Protecting the Rights in WEB 2.0 with WEB 1.0 Instruments or Self-Defense

Kurtoğlu O. K.[1]
Erol İ. E.[2]

[1] Ömer Kahraman KURTOGLU, İstanbul Aydın University, (Turkey)
email: omerkahramankurtoglu@gmail.com
[2]İhsan Emre EROL, İstanbul Aydın University, (Turkey)
e-mail: iemreerol@aydin.edu.tr

Abstract

The instruments used by law for the detection of the violations of the intranet and internet and the detection of the violators are insufficient. The instruments used by law to detect IP's for he violations made from cross border are insufficient. The verification of the digital evidences may not be made at most cases. There is a big discrepancy among the applications of the family law, penal code and civil law on the validations of the digital evidences. On the network-based user interfaces, it is quite easy to manipulate the content even without violating intellectual property rights. The hosting providers have a power to manipulate digital evidences. It is possible to record the communications without identified through some hardware's. The data transactions are about to start via blockchain infrastructure in which it is impossible to record the communication, so it will be easy to hide the evidences of the violations and the crimes. The personal data is in a great danger on the web-based applications. In addition to this "take it or leave it" type contracts are tending to eliminate all the rights on such data. User generated, participate web sites prefer to acquire IP rights of the content created by the users without intervening the disputes and the violations made by a third party. The regulations which covers the rights of the individuals are far to protect legal persons rights. The right of reply may not be granted in the event of the social manipulations and/or lynch. Internet service providers and publishers are not obliged to intervene to the violations unlike the hosting service providers, this passive attitude facilitate DDOS and similar attacks. In the extent of this facts, the legal instruments may be easily manipulated.

Keywords: Law, IP, Network Based User Interfaces, Self-Defense.

Introduction

To prevent irreversible damages, maybe we have to discuss the extent and/or the borders of the self-defense, the interference of and/or the diligence and the measures of the third parties to not be accepted as liable for the violations of any kind. In theory self-defenses is examinated in two main topic such as active self-defenses and passive self-defenses. The acts such as hiding IP's is accepted as passive self-defenses. Intervening to another person and/or system dominated by another person and similar acts is accepted as active self-defenses. As per Turkish Penal Code the use of the active self-defenses right against cyber-crimes is not granted. therefore on this essay we emphasize on the passive self- defense. We have to mention that public recognition of methods (such as alteration of DNS or VPN etc.) may increase the rate of cyber-crimes. To overcome such "hiding" acts, an international collaboration is needed. But the countries generally are not willing to give IP's and/or digital evidences to the countries in which the freedom of the speech and/or the protection of the personal data are not in same level with themselves. From this point of view, we may claim the regulations aimed the protection of the personal data as well as the freedom of the speech actually will be served to the public security and the stability of the nation with some parts.

DOI NO: 10.7456/ctc_2019_20

The Problematics:

1- Identification of the Breach or the Violation

It is quite difficult to identify an online violation due to the volatility of the content such as the graphics on the public user inter-face as well as the data. For example, A person who insults to another, may delete the content after sight. To avoid such situations, as a solution Turkish notary association put out into a service, an application called “e-tespit". In order prove the content of the web sites, the users may obtain a legally valid screenshot of any website through a personal computer, regardless of its location on due time before the delete of the content. Such screenshot captures are deemed to accepted as an admissible evidence. The person who wishes to captures any admissible screenshots shall reach to the website contents via e-tespit portal page. The information and the details of such operation is recorded to the information systems of the Turkish notary association. After the fulfillment of this phase with an application number, the applicant may receive the documents including form any public notary. The applicants may prove the violation even after the removal of the content (url1).

