INFO- 2206 UDK: 007:343(560)
Primljeno/Received:2019-05-31 Authors Review/Pregledni rad

10.32914/i.52.1-2.7

ISSUES OF INFORMATION TECHNOLOGY CRIME CONTROL IN THE REPUBLIC OF TURKEY

PITANJA KONTROLE INFORMACIJSKE TEHNOLOGIJE U REPUBLICI TURSKOJ

Aliya Shukan[1], Aitugan Abdizhami[2], Gulnar Ospanova[2], Dana Abdakimova[2]
Kazakhstan Humanitarian Law University, Astana, Republic of Kazakhstan [1]; Department of Legal Disciplines, Academy Bolashak, Karaganda, Republic of Kazakhstan [2]

Abstract
The problem of cybercrime is a problem not only of domestic character but also of the whole world. Therefore, we decided to consider the experience of other countries in combating cybercrime. The article discusses the policy issues of the Turkish Republic in the field of combating the cybercrime. And also it was considered the experience of the police organizations work in this field in Turkey. The article analyzed the legislative framework of the Turkish Republic on the fight against cybercrime. The history of the development of police organizations and their work in this area was investigated and described in detail. The article also contains information about the policy of continuous education of employees on the fight against cybercrime and there was shown a scheme of work in the field of education. According to the results of the study we can confidently say that Turkey is currently doing effective work in combating cybercrime. The experience in this field can be used in the CIS countries and other countries to effectively combat crime in the field of information technology.

Sažetak
Problem cyber kriminala je problem ne samo domaćeg karaktera, već i cijelog svijeta. Stoga smo odlučili razmotriti iskustva drugih zemalja u borbi protiv cyber kriminala. U članku se raspravlja o političkim pitanjima Turske Republike na području borbe protiv kiberkriminaliteta. Također se smatralo da iskustvo policijskih organizacija na tom području u Turskoj. U članku je analiziran zakonodavni okvir Turske Republike o borbi protiv kibernetičkog kriminala. Povijest razvoja policijskih organizacija i njihov rad na ovom području istražena je i detaljno opisana. U članku se također nalaze informacije o politici kontinuiranog obrazovanja zaposlenika o borbi protiv kibernetičkog kriminala te je prikazana shema rada u području obrazovanja. Prema rezultatima studije možemo pouzdano reći da Turska trenutno radi na učinkovitom radu u borbi protiv kibernetičkog kriminala. Iskustvo u ovom području može se koristiti u zemljama ZND-a i drugim zemljama za učinkovito suzbijanje kriminala u području informacijske tehnologije.

1. Introduction

Over the past two decades the Internet has become the fastest growing sector of the world. This sector can be viewed as a democratic or even anarchic platform which has no specific boundaries of control. This is the space where the moral foundations of society are largely violated /**1**/. For example, citizens of any other country without disclosing their personal data are free to express themselves and their thoughts on the Internet space.

