Bilgi Yönetimi Dergisi

Cilt: 3 Sayı: 2 Yıl: 2020

https://dergipark.org.tr/tr/pub/by

Hakemli Makaleler

Araştırma Makalesi

Makale Bilgisi

Gönderildiği tarih: 19.11. 2020
Kabul tarihi: 14.12. 2020
Yayınlanma tarihi: 31.12. 2020

Article Info

Date submitted: 19.11. 2020
Date accepted: 14.12. 2020
Date published: 31.12. 2020

Anahtar sözcükler

E-imzalı Belgeler, EBYS, Delil Değeri, Mevzuat

Keywords

E-signed Records, ERMS, Evidential Value, Legislation

DOI numarası

10.33721/by.828160

ORCID

0000-0002-1436-7431 (1)
0000-0002-9868-242X (2)

Elektronik İmzalı Belgelerin Delil Değerinin Korunmasında Mevzuatta Öngörülen Delil Özelliklerinin İncelenmesi*

Surveying the Evidential Features Prescribed in Legislation on Preserving the Evidential Value of Electronic Signed Records

Özhan SAĞLIK
İstanbul Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü Doktora Öğrencisi, *ozhan.saglik@gmail.com*

Niyazi ÇİÇEK
İstanbul Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü Öğretim Üyesi, *ncicek@istanbul.edu.tr*

Öz

E-imza teknolojileri, günümüzde e-imzalı belgelerin delil değerini koruması için sahip olması gereken özellikleri karşılayabiliyorken, ilerleyen yıllarda nasıl bir durumla karşılaşılacağıyla alakalı tereddütler henüz giderilememiştir. E-imza algoritmalarının teknolojik eskimeye uğraması, saldırı ihtimali gibi güvenlik açıkları, uygulama yazılımlarının eksikliği ve teknolojik göç yöntemleriyle ilgili sonuçların henüz yeteri kadar görülmemesi gibi çeşitli riskler söz konusudur. Bu riskler, e-imza doğrulanamazsa ya da doğrulama sırasında şüpheye düşülürse ne yapılabilir, belgelerin delil değeri nasıl korunabilir sorularını gündeme getirmektedir. E-imza ile ilgili şüpheye düşüldüğünde sertifika doğrulaması yapılmakta; bir karara varılamazsa bilirkişiye başvurulabilmektedir. Bunların yanı sıra elektronik belge yönetim sistemlerinde (EBYS) kayıt altına alınan e-imzalı belgelerin delil değerinin korunmasında başka mekanizmaların da kullanılabileceği düşünülmektedir. Bu mekanizmalardan biri olarak söz konusu belgelerin mevzuatta yer alan delil özelliklerine göre üretilip üretilmediğini değerlendirmek amacıyla kullanılabilecek bir kontrol listesinin belgelerin delil değerinin korunmasına olumlu bir katkı yapacağı kanaati savunulmaktadır. Çalışmada, nitel araştırma yöntemi kullanılmaktadır.Mevzuatta e-imzalı belgelerin sahip olması gereken özellikler,delil değerinin korunmasında bir kontrol listesi oluşturmak hedefiyle incelenmiştir.Bu kontrol listesi aracılığıyla e-imzalı belgelerin delil değerinin korunup korunmadığının değerlendirilebileceği önerilmektedir.

Abstract

While e-signature technologies can meet the features that e-signed records should have to preserve their evidential value, the doubts about what kind of situation will be encountered in the coming years have not been resolved yet.There are various risks such as technological ageing of e-signature algorithms, security vulnerabilities like the possibility of attacks, the lack of application software and the consequences of technological migration methods are not yet seen enough. These risks raise the questions of what can be done if the e-signature cannot be validated or if there is a doubt during the validation, how can the evidential value of the records are preserved. In case of doubt about e-signature, the certificate is validated, and if a decision cannot be reached, an expert can be consulted. In addition to these, it is considered that other mechanisms can be used to protect the evidential value of e-signed records recorded in electronic records management systems (ERMS). As one of these mechanisms, it is argued that a