"E-tespit” based on KVM technology. KVM works by reaching to a remote server via IP address by your mouse, and keyboard. In fact, this system proves whether the content really exists on your screen, by accessing your devices to the notary's computer. As this system shall be considered as a milestone comparing with the soft copies delivered to the prosecutors as a digital evidence; yet it has few weaknesses:

Firstly, there is no certainty whether which visual has been captured by the device of the notary association, the visual may be belonged to the website cached in the memory, secondly the name servers of the notary association shall be manipulated, once name server has cloned, the hacker may broadcast pretending to this server.

for the validity of the notarization on similar transactions, China highest court is seeking that the notary shall access from his computer after the delete of all the related data form his computers cache memory. According to the court the record may just be about the access of the recorded interface cached in the device’s memory. In some scenarios a visitor may reach to a recorded page of the notary’s computer rather than website itself (url2).

We may also add that this system may not working properly on the platforms in which a server of a website shall be reached through another process such as log-in. Therefore "e-tespit" still a bit is far to achieve its goal.

There are also legal problems about the right holders and the owners of the websites and their legal limits. In the event of a dispute, the court shall settle to which person the conflict shall be addressed. Therefore, primary the court shall investigate the holders of the IP rights of a website. After web 2.0; websites are accepted as a multimedia product which is not indicated in our copyright law. Multimedia is a content that uses a combination of different content forms such as text, audio, images, animations, video and interactive content. Multimedia contrasts with media that use only rudimentary computer displays such as text-only or traditional forms of printed or hand-produced material (url3). So, each element of a website shall be separately belonged to a one person. In Turkish law multimedia products is not accepted as a branch of a copyright. According to Turkish law, software producers shall have a copyright on the software, graphic designers on the interfaces etc. In addition to that the protection limit of the software which is the most important element of the online environment, is narrow scoped, covers just the front-end works. Despite of their commercial value, the computer software's are not able to be patented. Algorisms as a crucial element of a software, is not protected even as a copyright due to their structure. yet an algorithm shall be diverted from a software; may be used and put in the commercial area.

2- Identification of the transactions via electronic signature

Electronic signature is a form of a hand-written signature with a similar function, used on the telecommunication networks and the internet. It is an instrument created to achieve same legal results with the handwritten signatures. But in the online environment, not just the individuals but also the servers, platforms and intranets also use the electronic signatures. Electronic signatures may be used by the subjects who owns a certificate, which is a digital ID cart showing its qualifications and/or compliance (Keser, 2002:148).

Yet electronic signatures have some weakness. Firstly, digital signatures used by the individuals still activated by a pin. In the event of the leaking of a pin code it shall be used unauthorized. Due to practical reasons, in some sectors few digital signatures owned by one person are often used by a multiple person, therefore digital signatures shall be supported by a biometrical application.

Also, if a name server has implemented to the recipient router, the settings shall be manipulated and therefore, a message which is sent shall be seen as not received or vice versa. This kind of manipulation shall be made with the help of the hosting provider which is generally paid by the recipient.

3- Collection of the digital evidence

Digital evidences are the admissible materials for the trials and/or investigations aiming to establish a relation among all kind of digital value and material; established, transferred, shared, sanded, recorded, loaded and processed by the cyber systems and kept in the cyber systems such as networks and clouds or data storages located in the electronic devices capable of processing data and smart devices, mobile devices, computers capable of processing data's (Yetim, 2016).

a- Collection of the digital evidence on civil jurisdiction

For civil jurisdiction is enacted a special rule and the restrictions for the admissibility of the evidence. As per the article 200 of the code of civil procedure, legal acts performed in order to originate, assign, modify, renew, postpone, confess and redeem a right shall be proven by documentation if their value at the time they were performed exceeds two thousand five Turkish liras. Such legal acts cannot be proven by other means then documentation even if their amount or value falls under two thousand five hundred Turkish liras by payment or quittance (url4).

