PART 15

CEMAL ARAALAN

Digital Evidence in Turkish Law

Türk Hukukunda Dijital Deliller

ABSTRACT

The digital evidence has an important role due to recent developments in Turkish Law. Particularly, protection measures in Criminal Procedure Law which are related to digital evidence and the documents that are signed by electronic signature in Civil Procedure law are important issues to be considered. This Article examines various dimensions of the concept of the digital evidence and its place in Turkish law, and then it attempts to determine problematic aspects of the issue and propose solutions in that regard.

KEYWORDS:

Digital evidence, forensic computer, electronic documents, Turkish Civil Procedure law and Turkish Criminal Procedure Law

ÖZET

Dijital delil kavramının önemi, yasa koyucunun mevzuatımızda yer verdiği yeni düzenlemeler neticesinde her geçen gün artmaktadır. Özellikle Ceza Muhakemesi Kanunu açısından dijital delillerle yakından bağlantılı olan koruma tedbirleri ve Hukuk Muhakemeleri Kanunu açısından ise elektronik imzalı belgeler mahiyeti itibariyle dikkat çekmektedir. Bu makalede, dijital delil kavramı ve Türk Hukuku uygulamaları bakımından dijital deliller çeşitli boyutlarıyla ele alınıp, bu alandaki temel sorunlar tespit edilerek, çözüm önerileri ortaya konulmaya çalışılmaktadır.

ANAHTAR KELİMELER:

Dijital delil, adli bilişim, elektronik belge, HMK, CMK

PART 15

1. INTRODUCTION

IN PARALLEL WITH THE ADVANCEMENT OF TECHNOLOGY, THE use of computer systems to create and store documents is commonly preferred over traditional methods of hand writing and typing machine. With the development of social media in particular, people increasingly use digital world to share their ideas, private photos and information. Consequently, criminal activities or disputes take place on the digital world rather than physical world, and the concept of digital evidence is becoming more and more important every other day. This article examines the meaning of the digital evidence, pros and cons of the digital evidence, and it addresses the question of what can be regarded as digital evidence. The article then explores the enforcement of digital evidence in Turkish Law.

2. THE MEANING OF THE DIGITAL EVIDENCE

2.1. The Definition of Digital Evidence

Digital (numeric) evidence is a kind of evidence which could be collected in computer systems and data storage in the process of the digital forensic investigation[1]. Digital evidence is all sorts of data which can be stored, created, and transmitted in digital world. Indeed the critical question whether given data can be regarded as evidence is related to the facts of a case. The stage of collecting and storing data and documents is very important within the concept of the digital data. Digital data listed below can be regarded as evidence only if they are collected and stored in a correct and careful manner.

2.2. The Characteristic of Digital Evidence

In investigation process, findings must have certain qualifications to constitute evidence before the courts. These qualifications include "rationality", "admissibility", "relevance", "completeness" and "integrity", "reliability", "believability (trustfulness)", and "reproducibility"[2].

First of all, the digital evidence must be rational and admissible before courts. This very basic rule means that any data to be presented before courts as evidence should reveal the facts of the case and clarify any doubts/questions at issue in a rational manner.

1. GİRİŞ

TEKNOLOJİNİN GELİŞİMİNE BAĞLI OLARAK EL YAZISI ve daktilo kullanımı terk edilerek artık tüm dokümanların bilgisayar ortamında oluşturulması ve saklanması olağan hale gelmiştir. Özellikle sosyal medyanın gelişimiyle beraber bireyler kendi kişisel düşüncelerini, görüntülerini ve özel yaşamlarına dair birçok veriyi bilgisayar ortamında başkaları ile paylaşmaktadır. Bu durum ise toplumu ve toplumsal suç ve uyuşmazlıkları fiziksel den dijital ortama doğru hareketlendirmekte ve hukukumuz açısından "dijital delil" kavramına her geçen gün ayrı bir önem kazandırmaktadır. Bu makalede dijital delil kavramının ne anlama geldiği, ne tür delillerin dijital delil olarak nitelendirilebileceği, dijital delilin kuvvetli ve zayıf yanları ve Türk Hukukunda dijital delilin temel uygulama alanları incelenecektir.

