PART 1

THE SIGNIFICANCE OF DIGITAL EVIDENCE IN THE LEGAL DOMAIN

HUKUKTA DİJİTAL DELİLLERİN ÖNEMİ

SENA NUR AKKAPLAN
MUHAMMET AKİF GÖKSU

PART 1

ABSTRACT | ÖZET

This research examines the legal and technical aspects of digital evidence within the context of criminal proceedings, the importance of this type of evidence in judicial processes and the status of the current legal regulations in this field.

Bu çalışmada; dijital delillerin ceza yargılamasındaki hukuki ve teknik boyutları ele alınarak, bu delil türünün yargısal süreçlerdeki önemi ve bu alandaki yasal düzenlemelerin güncel durumu değerlendirilmektedir.

KEYWORDS | ANAHTAR KELİMELER

Evidence Acquisition Techniques, Information Law, Forensic Informatics, Digital Evidence, Data, Information Systems, Criminal Procedure, Evidence Collection Methods.

Delil Toplama Yöntemleri, Bilişim Hukuku, Adli Bilişim, Dijital Delil, Veri, Bilişim Sistemleri, Ceza Muhakemesi, Delil Toplama Yöntemleri.

I. INTRODUCTION

The exponential growth of technology and its ubiquitous integration into contemporary society have rendered digitalization an indispensable facet of modern life. Encompassing a broad spectrum of activities, from social interactions to legal and financial transactions, the majority of daily endeavors are now conducted within digital ecosystems. In the everyday lives of people and organizations, for instance, digital infrastructures that offer access to public services like E-Devlet, E-Nabız, Web Tapu, Mersis, e-commerce platforms, and social media platforms are crucial. These platforms are used in many areas such as the exchange of goods and services, access to public services, social interaction and communication. The penetration of digital transformation into all areas of life has also transformed the methods of committing offences, and digital evidence has gained an important place in criminal proceedings. New types of crimes committed in digital environments have emerged, new methods have been developed in which information technologies are used in the commission of traditional crimes, and situations where evidence suitable for proving the crime can be accessed electronically have become widespread. This situation has led to the inadequacy of combatting crimes with traditional methods in criminal proceedings. In this context, the need for digital evidence in criminal proceedings has increased; digital evidence has been accepted and regulated in criminal proceedings with the protection measures regulated in Articles 134 and 135 of the Code of Criminal Procedure No. 5271 (**"Code No. 5271"**). In this article, the legal and technical aspects of digital evidence will be analysed and the place and importance of this type of evidence in criminal proceedings will be evaluated.

I. GİRİŞ

Günümüzde teknolojinin hızla gelişmesiyle hayatımızın her alanına sirayet etmesi, dijitalleşmeyi kaçınılmaz hale getirmiştir. Sosyal ilişkilerimizden hukuki ve finansal işlemlere kadar uzanan geniş bir yelpazede, günlük işlerimizin büyük bir bölümü artık dijital ortamlarda yürütülmektedir. Örneğin E-devlet, E-nabız, Web Tapu, Mersis gibi kamu hizmetlerine erişimin sağlandığı dijital altyapılar, e-ticaret platformları ve sosyal medya platformları, bireylerin ve kurumların günlük yaşamlarında önemli bir rol oynamaktadır. Bu platformlar, mal ve hizmet alışverişi, kamu hizmetlerine erişim, sosyal etkileşim ve haberleşme gibi birçok alanda kullanılmaktadır. Dijital dönüşümün yaşamın her alanına sirayet etmesi, suç işleme yöntemlerini de dönüştürerek dijital delillerin ceza yargılamasında önemli bir yer edinmesini sağlamıştır. Dijital ortamlarda gerçekleştirilen yeni suç tipleri ortaya çıkmış, geleneksel suçların işlenmesinde bilişim teknolojilerinin kullanıldığı yeni yöntemler geliştirilmiş ve suçun ispatına elverişli delillerin elektronik ortamda erişilebildiği durumlar yaygınlaşmıştır. Bu durum, ceza yargılamasında geleneksel yöntemlerle suçlarla mücadele edilmesinin yetersiz kalmasına sebep olmuştur. Bu bağlamda, ceza muhakemesi süreçlerinde dijital delillere olan ihtiyaç artmış; 5271 sayılı Ceza Muhakemeleri Kanunu'nun (**"5271 sayılı Kanun"**) 134. ve 135. maddelerinde düzenlenen koruma tedbirleri ile dijital deliller ceza muhakemesinde kabul edilmiştir ve düzenleme alanı bulmuştur. Makalemizde, dijital delillerin hukuki ve teknik boyutları incelenerek bu delil türünün ceza yargılamasındaki yeri ve önemi değerlendirilecektir.

FOOTNOTE

1 Guidelines of the Committee of Ministers of the Council of Europe on Electronic Evidence in Civil and Administrative Proceedings, January 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 (Access date: 5 August 2024), p. 6.

2 U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Access date: 5 August 2024), p. 39.

II. THE CONCEPT OF DIGITAL EVIDENCE

The concept of digital evidence generally refers to any data produced, processed, stored or transferred on information systems or networks and used as evidence in legal proceedings[1].

Various sources offer divergent definitions of this concept. For instance, the United States Department of Justice's Guide for Law Enforcement characterizes digital evidence as "binary format information stored or transmitted on a computer that can be used as evidence in court"[2]. Collectively, numerous definitions converge on the notion that digital evidence constitutes digital data employed to ascertain the commission of a crime.

II. DİJİTAL DELİL KAVRAMI

Dijital delil kavramı, genel anlamıyla bilişim sistemleri veya ağları üzerinde üretilen, işlenen, depolanan veya aktarılan yasal süreçlerde kanıt olarak kullanılan her türlü veriyi ifade eder[1].

Bu kavram, farklı kaynaklarda çeşitli şekillerde tanımlanmıştır. Örneğin Amerika Birleşik Devletleri Adalet Bakanlığı Adli Bilişim Soruşturmaları Kılavuzu'nda dijital delil, "bilgisayar ortamında saklanan veya iletilen, mahkemede delil olarak kullanılabilen ikili biçimli bilgi" olarak tanımlanır[2]. Genel olarak, birçok tanım dijital delilin, bir suçun işlenip işlenmediğini tespit etmek için kullanılan dijital veri olduğunu ifade etmektedir.