According to article 205/2 of civil code of civil procedure, the electronic data's originated by a secured digital signature have a power of a documentation. In the ground of this article, the goal of this regulation is indicated; the aim attributed to this article, is to terminate the uncertainty about their power as an evidence. In our opinion apart from this kind of evidences, all other electronic evidences shall be a subject of an inspection of a judge or/and expert examination

The problems about the admissibility of an evidence in the civil law jurisdiction intensifies on the methods used to detect a violation of a software copyrights: the software companies use DRM methods: DRM divided in a two branch such as accessing control and copy controls: Accessing controls are based on passwords, copying controls means the mechanisms which prevents to record and copying of an accessed content. DRM includes, authentication and identification systems, meta-data systems, payment systems, systems related to the right of privacy, cryptography (Bayamlıoğlu, 2008: 303).

Legal problematics of DRM system arises from its on-line control mechanism. In that mechanism like off-line control system a file whether the permissions is not submitted to the users before; yet access to the device via network and recives permission for every use. Apart from other electronic commerce transactions, users are followed to control their compliance to the license agreement at every access. This method actually is a crime according to Turkish penal code unless the users is inquired detailly about this situation.

b- Collection of the digital evidence on criminal trials

On the investigation phase of the criminal jurisdiction, and the collection of evidence of the Cybercrimes and the crimes in which its evidences may be found in the data processing systems; a special process has been enacted:

Search of computers, computer programs and transcripts, copying and provisional seizure.

Article 134 – (1) Upon the motion of the pub lick prosecutor during an investigation with respect to a crime, the judge shall issue a decision on the each of computers and computer programs and records used by the suspect, the copying, analyzing, and textualization of those records, if it is not possible to obtain the evidence by other means.

(2) If computers, computer programs and computer records are inaccessible, as the passwords are not known, or if the hidden information is unreachable, then the computer and equipment that are deemed necessary may be provisionally seized in order to retrieve and to make the necessary copies. Seized devices shall be returned without delay in cases where the password has been solved and the necessary copies are produced

(3) While enforcing the seizure of computers or computer records, all data included in the system shall be copied.

(4) In cases where the suspect or his representative makes a request, a copy of this copied data shall be produced and given to him or to his representative and this exchange shall be recorded and signed.

(5) It is also permissible to produce a copy of the entire data or some of the data included in the system, without seizing the computer or the computer records. Copied data shall be printed on paper and this situation shall be recorded and signed by their lasted persons.

This disposition has been criticized basically on two grounds. Primary the seizure process is banded to the disability of the decrypted. Nevertheless, in some situations when there was a need of the detailed examinations, a lab process is required. As well as this, in the article, after the examination, the return of the hard disc to the suspect is indicated. It shall not mention about the return of a device in which there is a likelihood of the evidence and/or element of the crime. It is also indicated that the copied data shall be printed on paper; but in a hard disc it can be found a data which is equal and more to billions of pages, so practically it is impossible (url5).

On the interception of correspondence through telecommunication Location, listening and recording of correspondence Article 135 is enacted:

– (1) The judge or, in cases of peril in delay, the public prosecutor, may decide to locate, listen to or record the correspondence through telecommunication or to evaluate the information about the signals of the suspect or the accused, if during an investigation or prosecution conducted in relation to a crime there are strong ground s of suspicion indicating that the crime has been committed and there is no other possibility to obtain evidence. The public prosecutor shall submit his decision immediately to the judge for his approval and the judge shall decide within 24 hours. In cases where he duration expires or the judge decides the opposite way, the measure shall be lifted by the public prosecutor immediately. (2) The correspondence of the suspect or the accused with individuals who enjoy the privilege of refraining from testimony as a witness shall not be recorded. In cases where this circumstance has been revealed after the recording has been conducted, the conducted recordings shall be destroyed immediately. (3) The decision that shall be rendered according to the provisions of subparagraph 1 shall include the nature of the charged crime, the identity of the individual, upon whom the measure is going to be applied, the nature of the tool of communication, the number of the telephone, or the code that makes it possible to identify the connection of the communication, the nature of the measure, its extent and its duration. The decision of the measure may be given for maximum duration of 3 months; this duration may be extended one more time. However, for crimes committed within the activities of a crime organization, the judge may decide to extend the duration several times, each time for no longer than one month, if deemed necessary. (4) The location of the mobile phone may be established upon the decision of the judge, or in cases of peril in delay, by the decision of the public prosecutor, in order to be able to apprehend the suspect or the accused. The decision related to this matter shall include the number of the mobile phone and the duration of the interaction of locating (the establishment). The interaction of locating shall be conducted for maximum of three months; this duration ma y be extended one more time. (5) Decisions rendered and interactions con ducted according to the provisions of this article shall be kept confidential while the measure is pending. (6) The provisions contained in this article related to listening, recording a