2. DİJİTAL DELİL KAVRAMI

2.1. Dijital Delilin Tanımı

Dijital (sayısal) deliller, adli bilişimle ilgili bir çalışma esnasında, bilişim sistemleri ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli delillerdir[1].Dijital delil aslında dijital ortamda tutulan, oluşturulan, depolanan ve iletilen her türlü veri anlamına gelmektedir. Ancak esasında hukuki açıdan söz konusu veriye delil niteliği kazandıran maddi olayla ilgisinin bulunmasıdır. Dijital delil açısından kritik olan aşama çoğu zaman söz konusu bu delillerin toplanması ve belgelere kaydedilmesi aşamasıdır. Aşağıda sayılan niteliklere sahip olan herhangi dijital veri doğru ve hassas bir şekilde toplanmış olması koşuluyla delil niteliğini taşıyabilir.

2.2. Dijital Delilin Özellikleri

Elde edilen bulguların dijital delil olarak addedilebilmesi ve yargı makamlarına sunulabilmesi için bazı nitelikleri haiz olması gerekmektedir. Dijital delilin sahip olması gereken bu özellikler; akla uygunluk, kabul edilebilirlik, gerçeklik, tamam ve eksiksiz olma, güvenirlik, inanılabilirlik, tekrar edilebilirlik olarak sayılabilir[2].

Dijital delilin sahip olması gereken ilk özellik akla uygunluk, kabul edilebilirliktir. En basit kural olarak ifade edilen bu özellik herhangi bir bulgunun delil olarak nitelendirilerek mahkemeye sunulabilmesi için öncelikle

Second characteristic of admissible evidence is "relevance". Evidence must be directed to the material facts of a case or there must be a rational relationship between evidence and the matter to be proved in a case. In other words, evidence must be logically relevant to the point it is offered in support of.

Third, evidence that is related to perpetrator or suspect has to be collected and presented in full during the pre-investigation and investigation processes. Moreover, the submitted evidence should not be altered, (preservation of the integrity of evidence). In brief, this characteristic points out the completeness of digital evidence.

Fourth, digital data to be used as evidence must be reliable and believable. The procedure to be followed in collection and examination of digital evidence must comply with the law in order not to impair the "reliability", and "believability". The evidence to be collected and submitted to the court should be understandable and believable by an ordinary person. This characteristic of digital evidence carries particular importance to convince the court and to ensure the parties' and public trust on the verdict.

şüphe altındaki konuyu/olayı açıklığa kavuşturabilecek mantıki öğeleri içermesi gerekliliğini ifade eder.

Delil niteliği taşıyabilmesi için dijital delilde bulunması gereken bir diğer özellik gerçekliktir. Ceza hukukundaki fiille netice arasındaki nedensellik bağına benzer şekilde, delil ile ispatlanmak istenen maddi gerçek arasında mantıksal bir irtibat mevcut olmalıdır.

Dijital delillerin elde edilmesi veya inceleme/analiz aşamasında yapılan işlemler esnasında, sanık veya şüpheli ile ilgisi olabilecek tüm deliller eksiksiz olarak toplanmalı ve sunulmalıdır. Ayrıca, sunulan deliller herhangi bir nedenle değişmemiş (delil bütünlüğünün bozulmamış) olmalıdır. Bu özellikler özetle tam ve eksiksiz olma olarak ifade edilmektedir.

Delil olarak kullanılacak dijital verilerin güvenirlik ve inanılabilirlik kıstaslarını da sağlaması gerekmektedir. Dijital delillerin elde edilmesi ve incelenmesi esnasında izlenen yol ve uygulanan teknik yöntemler yasal prosedürlere tam olarak uygun olmalıdır. Elde edilen ve mahkemeye delil olarak sunulan tüm bulgular, herkes tara-

Finally, digital evidence must be reproducible in order to be scientifically credible. In other words, data to be presented as digital evidence before courts must be verifiable when analyzed by different methods and experts.

