data on personal life can only be collected by justified court decisions and relevant laws. The law and the court ensures that no one is exposed to arbitrary and illegal treatment to their personal and family life, honor and dignity. The law and the court protects everyone against the attempts of arbitrary and illegal treatment to their personal and family life, honor and dignity.

While the provision of the art. 22 of the Lithuanian Constitution is clear, the reason why the Lithuanian State is responsible in the event of the illegal acquisition of Bylock data is the illegal acquisition of the personal data and communication info in the devices of Cherry Servers LTD by Turkish intelligence which needed to be protected by the state as a result of national and international regulations and as a result, victimizing hundreds of thousands of people. These events are not simple judicial cases. The case is beyond the illegal acquisition of personal data, but became a severe crime against humanity and victimized hundreds of thousands of people with the possibility of continuing to be so as a social phenomenon.

The severity of this case requires Lithuanian prosecution offices to implement both the provisions in Lithuanian Penal Code and other legal regulations regarding the subject and punish the responsible persons. Being a sovereign state requires this procedure.

According to art. 4/3 of Lithuanian Penal Code, if any criminal activity is started, finished or interrupted on Lithuanian soil, it is considered as committed in Lithuania. The case is about **the illegal acquisition of data from the devices of Cherry Server LTD.** By acquiring the data from the devices, the activity is finished. Therefore, the crime scene in this case is Lithuania and it is clear that this crime must be investigated by Lithuanian authorities. According to art. 4/1 of Lithuanian Penal Code, the persons who committed crimes on Lithuanian soil will be subjected and punished in accordance with Lithuanian Penal Code.

On the other hand, according to the art. 4/3 of the same Code, a single criminal activity which is committed both on Lithuanian soil and abroad is considered as committed in Lithuania if it is started, finished or interrupted in Lithuania and therefore, the perpetrators of this crime must be punished in accordance with the Lithuanian Penal Code.

[11] https://www.ekicihukuk.net/post/hamzayamanbirlesmismilletlerkarari (Accessed: 14.05.2021)

Within this context, the act of the illegal acquisition of the personal data of the users of Bylock application was committed on Lithuanian soil and the act was finished in Lithuania. In this case, Lithuanian authorities are authorized and responsible for the investigation and prosecution of the committed crimes.

Even if we accept for a moment that those data were transferred to Turkey simultaneously, the act of illegal acquisition of data was started on Lithuanian soil. Therefore, in accordance with the clear provisions on the art. 4/3 of the Lithuanian Penal Code, it is Lithuanian authorities' duty and responsibility to investigate and prosecute the aforementioned crimes.

On the other hand, according to the art. 166/1 of Lithuanian Penal Code, if a person illegally acquires, records or surveillances a person's messages and calls transferred by the electronic communication networks or violates the right of communication with another method, he/she is punished. Similarly, collecting illegal data regarding people's private life is a crime within the context of the art. 167 of Lithuanian Penal Code and it must be punished. Again, within the context of the art. 168/1 of Lithuanian Penal Code, if someone exposes a person's private life without consent for his or someone else's sake by committing the acts described in art. 165-167 of the Law, he/she must be punished.

A person who illegally surveillances, records, acquires, purchases, stores, prepares, distributes or uses people's non-public electronic data in any form is punished in accordance with Lithuanian Penal Code (art. 198/1).

If the data has strategic importance for the national security just like in the case of illegal acquisition of Bylock data, the punishment will be imprisonment up to 6 years. (art. 198/2)

When the aforementioned provisions of the Lithuanian Penal Code are considered, the Lithuanian state has the obligation to implement the regulations and ensure that the perpetrators of this severe crime will not go unpunished for the crimes committed on Lithuanian soil. However, the Lithuanian state did not approach this issue with the responsibility of a state and did not conduct an effective and just investigation.[12] Therefore, Lithuania once again did not fulfill its positive obligation for protecting the fundamental human rights.

[12] Look at, the Decision of Dismissal of Charges with the date 30.05.2017 of Lithuanian Judicial Police Bureau, Important and Organized Crimes Investigation Branch, 5th Committee, 3rd Department and Refusal of Objection Decision of Lithuanian Attorney General's Office with the date 19.06.2017.