The intensive development of technology and the Internet has turned the world into a "small village" with many new "habits", such as computerized video chat, sharing data about privacy, shopping online and people have new opportunities related to the Internet. All these led to the emergence of a new phenomenon for science – as cyber psychology which explores the influence of new technologies on human behavior that can be considered as the inevitable result of the development of the Internet technologies /**1-3**/. However, there are also negative consequences: the number of such crimes as Internet fraud, cyber - forgery, violation of privacy, espionage, unauthorized access to protected information in the Internet environment is growing. Legislative policy to prevent or investigate the classic crime of any country has its own system. But at present such confidence in relation to cybercrime does not exist due to the fact that cybercrime is a new, unknown phenomenon for the world that is completely different from the classical types of crime /**3**/. The purpose of our work is to investigate the legislative framework and the policy of the Republic of Turkey to combat cybercrime. Turkish experience can be introduced into the system of the CIS countries as one of the effective models for combating crimes in the field of information technology. Many authors mainly wrote on the legislative framework for combating cybercrime in Turkey, and very little was written about the work of the police and their organization in this area /**4**/. For this reason, we decided to write in this article mainly about Turkey's policy and considered the history of the formation of police organizations dealing with cybercrime. The article uses the method of institutional research with the help of which we define the concept and the policy of the state in one or another sphere /**2**/. Comparative analysis was also used to compare domestic legislation with how the same area is regulated in one or more countries it became almost mandatory in doctrinal legal studies. The comparative method is mainly used as a tool for improving domestic law and legal doctrine in the country /**3**/. Comparative analysis was used as a tool for learning and knowledge (information about law in another place and a better understanding of this), law as an instrument of evolutionary and taxonomic science (general evolution, diachronic changes, legal families), promoting one's own legal system (better understand it, including its traditions, its improvement, its use as a means for interpreting the constitution) for the above reasons, we actively used this method in our article. The policy of the General Security Department of Turkey to combat cybercrime began in 1991 but the legal regulation of cybercrime came into force only in 1997 and only in 2011 and in subsequent years it reached a certain level /**5-7**/. Therefore, the analysis of the cybercrime policy of the GSDT and the analysis of the work of Turkish law enforcement agencies that are involved in identifying and implementing legal and other factors and their influence on the formation of policy in this area is considered necessary experience for other countries and institutions working in this area. In addition, the analysis of the cybercrime prevention policy of the GSDT can be an experience for our country in this area.

2. Turkish legislation on cybercrime

Law enforcement services are considered the most important security authority in any country as they effectively prevent crime. There are many units that are engaged in ensuring internal security the fight against cybercrime belongs to this area /**3**/. A distinctive feature of this group of crimes is that they are directly related to new technological developments. For this reason, the state needs to implement a policy aimed primarily at organizing not a force department but a very high-level team of intellectuals provided with high-tech equipment. The main elements of the cybercrime policy and strategy are the following: taking precautions, creating legislation, creating a special law enforcement agency in fighting cybercrime and special prosecutorial services, cooperation between institutions, training law enforcement officers and judges, and cooperation between public and private effective international cooperation /**8**/. The main mission of law enforcement and police officers is to prevent and uncover crimes. Effectively to carry out this task the legislation ought to provide the authorities with a specific legal basis for action. Without this they cannot fully act. In other words if certain actions are not a crime under the law the police cannot take any action when adequate procedural law is not available, the subsequent prosecution of cybercriminals is almost impossible. There is a list of laws below that specify the powers and responsibilities of police officers primarily those whose service is the fight against cybercrime. For the first time the term "cybercrime" was introduced into Turkish legislation in 1991 (Penal Code No. 765, Articles 525 / a, b, c, d). In the new criminal code No. 52373, adopted in 2004, the definition, exact logical definition, content of the concept "cybercrime" is given taking into account the level of development of cybercrime at that period:

- entering the information system or being in the system that violates the law (art. 243);
- interference with the operation of the information system, change or destruction of data in the system (Art.244 / 1-2);
- obtaining benefits through an information system in violation of the law (Art. 244/4);
- use of bank or credit cards for criminal purposes (Art. 138).

In addition, the following acts are criminalized in the Turkish Penal Code:
- violation of privacy, disclosure of personal or family secrets:
a. illegal registration of personal data (Article 135),
b. unlawful transfer or receipt of personal data (Art.136),
c. the intentional non-destruction of personal data (which must be destroyed) in the new criminal code is qualified as a crime (art. 138).

In addition to the Turkish Penal Code, cybercrime is also regulated by the Intellectual Property Law for Intellectual and Art Works No. 58464. This document covers copyright protection and illegal actions specifically related to computer programs and is also identified as illegal copyright infringement through the Internet. According to the Code it is a crime to use computer programs without permission, web pages, including all sorts of ideas and works of art, duplication, processing of technical tools that protect computer programs, dissemination of information about computer programs without the permission of the authors /**9**/.