2.3. The Advantages and Drawbacks of the Digital Evidence

Digital evidence has advantages and drawbacks compared to physical evidence. First of all, digital evidence involves a piece of information that is certain, precise, total, objective and unbiased. Digital evidence is also valid, useful, reliable, practicable, and it may be necessary to prove crimes that is not provable otherwise. Also, digital evidence is collected, stored, used and preserved easily. Electronic documents and electronic signature facilitate commerce by providing fast and reliable methods for electronic transactions. All these are main advantageous features of digital evidence compared to physical evidence.

fından anlaşılabilir ve inanılabilir nitelikte olmalıdır. Bu husus ilgili hukuki uyuşmazlık hakkında hüküm verecek olan hakimin vicdani kanaatinin oluşması bakımından öneminin yanı sıra, uyuşmazlığın tarafları ve toplum tarafından verilen hükme güven duyulması bakımından da önemlidir.

Son olarak, dijital delillerin bilimsel açıdan itibar edilebilir sayılabilmeleri için, tekrar edilebilirlik özelliğine de sahip olması gerekir. Yani elde edilen ve mahkemeye delil olarak sunulan tüm bulgulara, farklı kişiler tarafından, farklı yer ve zamanlarda da aynı yöntem ve metotlar kullanılarak ulaşılabilmelidir.

2.3. Dijital Delilin Kuvvetli ve Zayıf Tarafları

Dijital delillerin fiziki delillere kıyasla bazı kuvvetli ve zayıf tarafları bulunmaktadır. Öncelikle, dijital delilin içerdiği bilgi kesin, bütün, açık, sahih, nesnel ve tarafsızdır. İspat bakımından muteber, kullanışlı, güvenilir, uygulanabilirdir ve daha önce ispatlanamayan bazı suçlar bakımından gereklidir. Toplanması, kullanımı, muhafazası

In most cases, collecting digital evidence requires expertise and special knowledge. It is difficult to comprehend how to process digital data and its specific operation rules. It should also be taken into consideration that it is difficult to present and explain digital evidence in a clear manner before courts. Consequently, judges may request additional explanatory information or report and the use of digital evidence may be more demanding than physical evidence.

The high cost associated with analyzing and examining digital evidence is another drawback compared to physical evidence. Due to the complexity of understanding and interpreting digital data processing and its specific operation rules, it is difficult to assess legal value of digital evidence in advance. It is also difficult to store and protect digital data properly. Specific certification models are particularly important in this context[3].

3. THE APPLICATION OF DIGITAL EVIDENCE IN TURKISH LAW

Considering interdisciplinary nature of cyber law, the topic of digital evidence pertains to a wide range of legal practice areas such as criminal law, criminal procedure law, and civil procedure law. Due to limited time and space, it is beyond the scope of this article to cover all aspects of the topic. Therefore, this article will only examine protection measures regarding digital evidence in Criminal Procedural Law add: (**"CMK"**) and the use of electronically signed documents as digital evidence.

3.1. Protection Measures Regarding to Digital Evidence in Criminal Procedure Law

In some criminal cases, a search warrant for digital evidence may be necessary in order to conduct a proper investigation and prepare indictment, and digital evidence may help create reasonable doubt (Criminal Procedural Law Art. 170) and convince the judge accordingly (CPL Art. 217). In criminal proceedings, the ultimate purpose of

ve depolanması kolaydır. Elektronik belgeler, elektronik imzalar ile birlikte elektronik ticareti hızlı ve daha güvenli hale getirmek suretiyle kolaylaştırmaktadır. Bular dijital delilin fiziki delile kıyasla kuvvetli olduğu noktaların başlıcalarıdır.