DİPNOT

1 Guidelines of the Committee of Ministers of the Council of Europe on Electronic Evidence in Civil and Administrative Proceedings, Ocak 2019, https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5 (Erişim Tarihi: 5 Ağustos 2024), s. 6.

2 U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Nisan 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (Erişim tarihi: 5 Ağustos 2024), s. 39.

PART 1

III. CHARACTERISTICS OF DIGITAL EVIDENCE

In order for evidence to be considered valid, it must have various elements. These elements include; the evidence must have been obtained in accordance with the law, the evidence must be accessible (availability), it must be rational, it must be in accordance with reality, it must accurately reflect the event to be proved (relevance), it must be important in terms of proof, it must not contradict other evidence (commonality), it must be based on a solid and reliable foundation and, of course, it must be available. The existence of all of these elements is an absolute requirement for the admissibility of evidence in the judicial process.

In addition to these qualities that must be present in all kinds of evidence due to their computational nature, digital evidence has a number of qualities that are different from classical evidence. In our study, these distinctive qualities of digital evidence will be examined under six different headings: having a hidden structure, being copyable and reproducible, being easily altered or destroyed, being international in nature, being difficult to determine their ownership, and being dynamic and variable in nature.

A. The Hidden Structure of Digital Evidence

One of the most prominent characteristics of digital evidence that distinguishes it from other evidence is that it has a hidden structure that is invisible at first glance, as in the case of DNA and fingerprint evidence[3]. However, unlike digital evidence, the concretization of this evidence can be done at the time of the first examination at the crime scene. Unlike physical evidence, digital evidence does not have a tangible existence, and therefore the examination process may be longer and more difficult. This examination entails rendering digital evidence tangible through the utilization of technological devices.

Since electronic devices have a tangible structure, the technological devices at the crime scene are taken into consideration and these devices are examined with methods specific to digital evidence. The digital applications and stored data residing within these devices contribute significantly to the materialization of evidence.

III. DİJİTAL DELİLLERİN ÖZELLİKLERİ

Bir delilin geçerli kabul edilebilmesi için çeşitli unsurlara sahip olması gerekmektedir. Bunlar arasında; delilin hukuka uygun bir şekilde elde edilmiş olması, delile ulaşılabilmesi (elde edilebilirlik), mantık ve akla uygun (rasyonel) olması, gerçekliğe uygun olması, ispat edilmek istenen olayı doğru bir şekilde yansıtması (maksada elverişlilik), ispat bakımından önemli bir nitelik taşıması, diğer delillerle çelişmemesi (müştereklik), sağlam ve güvenilir bir temele dayanması ve tabi ki elde edilebilir olması sayılabilir. Bu unsurların tamamının varlığı, delilin yargılama sürecinde kabul edilebilirliği açısından mutlak bir gerekliliktir.

Dijital deliller, bilişimsel doğaları gereği her nevi delilde bulunması gereken bu niteliklerin yanında klasik delillerden farklı birtakım niteliklere sahiptir. Çalışmamızda dijital delillerin ayırt edici bu nitelikleri; gizli bir yapıya sahip olmaları, kopyalanabilir ve çoğaltılabilir olmaları, kolaylıkla değiştirilebilir veya yok edilebilir olmaları, uluslararası nitelikte olmaları, aidiyet tespitlerinin zor oluşu ve dinamik ve değişken yapıda olmaları olmak üzere altı ayrı başlıkta irdelenecektir.

A. Dijital Delillerin Gizli Yapısı

Dijital delilleri diğer delillerden ayıran en belirgin niteliklerinden biri, DNA ve parmak izi delilinde olduğu gibi ilk bakışta gözle görülmeyen, gizli bir yapıya sahip olmalarıdır[3]. Ancak fiziksel delillerin somutlaştırılması, dijital delillerden farklı olarak olay yerinde ilk inceleme anında yapılabilmektedir. Dijital delillerin ise, fiziksel delillerin aksine somut bir varlığa sahip olmamaları sebebiyle incelenme süreçleri daha uzun ve meşakkatli olabilmektedir. Bu inceleme, dijital delilin teknolojik aygıtlar vasıtasıyla irdelenerek somut bir hale getirilmesi ile gerçekleştirilmektedir.

Elektronik aygıtların somut bir yapıya sahip olması nedeniyle dijital delillerin tespiti yapılırken, öncelikle olay yerindeki teknolojik aygıtlar dikkate alınarak bu aygıtların dijital delillere özgü yöntemlerle incelemesi gerçekleştirilmektedir. Bu aygıtlarda yer alan dijital uygulamalar ve depolanan veriler delilin somutlaştırılmasında rol oynamaktadırlar.

FOOTNOTE

3 Electronic Crime Scene Investigation: A Guide for First Responders, July 2001, https://www.ojp.gov/pdffiles1/nij/187736.pdf (Access date: 5 August 2024), p. 6.

4 Electronic Evidence Guide, December 2014, https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf (Access Date: August 5, 2024), p. 12.

5 **Uğur Kaynakçıoğlu,** "Ceza Muhakemesinde Dijital Deliller", June 2015, p. 39.

6 Electronic Evidence Guide, p. 12.

However, apart from the cases where technological devices used in the crime and having a physical existence are examined, digital evidence can also be obtained by accessing the digital space in the computational world where the criminal act was committed. Therefore, in practice, digital evidence must be concretized through an examination that requires a certain period of time or a technical method. This examination is carried out by forensic informatics experts who have technical equipment in this field. This unique secret structure of digital evidence, which requires a technical examination process in terms of concretization, is one of the features that distinguishes it from other types of evidence.

B. The Copyable and Reproducible Structure of Digital Evidence

Digital evidence exhibits the unique characteristic of being copied countless times without degradation. Each replica is an exact facsimile of the original, enabling multiple copies to be examined independently and concurrently by various experts for diverse purposes, while the original data remains pristine[4]. This structure arises from the inherent capacity of digital devices to precisely replicate the code sequences constituting data. This characteristic of digital evidence expedites the examination process and facilitates the presentation of such evidence within judicial proceedings[5].