The growth of cybercrime in the Internet environment led to the formation of some private institutions related to the Internet, in order to establish a certain order and control in this area there was adopted in 2007 a Law No. 5651 "On Controlling the Content of Publications and Fighting Crimes in the Internet Environment". The law controls fulfillment of the obligations and obligations of the content provider, site provider, access provider and multiple use providers as well as the data content and location of specific crimes committed in the Internet environment, principles and procedures for dealing with cybercriminals /**10**/.

The law defines as illegal the following actions:
- incitement to suicide (Article 84),
- sexual abuse and child abuse (Article 103, first paragraph),
- the illicit sale of narcotic drugs using Internet networks (Article 190),
- the supply of hazardous substances (Article 194),
- distribution of obscene information on the Internet (Article 226),
- prostitution using the Internet and other technologies (Article 227),
- providing places and opportunities for online gambling (Article 228) /**10**/.

Procedures and principles to be followed by the police during interrogation of classic or cybercrime, arrest of suspects, acquisition of criminal evidence, protection of the activities of the judicial police under the supervision of prosecutors are explained in the Criminal Procedure Code No. 5271 which thoroughly and in detail examines the procedural principles that should be followed performance of police duties and judicial procedures. In contrast to other classic crimes the evidence and collected materials related to cybercrime are called digital evidence since they are processed through information systems /**11**/. For this reason, Law No. 5271 contains procedures and principles for the activities of law enforcement agencies related to cybercrimes in a separate article entitled "Search,

copy and seizure of computers, computer programs and files". According to this article:
1. When investigating a cybercrime, if it is not possible to obtain the necessary evidence with the permission of the state prosecutor a search is made for computer materials and computer programs, computer magazines, used by suspects upon request. The judge decides the issue of the need to make a copy of computer records in the form of text.
2. If the information is confidential and the receipt of the necessary copies is impossible due to the impossibility of decrypting information from the computer, computer programs and computer files the judge gives permission to confiscate the property. In the case of decoding and obtaining possibility the necessary copies of materials used devices are returned to the owner.
3. All files in the system are backed up during the confiscation of a computer or computer files.
4. In the case of a request a backup copy is issued to the suspect or authorized person on a receipt with a signature stating that the person received a copy.
5. If a computer or computer system is decrypted without difficulty a copy of some or all of the data in the system can be obtained without confiscating the computer or computer files /**8**/. But along with this in the named law there are some flaws listed below:

- how to find out if the computer is encrypted and contains hidden information,
- the fact that the permission to confiscate a computer is provided only in two cases makes it difficult for forensic researchers to collect sufficient information about the crime,
- it is not specified whether the equipment containing the prohibited material (child pornography, etc.) is to be returned to the owner and in what format,
- there was not determined the official who should keep backup copies and the terms of their storage /**12**/.

In addition to domestic legislation of combating cybercrime on October 10, 2010 Turkey signed and ratified the International Convention which is an important international agreement adopted in the fight against cybercrime in the European Council (EU). 6533 The Law on the Approval of the Convention on Crimes in the Sphere of Virtual Environment was adopted by Parliament and entered into force with some restrictions on May 2, 2014 /**4**/. This ratified document is the first international treaty on crimes committed over the Internet and computer networks. This law will pay special attention to the problems of copyright infringement in the Internet environment, fraud involving the use of computers, publication and distribution of child pornography and network security breaches. Thanks to the ratification of this document it was possible to create local criminal justice agencies necessary to investigate cybercrime and prosecute cybercriminals as well as to increase the effectiveness of the international cooperation regime /**12**/. In domestic policy of Turkey the International Convention on Crimes of Virtual Environment is regarded as an important external factor that effectively influences the fight against cybercrime.