Öne çıkan ilk husus dijital delillerin toplanmasının çoğu kez özel bilgi ve uzmanlık gerektirmesidir. Dijital delili oluşturan verinin nasıl işlem gördüğünü ve özel süreç kurallarının nasıl yorumlandığını bilmek güçtür. Dijital delillerin yargı makamlarına anlaşılabilir şekilde izah etmenin çoğu kez zor olduğu da dikkate alınmalıdır. Bu bağlamda, yargıçların, dijital delil konusunda klasik delillere oranla daha fazla destekleyici bilgi istemelerinden dolayı mahkemede kullanılması çoğu kez sorun arz etmektedir.

Dijital delilin delil olarak diğer delillere kıyasla bir başka dezavantajı ise dijital delilin incelenme ve analiz maliyetinin yüksek oluşudur. Dijital delili oluşturan verinin nasıl işlem gördüğünü ve özel süreç kurallarının nasıl yorumlandığını bilmek güçtür ve bu bağlamda dijital verilerin hukuki değerinin belirlemek zordur. Diğer yandan dijital delilleri aslına uygun olarak muhafaza ve depolama zordur. Bu bağlamda sertifikasyon modellerinin önemi öne çıkmaktadır[3].

3. TÜRK HUKUKU'NDA DİJİTAL DELİL UYGULAMALARI

Dijital deliller meselesine bilişim hukukunun disiplinler arası perspektifinden bakıldığında ceza hukuku, ceza muhakemesi hukuku, hukuk usulü gibi birçok hukuk dalı ile yakından ilişkili olduğu ve geniş bir uygulama alanına sahip olduğu görülmektedir. Ancak bu kapsamda bir çalışmada dijital delilin uygulama alanına ilişkin tüm bu başlıkların incelenmesi mümkün olmadığı için özellikle öne çıkan; Ceza Muhakemesi Kanunu'nda (**"CMK"**) dijital deliller ile ilgili yer alan koruma tedbirleri ve elektronik imzalı belgelerin delil niteliği konuları incelenecektir.

FOOTNOTE DİPNOT

1 Türkan Henkoğlu, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*, (İstanbul: Pusula, 2014), 5.
2 Henkoğlu, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*, 6.
3 Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil*, (Ankara: Seçkin Yayıncılık, 2014), 136.
4 Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil*, 309-312.
5 Mustafa Göksu, *Hukuk Yargılamasında Elektronik Delil (1086 Sayılı HUMK ve 6100 Sayılı HMK Çerçevesinde)*, (Ankara: Adalet Yayınevi, 2011), 41-42.
6 Ayşe Ece Akar, *Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği*, (İstanbul :XII Levha, 2013), 160-161.
7 Göksu, *Hukuk Yargılamasında Elektronik Delil*, 152.

searching, copying, and seizing digital data is to obtain evidence, especially digital evidence. Discovery of evidence is the first step to use digital evidence in criminal proceedings. Particularly in cybercrimes committed with and/or against information systems, the very information system is the only place to obtain the required evidence. CMK article 134 regulated the search and seizure procedure for digital evidence. According to the article, *"If reasonable suspect occur and there is no way to gather evidence in other method, Public prosecutor may require a permission from Judge to search and copy digital data in computers, computer programs and computer logs and encrypt the data to written statement."* This procedure is the most frequent method applied to obtain digital evidence. It should be noted, however, some data may be in transmission between suspect's data system and other data systems. In this case, data in transmit can be collected in accordance with CMK article 135, which regulates the surveillance, monitoring, and recording of communication[4].

3.2. Admissibility of Electronic Evidence and Electronically Signed Documents in Civil Procedure Law

This part of the article first explains the need to use electronic evidence and electronic data storing, it then examines electronic documentation as evidence and whether electronic documents may be considered as legal bonds.

Although principle of circumstantial evidence is widely accepted in the Criminal Procedure Law, the Civil Procedure Law contains special evidence rules and restrictions. According to Civil Procedure Law Article 200, legal transactions that create, alter, extinguish, affect, redeem, transfer or execute rights with a value of higher than two thousand and five hundred Turkish Liras must be proven by written bond. Even though the value of the right diminishes below this amount due to partial payment, it must be proven by written bond.