5. In terms of the Convention on Cybercrime

In addition, the Convention on Cybercrime (ETS: 185) which was prepared within the European Commission was opened for signature on 23 November 2001 and put into effect on 1 July 2004. The Convention is in force in Lithuania. [13]

In the art. 32 of this Convention, the ways of exchanging digital evidence between countries are clearly regulated.

According to that, in case of authorized or publicized content, cross-border access to the stored computer data is allowed by one of the signees without the consent of another signee no matter where the data is located geographically.

On the other hand, in case a signee provides the legal consent through the mentioned computer data by a computer system within its field of sovereignty, it can access or acquire the stored computer data on the other side.

Evidential data in a country can only be sent abroad or accessed from abroad in those two cases. In our case, none of those two cases can be applied. The prosecution office could not provide in its decision that these procedures are followed. [14]

Except the Convention on Cybercrime, Turkey and Lithuania are signees to the European Convention on Mutual Assistance in Criminal Matters (ETS: 30) which was put into force in 1969 within the European Commission and its protocol no.1. Therefore, the methods of collecting evidence and requesting information and documentation must be aligned with this Convention in penal procedures.

In the field of Law, "Agreement on Legal and Judicial Cooperation in Commercial and Civil Matters" was signed in 1954, of which Lithuania and Turkey are parties. Also, the bilateral agreement between Lithuania and Turkey was also signed for legal and commercial cooperation.

As it is seen, the cooperation agreements already exist for tens of years between Turkey and Lithuania in terms of penal law and the cooperation for legal evidence is maintained in accordance with the aforementioned Conventions and agreements.

The common point of the above-mentioned international agreements is that they all contain regulations on how the requests for legal or procedural documents, information and data should be made. In the case of the illegal acquisition of personal data of Bylock, none of the procedures and

---

[13] Lithuania signed the Convention in 23/06/2003 and approved it in 18/03/2004. https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/lithuania/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB (Accessed; 14.05.2021)

[14] Look at, the Decision of Dismissal of Charges with the date 30.05.2017 of Lithuanian Judicial Police Bureau, Important and Organized Crimes Investigation Branch, 5th Committee, 3rd Department and Refusal of Objection Decision of Lithuanian Attorney General's Office with the date 19.06.2017.

methods in the mentioned agreements and conventions were followed.

Even worse, Arvydas Anusauskas, who is a member of the parliament of Lithuanian Republic and also a member of the National Security and Defence Committee posted an update in his own Facebook account on 31 January 2017. In this post, the following are underlined: "Turkish authorities prepared a new list of possible suspects by using the userlist of Bylock mobile messaging app while coping with the "cemaat" which is managed by Fethullah GÜLEN whom they thought to have organized the coup attempt on 15 July 2016. The National Intelligence Organization ("the MIT") detected 18 million messages and 3.5 million e-mails on the server that is located in Lithuania. In September 2016, "Hürriyet Daily News" declared that the cyber team of the MIT accessed this server illegally and transferred all the data on this server to Ankara. The MIT officials identified 165.178 people out of a total number of 215.920 recorded accounts. Lithuanian officials declared that they decided to cooperate with Turkey in this matter after the Government of Turkey accused GÜLEN Movement for the assassination of the Russian Embassy Karlov in November 2016. After the assassination, it is claimed that the Lithuanian officials informed Turkey about 150.000 more Bylock users and the Turkish officials updated their suspect list regarding GÜLEN Movement afterwards.

When it is considered that the parliament member Arvydas Anusauskas, who published this notice and who is a member of the National Security and Defence Committee and the fact that Lithuanian authorities might have known about the cooperation with the Turkish authorities and when the subject is evaluated with the other issues in this text, it is quite possible for the Lithuanian state to have a responsibility far beyond the obligation of protecting only the fundamental rights in the event of the illegal acquisition of the personal data stored in the Bylock database.

6. In terms of Data Protection and related legal acquis

Another point that Lithuania did not pay attention to regarding the event of the illegal acquisition of the personal data stored in Bylock database is the legal acquis of the EU regarding Data Protection and legal regulations arising from that.

The Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) which was in force at the date of the event gives the obligation to the national regulatory authorities **to take the necessary precautions to protect the security and integrity of the data in the systems which was served by the public electronic communication networks or public electronic communication service providers** and when necessary, to inform a central agency which will be established in case of any security breach or integrity loss that will affect the operation of the networks.