3. Organizations that fight with the crime in the field of information technology

In the period from 1997 to 2011, the General Committee on Security created a department for combating crime in the field of information technology which belongs to the department for information processing. Although in 1991 crimes in the field of information technology were already identified in Turkish Penal Code No. 765, it should be noted that only six years later the fight against cybercrime entered the agenda of the SMC (Security Monitoring Committee). However, initially this unit was mainly engaged in administrative work, therefore, the staff recruited to the organization basically had no experience of judicial investigations. An important political step in the fight against cybercrime was the creation on April 18, 1998 at an extraordinary meeting of the Computer Crimes and Information Security organization, as well as the formation on March 1, 1999 of the Working Group on Information Crimes. There were determined objectives of the activity: to investigate violations of the law in the field of information technology, to qualify types of offenses, to define the necessary rules in the regulations for the relevant departments. As part of the study, international sources were studied and a cybercrime assessment system was introduced; in addition, SMC offices introduced a constant exchange of experience in their work practices. On April 20, 2003, the Turkish International Academy against Drugs and Organized Crime (TADOC), Office for the Control of Crime in Information Systems and High Technologies was established under the supervision of the Office for Combating Smuggling and Organized Crime (KOMDB). In 2006, the name of this unit was changed to the Information Crimes and Systems Department /**5**/. At this time, this department is referred to as "crimes in the field of information and high technology." In the new Criminal Code TR 5237, cybercrime was allocated in a separate section to strengthen the activities of the department to combat smuggling and organized cybercrime. Technical support was also provided for the provincial units; later this technical department which performs the tasks of studying digital data also became the coordinator in the General Directorate for Information Security /**6**/. In 2006, this department opened regional centers in the cities of Istanbul, Sakarya, Bursa, Izmir, Antalya, Adana, Van, Diyarbakir, Malatya, Erzurum, Samsun, Ankara and Kayseri. The center in Istanbul was named as a successful example of the fight against cybercrime. Despite the absence of a separate police unit to combat cybercrime in other provincial security departments and due to the fact that the headquarters or representative offices of many companies and institutions working in this field are located in Istanbul, the Istanbul Crime Department was established here in the information sphere with the approval of the Ministry of the Interior on April 25, 2007 /**7**/. It is logical for the provincial government to create its own structure due to the growth of cybercrime in the region. In order to unite the scattered structure of departments and units of the provincial organization and prevent duplication of investments as well as to ensure the effectiveness of the fight against cybercrime in accordance with the decision of the Council of Ministers No. 2011/202515, the Department for Combating Information Crime extraordinary meeting of the Council of Ministers /**13**/. Other objectives of this policy are: increase and diversification of crimes committed through information crimes and communication tools, the need for more complete specialization and new structures in combating this type of crime, saving resources, reducing duplicate responsibilities between departments, developing standard applications, uniting a limited organization the number of specialized employees of different departments, increasing their level of education and knowledge and, as a result, preventing Informatics, the effectiveness of crime investigations has also increased /**14**/. The name of this organization was changed to the Department for Combating Cybercrime (SSMDB) at the initiative of the Ministry on February 28, 2013. The organization has undergone structural changes in accordance with the emerging needs of social development and cultural development /**10**/. The main task of SSMDB is to provide forensic information services and combat online fraud, fraud in the payment systems, crimes related to obscene publications, illegal betting, gambling, and cyberterrorism. Consequently, this organization can be viewed as a specialized unit of high qualification in the fight against cybercrime providing technical support to other units. The SSMDB engages law enforcement officers (COMB) in combating drug trafficking, financial crime, human trafficking and in combating organized crime, the Department for Combating Terrorism, the Department of Public Security (ADB), and theft control and fraud extortion. The authorities use computer programs under Law No. 5846. The Security Authority deals with crimes involving copyright infringement to protect ideas and works of art. These units are engaged in the investigation of crimes that fall into their service areas, if necessary; use the tools of information systems and in carrying out judicial operations.