As it relates to the topic, the meaning of a bond should be explained briefly. Basically, a bond is a written and signed promise. In the Civil Procedure Law, a written promise must carry certain qualifications in order to be considered as a legal bond. The elements of a legal bond include a written document, promise (consideration), and signature. Whether a document is a legal bond or not has important consequences in terms of proof.

3.1. Ceza Muhakemesi Kanunu'nda Yer Alan Dijital Deliller İlgili Koruma Tedbirleri

Ceza muhakemesinin sağlıklı yürüyebilmesi, soruşturma evresinin sonucunda iddianamenin hazırlanabilmesi için ihtiyaç olan yeterli şüpheyi oluşturacak delillerin (CMK m. 170) ve kovuşturma evresinin sonunda hâkimin serbestçe kararını verebilmesi ve şüphesini yenebilmesi için gerekli olan delillerin elde edilmesi (CMK m. 217) amacıyla bilişim sistemlerinde veri arama tedbirine başvurmak bir ihtiyaç olarak karşımıza çıkmaktadır. Ceza muhakemesinde sıkça başvurulan bir tedbir olan bilişim sistemlerinde veri arama, kopyalama ve el koymanın nihai amacı delillere, özellikle dijital delillere ulaşmaktır. Özellikle bilişim sistemleri vasıtasıyla veya bilişim sistemlerine karşı işlenen suçlarda, delillerin elde edilebileceği nihai ve yegâne yer, yine bilişim sisteminin kendisi olmaktadır.

Dijital ortamda yapılacak arama, el koyma tedbiri CMK'nın 134. maddesinde düzenlenmektedir. *"bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine" hakim kararıyla "şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasını, bilgisayar kayıtlarından kopya çıkarılmasını, bu kayıtların çözülerek metin hâline getirilmesini"* düzenlemektedir. Bu tedbirin dijital delillerin elde edilmesi anlamında en sık başvurulan yöntem olduğu söylenebilir. Öte yandan, belirtmek gerekir ki bazı veriler şüphelinin kullandığı bilişim sistemi ile diğer bilişim sistemlerinin iletişimi anında akış halinde de bulunabilir. Böyle bir durumda akış halindeki verilerin toplanması, CMK'nın 135. maddesinde düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri kapsamında gerçekleştirilecektir[4].

3.2. Hukuk Yargılamasında Elektronik Deliller ve Elektronik İmzalı Belgelerin Delil Niteliği

Çalışmamızın bu kısmında öncelikle hukuk yargılamasında elektronik delillere başvurma ihtiyacı ve verilerin elektronik ortamda saklanması incelenecek, sonrasında ise özellikle elektronik imzalı belgelerin senet niteliğinde olup olmadığı hususuna ve delil niteliğine değinilecektir.

Ceza muhakemesinde delil serbestisi sistemi benimsenmiş, iken, hukuk muhakemesinde bazı durumlarda özel delil kuralları ve delil yasakları söz konusu olmaktadır.

Because computers are used in virtually every aspect of most individual's daily or business life, digital evidence may be useful in any disputes. Digital evidence is most frequently used in disputes such as stealing of trade secrets, discrimination, fraud, stealing of private information (divorcement cases), and deception cases[5].

Whether electronic bond is legal bond or not has important legal consequences. Documents missing above mentioned conditions are not considered as legal bonds, therefore, first thing to do is to examine the bond whether it has qualification or not. Furthermore, electronics documents must carry all these conditions together, otherwise they are not considered as legal bonds. For instance, documents stored in USB disks, CDs and similar devices cannot be regarded as legal bonds if they are not printed out and signed. Legal bonds do not have to be in hand writing but they must be signed by hand. In this respect, electronic documents can be verified by secured e-signature to be considered as legal bonds.