** "Bu çalışma, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalında Prof. Dr. Niyazi Çiçek'in danışmanlığında yürütülmekte olan Özhan Sağlık'ın "Elektronik Belge Yönetimi Uygulamalarındaki Koşullar Işığında E-İmzalı Belgelerin Delil Değerinin Arşivsel Güvenilirlik Açısından İncelenmesi" adlı doktora tezine dayanılarak hazırlanmıştır."*

***Bu makalenin araştırma ve yayın süreci "Araştırma ve Yayın Etiğine" uygun şekilde yürütülmüştür.*

checklist can be used to assess whether the records are produced according to the evidential characteristics in the legislation will make a positive contribution to the preservation of the evidential value of the records. A qualitative research method is used in the study. The features that e-signed records should have in the legislation have been examined with the aim of generating a checklist to protect the evidential value. It is suggested thatit can be assessed whether the evidential value of e-signed records is preserved through this checklist.

1. Giriş

Örgütler, elektronik ortamda yürüttükleri işlemlerin sonucunda oluşan belgeleri yapılan faaliyetlerin delili olarak EBYS'lerde kayıt altına alırlar. Deliller, bir uygulama ve işlemin nasıl yürütüldüğünü aynı zamanda bir konu hakkında iddia veya savunmaların dayandığı vakıaları ispata yarayan vasıtalar olarak kabul edilmektedir (Acar, 2012, s. 4). Geçmişte yaşandığı iddia edilen bir olayın gerçekten meydana gelip gelmediğini tespit etmek için kullanılırlar (Centel, 2012, s. 96).

Bir vakıayı ispata yarayan her nesne delil olabilir. Bir yazılı kayıt, ses dosyası ya da güvenli elektronik imza ile düzenlenmiş bir belge delil olarak kabul edilebilir. Ancak, kanunlar bazı durumlarda nelerin delil kabul edilebileceğini çeşitli şartlara bağlı kılmıştır. Mesela, 2 bin beş yüz Türk Lirası ve üzerindeki hukuki işlemlerin senetle ispat edilmesi gerekir (Hukuk Muhakemeleri Kanunu [HMK]). İdari işlemlerin delili olan belgelere de bir takım hukuki özellikler atfedilmiştir. Bunlar, hem kâğıt hem de elektronik ortamdaki belgeler için geçerlidir. Söz konusu özellikler, aynı zamanda belgelerin delil değeri olarak adlandırılmaktadır (Çiçek ve Sağlık, 2017, s. 258).

İdari işlemler sonucunda oluşan kayıtlardan bir kısmı belge değerine sahipken bazıları doküman statüsündedir. Senato kararlarından diplomalara, yazışmalardan tutanaklara kadar pek çok malzeme belge olarak değerlendirilir. Bunlardan kamu görevi neticesinde oluşanlar, aynı zamanda resmî belge statüsündedir. Hukuki işlemlerin doğruluğunu belirtme yetkisine sahip makam tarafından usulüne göre düzenlenmiş veya onaylanmış yazılı kayıtlar da resmî belge niteliği taşımaktadır. Bununla birlikte, devlet memurlarınca görev gereği gerçekleştirilen işlemleri ihtiva eden resmî defter ve dosyalar, askerî plân ve haritalar ile bir olayın gerçeğe uygunluğunu gösteren her türlü yazılar belge olarak kabul edilmektedir. Bu belgelerin güvenilir olup doğrulanabilmesi gerekir (Türkiye Büyük Millet Meclisi [TBMM], 2003, s. 172; Türk Ceza Kanunu [TCK], 2004). Bu noktadan hareketle, usulüne uygun düzenlenen, gerçeklik ve güvenilirlik içerip doğrulanabilen, düzenleyenin imza gibi bir kimlik tespiti aracı kullanılarak kendini belli ettiği her türlü yazının belge olarak kabul edildiği anlaşılmaktadır.

