NEU PRESS

HUKUK FAKÜLTESİ DERGİSİ

Vol: 7 No: 2 Yıl: 2024 | Araştırma Makalesi | e-ISSN: 2667-4076

https://doi.org/10.51120/NEUHFD.2024.127

Proving the Crime of Threat Through Digital Evidence in the Light of the Supreme Court Decisions

Alaaddin EGEMENOĞLU [1*]

[1] İstanbul Medipol Üniversitesi Hukuk Fakültesi, Türkiye

Article Info

Article History

Received: 21.02.2024
Accepted: 18.07.2024
Published: 22.07.2024

Keywords:
Digital evidence, Threat crime, Social networking sites, Audio and video recording, Judicial cooperation

ABSTRACT

Since the crime of threatening is frequently committed verbally in the society, it is difficult to prove it. Especially in recent years, with the development of technology, the crime of threatening has started to be committed through electronic means. This situation introduces the concept of digital evidence. As long as it is not obtained through illegal methods, it is possible to prove the threat with digital evidence. In this study, especially in the light of the Supreme Court decisions and taking into account the opinions of the doctrine, the issue of proving the crime of threat through digital evidence; the concept of digital evidence, judicial cooperation for the delivery of evidence, digital evidence will be examined under the headings of threats made through communication tools, threats made through social networking sites, threats made through e-mail, threats made through audio and/or video cameras and finally, proving the crime of threat with digital evidence within the scope of the Supreme Court of USA decisions.

Yargıtay Kararları Işığında Tehdit Suçunun Dijital Deliller Vasıtasıyla İspatı

Makale Bilgisi

Makale Geçmişi

Geliş Tarihi: 21.02.2024
Kabul Tarihi: 18.07.2024
Yayın Tarihi: 22.07.2024

Anahtar Kelimeler:
Dijital delil, Tehdit suçu, Sosyal paylaşım siteleri, Ses ve görüntü kaydı, Adli yardımlaşma

ÖZET

Tehdit suçu toplumda sıklıkla sözlü olarak işlendiğinden ispatında güçlük bulunmaktadır. Özellikle son yıllarda teknolojinin de gelişmesiyle tehdit suçu elektronik araçlar vasıtasıyla işlenmeye başlamıştır. Bu durum karşımıza dijital delil kavramını çıkarmaktadır. Hukuka aykırı yöntemlerle elde edilmediği müddetçe dijital delillerle tehdidin ispatı mümkündür. Bu çalışmamızda özellikle Yargıtay kararları ışığında ve doktrinin de görüşlerini dikkate alarak tehdit suçunun dijital deliller vasıtasıyla ispatı meselesi; dijital delil kavramı, delillerin ulaştırılması adına adli işbirliği, iletişim araçları vasıtasıyla yapılan tehdit, sosyal paylaşım siteleri vasıtasıyla yapılan tehdit, elektronik posta vasıtasıyla yapılan tehdit, ses ve/veya görüntü alan kameralar vasıtasıyla yapılan tehdit ve son olarak Amerikan Yüksek Mahkemesi kararları kapsamında tehdit suçunun dijital delillerle ispatlanması başlıklarıyla incelenecektir.

To cite this article:

Egemenoğlu, A. (2024). "Proving the Crime of Threat Through Digital Evidence in the Light of the Supreme Court Decisions", *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi*, Cumhuriyet'in 100'üncü Yılı Armağanı, s. 481-494. https://doi.org/10.51120/NEUHFD.2024.127

***Sorumlu Yazar:** Alaaddin Egemenoğlu, aegemenoglu@medipol.edu.tr

This article is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0)

INTRODUCTION

In Turkish criminal procedure law, whether an act has been committed or not is proved by means of evidence. Proof, on the other hand, is defined as the situation in which the judge, who is the judicial authority, reaches certainty by means of lawful means whether the act has been committed by the defendant or not[1]. The judge, while ruling as a result of the criminal procedure, may decide to convict if it is certain that the act constituting a crime was committed by the defendant. Otherwise, if there is doubt, it is interpreted in favor of the defendant, and if it is not fixed that the charged crime was committed by the defendant, an acquittal decision is given in accordance with the principle that the defendant benefits from doubt (Article 223/1-e of the Turkish Criminal Procedure Code no. 5871). In the decision of the Criminal General Assembly of the Supreme Court, it was emphasized that the principle of the defendant benefits from doubt is universal in criminal proceedings, and it was stated that the criminal procedure should be based on proof, not probability, that it depends on proving that the defendant committed the crime with certainty that leaves no room for doubt, and that the defendant should be sentenced by investigating the material truth[2].

There is no obligation of proof problem in criminal procedure. Evidence is the means of proving the claim. Assumptions are not considered as evidence. The judge must reach the material truth in order to make a decision. The material truth is tried to be revealed through evidence that can prove a part of the event (Article 206/2-b of the Criminal Procedure Code). Evidence must have a material structure that can be perceived by the five senses[3].

With the development of technology, the methods that we can call classical from (such as; bloody knife, blood, letter) the oldest time to the present day have changed. Today, digital evidence (electronic evidence) is also frequently used in criminal procedure. As technology advances to become more portable and powerful, the creation, storage, and access to large amounts of information have increased. Modern devices can act as vast repositories for personal information[4]. Developing electronic devices help to elucidate crimes that are difficult to prove.