Hukuk Muhakemeleri Kanunu'nun (**"HMK"**) 200. maddesi gereğince; bir hakkın doğumu, düşürülmesi, devri, değiştirilmesi, yenilenmesi, ertelenmesi, ikrarı ve itfası amacıyla hukuki işlemlerin, miktar ve değeri iki bin beş yüz Türk Lirasını geçtiği takdirde senetle ispat olunması gerekir. Bu hukuki işlemlerin miktar ve değeri ödeme veya borçtan kurtarma gibi bir nedenle iki bin beş yüz Türk Lirasından aşağı düşse bile senetsiz ispat olunamaz.

Konuyla yakından bağlantısı olması sebebiyle öncelikle senedin ne anlama geldiğini belirtmek uygun olacaktır. Senet, bir kimsenin iradesini dış dünyaya yazılı olarak açıklamasına yarayan bir vasıtadır. Hukuk muhakemesi açısından konuya bakıldığında ise bir düşüncenin yazılı hali, yani belge hali (başka bazı unsurları taşıyor olmak kaydıyla) senettir. Başka bir deyişle, senet bir belge olup, kanun tarafından bazı şartları (somut bir cisim olma, yazılılık, irade beyanı içerme, imza gibi) taşıması halinde bu belgeye özel bir anlam yüklenmektedir. Bir belgenin senet niteliğini haiz olup olmaması ise senetle ispat kuralı bakımından önem taşımaktadır.

At this point, the use of e-mail and e-signature as evidence must be addressed briefly. E-mail cannot be regarded as reliable evidence due to security vulnerability. For example, message sender or someone may change the IP number, hack the computer, manipulate the context of the email or draft the email differently.

Turkish legislator regulate the electronic signature technical and legal issues in Electronic Signature Code (**"ESC"**), Law no 5070. According to ESC, electronic signature is a signature added to electronic data for the purpose of verification of the content and identity. Turkish Civil Procedure Law numbered 6100 which entered into force in 2012 regulate electronic documents evidence in a similar way to the repealed Law Judgment and Procedure Law numbered 1086 (**"HMUK"**) According to Turkish Civil Procedure Law article 205/2 the documents which are signed by electronic signature are legal bonds. According to the purpose of the law stated in preamble, the law maker intends to eliminate the hesitation

Dijital delillere hemen her tür uyuşmazlıkta ihtiyaç duyulabilir. Elektronik delillere başvurmanın en çok rastlandığı ve bu delillere en çok ihtiyaç duyulduğu uyuşmazlıklar ticari sırların çalınması, ayrımcılık, dolandırıcılık, bilgilerin çalınması, (özellikle boşanma vb. durumlarda) mal gizleme ve hile ile ilgilidir[5].

Elektronik belgelerin senet olup olmayacağı, özellikle senede bağlanan sonuçlar itibariyle tartışılmaktadır. Yukarıda sayılan şartları taşımayan bir belgenin senet sayılması mümkün değildir. Bu sebeple elektronik belgelerin senet olarak değerlendirilip değerlendirilmeyeceğinin belirlenmesi için öncelikle bu şartları taşıyıp taşımadığının tespiti gerekir. Elektronik belgeler yukarıda belirttiğimiz şartları bir arada taşımadıkları sürece senet niteliğinde olmalarından bahsedilemez. Bu belgelerin senet olarak kabulü, ancak çıktı veya suretlerinin imzalanması durumunda söz konusu olacaktır. Öte yandan, senedin tamamının elle yazılmış olması da gerekmemektedir, sadece imzanın elle atılması yeterlidir. Bu bağlamda, elekt-

about the power of evidence in secured electronic signed papers. Indeed, the regulation (Article 205/2) repeated the former 1086 numbered Law Judgment and Procedure Law article 295/A c.1, and there is no difference between current civil procedure law and former civil procedure law in this regard[6].