Kamu kurumlarında oluşan yazışmaların hangi usullere göre üretileceğinin belirlendiği Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te (Resmî Yazışma Yönetmeliği) bir yazılı kaydın belge olabilmesi için "bir işlemin yerine getirilmesi için oluşturulması, aidiyet zincirini muhafaza etmesi, el yazısı ya da güvenli e-imza ile imzalanması ve kurumsal belge yönetim sisteminde kayıt altına alınmış olması" gerektiği belirtilmektedir. E-imzalı belgelerin delil değeri teşkil etmesi için elektronik belge yönetim sistemlerinde kayıt altına alınması, güvenli e-imza ile imzalanması, üstveri, format ve ilişkisel özelliklerini koruyarak aidiyet zincirini muhafaza etmesinin gerekli olduğu görülmektedir (Resmî Yazışma Yönetmeliği, 2020). Çalışmada kullanılan e-belge/e-imzalı belge kavramı, buradaki tanım çerçevesinde anlaşılmalıdır. E-imza kavramı da çalışmada güvenli e-imzayı ifade etmektedir.

Belge tanımının yapıldığı diğer mevzuatları incelemenin belgelerin sahip olması gereken özellikleri anlayabilmeye olumlu bir katkı yapacağı düşünülmektedir. Güvenli elektronik imzalı belgelerin senet hükmünde olduğunu belirten Hukuk Muhakemeleri Kanunu'nda (HMK) da belge tanımı bulunmaktadır. Kanun'da, belgenin bir bilgi taşıyıcısı olduğu yönünde çok geniş bir tanım yapıldığı görülse de, belge hüviyeti taşımanın bir özelliğinin de uyuşmazlık konusu vakıaları ispata elverişli araç olması gerektiği anlaşılmaktadır (HMK, 2011). HMK'daki bu tanım, Bilgi Edinme Hakkı Kanunu'nda da görülmektedir (Bilgi Edinme Hakkı Kanunu, 2003). Belge tanımına tanık olunan bir diğer prosedür ise Damga Vergisi Kanunu'dur. Kanun'a göre, belgelerin yazılı olması, imza içermesi ve herhangi bir hususu ispat edebilmesi gerekmektedir (Damga Vergisi Kanunu, 1964).

Bununla birlikte Yargıtay kararlarında da belgenin tanımı yapılmıştır. Belgenin, belirli bir düşünce, hukuki ilişki veya vakayı yansıtan, başka bir deyişle hukuki sonuç doğurmaya elverişli bir irade beyanını içeren ve düzenleyicisinin kim olduğunu gösteren yazılı evrak olarak tanımlandığı görülmektedir.

Bunun yanı sıra, belgenin unsurları da belirtilmektedir. Bu unsurlar şöyle ifade edilebilir (Yargıtay, 2017):

1. Yazılı olmak
    a. Bir dilin kullanılması
    b. Yazının bir vasıtayla kaydedilmesi
    c. Yazının elverişli bir cisme kaydedilmiş ve taşınabilir olması
    d. Yazının okunabilir olması
2. Hukuki sonuç doğurmaya elverişli bir içeriğinin bulunması
3. Düzenleyenin belli olması

Ayrıca, aynı kararda, belgenin belirli bir düşünce veya olayın aktarımını ya da bir hukuki ilişkinin varlığını veya yokluğunu gösterme gibi bir irade beyanını içermesi hâlinde hukuken korunduğu ve delil niteliğinin bulunduğu belirtilmektedir. Bununla birlikte, bir irade açıklamasının hukuki bir sonuca yol açacak nitelikte olması hâlinde, belgenin hukuki sonuç doğurmaya elverişli bir içeriğinin bulunması şartı da karşılanmış olacaktır. O hâlde, bir yazılı kaydın belge olabilmesi için yazılı olması, kâğıt veya elektronik gibi taşınabilir kayıt ortamında bulunması, hukuki sonuç doğuracak içeriğinin bulunması ve düzenleyenin belli olması gerekmektedir.