The offense of threat, which can be committed verbally or in writing, is completed with the perception of the addressee. In this sense, problems arise for its proof. Especially with the development of technology, the crime is tried to be proved through digital evidence. Since the centers that provide some digital evidence are outside Türkiye, international judicial cooperation is also needed. The most concrete example of this is the Council of Europe Convention on Cybercrime. In this sense, the center of social networking sites such as *"Twitter"*, *"Facebook"*, *"Instagram"*, *"YouTube"* and *"Tiktok"* which are widely used all over the world, is the USA, which has adopted the common law system. In this sense, it is the US and Turkish Supreme Court decisions need to be reviewed.

[1] Öztürk, Bahri / Erdem, Mustafa Ruhan / Özbek, Veli Özer. *Uygulamalı Ceza Muhakemesi Hukuku*, 11. Baskı, Seçkin Yayıncılık, Ankara, 2007, p. 404; Yavuz, Mehmet. "Ceza Muhakemesinde İspat Sorunu", *Türkiye Adalet Akademisi Dergisi*, Y. 3, I. 9, April 2012, p. 154.

[2] Yargıtay Ceza Genel Kurulu, E. 2019/412, K. 2021/44, KT. 18.02.2021, https://kararara ma.yargitay.gov.tr, (Date of Access: 21.02.2024).

[3] Centel, Nur / Zafer, Hamide. *Ceza Muhakemesi Hukuku*, 21. Bası, Beta Yayıncılık, İstanbul, 2022, p. 255.

[4] Goodison, Sean / Davis, Robert / Jackson, Brian. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, *RAND Corporation*, 2015, p. 1.

I. PROOF OF THREAT CRIME THROUGH DIGITAL EVIDENCE

A. General Information About The Concept of Digital Evidence

Threat crime is frequently committed through digital devices with the development of technology. This leads to the concept of digital evidence[5]. Digital evidence refers to information and data of importance in criminal proceedings that are stored in or transmitted through an electronic device[6]. Although the first thing that comes to mind when it comes to digital devices is computers, cell phones or the internet, any electronic device, including robots containing artificial intelligence algorithms, can be within the scope of digital evidence. For example, the crime of threat can be committed by giving commands to the robot. The threatening action sent by a drone can be used as evidence in the judgment phase. In summary, digital evidence refers to data, records and documents that are produced, modified, transmitted to others or stored in an electronic environment, which serve to prove the alleged act[7]. Data, records and documents stored in this way can only be used as digital evidence in the proceedings, provided that their authenticity is determined by an expert witness in court[8]. Digital evidence is of an abstract nature rather than what we can call classical evidence in the sense of the Criminal Procedure Code. However, if digital evidence is contained in a hardware device, it is not the hardware device itself that constitutes the main evidence in criminal proceedings. It is the digital evidence contained in the hardware device[9].

Depending on the nature of the digital evidence and the method of obtaining it, digital evidence may be indicative in some cases and documentary in others[10]. In Turkish criminal law, one view considers digital evidence as documentary evidence. This is because electronic loads can be read with digital devices. In this way, the data takes on a meaning. Therefore, since it contains a statement of will and the person who issued it can be identified, it is accepted as documentary evidence[11]. Another opinion, which I also agree with, accepts digital data, which are duly filled in and protected and duly submitted to the court, as documentary evidence. Since there is a possibility that it may have been forged in the virtual environment, it may be documentary evidence after its authenticity is proven through forensic medicine. Before that, it is indicative evidence that shows a part of the event and must be supported by other evidence[12]. As I will discuss below, Supreme Court of Türkiye accepts digital evidence as evidence of scientific reliability until its authenticity is proven. On the other hand, Supreme Court of USA, has followed the general acceptance standard, requiring that digital evidence be accepted by science. Otherwise it is ignored.

---

[5] Digital data is defined in paragraph (a) of Article 3 of the Electronic Signature Law No. 5070. Accordingly; "Electronic data refers to records produced, transported or stored by electronic, optical or similar means."
[6] Berber, Leyla Keser. *Adli Bilişim,* Yetkin Yayıncılık, Ankara, 2004, p. 46.
[7] Arslan, Çetin. "Dijital Delil ve İletişimin Denetlenmesi", *Ceza Hukuku ve Kriminoloji Dergisi*, V. 3, I. 2, 2015, p. 253.
[8] Tezcan, Durmuş / Sırma Gezer, Özge / Saygılar Kırıt, Yasemin / Altınok Çalışkan, Elif / Alan, Esra / Özaydın, Özdem / Erden Tütüncü, Efser / Güzel, İdris / Köker, Nilüfer / Altınok Villemin, Derya / Tok, Mehmet Can. *Dijital Ceza Muhakemesi Hukuku*, 2. Baskı, Seçkin Yayıncılık, Ankara, 2022, p. 401.
[9] Özen, Muharrem / Özocak, Gürkan. "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)", *Ankara Barosu Dergisi*, I. 1, 2015, p. 59.
[10] Değirmenci, Olgun. *Ceza Muhakemesinde Sayısal (Dijital) Delil*, Seçkin Yayıncılık, Ankara, 2014, s. 130.
[11] Yenisey, Feridun / Nuhoğlu, Ayşe. *Ceza Muhakemesi Hukuku*, 10. Baskı, Seçkin Yayıncılık, Ankara, 2022, s. 576.
[12] Tezcan and others, p. 402.