DOI NO: 10.7456/ctc_2019_20

devaluating the information about the signals shall only be applicable for the crimes as listed below: a) The following crimes in the Turkish Criminal Code; 1. Smuggling with migrants and human traffic king (Arts. 79, 80), 2. Killing with intent (Arts. 81, 82, 83), 3. Torture (Arts. 94, 95), 4. Sexual as sault (Art. 102, except for subsection 1), 5. Sexual abuse of children (Art. 103), 6. Producing and trading with narcotic or stimulating substances (Art. 188), 7. Forgery in money (Art. 197), 8. Forming an organization in order to commit crimes (Art. 220, except for subsections 2, 7 and 8), 9. Prostitution (Art. 227, subparagraph 3), 10. Cheating in bidding (Art. 2 3 5) , 11. Bribery (Art. 252), 12. Laundering of assets emanating from crime (Art. 282) , 13. Armed criminal organization (A rt. 314) or supplying such organizations with weapons (Art. 315), 14. Crimes against the secrets of the state and spying (Arts. 328, 329, 330, 331, 333, 334, 335, 336, 3 3 7). b) Smuggling with guns, as defined in Act on Guns and Knifes and other Tools (Art. 12), c) The crime of embezzlement as defined in Act on Banks, Art. 22, subparagraphs (3) and (4), d) Crimes as defined in Combating Smuggling Act, which carry imprisonment as punishment, e) Crimes as defined in Act on Protection of Cultural and Natural Substances, Art. 68 and 74. (7) No one may listen and record the communication through telecommunication of another person except under the principles and procedures as determined in this Article (url6).

At article 135 of the Criminal Procedure Code, the measures and the methods of the recording is not detailly indicated. In the mentioned article it is indicated just the decisions shall be send to the presidency of telecommunication to be executed.

The communication of the suspect or the accused can be recorded provided to not be able to achieve to an evidence as well as the existence of solid grounds for the crime, in the event of investigation and prosecution. For the crimes indicated in the article 135/6 of Criminal Procedure Code, the signals may be recorded and evaluated.

Recording and listening of the correspondence means obtain the inquiry about the correspondence and record such correspondence through a device about the communication made by telecommunication devices by a suspect or a accused. But apart from the correspondence with other parties, recording and listening through a device as a sensor is a technical surveillance indicated in article 140 of Criminal Procedure Code (Özbek, 2005: 564).

The record of correspondence is historical traffic search, listening and recording is not included. The assessment of the information about signals means to receive a results by evaluating and assessing the traces of the recorded signals without intercepting and intervening to the content of the correspondence and information about signals means all kinds of data processed on a network for invoicing and for the transmission.

Telecommunication means, is the transmission, sent and received by wire, optical, electrical, electromagnetically, electrochemical, electromechanical and other transmissions systems of all kind of mark, symbol, voice and the visuals and all kind of data transformable to the electrical signals. So, this article covers recordable all kind of correspondence.

According to article 135/4; The location of the mobile phone may be established upon the decision of the judge, or in cases of peril in delay, by the decision of the public prosecutor, in order to be able to apprehend the suspect or the accused. The decision related to this matter shall include the number of the mobile phone and the duration of the interaction of locating (the establishment) (url7). So, this is differing from article 135/1 who aim to acquire evidences, this article aims to detain the accused or the suspect, so its applicable to all kind of crimes.

But we shall note that in practice the experts obtain main evidences by a technical surveillance according to article 140, technically officials hack the operator devices close to possible location of the suspect and the accused, this method is called “hooking”.