For example, in the United States there is a department for monitoring information systems that duties include control of prostitution in the Internet environment, as well as crime control in the Internet environment, the relevant units are notified of the detected criminal elements. In this division there was created a Cyber Patrol Bureau, its functions include the use of criminal sanctions in combating sites that adversely affect the general moral and order of society, especially the psychological and physiological state of children, even if negative material is not published on other websites or websites containing direct elements of crime. Cyber - patrol is designed to combat criminals who open various files for sharing; its goal is to prevent crime by raising the awareness of Internet users /**15**/.

Information about the powers of the Turkish cybercrime unit can be found at www.bugun.com.tr. The main ones are listed below:

1. To be informed to prevent crime, to have the opportunity to use informants and secret investigators in the investigation, to penetrate into the criminal organization and collect evidence.
2. Special expertise aimed at preventing crime investigating and disclosing evidence may use the services of individuals or legal entities.
3. The unit has the authority to listen to any messages and calls, monitor suspicious or suspected persons and install technical equipment in public places and at workplaces of suspects.
4. They are entitled to receive the necessary data, audio and video records for security purposes and in the interests of the state and society, for political, social and cultural purposes, as well as to enjoy the benefits of emergency services.
5. Cyber -police provide access to a remote information system at a different geographic location during important research.

The Turkish Cyber Crime Unit does not only perform information technology monitoring functions, it is also a police unit operating in police operations. 81 cybercrime departments have been established within the framework of the provincial security department under the Cybercrime Department. The sectorial department has the following divisions: Bureau of Forensic Operations, Bureau for Research and Investigation of Crimes, Bureau for the Supervision of Judicial Transactions, supervision of the virtual patrol and supervision of the Bureau of Operations Support /**16**/. We see that the functions of these departments are mainly aimed at combating criminality. A notable element is the virtual patrol office. It is stated that security units should make the most of social media platforms to strengthen their presence on the Internet, spread messages to prevent crime and communicate with the Internet community. It should be noted that the Department of Internal Affairs for the fight against cybercrime has created an effective central apparatus in the cities of Turkey with a large number of inhabitants, since most of the cybercrime are committed in cities where the Internet is widely used. The current state of the police service is 269,898, serving 86% of the country's citizens /**17**/, which confirms that the majority of the population lives in cities. The European Union’s General Secretariat which aims to effectively combat cybercrime and cooperate in areas such as the exchange of information between national and international government agencies and the private sector, also contributes to the enhancement of law enforcement and judicial capacity through the implementation of the project information crimes. This collaboration has been ongoing since 2009. The cooperation of the General Secretariat of the European Union extends not only to the Department of the Interior but also to the General Command of the gendarmerie and organizations associated with the telecommunications services. This project which began in 2013 is scheduled to be completed in 2019, it is also planned to hold 138 training events and seminars at home and abroad. The project cost is 4,400,000 euros /**18**/. Since 2015, the Ministry of Communications and the Department of Communications has been cooperating with the department on combating cybercrime in order to protect children from such crimes as violence, suicide, selling, using drugs, raising awareness about children and parents by creating intellectual classes in planned areas. A 24/7 communication network has also been established in Turkey. It serves for the exchange and storage of information in the country and in accordance with the network’s contract 43 countries cooperate with this service /**10**/.

4. Increasing the capacity of organizations, educational policies and personnel

Since 2013, 842 police officers have been working in the field of combating cybercrime: 106 of them in the Department for Combating Cybercrime (SSMDB) and 736 police officers in 59 provinces /**10**/. The staff of these units works in both civil and administrative organizations. The use of civil servants in the police force is one of the old methods of the state. The reasons for the use of civil servants in police organizations are many. First of all, it is connected with financial expenses and with the level of remuneration: the salary of civil servants is 20% lower than that of the police officers /**19**/. In addition, it is expected that this unit is likely to act when carrying out operations in civilian clothes, its functions being the search, seizure and physical prosecution of criminals.