Bu noktada, e-imzalı belgeler, yukarıda belirtilen özellikleri yaşam döngüsü boyunca koruyabilecek mi, bunların yanı sıra başka özelliklere ihtiyaç duyulabilir mi gibi sorular akla gelmektedir. Çünkü e-imzaların kırılgan bir yapıya sahip olduğu bilinmektedir. İhtiyaç duyulan teknolojik gereksinimlerin sağlanamaması durumunda e-imzalı belgelerin gelecekte doğrulanamaması riski söz konusudur. Bu risk, e-imzalı belgelerin mevzuatta yer alan diğer özelliklere göre üretilip üretilmediğini değerlendirme imkânı sunacak bir kontrol listesinin oluşturulabileceği düşüncesini gündeme getirmektedir.

1.1. Problem, Amaç ve Yöntem

Kâğıt ortamında oluşan belgelerin delil değerini korumak için ısı ve nem gibi koşulları olması gereken seviyede tutmak yeterliyken, elektronik ortamda paradigma değişmiştir. Elektronik belgelerin muhatabına gönderildiğinde, sistemler arasında iletildiğinde, saklama ortamlarında veya kullanılan donanım/yazılım güncellendiğinde ya da değiştirildiğinde özgünlüklerini koruyamama riski bilimsel çalışmalarda sık tartışılan konulardandır (International Research on Permanent Authentic Records in Electronic Systems [INTERPARES], 2002, s. 30). Bu riski azaltmak amacıyla belgenin bütünlüğünü koruyan ve irade beyanında bulunanın kimlik tespiti işlevine sahip olan e-imzanın, 2004 yılında yayınlanan Elektronik İmza Kanunu (EİK) ile elle atılan imzayla aynı hukuki sonucu doğurduğu hüküm altına alınmıştır (EİK, 2004). E-imzalı belgelerin delil değeri taşıması için belgeyi imzalayan kişinin açıkça belirtilmesi, gerçekleştirilen fiili göstermesi ve imzanın gerçekten o kişi tarafından atıldığını ispat etmesi gerekir. E-imza, gerçekleştirildiği iddia edilen işlemin yapıldığını ispat ettiği müddetçe belgenin delil değerinin korunmasında kullanılan bir araç olarak kabul edilecektir (Leroux, 2004, s. 201). Fakat, e-imza algoritmalarının teknolojik eskimeye uğraması, saldırı ihtimali gibi güvenlik açıkları, uygulama yazılımlarının eksikliği ve teknolojik göç yöntemleriyle ilgili sonuçların henüz yeteri kadar görülmemesi e-imzalı belgelerde görülen riskler arasında değerlendirilmektedir (Kamu Sertifikasyon Merkezi [Kamu SM], 2015; Boudrez, 2007, s. 182-183).

Bununla birlikte, her ne kadar iflas ve benzeri durumlar karşısında e-imza sertifika sağlayıcılarının mevcut sertifikaları benzer bir mahiyetteki kuruluşlara devretmeleri hüküm altına alınsa da ilerleyen dönemlerde bu devrin sağlıklı bir şekilde gerçekleşip sertifikaların geçerliliğinin korunduğuna dair yeteri kadar tecrübe söz konusu değildir. Ayrıca, Kamu SM'nin belgeleri istemeyerek de olsa değiştirmek gibi bir ihtimalin söz konusu olabileceği ifade edilmektedir (Bralic, Kules ve Stancic, 2017, s. 91-92). E-imzaların teknolojik göçü meselesi karşılaşılan bir diğer sorun olarak öne çıkmaktadır. Bu göç sırasında belgenin okunabilirliğinin olumsuz etkilenmesi riski gündeme gelmektedir. Bundan dolayı teknolojik göçten sonra belgenin yeniden imzalanması, belgedeki imzanın sahihliğinin doğrulanması, ilk oluşan bit akışı ve doğrulama zincirinin korunması ile teknolojik göç sürecinin sertifikalandırılmasına ihtiyaç duyulmaktadır. Çünkü teknolojik göç sonrası belgenin yeni bir bit akışı