The court of cassation in one verdict try to fill the gaps of the article 134, added some details for the collection and the examination of the data: Firstly the examination shall be made immediately, unless otherwise such computer is not be used until the examination, as a first phase the files shall be backed up sector by sector and after that backed up the data shall be hashed and the integrity of the data shall be maintained. By this the experts in the trial shall investigate whether the backup data is the real copy of the file or not.

c- Identification of the IP Address

In the event of any conflict, traffic records demanded from third parties. According to law 5651 Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication; The hosting provider shall be responsible for retaining traffic information concerning services it provides, as shall be specified by a regulation, for a period of at least one year and not more than two years, and shall be responsible for ensuring the accuracy, integrity and confidentiality of that information.

Traffic information are the information such as parties' IP address, the start and finish time of service provided, type of service used, quantity of data transferred, and subscriber identification details, if available, included the IP address of the parts, the start and the finish of the service, the type of the service, source IP address, target IP, the hour and the date information of the access, the webpage requested, transmission information. The identification of the IP address is important for the disposition but for the hosting providers there is not a standardization about recording and they are generally paid by one part of the conflict.

4- Manipulability nature of the digital evidence

As a mentioned above, the manipulation of the digital evidences is easy, even on the identification of the violation phase the manipulation is possible in addition third parties who are obliged to record the traffic information, are generally are paid by one of the parts of the dispute. It is not easily claimed their impartiality. It shall be added that, especially in the b2c web sites, on the user inter-faces was a dialog box to receive the messages. To prove whether the message is sent, consumers shall rely on the bona fide of this website's admins.

5- Cross-border Access to the Digital evidence

In practice bilateral and unilateral agreements has been in force, apart from this agreements, Turkish penal code article 11-19 some regulations and process has been set forth. For the cybercrimes Judicial assistance has been made according to European cybercrimes convention where the judicial assistance has been detailly regulated (Dülger, 2015).

The centers/servers/hosts of the social media platforms which cybercrimes is actually committed are in USA California, according to USA law the states shall refuse the judicial assistance demands according to their domestic disposition. The grounds of such refusals intensify on the personal data and the individual rights. But sometimes social media platforms shall provide evidences. Despite of not received from the official state body, the courts grounded their decisions according to these platforms' declaration. But the problem is these media platforms shall be the part or related to the part of this disputes, it won' t be reasonable to wait an impartial evidence from such platforms as well as this we shall not able to control whether such evidences is manipulated or not.

6- Computer forensic analysis versus Tech

Developing techs brings some methods which disfunctions the instruments mentioned above. For example, not just the payments but every kind of data transactions and transmissions such as file, text, visual and voice transmissions from now on shall be made by a blockchain infrastructure. Even with this infrastructure the broadcasting shall be made. In this infrastructure the data is been transmitted deciphered, therefore it is literally impossible to detect, identify or investigate without a detailed international cooperation. Computer forensic experts achieve the results about blockchain infrastructure through the wallets and/or tokens whether their content is made publicly accessible by their owners or creators.

On cloud computing any kind of computer forensic has been developed yet, the service models of the cloud computing mainly vary as, serves as an infrastructure, service as a platform, service as a software. In addition to this; an instant visual, voice and voice transmission through the switchboards is considered in a cloud computing. In a service as an infrastructure the data belonging to one person scattered to a different hard discs philocaly, it is possible to disintegrate a data and, scatter to the discs located in different countries. Therefore, we shall not obtain an admissible digital evidence without international cooperation (Topaloğlu, 2017: 28-34).