C. Easily Altered or Destroyed Structure of Digital Evidence

The memory state of computer systems undergoes constant modification during routine operation. These alterations can be attributed to user-initiated actions, such as saving or copying data, or to automated processes executed by the operating system, including memory allocation and data swapping[6]. Consequently, digital data are susceptible to corruption or destruction even under normal usage conditions. This inherent characteristic of digital evidence necessitates a meticulous approach to forensic examination.

In addition, although digital evidence can be easily altered, it should not be ignored that these alterations and manipulations

Bununla birlikte, suçta kullanılan ve fiziki bir varlığı bulunan teknolojik aygıtların incelendiği durumlar dışında, bilişimsel dünyada suç konusu fiilin gerçekleştirildiği dijital alana erişimin sağlanması ile de dijital delillere ulaşılabilmektedir. Dolayısıyla uygulamada dijital delillerin belirli bir süre veya teknik bir yöntem gerektiren bir inceleme ile somutlaştırılması gerekmektedir. Bu inceleme ise, bu alanda teknik donanıma sahip adli bilişim uzmanları tarafından gerçekleştirilmektedir. Dijital delillerin, somutlaştırılması bakımından teknik bir inceleme sürecine ihtiyaç duyan kendine has bu gizli yapısı, onu diğer delil türlerinden ayıran özelliklerden biridir.

B. Dijital Delillerin Kopyalanabilmesi ve Çoğaltılabilmesi

Dijital deliller, bozulmadan sayısız kez kopyalanabilme özelliğine sahiptir; her kopya orijinaliyle tamamen aynı özelliklere sahiptir. Bu eşsiz niteliği sayesinde, delilin birden fazla kopyası farklı uzmanlar tarafından bağımsız olarak ve aynı anda farklı amaçlarla incelenebilirken orijinal veri etkilenmez[4]. Zira dijital cihazlarda, verileri oluşturan kod dizilimlerinin birebir aktarılması için gerekli komut ve yöntemler bulunmaktadır. Dijital delillerin bu niteliği, incelenme süreçlerini hızlandırdığı gibi bu delillerin mahkemeye sunulmasını da kolaylaştırmaktadır[5].

C. Dijital Delillerin Kolaylıkla Değiştirilebilir veya Yok Edilebilir Olmaları

Normal kullanım sırasında, bilgisayar sistemlerinin hafıza durumları sürekli olarak değişime uğrar. Bu değişim, kullanıcı talimatları (örneğin, veri kaydetme, kopyalama) veya bilgisayar işletim sistemi tarafından otomatik olarak gerçekleştirilen işlemler (örneğin, bellek ayırma, veri takası) nedeniyle meydana gelebilmektedir[6]. Bu sebeple, dijital veriler normal kullanım esnasında dahi bozulma veya yok olma riski ile karşı karşıyadır. Dijital delillerin bu niteliği, bu tür delillere yönelik adli incelemelerde daha titiz bir yaklaşım gerektirmektedir.

Buna ek olarak, her ne kadar dijital deliller üzerinde kolaylıkla değişiklik yapılabilse de yapılan bu değişiklik ve manipülasyonların

DİPNOT

3 Electronic Crime Scene Investigation: A Guide for First Responders, Temmuz 2001, https://www.ojp.gov/pdffiles1/nij/187736.pdf (Erişim tarihi: 5 Ağustos 2024), s. 6.

4 Electronic Evidence Guide, Aralık 2014, https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf (Erişim Tarihi: 5 Ağustos 2024), s. 12.

5 **Uğur Kaynakçıoğlu,** "Ceza Muhakemesinde Dijital Deliller", Haziran 2015, s. 39.

6 Electronic Evidence Guide, s. 12.

PART 1

can be detected by methods developed by experts.

D. International Nature of Digital Evidence

A salient characteristic of digital evidence is its capacity to transcend geographical boundaries. Given the intricate network of electronic communication, digital data can be dispersed across the globe[7]. This circumstance renders the acquisition of digital evidence within judicial proceedings notably complex.

Even identifying the source of a piece of digital evidence can pose significant challenges. The situation is further complicated if the source is located in a country outside the jurisdiction of the relevant country. For instance, data accessed through cloud technologies or internet infrastructure may be physically stored in a different country.

Therefore, the acquisition of digital evidence takes on an international character. Judicial authorities have to cooperate not only with institutions in their own country, but also with authorities in foreign countries and international organizations. The insufficiency of international judicial cooperation mechanisms is an important obstacle in this process.

E. Difficulty in Determining the Ownership of Digital Evidence

The primary reason for the international scope of digital evidence, transcending geo-

uzmanlarca geliştirilen yöntemlerle tespit edilebildiği de göz ardı edilmemelidir.

D. Dijital Delillerin Uluslararası Niteliği

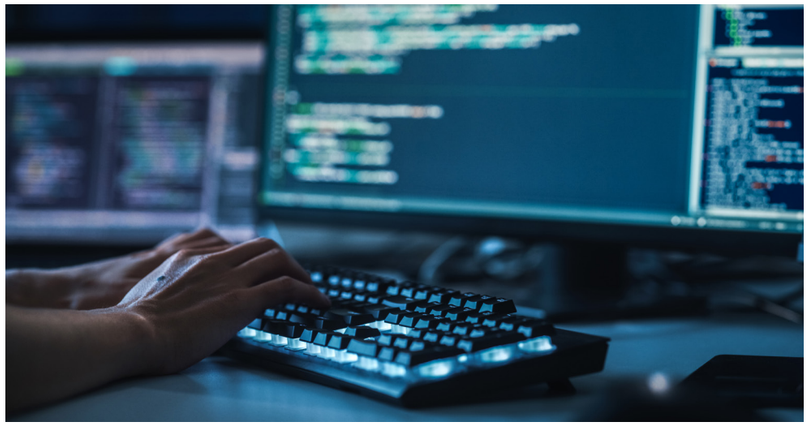
Dijital delillerin en belirgin özelliklerinden biri, coğrafi sınırları aşabilen bir yapıya sahip olmalarıdır. Özellikle elektronik cihazlar arasındaki yoğun iletişim ağı göz önüne alındığında, dijital verilerin dünya genelinde dağılmış olabileceği görülmektedir[7]. Bu durum, adli süreçlerde dijital delil toplama işlemini oldukça karmaşık hale getirmektedir.