olacak ve daha önce oluşturulan bit akışı ile örtüşme gerçekleşmeyecek, bunun neticesinde belgenin formatı değiştikten sonra e-imzanın doğrulama fonksiyonu geçerli olamayacaktır. Bu noktada, teknolojik göç sonrası oluşturulan belgelerin yeniden imzalanacağı söylenmektedir. Mesela, e-imza sahibi artık hayatta olmayabilir veya kurumda o fonksiyonu gerçekleştirmekle ilgili bir görevi bulunmayabilir. Böyle bir durumda e-imzayı aynı kişinin yeniden oluşturması ne ölçüde mümkün olabilir? Bu konuda henüz yeterli pratikler sergilenememiştir. (Boudrez, 2007, s. 186-188).

Söz konusu riskler, e-imzalı belgelerin delil değerini olumsuz yönde etkileyebilir. Her ne kadar mevzuat, e-imzalı belgelerde gerekli olan delil değeri özelliklerinin e-imza sertifikalarında mevcut olduğuna karar verse de, bu sertifikaların doğrulanamaması gibi bir ihtimal karşısında e-imzalı belgelerin delil olarak kullanılamaması riski hep gündemdedir. Bu noktada, e-imzalı belgelerin delil değerinin korunması için e-imzanın yanı sıra mevzuatta belirtilen diğer delil özelliklerinin neler olduğu ve bunların delil nitelemesiyle uyumlu olup olmadığının değerlendirilmesi gerektiği düşünülmektedir. Makalede bu amaçla kullanılabilecek bir kontrol listesi oluşturulmaya çalışılmıştır. Böylece e-imza dışında başka faktörlerin de bir kriter olarak kullanılabileceği konusuna dikkat çekmek amaçlanmıştır.

Bu makalede nitel araştırma yöntemi kullanılmış olup durum çalışması anlayışı benimsenmiş, belgesel analiz gerçekleştirilmiştir (Yıldırım ve Şimşek, 2016). Külcü ve Turan'ın (2013) kamudaki belge yönetimine ilişkin mevzuatı incelediği çalışmasından faydalanılmakla birlikte mevzuatta "belge" ve "arşiv" anahtar kelimeleriyle taramalar yapılmış ve HMK, Ceza Muhakemesi Kanunu (CMK), Türk Borçlar Kanunu (TBK), Türk Ticaret Kanunu (TTK), Vergi Usul Kanunu (VUK), Noterlik Kanunu, Tebligat Kanunu ve Kayıtlı Elektronik Posta (KEP) Yönetmeliği, Bankacılık Kanunu, Elektronik Haberleşme Kanunu, Sigortacılık Kanunu EİK ve Resmî Yazışma Yönetmeliği'nde belgelerin delil değerinin korunmasıyla ilişkilendirilebilecek hükümler bulunduğu görülmüştür.