Speaking of cloud computing we shall mention of the VoIP. The numbers which begins by 0850 is a good example. VoIP, voice over internet protocol actually based on open source software, the parties may message instantly, may send a file voice or visuals. WhatsApp, facetime and the similar applications based on this technology. the companies used this technology due to its cheapness and its security. Some switchboards used for this service do not log and/or not capable to log the traffic information therefore if there was not an instant recording or collecting of digital evidence, it is impossible to obtain a digital evidence. In most cases IPs has been hidden to avoid DDOS attracts through vpn. The VoIP services doesn't record the content and due to technological reasons, they can' t manage to log the traffic information properly. So, it is really hard to acquire an admissible evidence in VoIP services. In some scenarios the evidences related to VoIP systems can bug found through the investigation of the devices, but the company's product new devices and software's which prevents the examination of the deleted files and which deletes a file in an irreversible way.

7- Appraisal

In the extent of the mentioned as above, due to multiple reasons; including but not limited to the manipuled characteristic of the digital evidences, the failures on the detection, examination of the violation of the instruments, Current situation urge the real and legal persons to act beyond the courts, so we may argue the methods of the self-defense in all meanings and its extent.

Conclusion

Online Use of The Self Defense Right and Similar Instruments

To mention about self-defense and similar instruments we must indicate their legal definitions and its limits:

a- Self-Defense

On article 25 /1 No punishment is given to an offender who acts with immediate necessity, according to the prevailing conditions, to repulse or eliminate an unjust assault against his or another person's rights, of which the recurrence is highly expected (url8).

Existence of aggression is prerequisite for acting in self-defense, aggression shall be unlawful and shall address to a right, Aggression shall be still present, there shall be an imminent necessity of defense and the defense shall be proportionate with the attack.

b- State of Necessity

On article 25/2 No punishment is given to the offender for an act executed to protect himself from a severe and definite danger or an assault against his or another person's rights, where he has no other choice to eliminate this danger. However, there should be proportional relation between the imminent necessity to protect oneself and the seriousness of danger, and the means used to eliminate this danger (url9).

The defense of necessity may apply when an individual commits a criminal act during an emergency situation in order to prevent a greater harm from happening. In such circumstances, our legal system typically excuses the individual's criminal act because it was justified, or finds that no criminal act has occurred. Although necessity may seem like a defense that would be commonly invoked by defendants seeking to avoid criminal charges, its application is limited by several important requirements: The defendant must reasonably have believed that there was an actual and specific threat that required immediate action. The defendant must have had no realistic alternative to completing the criminal act. The harm caused by the criminal act must not be greater than the harm avoided. The defendant did not himself contribute to or cause the threat (url10).

2- Self Defense on Cyber Crimes

The availability of the self-defense shall be argued in the event of the cybercrimes , for example in the event of a DDOS attack, it shall be argued whether self –defense is possible, it is deemed to be accepted possible in one scenario; firstly to use self-defense, the person who wishes to use self-defense right, shall take all the measures to protect his system, after that he shall be identify the attacker and his IP address. But it shall not be possible, the attack shall be made form a zombie device or the IP shall be manipulated, therefore in order to defend, a cybercrime may be committed to an innocent. We may claim that self-defense is not possible for cybercrimes.

3- Self-Defense Applications in The World

The Active Cyber Defense Certainty Act was introduced to Congress as legislation that would give companies and individuals the right to strike back after a "persistent unauthorized intrusion." The legislation is designed to extend the powers of cyber attract victims beyond the limits imposed by the CFAA.

At its core, the CFAA prohibits the intentional accessing of a computer without authorization and obtaining information from a protected computer involving interstate or foreign communications. As such, any “hack back” by a corporate victim of a cyberattack is prohibited under the CFAA. But the Active Cyber Defense Certainty Act would lift this restriction, allowing a company to implement active cyber defense measures to not only identify the attackers, but even destroy information originally stolen from their network.