In order to combat cybercrime and work with electronic evidence it is required expertise of the criminal justice authorities. Therefore, the employee must possess the skills and abilities to investigate crimes committed by electronic technologies, as well as any crimes related to electronic evidence. In addition, security units fighting cybercrime should improve their professional level: for example, to speak foreign languages, it is necessary for successful cooperation with foreign colleagues in accordance with the situation. And also it is necessary for revealing cybercrime the knowledge of information technology. In particular, the acquisition of cyber-criminal evidence is an activity requiring examination. To investigate traditional classic crimes there are investigative units in the field to collect and verify evidence. However, when cybercrimes are committed evidence is completely contained in information technologies and it is required an expert specialist to collect data, review and report. For this reason, law enforcement agencies collecting evidence should also develop technical and administrative capabilities. Additional specialists are needed in the field of digital forensic investigation. The actual lack of capacity, capabilities and resources to combat cybercrime in police departments is considered as a problem on a global scale, as there investigated the cases that are reported by the victims themselves. Thus, forensic information services aimed at obtaining electronic traces and evidence that will be used in criminal investigations of crimes and crimes in the field of cybercrime, increase the effectiveness of the fight against cybercrime in collaboration with organizations that have the ability to directly or indirectly help to prevent the crime.

Applying strategies for sustainable education of personnel in the fight against cybercrime should be a strategic priority. The general principles are as follows.

- Introduce a local law enforcement training strategy with the goal of acquiring competencies necessary for investigating cybercrime to provide electronic evidence, conducting forensic examinations in criminal cases, to assist other institutions and promote network security;
- to provide training in electronic evidence not only for specialized units but also for all law enforcement officers, police units and police schools; to increase the staff of high-level investigations and digital analytical surveys in connection with the constant updating of technology and the increase in crime in this area;
- due to the high cost of training specialists in the fight against cybercrime staff must constantly improve their skills, training should be free which will ensure maximum return on investment in employees.

The following seminars and trainings were held within the framework of the KOMDB (Committee on Combating Organized and International Crime): “Computer and Internet - crime and data recovery methods and expertise”, “Seminar on the analysis of crime”, “Seminar on digital traces”, “Investigation processes of digital evidence "," Internet crime seminar "," Collection course "," SECI secret course on electronic and computer crimes "," Criminal practice and data recovery course ","Investigation of information crimes”,“ Methodology, Windows Forensic Informatics-Vista ”and“ Internet Forensic ”. In 2014, over 45 semesters in accordance with the basic and expanded training needs of personnel, 909 interns were trained to effectively and successfully cope with various types of cybercrime and criminal groups related to information technology. The Security Committee also conducted training for cybercrime units in foreign police organizations. In 2014, within the framework of the international relations project in Kosovo, Georgia, Kazakhstan, Bosnia and Herzegovina 47 staff members were trained for six semesters /**20**/. Cooperation and exchange of information with other countries is very important due to the international nature of this type of crime. In this context, the Turkish police concluded bilateral agreements with security organizations of 39 countries and plans to increase the number of countries with which they cooperate by 2019 to conduct international operations to combat cybercrime /**21**/.

5. Conclusion

It can be said that structural reforms in the fight against cybercrime have improved after the extraordinary meeting of the Committee on Internal Security in 2003. In particular, the signing in 2010 by Turkey and the endorsement by the Parliament in 2014 of the Council of Europe Convention on Cybercrime gave impetus to the policy of the Internal Security Committee to combat cybercrime. In 2011, the creation of the Anti-Cyber Crime Committee was an important step in this area. Department of Security, Public Security, Department for Combating Terrorism in the event of cybercrime in their areas of service can receive technical and informational support from the Committee on combating cybercrime and this has become an effective policy. Police training to combat cybercrime is an important part in this area. In order to effectively combat cybercrime police departments need specially trained experts in the field of information technology. This is inevitable since these crimes have different characteristics in compare with classic crimes. It would be very appropriate to start preparing for cybercrimes starting with the police schools. For this purpose there should be organized regular in-service training seminars. However, it is important that the personnel working in these units are to be chosen very carefully and their safety must be ensured. These organizational workings increase the success of the staff and institutions. Every year with the combating of cybercrime the fiscal policy increases and improves technical capacity of the police, education and growths the number of personnel.