Accordingly, electronically signed documents are legal bonds in Turkish Law. If a party objects the authenticity of the electronic document, he or she must raise this issue before courts. If the objecting party fails to do so, the electronic document may be used against him. According to relevant provision in the Civil Procedure Law, if one of the parties objects the authenticity of the electronic signed document context, judge must hear the objecting party. If the judge cannot reach a conclusion after hearing, he may appoint an expert to analyze the content of the document. Thus, if there is hesitation about the document context, judge may appoint the expert to eliminate the hesitation. However, the appointment of an expert is required only if the judge cannot reach an opinion based on the arguments of the objecting party. The expert opinion is not required if the judge reaches a decision based on the arguments[7].

In litigation, parties must submit all relevant electronically signed documents. Electronic documents must be properly submitted both in print and digitally. This regulation extends to both securely and insecurely signed documents, as well as electronic documents without signature.

4. CONCLUSION

In today's world, the use of internet and computers are increasing in every aspect of live. Similarly, digital documents are increasingly used in litigation processes. For example, in Turkey, the petitions or other documents may be submitted to courts either in paper or digitally through UYAP system. Indeed, after the introduction of UYAP system, it has been increasingly preferred to litigate or submit documents electronically. Undoubtedly, new regulations contribute to this process by facilitating the use of digital systems in litigation. It may be said that submission of documents in litigation process will be made electronically in the future. The new regulations in Turkish Law regarding digital evidence, especially provisions regarding protection measures in Criminal Procedure Law and electronic documents in Civil Procedure Law carry great importance in this regard. ■

ronik belgelerin elektronik ortamda güvenli elektronik imza ile teyidi, yani doğrulanması mümkündür.

Konuyla ilgili önemi dolayısıyla kısaca elektronik delillerin incelenmesi noktasında özellikle delil niteliği tartışmalı olan elektronik posta ve elektronik imza kavramlarına kısaca değinmek faydalı olacaktır. Özellikle elektronik postanın niteliği gereği tek başına güvenilir bir kaynak olmadığı için delil olarak kullanılmasında da bazı sakıncaların bulunduğu, elektronik postanın pek çok güvenlik açığını da beraberinde getirdiği, mesaj göndericisinin farklı şekillerde yazılabildiği, içeriğinin değiştirilebildiği, IP numarasının değiştirilmek suretiyle başka bir IP adresinden gönderiliyormuş gibi gösterilebileceği, bir bilgisayara dışarıdan erişim yoluyla da o bilgisayardan gönderilebileceği söylenebilir.

Hukukumuzda elektronik imzanın hukuki ve teknik yönleri ile kullanımına ilişkin esaslar 5070 Sayılı Elektronik İmza Kanunu (**"EİK"**) ile düzenlenmiş olup, EİK elektronik imzayı "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri" olarak tanımlamaktadır (EİK m. 3/b). 2012 yılında yürürlüğe giren 6100 Sayılı HMK'da da, mülga 1086 Sayılı Hukuk Muhakemesi Usulü Kanunu'nda (**"HMUK"**) olduğu gibi elektronik belgelerin delil niteliğine açıkça yer verilmiştir. HMK m. 205/2'de usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olduğu düzenlemesi yer almaktadır. Maddenin gerekçesinde ise elektronik imzalı belgelere dair getirilen bu düzenlemenin amacı belirtilmiştir. Gerekçeye göre, bu düzenleme ile güdülen amaç, elektronik imzalı belgelerin delil gücü konusunda tereddüdün ortadan kaldırılmasıdır. Her ne kadar gerekçede, maddenin getiriliş amacının elektronik imzalı belgelerin delil gücü konusundaki tereddüdün giderilmesi olduğu belirtilmiş olsa da, HMK m. 205/2, usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olduğu düzenlemesiyle, HUMK m. 295/A, c.1'in tekrarıdır[6].