Bir dijital delilin kaynağının belirlenmesi dahi büyük zorluklar içerebilir. Kaynak, ilgili ülkenin yargı yetkisinin dışında bir ülkede bulunuyorsa, durum daha da karmaşıklaşır. Örneğin, bulut teknolojileri veya internet altyapısı üzerinden erişilen veriler, fiziksel olarak farklı bir ülkede depolanıyor olabilir.

Bu nedenle, dijital delil toplama işlemi, uluslararası bir karakter kazanmaktadır. Adli makamlar, sadece kendi ülkesindeki kurumlarla değil, yabancı ülkelerdeki ve uluslararası kuruluşlardaki yetkililerle de iş birliği yapmak zorunda kalmaktadır. Uluslararası adli yardımlaşma mekanizmalarının yetersizliği, bu süreçte önemli bir engel olarak karşımıza çıkmaktadır.

E. Dijital Delillerin Aidiyetinin Belirlenmesinin Güçlüğü

Dijital delillerin coğrafi sınırları aşan uluslararası bir yapıda olmasının temel nedeni,



FOOTNOTE

7 **Mustafa Göksu,** Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayinevi, 2011, p. 31-32.

8 **Göksu,** op. cit. , p. 32

9 **Göksu,** op. cit. , p. 32.

graphical boundaries, lies in its accessibility for creation by any individual. However, this ease of production significantly complicates the determination of ownership. In particular, environments prioritizing anonymity, such as the internet, obfuscate the identification of data sources. Even if the origin of information is ascertained, determining the true owner of that source remains a distinct challenge. This predicament necessitates the development of innovative evidentiary methodologies to substantiate ownership within legal proceedings. Technologies such as secure electronic signatures have emerged as pivotal solutions for establishing ownership[8].

F. The Evolving and Mutable Nature of Digital Evidence

Another salient characteristic of digital evidence is its mutable and evolving nature[9]. The rapid advancement of technology affects both the methods of producing digital evidence and the ways in which it is stored and processed. This rapid change creates significant difficulties in the processes of examining and evaluating digital evidence.

herkes tarafından kolayca üretilebilmeleridir. Ancak bu kolay üretilebilirlik, dijital delillerin aidiyetinin belirlenmesini oldukça zorlaştırmaktadır. Özellikle internet gibi anonimliğin ön planda olduğu ortamlarda, verilerin kaynağını tespit etmek oldukça güçtür. Bilginin üretildiği kaynağa ulaşılsa dahi, bu kaynağın gerçek sahibinin belirlenmesi ayrı bir sorun olarak karşımıza çıkmaktadır. Bu durum, hukuki süreçlerde aidiyetin ispatı için yeni kanıtlama yöntemlerinin geliştirilmesini zorunlu kılmaktadır. Güvenli elektronik imza gibi teknolojiler, aidiyetin belirlenmesi hususunda önemli bir çözüm olarak ortaya çıkmıştır[8].

F. Dijital Delillerin Dinamik ve Değişken Yapısı

Dijital delillerin bir diğer önemli özelliği, sürekli bir değişim ve gelişim içerisinde olmalarıdır[9]. Teknolojinin hızla gelişmesi gerek dijital delillerin üretilmesi gerekse bunların saklanması ve işlenmesi yöntemlerinde değişikliklere yol açmaktadır. Bu hızlı değişim, dijital delillerin incelenmesi ve değerlendirilmesi süreçlerinde önemli zorluklar yaratmaktadır.

IV. LEGAL REGULATIONS REGARDING DIGITAL EVIDENCE

The international nature of digital evidence has brought about the need to determine common standards in legal regulations to be made in this field; in the process, countries and international legal personalities have carried out various legal studies in cooperation with each other in order to determine an international legal framework in this field.

As a result of these international studies, important regulations have been made in the legislation of many countries regarding information technologies. However, these regulations are not yet considered fully sufficient due to the dynamic structure of the rapidly changing technological environment. The continuous development of technology makes it difficult for legal regulations to keep up with these developments. However, since excessively restrictive regulations will cause fundamental rights and freedoms to be restricted, legal regulations to be made in this area require a careful approach.

IV. DİJİTAL DELİLLERE İLİŞKİN YASAL DÜZENLEMELER

Dijital delillerin uluslararası yapısı, bu alanda yapılacak hukuki düzenlemelerde ortak standartların belirlenmesi ihtiyacını beraberinde getirmiş; süreç içinde ülkeler ve milletlerarası hukuk kişileri birbirileriyle iş birliği içinde bu alanda uluslararası bir hukuki çerçeve belirlemek amacıyla çeşitli hukuki çalışmalar yapmıştır.

Uluslararası çapta yapılan bu çalışmalar sonucunda, pek çok ülke mevzuatında bilişim teknolojilerine ilişkin önemli düzenlemeler yapılmıştır. Ancak bu düzenlemeler, hızla değişen teknolojik ortamın dinamik yapısı nedeniyle henüz tam anlamıyla yeterli görülmemektedir. Teknolojinin sürekli gelişimi, hukuki düzenlemelerin bu gelişmelere ayak uydurmasını zorlaştırmaktadır. Bununla birlikte, aşırı derecede kısıtlayıcı düzenlemeler, temel hak ve özgürlüklerin kısıtlanmasına sebep olacağından, bu alanda yapılacak hukuki düzenlemeler dikkatli bir yaklaşım gerektirmektedir.

DİPNOT

7 **Mustafa Göksu,** Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayınevi, 2011, s. 31-32.

8 **Göksu,** a.g.e. , s. 32.

9 **Göksu,** a.g.e. , s. 32.

PART 1

However, current international and national legal regulations are comprehensive enough to allow us to make a comprehensive assessment of the legal status of digital evidence. The examples to be examined in this section will help us better understand the legal dimension of digital evidence.

A. Regulations Regarding Digital Evidence in International Law

Given the transnational nature of cybercrimes, which transcend geographical boundaries, it is impossible to combat them solely through national legal frameworks. Consequently, numerous international organizations are engaged in legal efforts in this field. The subsequent sections of this paper will delve into the primary regulations enacted in this domain.