Notes

/1/ Servet I. (2017). 'Cybercrime, Jurisdiction and Proposal of a New Model', Turkey Journal of the Academy of Justice, 17 177-230.

/2/ Howard R.D., McLaughlin G.W., Knight W.E. (2012). The handbook of institutional research, John Wiley & Sons

/3/ Chevik H.H., Demirzhi S. (2016). Legal Policy: Concepts, Actors, Processes, Models, Analysis, Decision Making, Sechkin Publications Press House: Ankara

/4/ Bahaddin A. (2008). Cyber Crime in Turkey and the Impact of the Internet on Crime (with anthropological and legal aspects), Ankara University Institute of Social Sciences, Department of Anthropology, Unpublished Master's Thesis: Ankara, pp. 105.

/5/ Omer T. (2011). 'The place of the police in the fight against cybercrime', Sider Journal, 183

/6/ Yerkan A.A. (2013). 'Management Development: An Approach to Assessing a Turkish Police Organization from a Structural Point of View', Journal of Police Sciences, 109

/7/ Gül A. (2018). Bişim suçları, Seçkin yayıncılık, Ankara, pp. 223.

/8/ Criminal Code of Turkey, Date of receipt of the information 09/16/2018. http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf.

/9/ Gursel K. (2015). Information Law, Association of Turkish Banks Publications, Istanbul, pp. 148.

/10/ Taşci U., Ali C.A.N. (2015). 'Türkiye'de Polisin Siber Suçlarla Mücadele Politikasi: 1997-2014', Fırat Üniversitesi Sosyal Bilimler Dergisi, 25(2)

/11/ Apay C. (2017). 'Bilişim suçları ve bilişim ceza huku', Yazarın Kendi Yayını, 177

/12/ Dülger M., Bilişim, Kişisel Verilerin korunması ve internet iletişimi mevzuatı, Seçkin yayıncılık, Ankara, 2018, pp. 123.

/13/ Yılmaz Y.R. (2005)., 'Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi', Yeditepe Üniversitesi Hukuk Fakültesi Dergisi, 2(2)

/14/ Kleijssen J., Perri P. (2017). Cybercrime, Evidence and Territoriality: Issues and Options, In Netherlands Yearbook of International

Law 2016. TMC Asser Press, The Hague, pp. 147-173.

/15/ Hert P. de, Parlar C., Sajfert J. (2018). 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law', Computer Law & Security Review, 34(2) 327-336.

/16/ Kahveci F. (2014). Türkiyede en cok karşılaşan bilişim suçlari, 2014. https://www.webtekno.com/internet/turkiye-de-en-cok-karsilasilan-bilisim-suclari-h2642.html

/17/ Atalayv A., Sanci G. (2015). Cyberterrorism And Turkey's Countercyberterrorism Efforts, https://procon.bg/system/files/3203_turkey_cyberterrorism.pdfhttps://procon.bg/system/files/3203_turkey_cyberterrorism.pdf

/18/ Akgül M. (2015). Internet censorship in Turkey Internet censorship in Turkey, 2015. https://policyreview.info/articles/analysis/internet-censorship-turkey

/19/ Akgul M., Kirlidog M. (2015). 'Internet censorship in Turkey', Internet Policy Review, 4(2) 1-22.

/20/ Yılmaz K., Güneştaş M., Başıbüyük O. (2016). 'Cyber Terrorism: Motivation and Method on Global Scale and the Situation in Turkey', Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations, 125 (2016) 82.

/21/ Reich P.C. (2011). Cybercrime & Security, West Publications