Çalışmada ilk olarak e-imzayı el ile atılan imzayla aynı hukuki sonucu doğurduğunu ifade etmesi nedeniyle EİK incelenmiştir. Resmî Yazışma Yönetmeliği, kurumsal fonksiyonların yürütülmesi sırasında oluşan yazışmaların sahip olması gereken özelliklere ilişkin hükümleri belirlemektedir. Kamu kurumlarının oluşturduğu yazışmalar, bu Yönetmelik'e uygun olmakla birlikte, delil değerini korumak için diğer mevzuat hükümlerinde belirtilen niteliklere de sahip olmalıdır. İncelenen kanunlardan ilki HMK'dır. Bunun seçilmesinin nedeni, e-imzalı belgelerin delil değerine ilişkin hükümler içermesidir. Bununla birlikte, belgede sahtecilikle ilgili hususlar yer aldığından CMK'daki hükümler incelenmiştir. TBK'da belgelerin şekil özellikleriyle ilgili hükümlerin mevcut olması Kanun'un incelenmesini gerekli kılmıştır. TTK ve VUK'a bakılmasının nedeni ticari faaliyetler sonucunda oluşan belgelerin yapılan faaliyete göre dosyalanması gerektiğini belirtmek gibi normların mevcut olmasıdır. Noterlik Kanunu, e-imza ile düzenlenecek belgelere ilişkin hükümler içerdiğinden kapsam dışında tutulmamıştır. Kurumlara yapılacak elektronik tebligatlara ilişkin hükümler barındırması nedeniyle Tebligat Kanunu analiz edilmiştir. Kamu kurumlarının elektronik ortamda birbirlerine iletecekleri resmi yazışmalar için KEP Yönetmeliği hazırlanmıştır. E-imzalı belgelerin geçerliliğiyle ilgili hükümler bulunduğundan bahsi geçen Yönetmelik de değerlendirilmiştir. Diğer kanunlardan farklı olarak kapsamlı yaklaşımlar getirmesi nedeniyle Bankacılık Kanunu analiz edilmiştir. Kurumların risk değerlendirmesine ilişkin hükümler içermesinden dolayı Elektronik Haberleşme Kanunu ele alınmıştır. Belgelerin sahip olması gereken özellikler belirtildiğinden Sigortacılık Kanunu da bu kapsamda değerlendirilen prosedürler arasında yer almıştır.

Çalışma, üç kısımdan meydana gelmektedir. Birinci bölümde literatür analizi yapılmıştır. Burada daha çok hukuk alanındaki yayınlar incelenmiştir. İkinci bölümde e-imzalı belgelerin delil değerinin korunması için gerekli olan özelliklerin belirtildiği mevzuat hükümleri değerlendirilmiştir. Üçüncü bölümde ise EBYS'lerde kayıt altına alınan e-imzalı belgelerin delil değerinin korunmasına yardımcı olabilecek kontrol listesi tablosunun gösterilmesine gayret edilmiştir.

2. Literatür İncelemesi

2004 yılında yayınlanan EİK ile, e-imzanın elle atılan imza ile aynı hukuki sonucu doğuracağı hüküm altına alınmıştır. Bu nedenle, daha çok 2004 yılından sonra çıkmış olanlar ile bu tarihten itibaren güncellenerek e-belge konusunda hüküm koyan prosedürler incelenmiştir. Prosedürlerin yanı sıra düzenleyici işlem türü belgeler ile makale, kitap ve tez gibi diğer literatür de değerlendirilmiştir. Mine Erturgut'un e-imzalı belgelerin geçerliliğiyle ilgili yaptığı doktora tezi, e-belgelerin senedin özelliklerini

karşılayamadığını ifade etmesi bakımından önemli bir tartışmaya öncülük etmiştir (Erturgut, 2004). Bu tartışmanın sebebinin orijinalin sadece bir tane olması nedeniyle elektronik ortamda mevcut olamayacağı düşüncesinden kaynaklanabileceği değerlendirilmektedir. Aynı zamanda, HMK'da e-imzalı belgelerin adi senet hükmünde olduğu maddesi eklenirken, gerekçede e-imzanın dar ve teknik anlamda senet olmadığı belirtilmiştir (Özbek, 2013, s. 2233). Böyle bir kanaatin gelişen teknoloji karşısında kesin bir tanım yapmak istenmemesinden veya güvenli e-imzanın oluşturma ve doğrulama yöntemlerinin ıslak imza ile farklılığından kaynaklanabileceği düşünülmektedir. Fakat, söz konusu husus adi senet/resmi senet tartışmalarını da beraberinde getirmiş ve öğretide konu üzerinde incelemeler yapılmıştır (Pekcanıtez, Atalay ve Özkes, 2011; Acar, 2012; Göksu, 2010; Yardım, 2013). HMK'da e-imzalı belgelerin senet hükmünde olduğunun kararlaştırılması (HMK, 2011), TTK ve TBK'da e-imzanın elle atılan imza ile aynı sonucu doğuracağının hüküm altına alınması (TTK, 2011; TBK, 2011), UYAP'ta e-imza ile ıslak imzalı kararın çelişmesi hâlinde e-imzalı kararın benimsenecek olması (CMK, 2003), Danıştay ve Yargıtay kararlarında da e-imza ile oluşturulan belgenin ıslak imzayla oluşturulmasına gerek olmadığına dair verilen kararlar e-imzalı belgelerin delil değerini güçlendiren hususlar olarak değerlendirilmektedir (Danıştay, 2018; Danıştay, 2019; Yargıtay, 2020; Yargıtay, 2020a).