Specifically, under the Active Cyber Defense Certainty Act, a cyberattack victim (or “defender”, to use the bill’s terminology) would be able to access “without authorization the computer of the attacker to the defender’s own network to gather information in order to”: Establish attribution (i.e. the nature, cause and source) of criminal activity to share with law enforcement and other US Government agencies responsible for cybersecurity; Disrupt continued unauthorized activity against the defender’s own network (though without damaging the computer systems of the presumed attacker or anyone else), Retrieve and destroy any stolen data, Monitor the behavior of an attacker to assist in developing future cyber defense techniques, Use beaconing technology, a beacon is a piece of software or a link that has been hidden in a file and can send information back to a defender with details about the structure and location of the attacker’s computer system. Essentially, within this framework, companies and individuals will be authorized to take a more active role in cyber defense by using and developing tools which are currently restricted under the CFAA. That specific law is allowed a DRM method which shall be a cybercrime as itself.

4- Online Self-Defense

Specially after the visibility of the personal data, a tendency is developed for keeping an individual and his actions: Technology has answered very fast to this demand and create a secured infrastructure. For example, opera browser has developed its VPN system, satellite services is chosen to prevent hooking, more and more people has used “tor” browser. Apart from this DDOS attracts which are still a great thread for the companies and will be aggravated with the similar momentum of the bandwidth. DDOS is a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet (url11). Only way to stop this attact is to counter attack to the attacker IP address, but in this scenario, the line may be loaded so much; related to the qualification and the capacity of the lines, different systems may be damaged. The reasonable measure may to give authorization the ISP to prevent such IP (url12).

5- What shall be the approach of The State

Despite the aggressive attitude of the companies and the states about the data, we have indicated that the measures easily dysfunctioned by the duly informed educated people. New developing technologies always defeat the old measures. From this point of view, instead of wasting the public sources to the ineffective measures, the state may cooperate with other subjects. that cooperation will be also a good base to develop effective legal measures. The measures like the control of the internet or all the transmissions are not just expensive but also ineffective. For example, a considerable amount of the users in China uses VPN. Russia which the data is distributed from one point by a mirror data, is a source of a DDOS attacks. Blockchain infrastructure is used for broadcast or instant messaging, there is no technical measure to record of the correspondence, listening or interception through hooking or other measures, also this service does not record the content nor the log. Without an international cooperation it is nearly impossible to obtain an admissible device.

In this point we have to mention that after GDPR, the nations of the EU have not given the logs or other evidences due to reason whether Turkey has not signed and/or implemented GDPR. To obtain an admissible digital evidence from Europe or USA, turkey shall meet their standards on individual rights. To this extent, the public security of Turkey relies on the democratization.

References

[1] Bayamlıoğlu, A. (2008). Fikir ve Sanat Eserleri Kanunu'nda Teknolojik Korunma, Bilişim ve Eser Koruması WIPO, AB; ABD ve Türkiye' deki Teknolojik Önlemler DRM, Hukuki ve Sosyal Araçlar. İstanbul: Levha Yayınları.

[2] Dülger, V. (2015). Bilişim Suçları ve İnternet Bilişim Hukuku. Ankara: Seçkin Yayınları.

[3] Keser, B. (2002). İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, İstanbul: Yetkin Yayınları.

[4] Özbek, V.Ö. (2005). Yeni Ceza Muhakemesi Kanunun Anlamı. Ankara: Seçkin Yayınevi.

[5] Topaloğlu, Ö.T. (2017). Bulut Bilişim. Ankara: Seçkin Yayınları.

[6] Yetim, S. (2016). Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği). Ankara: Seçkin Yayıncılık.

[7] url1 https://bit.ly/2lQRDLG

[8] url2 https://bit.ly/2kHbpJu

[9] url3 https://bit.ly/2kGsqDB

[10] url3 https://bit.ly/2mbwJHk

[11] url4 https://bit.ly/2Kx2vIq

[12] url5 https://bit.ly/37glbFX

[13] url6 https://bit.ly/2NVqx1M

[14] url7 https://bit.ly/32Rzz40

[15] url8 https://bit.ly/2QpuPjA

[16] url9 https://bit.ly/2pru1zu

[17] url10 https://bit.ly/2CRevzV

[18] url11 https://bit.ly/35dJ6Ec

[19] url12 https://bit.ly/2qZb4Vs

DOI NO: 10.7456/ctc_2019_20