B. Judicial Cooperation in Digital Evidence

The possibility of loss of digital evidence[13] and the fact that some companies are headquartered outside of Turkey brings with it the need for judicial cooperation. The process of cooperation should be fast[14]. In a world developing with technology, there is a need for a new and fast judicial cooperation. Rather than classical judicial cooperation, a large-scale cooperation with the participation of every country is required[15]. One manifestation of this cooperation is the Council of Europe Convention on Cybercrime. The convention emerged in Budapest on 23.11.2001 with the aim of introducing a common criminal policy for cybercrime through international judicial cooperation and was signed by 68 countries, including the USA, which is not a member of the Council of Europe. Turkey signed the convention on 10.11.2010 and it entered into force on 29.09.2014[16].

Article 3 of the Convention includes a section on judicial assistance. Since digital evidence can be lost quickly, effective and rapid international cooperation is necessary to combat it. In order to ensure judicial cooperation, the Convention regulates general principles in Article 23. Accordingly, judicial cooperation should cover not only crimes linked to information systems, but also other crimes where evidence is available in electronic form[17]. Therefore, even if some companies are headquartered in the United States, in accordance with the agreement, the information of suspects in the crime of threats committed by electronic means must be shared with the request through the Ministry of Justice within the scope of cooperation.

In addition, initiatives are envisaged to establish a 24/7 contact point at the General Directorate of International Law and Foreign Relations of the Ministry of Justice[18], which is the central authority for legal assistance[19].

II. PROOF OF THREAT CRIME IN TURKISH CRIMINAL LAW THROUGH DIGITAL EVIDENCE

When the crime of threatening is committed through digital tools such as communication tools, social networking sites, electronic mail and cameras that take audio and / or video, a number of problems arise in its proof. The decisions of the Supreme Court, which is subject to the continental European legal system, and Supreme Court of USA, which is dominated by Common law, have different approaches in solving these problems.

A. Proof in Threats Made Through Communication Tools

Telephone conversations, text messages and correspondence via *"Whatsapp"*, *"Bip"*, *"Telegram"* and similar messaging applications are within the scope of communication tools. Since

[13] Kiziroğlu, Serap Keskin. "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, V. 59, I. 1-2, 2001, p. 155.
[14] Csonka, Peter. "The Council of Europe's Convention On Cyber-Crime And Other European Initiatives", *International Review of Penal Law*, V. 77, p. 480.
[15] Önok, Murat. "Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Prof. Dr. Nur Centel'e Armağan, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, V. 19, I. 2, 2013, p. 1235-1236.
[16] Aliusta, Cahit / Benzer, Recep. "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, V. 4, I. 2, 2018, p. 37-38.
[17] The Budapest Convention, https://www.coe.int/en/web/cybercrime/the-budapest-convention, (Date of Access: 12.07.2024).
[18] https://diabgm.adalet.gov.tr/Home/SayfaDetay/ceza-istinabe14022020012410, (Date of Access: 12.07.2024).
[19] Önok, p. 1247.

communication tools are widespread today, the crime of threatening is frequently committed with these tools. The proof of the threats made in this way appears as a problem in the judgment phases.

In threats made through text messages on the phone, if the message is not deleted, it is possible to identify the person who made the threat by asking the GSM operator, since the number that sent the message appears. If the message has been deleted, the phone number should be determined by asking the complainant about the time interval in which the message was received and by requesting from the GSM operator the list of messages received on the complainant's phone during that time interval. Depending on the defense of the phone number owner, the investigation should be expanded and the suspect should be investigated, or if he/she does not have a consistent defense, it should be deemed to have committed the crime[20]. As a matter of fact, in a decision of the Supreme Court, in the face of the detection that the messages sent to the victim's mobile phone number were sent from the number registered in the name of the relative, the decision of the local court, which made an incomplete investigation was overturned in the face of the defense that the suspects did not use the line without asking whether the owner of the line to which the message was sent was using the line within the knowledge of the owner, and if not, who was using the line, and without looking at which IMEI number phone the lines were used from. Therefore, a decision should be made after the material truth is fully reached[21].

Recording the conversation via the voice recording program on the phone is one of the frequently used methods to prove verbal threats. Recording conversations without consent fits the legal definition of the offense of violating the confidentiality of communication (Article 132/1, second sentence of the Turkish Penal Code). Because in this article, the legislator punishes the person who illegally records the content of the communications made to him/her without the consent of the party to the conversation[22]. However, the Supreme Court gives an exception to the use of conversations recorded in this way only within the scope of criminal proceedings. Threats made in public or verbally are very difficult to prove. The Supreme Court requires that the evidence obtained in this way must be done without trapping and directing people in advance. Here, the sudden development of the event and the inability to obtain evidence by other means are adopted as criteria for the evaluation of sound recordings as evidence[23].

One opinion in the doctrine, which examines the state of necessity among the reasons for compliance with the law, suggests that voice recording can be made in order to protect the rights of the person who is exposed to threats via phone proportionally in order to escape from a serious and certain danger or to save someone else, and to ensure the capture of the perpetrator[24]. Another opinion suggests that the use of the right should be evaluated within the scope of the use of the right to sue and complain within the context of the reason of compliance with the law in the event of a sudden development and in order to obtain evidence[25]. The opinion I also agree with in the doctrine is; It argues that in cases of