Hukuk alanında yapılan çalışmaların e-imzalı belgelerin uzun vadede geçerliliklerini nasıl koruyabileceğinden ziyade, tabii olarak günümüzdeki geçerliliği üzerine yapıldığı görülmektedir. 2004'den sonra e-imzalı belgelerin geçerliliği konusuna değinen ilk akademik çalışmalardan biri Mustafa Göksu'ya ait doktora tezidir. Göksu, e-imzalı belgelerin senedin özelliklerini karşılayamadığını (Göksu, 2010, s. 154) belirtmekte; hâkimin bu belgelerin geçerliliğini nasıl inceleyeceğini aktarmaktadır. Ayşe Ece Acar'ın yüksek lisans tezinden kitaplaştırdığı anlaşılan çalışması, e-imzalı belgelerin senedin özelliklerini karşıladığını ifade etmesi bakımından önemli bulunmaktadır (Acar, 2012). Ertan Yardım, karşılaştırmalı hukuktan örnekler vererek e-imzalı belgelerin senedin özelliklerini karşıladığını öne sürmektedir (Yardım, 2013). Mustafa Yılmaz, e-imzalı belgelerin idari yargılama hukukundaki delil niteliğini incelediği çalışmasında, bunların hangi şartlarda delil olarak kullanılabileceğini açıklamış fakat İdari Yargılama Usul Kanunu'nda bir ifade geçmemesini eksiklik olarak öne çıkarmıştır (Yılmaz, 2013). Bununla birlikte, Mustafa Serdar Özbek, elektronik ortamda düzenlenen noter senetlerini incelemiş ve bunların hangi şartlar dâhilinde geçerli olduğunu aktarmıştır (Özbek, 2013).

Söz konusu çalışmalar, genel olarak e-imzalı belgelerin geçerliliğini incelemektedir. Buna karşın, acaba e-imza işlevini yerine getiremezse söz konusu belgeler nasıl doğrulanabilir sorusu henüz yeteri kadar tartışılmamıştır. Bu soruya cevap arayan yazılardan biri 2017'de bu çalışmanın yazarları tarafından yapılmıştır (Çiçek ve Sağlık, 2017). Çalışmada elektronik delil elde etme yöntemleri kullanılarak belgelerin delil değerinin korunabileceği ifade edilmiştir. Bununla birlikte, Resul Göksoy'un yüksek lisans tezine dayanarak yayınladığı anlaşılan kitabında elektronik delillerin geçerliliği için sadece e-imza ve iz değerlerinin dikkate alınmasının sorun oluşturabileceği belirtilmiştir (Göksoy, 2019, s. 113-115, 119). Durum böyle olunca, e-belgelerin delil değerini nitelemek için mevzuatta belirtilen delil özelliklerini açığa çıkarmanın faydalı olabileceği düşünülmektedir.

3. Mevzuatta E-Belgelerin Delil Özellikleri

E-belgelerin delil değerine ilişkin hükümlerin yer aldığı düşünülen kanunlar ve yönetmelikler analiz edilmiş, kanunlardan tebliğlere ve yönetmeliklere giden bir seyir izlenmiştir. Bu seyir izlenirken önce kamu hukuku, sonra özel hukukla ilişkili mevzuat incelenmiştir. Bunun neticesinde elde edilen delil özelliklerinin bir tablo ile üçüncü bölümde açıklanmasına çalışılmıştır.