Elektronik imzalı belgelerin senet hükmünde olduğu düzenlemesinden hareketle, HMK'nın 208. maddesinde taraflardan biri, kendisi tarafından düzenlendiği iddia edilen bir belgedeki yazı ve imzayı inkâr etmek isterse, sahtelik iddiasında bulunması gerektiği; aksi halde elektronik imzalı belgenin, aleyhe delil olarak kullanılacağı belirtilmektedir Öte yandan, güvenli elektronik imzalı belgelerin inkarını düzenleyen HMK'nın 210. maddesi

ile, HUMK'da olmayan yeni bir düzenleme getirilmiştir. Bu düzenlemeye göre, güvenli elektronik imza ile oluşturulmuş verinin inkârı halinde hâkim, veriyi inkâr eden tarafı dinlemesine rağmen bir kanaate varamamış olması halinde bilirkişi incelemesine başvuracaktır. Dolayısıyla, güvenli elektronik imzaya yönelik bir inkârın söz konusu olduğu durumlarda bu konunun uzmanı olan bilirkişilerin yapacağı inceleme ile bu tereddütler giderilecektir. Ancak bu incelemeden önce, güvenli elektronik imzayı inkâr eden taraf hâkim tarafından dinlenecektir. Bunun üzerine hâkimde kanaat oluşursa, bilirkişi incelemesi aşamasına geçilmeyecektir. Ne var ki, yapılan açıklama hâkimde yeteri derecede bir kanaat oluşturmazsa bilirkişi incelemesine başvurulması zorunludur[7].

Elektronik belgeler, belgenin çıktısı alınarak ve talep edildiğinde incelemeye elverişli şekilde elektronik ortama kaydedilerek mahkemeye ibraz edilecektir (HMK m. 219/1). Bu düzenleme hem güvenli veya güvenli olmayan elektronik imza ile imzalanmış, hem de hiç imzalanmamış elektronik belgeler için geçerlidir.

4. SONUÇ

Günümüzde hayatın her alanında dijital ortama geçiş söz konusudur. Adli yargı hizmetlerinin yürütülmesinde de dijital ortam ve fiziki ortam (kağıt belgeler) eşgüdümlü yürütülmektedir. Bu konuda en bariz örnek adliyelerde elden dilekçe sunulması ve dava açılması mümkün olmakla beraber, UYAP sisteminin devreye girmesi ile UYAP aracılığıyla dava açılması, dilekçe sunulmasının da olağan bir uygulama haline gelmiş olmasıdır. Özellikle kanun koyucunun dijital deliller konusunda her geçen gün yeni mevzuat düzenlemeleri öngörmesi hukuk uygulamasını fiziki ortamdan dijital ortama kaydırmaktadır. Hatta teknolojinin gündelik hayatımızda yerinin artması ile gelecekte ve adli süreçlerin sadece dijital evraklar üzerinden yürüyeceği öngörüsünde bulunulabilir. Hayatın hemen her alanında yaşanan bu dönüşüm karşısında ceza muhakemesi sürecinde dijital deliller kapsamında uygulanan koruma tedbirleri ile Hukuk Muhakemeleri Kanunu'nda özellikle elektronik imzalı belgeler konusunda sağlanan gelişmeler ülkemiz açısından önemli kazanımlardır. ■

BIBLIOGRAPHY KAYNAKÇA

Akar, Ayşe Ece. Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği. İstanbul: XII Levha, 2013

"Bilişim Suçları Kapsamında Dijital Deliller", (10.04.2015), http://ab.org.tr/ab05/tammetin/134.pdf

Çakır, Hüseyin ve Kılıç, Mehmet Serkan. Adli Bilişim ve Elektronik Deliller. Ankara: Seçkin Yayıncılık, 2014

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

"Dijital Delil", (10.04.2015), http://kripteks.com.tr/adli-bilisim/dijital-delil

Dülger, Volkan. Bilişim Suçları ve İnternet İletişim Hukuku. Ankara: Seçkin, 2013.

Göksu, Mustafa. Hukuk Yargılamasında Elektronik Delil (1086 Sayılı HUMK ve 6100 Sayılı HMK Çerçevesinde). Ankara: Adalet Yayınevi, 2011

Henkoğlu, Türkan. Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi. İstanbul: Pusula, 2014