[20] Gökcan, Hasan Tahsin / Artuç, Mustafa. *Yorumlu-Uygulamalı Türk Ceza Kanunu Şerhi*, Adalet Yayınevi, Ankara, 2022, p. 4122.
[21] Yargıtay 4. CD, E. 2016/8682, K. 2020/6996, KT. 16.06.2020, https://kararara ma.yargitay.gov.tr, (Date of Access: 08.11.2022).
[22] Sevük, Handan Yokuş. *Türk Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, 4. Baskı, Ankara, 2022, p. 529-530; Tezcan, Durmuş / Erdem, Mustafa Ruhan / Önok, Murat. *Teorik ve Pratik Ceza Özel Hukuku*, 20. Baskı, Seçkin Yayıncılık, Ankara, 2022, p. 701.
[23] Yargıtay Ceza Genel Kurulu, E. 2012/1270, K. 2013/248, KT. 21.05.2013; Yargıtay Ceza Genel Kurulu, E. 2020/430, K. 2021/161, KT. 02.04.2020, https://kararara ma.yargitay.gov.tr, (Date of Access: 28.03.2022).
[24] Zafer, Hamide. "Haberleşmenin Gizliliğini İhlal", *Özel Ceza Hukuku, C. III, Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar*, On İki Levha Yayıncılık, İstanbul, 2018, p. 515.
[25] Tezcan/Erdem/Önok, p. 709; Birtek, Fatih. *Ceza Muhakemesinde Delil ve İspat*, 2. Baskı, Adalet Yayınevi, Ankara, 2017, p. 324.

verbal crimes such as insults, threats or blackmail, obtaining evidence by recording the conversations of those who are exposed to these actions can be accepted within the scope of legitimate defense, which is a reason for compliance with the law[26]. Since he/she does not have the opportunity to prove the threatening attack against him/her in any other way, he/she defends himself/herself by committing the crime of violating the confidentiality of communication by recording against this attack. However, it considers the planned recordings of the victim (through a mechanism he/she has previously set up, by provocation, and without his/her knowledge) as unlawful. In a decision that the Supreme Court evaluated within the scope of legitimate defense; Since it is not possible to obtain evidence in insult and threat crimes, it overturned the decision of the first instance court, stating that the voice recordings taken as soon as the criminal words were uttered were lawful[27].

In threats made through *"Whatsapp"*, *"Bip"*, *"Telegram"* and similar messaging applications, the output of the messaging history can be classified as indicative evidence. Because their reality also needs to be proven. It is possible to change the correspondence, names or phone numbers in the messaging history by means of a computer. The authenticity of the messages is verified by matching the message contents in the correspondence printouts with the correspondence and phone number on the smartphone, and indicative evidence is proven and affects the judgment as a document whose authenticity has been proven. As a matter of fact, the Supreme Court overturned the decision of the court of first instance that disregarded these messages and returned the indictment[28].

B. Proof in Threats Made Through Social Networking Sites

On social networking sites such as *"Twitter"*, *"Facebook"*, *"Instagram"*, *"YouTube"*, *"Tiktok"* and similar, the user creates an account and posts through this account. Even if the name and surname are written on the account, its accuracy cannot be determined. When the crime of threatening with fake accounts is committed, determining who committed the crime has revealed the possibility of detecting crimes from the IP number, which is a digital evidence process[29]. In this case, who owns the account is determined by learning from the company that is the hosting provider of the social networking site, when and from which IP number the message came, and then by investigating who the IP number to be determined belongs to[30]. However, it is problematic to access and get information from social networking sites such as Facebook, Twitter and Instagram, whose corporate headquarters are located in the USA. In the event that there is no response from the companies despite the warrant written during the investigation phase, a decision of non-prosecution is made. In accordance with the Article 160/1 of the Criminal Procedure Code, the prosecutor is obliged to investigate the material truth. Therefore, in the decisions of the Supreme Court, it is stated that since the prosecutor has to investigate the perpetrators and evidence of the crime during the statute of limitations, he/she should not decide that there is no prosecution based on the negative answer without resorting to other methods (such as contacting the hosting provider by a forensic computer expert or conducting an investigation through

[26] Şen, Ersan. *Türk Hukukunda Telefon Dinleme Gizli Soruşturmacı X Muhbir*, 2. Baskı, Seçkin Yayıncılık, Ankara, 2008, p. 74; Erdağ, Ali İhsan. "İletişimin Denetlenmesi Kapsamında İki Önemli Sorun Olarak: Mağdurun İletişiminin Tespiti ve İletişimin Mağdur Tarafından Kaydedilmesi", *Türkiye Barolar Birliği*, I. 92, 2011, p. 49-54; Aydın, Devrim. *Ceza Muhakemesinde Deliller*, Yetkin Yayınları, Ankara, 2014, p. 213-214.

[27] Yargıtay 4. CD, E. 2019/5283, K. 2021/27483, KT. 24.11.2021, https://kararara ma.yargitay.gov.tr, (Date of Access: 04.11.2022).

[28] Yargıtay 4. CD, E. 2017/22735, K. 2018/467, KT. 11.01.2018; Yargıtay 4. CD, E. 2021/30760, K. 2021/27721, KT. 25.11.2021, https://kararara ma.yargitay.gov.tr, (Date of Access: 24.03.2022).

[29] Gedik, Doğan. "Bilişim Suçlarında Ip Tespiti İle Ekran Görüntüleri Çıktılarının İspat Değeri", *Bilişim Hukuku Dergisi*, V. 1, I. 1, Ankara, 2019, p. 56.

[30] Yargıtay 4. CD, E. 2018/1629, K. 2021/12536, KT. 07/04/2021, https://kararara ma.yargitay.gov.tr, (Date of Access: 24.03.2022).

the IP address)[31]. The investigation file must be followed by the prosecutor's office until the perpetrator is found during the statute of limitations.