1. United Nations

The evolution of technology has elevated the significance of digital evidence within judicial proceedings, gradually supplanting traditional physical evidence. This paradigm shift necessitates the establishment of novel regulations governing the collection, preservation, and evaluation of digital evidence by judicial systems. The four fundamental areas identified by the United Nations within the UNMPCCR framework (coercive measures, personal data, admissibility of digital evidence, and international cooperation)[10] underscore the intricate legal challenges inherent in digital evidence.

The legal and practical implications of coercive procedures employed in the collection of digital evidence have been a subject of ongoing discourse. A significant challenge within this context lies in the complexities associated with search and seizure operations. While the rules of search and seizure in criminal proceedings target tangible objects, the abstract nature of digital data makes it difficult to apply these rules. However, with the acceptance of digital data as evidence, the legal gaps in this area have become even more apparent.

Assistance obligations are another problem in this area. In the case of new legal regulations regarding search and seizure in the examination of digital evidence, the technical inadequacy of judicial authorities in this area may cause problems in practice. In particular, if the delivery of the seized item is requested, cooperation in obtaining the data will differ from the assistance expected in obtaining classical evidence.

Ne var ki, mevcut uluslararası ve ulusal hukuki düzenlemeler, dijital delillerin hukuki statüsü hakkında kapsamlı bir değerlendirme yapmamıza imkan tanıyacak derecede kapsamlıdır. Bu bölümde incelenecek örnekler, dijital delillerin hukuki boyutunu daha iyi anlamamıza yardımcı olacaktır.

A. Uluslararası Hukukta Dijital Delillere İlişkin Düzenlemeler

Bilişim suçlarının coğrafi sınırları aşan, uluslararası düzlemde işlenmeye elverişli yapısı nedeniyle, bu suçlarla salt ulusal hukuki düzenlemeler ile mücadele etmenin imkanı bulunmamaktadır. Bu doğrultuda, pek çok uluslararası örgüt bu alanda hukuki çalışmalar yürütmektedir. Yazımızın devamında bu alanda yapılan başlıca düzenlemelere yer verilecektir.

1. Birleşmiş Milletler

Teknolojinin ilerlemesiyle birlikte, adli süreçlerde dijital delillerin önemi artmakta ve dijital deliller geleneksel fiziksel delillerin yerini almaya başlamaktadır. Bu durum, yargı sistemlerinin; dijital delillerin toplanması, saklanması ve değerlendirilmesi konusunda yeni düzenlemelere ihtiyaç duymasına neden olmuştur. UNMPCCR kapsamında Birleşmiş Milletlerin belirlediği dört temel alan (cebri güç, kişisel veriler, dijital delillerin kabul edilebilirliği ve uluslararası iş birliği)[10], dijital delillerin hukuki boyutunda karşılaşılan zorlukları içeren alanlar olarak karşımıza çıkmaktadır.

Dijital delil toplamada kullanılan cebri işlemlerin mevzuata uygunluğu ve etkinliği konusunda tartışmalar bulunmaktadır. Bu konudaki en büyük sorun, arama ve el koymada yaşanan güçlüklerdir. Zira ceza muhakemesinde arama ve el koyma kuralları somut eşyaları hedef alırken, dijital verilerin soyut yapısı bu kuralların uygulanmasını zorlaştırmaktadır. Dijital verilerin delil olarak kabul edilmesiyle birlikte, bu alandaki hukuki boşluklar daha da belirgin hale gelmiştir.

Yardım yükümlülükleri, bu alandaki bir diğer problem olarak karşımıza çıkmaktadır. Dijital delillerin incelenmesi konusunda arama ve el koymaya ilişkin yeni yasal düzenlemeler getirilmesi halinde, adli makamların bu alandaki teknik yetersizliği uygulamalarda sorunlara yol açabilecektir. Özellikle; el konulacak eşyanın tesliminin istenmesi halinde, verilerin elde edilmesine yönelik iş birliği klasik delil elde edilmesinde beklenen yardıma göre farklılık gösterecektir.

However, in the case of monitoring communications, the balance between the fundamental rights of individuals and public safety must be delicately established. Although monitoring telecommunications lines and computer systems is an important tool in criminal investigations, strong legal safeguards must be established to prevent arbitrary use of these practices. In this context, detailed legal regulations must be made regarding the scope, duration and procedures of monitoring authority.

Whether digital evidence can be accepted as evidence in judicial processes is one of the biggest debates in this area. This issue is not just a theoretical debate, but a practical one that directly concerns the authority of judicial authorities to collect evidence. In many jurisdictions, digital data is not accepted as evidence in criminal cases because it can be easily changed and its originality cannot be verified[11].

Another important problem in this area is the lack of coordination at the international level. In order to overcome these difficulties faced by criminal procedural law, international cooperation mechanisms are becoming increasingly important. International courts such as the European Court of Human Rights play an important role by assessing the powers of the relevant authorities within the framework of Article 8 of the European Convention on Human Rights (**"ECHR"**), especially in matters such as the surveillance of communications[12].

2. European Union

The European Union (**"EU"**) has made various regulations to determine the legal status of digital evidence and to strengthen international cooperation in this field. Early regulations such as the Data Protection Directive of 1995[13] and the Directive on the protection of private life and the processing of personal data in the telecommunications sector of 1997[14] have determined the principles of protection of personal data and confidentiality in the telecommunications sector. The Charter of Fundamental Rights of the European Union has established the principle

Bununla birlikte iletişimin denetlenmesi durumunda, bireylerin temel hakları ile kamu güvenliği arasındaki denge hassas bir şekilde kurulmalıdır. Telekomünikasyon hatları ve bilgisayar sistemlerinin denetlenmesi, ceza soruşturmalarında önemli bir araç olsa da bu uygulamaların keyfi olarak kullanılmasının önüne geçmek için güçlü hukuki güvenceler oluşturulmalıdır. Bu bağlamda, denetleme yetkisinin kapsamı, süresi ve usulleri hakkında detaylı yasal düzenlemeler yapılması gerekmektedir.