Again, the Directive 2002/58/Ec Of The European Parliament And Of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) which was in force at the date of the mentioned event demands from the member states to take necessary technical and organizational precautions to protect the security of the IT and communication services and to protect the privacy of the relevant traffic data and public electronic communication services.

Also, the Directive 2002/58/EC requires the notification of the relevant authorities in cases of the violations of personal data for the electronic communication service providers.

The Directives of 2002/21 and 2002/58/EC were legally regulated within the Law of Electronic Connections[15] by the Republic of Lithuania. The art. 8 of this Law indicated the purpose and responsibilities of the Institution of Regulating Communication which is established by this Law. Among these responsibilities, the following duty was given to this institution in the provision nr. 9: "Ensuring that the providers of the public communication networks and / or the common electronic communication services to take the necessary technical and organizational precautions to provide the security and integrity to the common electronic communication services and / or the public communication networks."

However, in practice, neither the Directive 2002/21/EC nor the Directive 2002/58/EC were taken into consideration by Lithuania in the event of the illegal acquisition of personal data stored in Bylock database. Likewise, there is no indication that any regulations, check and balance mechanisms or necessary technical and organizational precautions are taken by Lithuania to ensure that the security and integrity of the public communication networks of Bylock servers and / or the common electronic communication services. There is no information for this context in the prosecutions as well. [16]

All these issues indicate that Lithuania did not fulfill its obligations arising from the legal acquis that was in force at the date of the event regarding the Data Security and legally responsible in the event of the illegal acquisition of personal data in Bylock database.

7. In terms of the regulation of protection of private data and Directive of 95/43/EC

The Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data was accepted in 1995. The main purpose of this Directive is to integrate the regulations in the

[15] (lit. Lietuvos Respublikos elektroninių ryšių įstatymas)

[16] Look at, the Decision of Dismissal of Charges with the date 30.05.2017 of Lithuanian Judicial Police Bureau, Important and Organized Crimes Investigation Branch, 5th Committee, 3rd Department and Refusal of Objection Decision of Lithuanian Attorney General's Office with the date 19.06.2017.

member states regarding data protection.[17] The EU member states, including Lithuania, had to organize their regulations related to data protection in accordance with this Directive and they actually did so.

According to the art. 1 provision 3 of the Law of Protection of Personal Data which was put in force within the context of the Directive 95/43/EC, this Law will be applied for the processing of personal data in the following events;

1) personal data is processed by a data controller or data processor with establishment located in the Republic of Lithuania, in the course of its activities, regardless of whether data are processed in the European Union or not;

2) personal data is processed by a data controller established outside the Republic of Lithuania and which is bound by the laws of the Republic of Lithuania in accordance with international public law (including diplomatic missions of the Republic of Lithuania and consular posts);

3) personal data of data subjects in the European Union are processed by a data controller or data processor established outside the European Union which has appointed a representative established in the Republic of Lithuania in accordance with Article 27 of Regulation (EU) 2016/679 and data processing activity relates to offering the goods or services for these data subjects in the European Union, irrespective of a payment of the data subject is required for these goods or services, or monitoring of behaviour when these data subjects operate in the European Union. **In the situation described here, the data controller must have a representative office or an established branch in the Republic of Lithuania.**

As the personal data are processed and stored in the devices in Lithuania which is a member of the EU, both the Lithuanian and EU regulations on protection of personal data should be applied in the concrete Bylock dispute. According to our opinion, the rule in Lithuanian Law which is applied for data controllers for the companies with representative offices, branches or established offices is both against the Lithuanian Constitution and the principles of the Directive 95/43/EC. When considered the wide IT infrastructure provided within cloud technologies to both its field and worldwide by Lithuania, this regulation takes a significant part of the personal data out of the law of protection of personal data, which clearly violates Lithuanian Constitution, the ECHR and the UN Convention on Civil and Political Rights. Therefore, the Lithuanian State was insufficient in protecting the persona data of hundreds of thousands of people which were acquired illegally from Bylock database and, **so to speak, did not even lift a finger,** and therefore, acted completely against its obligations arising from its national and international agreements and regulations.

[17] https://www.kvkk.gov.tr/Icerik/4183/Kisisel-Verilerin-Korunmasi-Alaninda-Uluslararasi-ve-Ulusal-Duzenlemeler (Accessed; 14.05.2021)