In cases of threats made through fake accounts on social networking sites, the judge makes an interrogation to obtain the defendant's confession. As a result of the interrogation, if the defendant confirms that he/she is the owner of the account, the defendant is convicted, supported by other evidence[32].

C. Proof in Threats Made Via Electronic Mail (E-Mail)

The offense of threat can be committed through e-mails such as *"Gmail"*, *"Hotmail"*, *"Yahoo"* and similar e-mail tools. When the threat crime is committed via e-mail, it becomes difficult to determine who the e-mail address belongs to in threatening e-mails, since companies whose headquarters are in the USA do not have representative offices in Türkiye and rogatory requests are answered negatively[33]. However, the Supreme Court does not accept the decision that there is no need for prosecution, since the prosecutor is obliged to investigate the material fact ex officio. In such a case, it states that there is an obligation to continue to investigate the truth of the matter and overturns the decisions made solely on the grounds that the identity of the person in the United States could not be reached. Accordingly, the testimony of the witnesses indicated by the person making the criminal complaint should be taken, the telephone transcripts subject to the crime should be obtained, and the electronic devices (such as laptop, computer, cell phone) that are suitable for using the e-mail addresses of the victim and the suspect on the date of the crime and whether they are still in use should be evaluated. An expert witness should be consulted for the evaluation of documents and information[34].

D. Proof in Threats Made Through Audio and/or Cameras

If the crime of threatening is committed verbally, there is difficulty in proving it. With the development of technology, cameras that capture audio and/or images are frequently used in social life for the prevention of crime or the proof of crimes committed. The images taken with the camera can be used as evidence in criminal proceedings as long as their reliability is determined[35]. The Supreme Court also accepts the failure to investigate the records of workplace security cameras[36], mobile electronic system integration cameras and other devices[37] at the trial stage in terms of proving the crimes as a reason for reversal.

In order to benefit from camera recordings, it is necessary to determine their authenticity by transferring them from the virtual world to the real world in a state suitable for examination and

[31] Yargıtay 4. CD, E. 2018/819, K. 2018/4172, KT. 01/03/2018; Yargıtay 4. CD, E. 2020/18650, K. 2020/18542, KT. 07/12/2020, https://kararara ma.yargitay.gov.tr, (Date of Access: 25.03.2022).
[32] Yargıtay 12. CD, E. 2014/1409, K. 2014/20943, KT. 27.10.2014, https://kararara ma.yargitay.gov.tr, (Date of Access: 25.03.2022).
[33] Özsoy, Nevzat. "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK 243 ve 244)", *Yaşar Hukuk Dergisi*, V. 1, I. 2, July 2019, p. 340.
[34] Yargıtay 4. CD, E. 2019/2277, K. 2019/9064, KT. 15.05.2019, https://kararara ma.yargitay.gov.tr, (Date of Access: 28.03.2022).
[35] Yıldız, Ali Kemal. "Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu", *Ceza Hukuku Dergisi*, I. 2, December 2006, p. 256; Arslan, p. 263.
[36] Yargıtay 6. CD, E. 2021/2766, K. 2021/18235, KT. 25.11.2021, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[37] Yargıtay 17. CD, E. 2020/2630, K. 2020/6574, KT. 29.06.2020, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).

evaluation[38]. Digital evidence sheds light on the incident in question. However, since it is difficult to determine whether there is any intervention in the content of digital evidence or in which environment it was created, it is inconvenient to use it as evidence alone. Therefore, it must be supported by other evidence and the evidence must be confirmed by an expert[39]. Hence, if the judge has only digital evidence as evidence in the trial, even though the evidence is examined meticulously, any hesitation about whether the defendant committed the crime should be interpreted in favor of the defendant. Considering the principle that the defendant gets the benefit of the doubt, an acquittal decision should be given in terms of digital evidence that is likely to be mistaken[40]. In the decisions of the Supreme Court, it is seen that a decision of reversal is made considering this nature of digital evidence[41].

Digital evidence must be obtained through legal means in order to be used in criminal proceedings. The legislator regulated in Article 217/2 of the Criminal Procedure Code that unlawful evidence shall not constitute the basis of the verdict and accepted that it is absolutely unlawful. When the illegality of the evidence is mentioned, it should be noted that it is possible to benefit from this evidence if there is a reason for compliance with the law[42]. In its decision, the Supreme Court ruled that obtaining evidence in the crime committed by placing a camera in the room used as a private room is lawful based on the exercise of the right within the scope of the right to claim and defense. (Article 26/1 of the Turkish Penal Code)[43]. The Supreme Court, in its jurisprudence developed in terms of the use of camera recordings, did not accept hidden camera footage taken without the person's knowledge as evidence, except for threats or insult crimes where it is not possible to obtain evidence in any other way[44]. The Supreme Court states that even if the records taken in this way were made for the purpose of obtaining evidence, they constitute an attack on personal rights and require moral compensation[45].