Dijital delillerin yargısal süreçlerde delil olarak kabul edilip edilemeyeceği, bu alandaki en büyük tartışma konularından biridir. Bu sorun, sadece teorik bir tartışma olmaktan öte, adli makamların delil toplama yetkilerini doğrudan ilgilendiren pratik bir sorundur. Birçok yargı sisteminde, dijital verilerin kolaylıkla değiştirilebilmesi ve orijinalliğinin teyit edilememesinden dolayı ceza davalarında delil olarak kullanılması kabul görmemektedir[11].

Son olarak bu alandaki önemli sorunlardan diğeri ise, uluslararası düzeyde koordinasyon eksikliğidir. Ceza usul hukukunun karşılaştığı bu zorlukların üstesinden gelmek için uluslararası iş birliği mekanizmaları giderek önem kazanmaktadır. Avrupa İnsan Hakları Mahkemesi (**"AİHM"**) gibi uluslararası mahkemeler, özellikle iletişimin denetlenmesi gibi konularda, ilgili makamların yetkilerini Avrupa İnsan Hakları Sözleşmesi (**"AİHS"**) 8. maddesi çerçevesinde değerlendirerek önemli bir rol üstlenmektedir[12].

2. Avrupa Birliği

Avrupa Birliği (**"AB"**), dijital delillerin hukuki statüsünü belirleme ve bu alanda uluslararası iş birliğini güçlendirme amacıyla çeşitli düzenlemeler yapmıştır. 1995 tarihli Veri Koruma Direktifi (Data Protection Directive)[13] ve 1997 tarihli telekomünikasyon sektörüne ilişkin olarak özel hayatın korunması ve kişisel verilerin işlenmesine ilişkin Direktif[14] gibi ilk düzenlemeler, kişisel verilerin korunması ve telekomünikasyon sektöründeki gizlilik ilkelerini belirlemiştir. Avrupa Birliği Temel Haklar Bildirgesi ise, bireylerin özel hayatına ve kişisel verilerine saygı gösterilmesi

FOOTNOTE

10 UNMPCCRC, p. 147.

11 UNMPCCRC, p. 171.

12 UNMPCCRC, p. 177.

13 Directive 95/46/EC, (24.11.1995).

14 Directive 97/66/EC, (15.12.1997).

DİPNOT

10 UNMPCCRC, s. 147.

11 UNMPCCRC, s. 171.

12 UNMPCCRC, s. 177.

13 Directive 95/46/EC, (24.11.1995).

14 Directive 97/66/EC, (15.12.1997).

PART 1

that individuals' private life and personal data must be respected on a legal basis.

In response to the escalating prevalence of cybercrime, the European Union has established a comprehensive framework to counter digital offenses, encompassing regulations such as the Council Framework Decision on Attacks Against Information Systems[15] and the Data Retention Directive[16]. Instruments like the European Evidence Warrant[17] and the European Judicial Network have facilitated judicial collaboration among member states, enabling the efficient acquisition and dissemination of digital evidence.

The Lisbon Treaty conferred upon the European Union enhanced authority within the domain of criminal law, imposing more binding obligations on member states concerning judicial cooperation and harmonization. In particular, computer crimes were defined as cross-border crimes and common standards were set to combat these crimes. These developments contributed to the EU playing a more active role in digital evidence and progressing towards the establishment of a common European Criminal and Criminal Procedure Law.

However, EU regulations on digital evidence face a number of challenges, including privacy concerns and legal uncertainties. Regulations, particularly the Data Retention Directive, have been criticized for posing serious threats to individuals' privacy rights. Therefore, the EU needs to adopt a balanced approach to digital evidence and update its regulations in line with technological developments.

3. The Council of Europe

The Convention on Cybercrime (**"CCC"**), which emerged as a result of the work of the Council of Europe (**"CoU"**), has become an important milestone in determining the legal status of digital evidence and strengthening international cooperation.

The majority of the convention's regulations on digital evidence are gathered between Articles 14 and 21 in the procedural law section. The provisions here have determined the fundamental principles on issues such as the collection, storage and use of digital evidence. These articles require party states to act in accordance with international human rights standards when making domestic legal arrangements regarding digital evidence.

The Convention requires that the party states take into account the principles set out in the ECHR and other international human rights treaties when making regulations regarding digital evidence. In this way, it is aimed to protect the fundamental rights and freedoms of individuals during the collection and use of digital evidence. The Convention establishes a legal framework for the use of digital evidence by referring to fundamental legal principles such as the principle of legality and the principle of proportionality.

In consequence, the CCC has created an international cooperation platform to combat the increasing crimes in the digital world and has played an important role in determining the legal status of digital evidence. The Convention ensures that the parties respect human rights and observe the rule of law when making regulations regarding digital evidence. However, with the rapid development of technology, the complexity of digital evidence is also increasing, which can create new challenges in the implementation process of the Convention. Therefore, the CCC needs to be constantly updated and developed.

B. The Role of Digital Evidence within the Turkish Legal Framework: Examining the Provisions of the Turkish Code of Criminal Procedure

Criminal procedure law in Türkiye is based on a system based on freedom of evidence. This means that any type of evidence can be used in the trial process, and digital evidence is also considered within this scope. The CCC, approved in 2014, accelerated Türkiye's efforts to bring its legislation on digital evidence into line with international standards.

Currently, there are various regulations regarding digital evidence in the Turkish legal system, but there are ongoing discussions on the scope and effectiveness of these regulations. In particular, Code No. 5271 provides a basic framework for the processes of obtaining, evaluating and using digital evidence. However, the question of how well the reg-

FOOTNOTE

15 Framework Decision 2005/222/JHA, (24.02.2005). http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN (Access date: August 6, 2024)

16 Directive 2006/24/EC, (15.03.2006). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (Access date: August 6, 2024)

17 Framework Decision 2008/978/JHA, (18.12.2008). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:en:PDF. (Access date: August 6, 2024)

gerektiği ilkesini hukuki bir zemine oturtmuştur.

Siber suçların artmasıyla birlikte, AB; Bilişim Sistemlerine Yönelik Saldırılara Dair Çerçeve Kararı (Council Framework Decision on Attacks Against Information Systems)[15], Veri Saklama Direktifi (Data Retention Directive)[16] gibi düzenlemelerle dijital suçlarla mücadeleye yönelik kapsamlı bir çerçeve oluşturmuştur. Avrupa Delil Müzekkeresi (European Evidence Warrant)[17] ve Avrupa Yargı Ağı (European Judicial Network) gibi araçlar ise, üye devletler arasında adli iş birliğini kolaylaştırarak dijital delillerin etkin bir şekilde toplanmasına ve paylaşılmasına olanak sağlamıştır.