III. PROVING THE CRIME OF THREATENING WITH DIGITAL EVIDENCE IN COMPARISON WITH THE SUPREME COURT OF USA DECISIONS

The American legal system is based on "common law" which places significant emphasis on court precedents in formal rulings. In this system, previous judicial decisions play a crucial role in how courts resolve current cases, even when a statute is involved[46]. In other words, Common law is typically uncodified, meaning there isn't a comprehensive collection of legal rules and statutes. While it does incorporate some scattered statutes, which are legislative decisions, it primarily relies on precedent judicial decisions made in previous, similar cases[47]. These precedents are preserved through court records and historically documented in collections of case law known as yearbooks and reports. The

[38] Yargıtay 1. CD, E. 2008/10249, K. 2012/48, KT. 16.01.2012, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[39] Yargıtay 2. CD, E. 2014/37084, K. 2017/6480, KT. 05.06.2017, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[40] Yıldız, p. 257; Arslan, p. 263.
[41] Yargıtay 13. CD, E. 2012/2260, K. 2013/12578, KT. 30.04.2013, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[42] Arslan, p. 264.
[43] Yargıtay 13. CD, E. 2011/7180, K. 2012/8523, KT. 26.03.2012; Yargıtay 8. CD, E. 2018/7510, K. 2018/9642, KT. 20.09.2018, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[44] Yargıtay 4. CD, E. 2007/11957, K. 2009/21077, KT. 22.12.2009, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[45] Yargıtay 4. HD, E. 2014/10463, K. 2015/6652, KT. 25.05.2015, https://kararara ma.yargitay.gov.tr, (Date of Access: 03.06.2022).
[46] Lewis, Sebastian. "Precedent and the Rule of Law", *Oxford Journal of Legal Studies*, V. 41, I. 4, 6 March 2021, p. 876.
[47] Dainow, Joseph. "The Civil Law and the Common Law: Some Points of Comparisons", *The American Journal Of Comparative Law*, V. 15, 1967, p. 426.

judge presiding over a new case determines which precedents to apply. Consequently, judges play a significant role in shaping American law. Common law operates as an adversarial system, where two opposing parties present their cases before a judge who moderates. A jury, composed of ordinary individuals without legal training, decides on the facts of the case. Based on the jury's verdict, the judge then determines the appropriate sentence[48].

Civil law, on the other hand, is based on codified law[49]. Countries with civil law systems have extensive, continually updated legal codes that detail all matters that can be brought before a court, the procedures to be followed, and the penalties for each offense. These codes differentiate between various categories of law: substantive law defines which actions are subject to criminal or civil prosecution, procedural law outlines the process for determining whether an action is criminal, and penal law specifies the penalties. In a civil law system, the judge's role is to establish the facts and apply the relevant provisions of the code. The judge often initiates formal charges, investigates the case, and makes a decision, but operates within the boundaries set by a comprehensive, codified set of laws. As a result, the judge's decision is less influential in shaping the law compared to the role of legislators and legal scholars who create and interpret these codes[50].

In Turkish criminal law, which is subject to the Civil law system, verbal threats are usually proved by witnesses and by the defendant's confession in court. On the other hand, if another witness who has a relevant contribution to the concrete incident testifies that “no threatening words were spoken”, no punishment is given. Supreme Court of Türkiye and Supreme Court of USA offer different solutions to the problems in proving threats with digital evidence.

To summarize;

Supreme Court of Türkiye

1- In the case of threats made by sending a message via cell phone, the GSM operator can be asked about the owner of the line to determine the authenticity of the message and the identity of the person making the threat. Since the phone owner will be a suspect, the investigation proceeds according to his/her statement. If the line owner and the phone owner are different people, it is accepted that it is necessary to expand the investigation and determine who sent the threatening message.

2- In the event that someone makes a threat during a phone call or while talking in an environment, the threat is proved through the voice recording program on the mobile phone. Although the recording made in this way constitutes the crime of violating the confidentiality of communication, Turkish Supreme Court accepts the use of such recordings only within the scope of criminal proceedings as an exception if one of the parties did not set a trap in advance (the event developed suddenly and the recording was taken in this way) or did not direct the other party to the threat. In addition, it is stated that although taking voice recordings is a violation of the confidentiality of communication, the provisions of legitimate defense should be applied by accepting the threat as an attack and recording against it as a self defense.

3- In case of threats through messaging applications such as "Whatsapp", "Bip", "Telegram", etc., it is stated that it is documentary evidence that affects the judgment if its reality can be proven.

[48] Dainow, p. 431-432.
[49] Dainow, p. 426.
[50] https://www.law.berkeley.edu/wp-content/uploads/2017/11/CommonLawCivilLawTraditions.pdf, (Date of Access: 11.07.2024).

Otherwise, it is accepted as indicative evidence showing a part of the event that needs to be supported by other evidence.

4- In threats made through social networking sites and e-mails, where the user can open an account without his/her own name and surname, it is not possible to prove who committed the act. Here, the suspect is first contacted by name and surname and a decision is made. In the case of fake accounts, if the suspect, who is reached from the IP number, confirms that the account belongs to him/her, he/she is criminally liable. Otherwise, the identity of the account is requested from the company that is the hosting provider of the social networking site. Those whose company headquarters are not in Türkiye do not provide information. Supreme Court of Türkiye argues that the truth should continue to be investigated in this case as well.

5- In proving the threat by means of audio and/or video recording cameras, Supreme Court of Türkiye considers these recordings to be suitable for examination and evaluation if the reality is determined by transferring them from the virtual world to the real world. Camera recordings are not accepted as evidence if they were taken secretly without the knowledge of the person who planned and threatened to trap people.

Supreme Court of USA

When the case law in Anglo-American law is examined in general, it is seen that a number of evaluation criteria are set out in terms of the use of digital evidence in the proceedings. The first criterion, the general acceptance criterion, which was applied for seventy-two years, was determined by the 1923 Fyre v. United States decision[51]. According to the criterion, there should be a standard recognized by science and this standard should be used to obtain evidence[52]. This criterion has been criticized as limiting, since evidence cannot be used in American courts if it is not accepted by science[53]. Therefore, the decision of Supreme Court of USA in William Daubert v. Merrell Dow Pharmaceuticals in 1995 is important[54]. In this decision, it is stated that the general admission criterion does not meet the requirements of the federal rules of evidence for the admission of evidence. It is the judge who determines the scientific reliability of digital evidence. In this case, the judge is required to make a preliminary inspection on whether the digital evidence that comes before him with the allegation that the offence of threatening has been committed can be used in the trial[55]. For example, in Counterman v. Colorado, Supreme Court of USA has seen that Billy Counterman sent hundreds of messages, many of them threatening, to local singer and musician C.W. between 2014 and 2016, each time opening a new Facebook account. Therefore, C.W. has suffered a mental breakdown. The Supreme Court accepted threatening messages on Facebook as evidence and completed its assessment on the basis of the material facts[56].

[51] https://casetext.com/case/frye-v-united-states-7, Submitted November 7, 1923, Decided December 3, 1923, (Date of Access: 21.02.2024).
[52] Değirmenci, p. 117; Sarsıkoğlu, Şenel. "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi*, Y. 6, I. 22, July 2015, p. 518.
[53] Değirmenci, p. 118; Sarsıkoğlu, p. 518.
[54] https://caselaw.findlaw.com/court/us-9th-circuit/1430422.html, Argued and Submitted March 22, 1994, Decided January 4, 1995, (Date of Access: 21.02.2024).
[55] Değirmenci, p. 118; Sarsıkoğlu, p. 518.
[56] Between 2014-2016, Billy Counterman created a new Facebook account each time and sent hundreds of messages to C.W., a local singer and musician, many of which contained threatening messages. As a result, C.W. suffered a mental breakdown and was unable to participate in social life. The decision of the local court, 497 P.3d 1039, which did not investigate the content of the messages, was reversed and remanded. Counterman v. Colorado, No. 22–138. Argued April 19, 2023–Decided June 27, 2023, https://www.supremecourt.gov/opinions/22pdf/22-

CONCLUSION

With the development of technology, it is seen that the crime of threatening is proved through digital evidence. There are difficulties in the prosecution of the crime, especially in terms of proving verbal threats. In this context, the crime of threatening is proved by means of communication tools, social networking sites, electronic mail, audio and / or video cameras.

With the voice recording application available on smartphones, one of the parties to the conversation can record the other party's voice. Although this situation constitutes the elements of the crime of violating the confidentiality of communication, there is difficulty in proving verbal threats in particular and it is not possible to obtain evidence in any other way. Therefore, if those who are exposed to these actions have not previously set a trap for the party involved in the conversation, recording their voice in order to present it to the court does not constitute a crime, as it will be within the scope of legitimate defense, which is a reason for compliance with the law.

On social networking sites, the user creates an account and can post through this account. Since the owners of the account use a pseudonym, the owner of the account is often not identified. In this case, as the prosecutor is obliged to investigate the material truth pursuant to Article 160/1 of the Criminal Procedure Code, he/she should investigate the IP address. Even if he/she receives a negative answer that the owner of the account cannot be identified, he/she should not decide that there is no need for prosecution and should investigate the truth by resorting to other methods.

In cases where the crime of threat is committed via e-mail, it becomes difficult to determine who the e-mail address belongs to in threatening e-mails, since companies whose headquarters are in the USA do not have representative offices in Türkiye and rogatory requests are answered negatively. However, the prosecutor's office has the obligation to investigate the material truth despite negative answers.

It is possible to prove the crime of threat through cameras that capture audio and/or images. However, in order to benefit from these records in the trial, they must be made suitable for the judge's review and evaluation. This is possible by transferring the audio and/or video from the virtual world to the real world. Since it is difficult to determine whether the content of digital evidence has been interfered with, this alone is not sufficient for conviction. Therefore, the material truth should be investigated by confirming the evidence and supporting the confession of crime with other evidence such as witnesses or documents. Therefore, even though there is only digital evidence in the trial, if the judge has doubts about whether the defendant committed the crime, he/she should interpret it in favor of the defendant.

In its judgements, Supreme Court of USA has stated that digital evidence should be subjected to a preliminary examination in order to ensure that it complies with federal terms and that the evidence can be used before the trial. The determination here is left entirely to the judge. In Turkish criminal procedure, the prosecutor must determine the lawfulness of digital evidence during the investigation phase. If it is determined during the prosecution phase, the judge cannot take it as a basis for the judgement since there is an absolute prohibition of evaluation.

138_43j7.pdf, (Date of Access: 21.02.2024).

Conflict of Interest

There is no conflict of interest.

Author Contributions

The authors did not specify the contribution rate.

REFERENCES

Aliusta, Cahit / Benzer, Recep. "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, V. 4, I. 2, 2018 s. 35-42.

Arslan, Çetin. "Dijital Delil ve İletişimin Denetlenmesi", *Ceza Hukuku ve Kriminoloji Dergisi*, V. 3, I. 2, 2015, p. 253-266.

Aydın, Devrim. *Ceza Muhakemesinde Deliller*, Yetkin Yayınları, Ankara, 2014.

Berber, Leyla Keser. *Adli Bilişim*, Yetkin Yayıncılık, Ankara, 2004.

Birtek, Fatih. *Ceza Muhakemesinde Delil ve İspat*. 2. Baskı, Adalet Yayınevi, Ankara, 2017.