Lizbon Antlaşması ile birlikte, AB; ceza hukuku alanında daha fazla yetkiye kavuşmuş ve üye devletlere adli iş birliği ve uyum konusunda daha bağlayıcı yükümlülükler getirmiştir. Özellikle bilgisayar suçları, sınır aşan suçlar olarak tanımlanmış ve bu suçlarla mücadele için ortak standartların belirlenmesi öngörülmüştür. Bu gelişmeler, AB'nin dijital deliller konusunda daha etkin bir rol oynamasına ve ortak bir Avrupa Ceza ve Ceza Muhakemesi Hukuku oluşturma yolunda ilerlemesine katkı sağlamıştır.

Ancak, AB'nin dijital deliller konusundaki düzenlemeleri, mahremiyet endişeleri ve hukuki belirsizlikler gibi bazı zorluklarla karşı karşıyadır. Özellikle Veri Saklama Direktifi gibi düzenlemeler, bireylerin mahremiyet haklarına yönelik ciddi tehditler oluşturduğu gerekçesiyle eleştirilmiştir. Bu nedenle, AB'nin dijital deliller konusunda dengeli bir yaklaşım benimsemesi ve teknolojik gelişmelere paralel olarak düzenlemelerini güncellemesi gerekmektedir.

3. Avrupa Konseyi

Avrupa Konseyi'nin (**"AK"**) çalışmaları ile ortaya çıkan Siber Suçlar Sözleşmesi (Convention on Cybercrime) (**"SSS"**), dijital delillerin hukuki statüsünü belirleme ve uluslararası iş birliğini güçlendirme amacıyla önemli bir dönüm noktası olmuştur.

Sözleşmenin dijital delillere dair düzenlemelerinin büyük bir kısmı, usul hukuku bölümünde yer alan 14. ve 21. maddeler arasında toplanmıştır. Burada yer alan hükümler, dijital delillerin toplanması, saklanması ve kullanılması gibi konularda temel ilkeleri belirlemiştir. Bu maddeler; taraf devletlerin dijital delillerle ilgili iç hukuk düzenlemelerini yaparken, uluslararası insan hakları standartlarına uygun hareket etmelerini zorunlu kılmaktadır.

Sözleşme; taraf devletlerin dijital delillere ilişkin düzenlemelerini yaparken, AİHS ve diğer uluslararası insan hakları sözleşmelerinde yer alan ilkeleri dikkate almasını öngörmektedir. Bu sayede, dijital delillerin toplanması ve kullanılması sürecinde bireylerin temel hak ve özgürlüklerinin korunması amaçlanmaktadır. Sözleşme; kanunilik ilkesi, orantılılık ilkesi gibi temel hukuk ilkelerine atıf yaparak, dijital delillerin kullanımı konusunda hukuki bir çerçeve oluşturmaktadır.

Sonuç olarak SSS, dijital dünyada artan suçlarla mücadele etmek amacıyla uluslararası bir iş birliği platformu oluşturmuş ve dijital delillerin hukuki statüsünü belirlemede önemli bir rol oynamıştır. Sözleşme; taraf devletlerin dijital delillere ilişkin düzenlemelerini yaparken, insan haklarına saygılı olmalarını ve hukukun üstünlüğünü gözetmelerini sağlamaktadır. Ancak, teknolojinin hızla gelişmesiyle birlikte dijital delillerin karmaşıklığı da artmakta olup, bu durum sözleşmenin uygulanması sürecinde yeni zorluklar ortaya çıkarabilmektedir. Bu nedenle, SSS'nin sürekli olarak güncellenmesi ve geliştirilmesi gerekmektedir.

B. Türk Hukuk Sisteminde Dijital Delillerin Yeri ve Ceza Muhakemesi Kanunu'ndaki Düzenlemeler

Türkiye'de ceza muhakemesi hukuku, delil serbestisine dayalı bir sistem üzerine kurulmuştur. Bu durum, her türlü delilin yargılama sürecinde kullanılabileceği anlamına gelmekte olup, dijital deliller de bu kapsam içerisinde değerlendirilmektedir. 2014 yılında onaylanan SSS, Türkiye'nin dijital delillerle ilgili mevzuatını uluslararası standartlara uygun hale getirme çabalarını hızlandırmıştır.

Mevcut durumda, Türk hukuk sisteminde dijital delillere ilişkin çeşitli düzenlemeler bulunmakla birlikte, bu düzenlemelerin kapsamı ve etkinliği konusunda tartışmalar sürmektedir. Özellikle 5271 sayılı Kanun, dijital delillerin elde edilmesi, değerlendirilmesi ve kullanılması süreçlerinde temel bir çerçeve sunmaktadır. Ancak, 5271 sayılı Kanun'daki

DİPNOT

15 Framework Decision 2005/222/JHA, (24.02.2005). http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN (Erişim tarihi: 6 Ağustos 2024)

16 Directive 2006/24/EC, (15.03.2006). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF (Erişim tarihi: 6 Ağustos 2024)

17 Framework Decision 2008/978/JHA, (18.12.2008). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:en:PDF. (Erişim tarihi: 6 Ağustos 2024)

PART 1

ulations in Code No. 5271 adapt to current technological developments and respond to new problems is still being discussed.

In the previous section of this study, the theory of evidence in criminal procedure and the general place of digital evidence were examined in detail. In this section, the regulations regarding digital evidence in Code No. 5271 will be discussed.

1. Regulations Regarding Digital Evidence in Code No. 5271

Code No. 5271, which is the fundamental basis of criminal procedure law in Türkiye, contains important regulations on the use of digital evidence in the trial process, and Article 134 of the law regulates methods of obtaining digital evidence such as searches, copying and seizure of computers, computer programs and files.

The main justification for the adoption of the said article is that new types of evidence that emerge as a result of technological developments cannot be obtained through traditional evidence collection methods. Therefore, the relevant regulation is an important provision as it determines the legal status of digital evidence and regulates the methods of obtaining this evidence during the trial process.