Centel, Nur / Zafer, Hamide. *Ceza Muhakemesi Hukuku*, 21. Bası, Beta Yayıncılık, İstanbul, 2022.

Counterman v. Colorado, No. 22–138, Argued: April 19, 2023–Decided: June 27, 2023, https://www.supremecourt.gov/opinions/22pdf/22-138_43j7.pdf (Date of Access: 21.02.2024).

Csonka, Peter. "The Council of Europe's Convention on Cyber-Crime And Other European Initiatives", *International Review of Penal Law*, V. 77, p. 473-501.

Dainow, Joseph. "The Civil Law and the Common Law: Some Points of Comparisons", *The American Journal Of Comparative Law*, V. 15, 1967, p. 419-435.

Daubert v. Merrell Dow Pharmaceuticals Inc, No. 90-55397, Argued and Submitted: March 22, 1994, Decided: January 4, 1995, https://caselaw.findlaw.com/court/us-9th-circuit/1430422.html, (Date of Access: 21.02.2024).

Değirmenci, Olgun. *Ceza Muhakemesinde Sayısal (Dijital) Delil*, Seçkin Yayıncılık, Ankara, 2014.

Erdağ, Ali İhsan. "İletişimin Denetlenmesi Kapsamında İki Önemli Sorun Olarak: Mağdurun İletişiminin Tespiti ve İletişimin Mağdur Tarafından Kaydedilmesi", *Türkiye Barolar Birliği Dergisi*, I. 92, 2011, p. 31-61.

Fyre v. United States, No. 3968, Submitted: November 7, 1923-Decided: December 3, 1923, https://casetext.com/case/frye-v-united-states-7 (Date of Access: 21.02.2024).

Gedik, Doğan. "Bilişim Suçlarında Ip Tespiti ile Ekran Görüntüleri Çıktılarının İspat Değeri", *Bilişim Hukuku Dergisi*, V. 1, I. 1, 2019, p. 51-84.

Gökcan, Hasan Tahsin / Artuç, Mustafa. *Yorumlu-Uygulamalı Türk Ceza Kanunu Şerhi*, Adalet Yayınevi, Ankara 2022.

Jurisprudence, https://karararama.yargitay.gov.tr/

Kiziroğlu, Serap Keskin. *"Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, V. 59, I. 1-2, 2001, p. 155-180.

Legislation, https://www.mevzuat.gov.tr/

Lewis, Sebastian. "Precedent and the Rule of Law", *Oxford Journal of Legal Studies*, V. 41, I. 4, 2021, p. 873-898.

Önok, Murat. "Avrupa Konseyi Siber Suç Sözleşmesı Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", Prof. Dr. Nur Centel'e Armağan, *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, V.19, I. 2, 2013, p. 1229-1270.

Özen, Muharrem / Özocak, Gürkan. "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)", *Ankara Barosu Dergisi*, I. 1, 2015, p. 43-77.

Özsoy, Nevzat. "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK 243 ve 244)", *Yaşar Hukuk Dergisi*, V. 1, I. 2, July 2019, p. 296-352.

Öztürk, Bahri / Erdem, Mustafa Ruhan / Özbek, Veli Özer. *Uygulamalı Ceza Muhakemesi Hukuku*, 11. Baskı, Seçkin Yayıncılık, Ankara, 2007.

Goodison, Sean / Davis, Robert / Jackson, Brian. Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence, *RAND Corporation*, 2015, p. 1-32.

Tezcan, Durmuş / Erdem, Mustafa Ruhan / Önok, Murat. *Teorik ve Pratik Ceza Özel Hukuku*. 20. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Tezcan, Durmuş / Sırma Gezer, Özge / Saygılar Kırıt, Yasemin / Altınok Çalışkan, Elif / Alan, Esra / Özaydın, Özdem / Erden Tütüncü, Efser / Güzel, İdris / Köker, Nilüfer / Altınok Villemin, Derya / Tok, Mehmet Can. *Dijital Ceza Muhakemesi Hukuku*, 2. Baskı, Seçkin Yayıncılık, Ankara, 2022.

The Common Law and Civil Law Traditions, https://www.law.berkeley.edu/wp-content/uploads/2017/11/CommonLawCivilLawTraditions.pdf

Sarsıkoğlu, Şenel. "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil

(E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi*, Y. 6, I. 22, July 2015, p. 507-534.

Sevük, Handan Yokuş. *Türk Ceza Hukuku Özel Hükümler*, 4. Baskı, Adalet Yayınevi, Ankara, 2022.

Şen, Ersan. *Türk Hukukunda Telefon Dinleme Gizli Soruşturmacı X Muhbir*, 2. Baskı, Seçkin Yayıncılık, Ankara, 2008.

Sarsıkoğlu, Şenel. "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi*, Y. 6, I. 22, July 2015, p. 507-534.

Yavuz, Mehmet. "Ceza Muhakemesinde İspat Sorunu", *Türkiye Adalet Akademisi Dergisi*, Y. 3, I. 9, April 2012, p. 151-176.

Yenisey, Feridun / Nuhoğlu, Ayşe. *Ceza Muhakemesi Hukuku*, 10. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Yıldız, Ali Kemal. "Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu", Ceza Hukuku Dergisi, I. 2, December 2006, p. 253-264.

Zafer, Hamide. "Haberleşmenin Gizliliğini İhlal", *Özel Ceza Hukuku, C. III, Hürriyete, Şerefe, Özel Hayata, Hayatın Gizli Alanına Karşı Suçlar*, On İki Levha Yayıncılık, İstanbul, 2018.