However, there are some debates about the scope and application areas of the provision. In particular, the limitation of the article to the expression "computers, computer programs and files" creates concerns that various digital devices and environments used today may fall outside this scope. This situation may lead to the emergence of legal gaps as the variety of digital evidence increases.

düzenlemelerin güncel teknolojik gelişmelere ne kadar uyum sağladığı ve ortaya çıkan yeni sorunlara cevap verebildiği sorusu hala tartışılmaktadır.

Bu çalışmanın önceki bölümünde, ceza muhakemesinde delil teorisi ve dijital delillerin genel yeri detaylı bir şekilde incelenmiştir. Bu bölümde ise, 5271 sayılı Kanun'da yer alan dijital delillere ilişkin düzenlemeler üzerinde durulacaktır.

1. 5271 sayılı Kanun'da Dijital Delillere İlişkin Düzenlemeler

Türkiye'de ceza muhakemesi hukukunun temel dayanağı 5271 sayılı Kanun, dijital delillerin yargılama sürecinde kullanımı konusunda önemli düzenlemeler içermekte olup, kanunun 134. maddesinde; bilgisayarlarda, bilgisayar programlarında ve kütüklerde yapılan aramalar, kopyalama ve el koyma işlemleri gibi dijital delil elde etme yöntemleri düzenlenmektedir.

Mezkur maddenin kabul edilmesindeki temel gerekçe, teknolojik gelişmeler doğrultusunda ortaya çıkan yeni delil türlerinin, geleneksel delil toplama yöntemleriyle elde edilemeyecek olmasıdır. Bu nedenle ilgili düzenleme, dijital delillerin hukuki statüsünü belirlemesi ve bu delillerin yargılama sürecinde elde edilme yöntemlerini düzenlemesi nedeniyle önemli bir hükümdür.

Ancak, hükmün kapsamı ve uygulama alanları konusunda bazı tartışmalar bulunmaktadır. Özellikle, maddenin "bilgisayarlar, bilgisayar programları ve kütükleri" ifadesiyle sınırlandırılması, günümüzde kullanılan çeşitli dijital cihaz ve ortamların bu kapsam dışında kalabileceği endişesi yaratmaktadır. Bu durum, dijital delillerin çeşitliliğinin artmasıyla birlikte, hukuki boşlukların ortaya çıkmasına neden olabilmektedir.

V. CONCLUSION

In conclusion, although Article 134 of Code No. 5271 has been an important step in the use of digital evidence in the trial process in Türkiye, the scope of the Law needs to be constantly updated and developed in the face of rapidly developing technology. In particular, with the emergence of new generation digital devices and data storage methods, it is important to expand the scope of Article 134 accordingly and to provide a clearer regulation of digital evidence.

V. SONUÇ

Neticeten; 5271 sayılı Kanun'un 134. maddesi, Türkiye'de dijital delillerin yargılama sürecinde kullanılması konusunda önemli bir adım olmuşsa da, yasa kapsamının hızla gelişen teknoloji karşısında sürekli olarak güncellenmesi ve geliştirilmesi gerekmektedir. Özellikle, yeni nesil dijital cihazlar ve veri depolama yöntemlerinin ortaya çıkmasıyla birlikte, 134. maddenin kapsamının bu doğrultuda genişletilmesi ve dijital delillerin daha net bir düzenlemeye kavuşturulması önemlidir.

BIBLIOGRAPHY

UĞUR KAYNAKÇIOĞLU, "Ceza Muhakemesinde Dijital Deliller", June 2015, p. 39.

MUSTAFA GÖKSU, Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayinevi, 2011, p. 31-32.

Guidelines of the Committee of Ministers of the Council of Europe on Electronic Evidence in Civil and Administrative Proceedings, January 2019, (Access Date: August 5, 2024), p. 6. https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

Council of Europe, Convention on Cybercrime, CETS N. 185, Budapest, November 2001, (Access Date: August 5, 2024) http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, April 2004, (Access Date: August 5, 2024), p. 39. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Electronic Crime Scene Investigation: A Guide for First Responders, July 2001, (Access Date: August 5, 2024), p. 6. https://www.ojp.gov/pdffiles1/nij/187736.pdf

Electronic Evidence Guide, December 2014, (Access Date: August 5, 2024), p. 12. https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

Framework Decision 2005/222/JHA, (24.02.2005), (Access Date: August 6, 2024) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN

Directive 2006/24/EC, (15.03.2006), (Access Date: August 6, 2024) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

Framework Decision 2008/978/JHA, (18.12.2008), (Access Date: August 6, 2024) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:en:PDF

KAYNAKÇA

UĞUR KAYNAKÇIOĞLU, "Ceza Muhakemesinde Dijital Deliller", Haziran 2015, s. 39.

MUSTAFA GÖKSU, Hukuk Yargılamasında Elektronik Delil, Ankara: Adalet Yayınevi, 2011, s. 31-32.

Guidelines of the Committee of Ministers of the Council of Europe on Electronic Evidence in Civil and Administrative Proceedings, Ocak 2019, (Erişim Tarihi: 5 Ağustos 2024), s. 6. https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5

Council of Europe, Convention on Cybercrime, CETS N. 185, Budapest, Kasım 2001, (Erişim Tarihi: 5 Ağustos 2024). http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=&CL=ENG

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, Nisan 2004, (Erişim tarihi: 5 Ağustos 2024), s. 39. https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

Electronic Crime Scene Investigation: A Guide for First Responders, Temmuz 2001, (Erişim tarihi: 5 Ağustos 2024), s. 6. https://www.ojp.gov/pdffiles1/nij/187736.pdf

Electronic Evidence Guide, Aralık 2014, (Erişim Tarihi: 5 Ağustos 2024), s. 12. https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf

Framework Decision 2005/222/JHA, (24.02.2005), (Erişim tarihi: 6 Ağustos 2024) http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005F0222&from=EN.

Directive 2006/24/EC, (15.03.2006), (Erişim tarihi: 6 Ağustos 2024) http://eur-.lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

Framework Decision 2008/978/JHA, (18.12.2008), (Erişim tarihi: 6 Ağustos 2024) http://eur-.lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0072:0092:en:PDF