Çalışmada ilk olarak e-imzayı el ile atılan imzayla aynı hukuki sonucu doğurduğunu ifade etmesi nedeniyle EİK ele alınmıştır. Sonrasında medeni muhakeme hukukunun temel kanunu olan HMK ve ceza muhakemesinin temel kanunu olan CMK, belgelerin delil değeriyle ilişkili olduğu düşünülen hükümleri açısından incelenmiştir. Yargıtay kararlarıyla CMK hükümleri birlikte değerlendirilmiştir. Bunlarla e-imzalı belgeler arasında ilişki kurulmasına çalışılmıştır. Bununla birlikte, VUK ve ilişkili mevzuat gözden geçirilmiştir.

Bankacılık Kanunu'nda diğer kanunlardan farklı olarak daha kapsamlı yaklaşımlar olduğu görülmektedir. Bu kanun ve ilişkili mevzuattaki hükümler e-imzalı belgelerin delil değeriyle ilişkilendirilerek açıklanmıştır. Aynı zamanda kurumların risk değerlendirmesine ilişkin hükümler

içermesi nedeniyle Elektronik Haberleşme Kanunu ve ilişkili mevzuat analiz edilmiştir. Ayrıca, Sigortacılık Kanunu ve ilişkili mevzuatta belgelerin sahip olması gereken özellikler belirtilmektedir. Kamu hukukundaki kanunlardan son olarak onaylama ve düzenleme şeklindeki e-imzalı belgelere ilişkin hükümler içermesi nedeniyle Noterlik Kanunu da çalışmanın kapsamına alınmıştır.

Yukarıda belirtilen kanunlardan sonra kamu hukukundaki yönetmelikler analiz edilmiştir. Kurumlara yapılacak elektronik tebligatlara ilişkin hükümler içeren Tebligat Kanunu Yönetmeliği analiz edilmiştir. Kurumsal fonksiyonların yürütülmesi sırasında oluşan yazışmaların sahip olması gereken özelliklere ilişkin hükümleri belirleyen Resmî Yazışma Yönetmeliği incelenmiştir. Sonrasında özel hukukun kapsama alanında bulunan ve belgelerin şekil özellikleriyle ilgili hükümler içeren TBK ile ticari faaliyetler sonucunda oluşan belgelerin delil değeriyle ilgili hükümler barındırdığı düşünülen TTK ve ilişkili mevzuat irdelenmiştir. Son olarak hem ticari tarafların hem de kamu kurumlarının elektronik ortamda birbirlerine iletecekleri e-imzalı belgelere ilişkin hükümler ihtiva eden KEP Yönetmeliği analiz edilmiştir.

Elektronik imzalı belgelerin delil değeri taşıması için güvenli elektronik imza ile oluşturulmaları gerekir. Güvenli elektronik imza, sadece imza sahibine bağlı olan ve onun tasarrufundaki güvenli elektronik imza oluşturma aracı ile atılan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimlik tespitine imkân veren imzalanmış elektronik veride sonradan değişiklik yapılıp yapılmadığının belirlenmesini sağlayan araç olarak tarif edilmektedir. Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurmaktadır. Fakat kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler (tapu alım-satımı, evlilik akdi gibi) ile banka teminat mektupları dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilememektedir (EİK, 2004). Bu gibi durumlar 2020 yılından güncellenen Resmî Yazışma Yönetmeliği'nde de zorunlu hâl olarak tarif edilmiştir (Resmî Yazışma Yönetmeliği, 2020).

Elektronik imzalı bir belgenin delil değeri taşıması için yukarıdaki hususları sağlaması gerekir. Bu noktada güvenli elektronik imza oluşturma ve doğrulama araçlarının özelliklerinin açığa çıkarılması gerekli görülmektedir. Güvenli elektronik imza oluşturma aracı, ürettiği imza verilerini eşsiz kılmalı, bunların gizliliğini ve üçüncü kişilerce elde edilemeyip kullanılamamasını sağlamalı ve e-imzayı sahteciliğe karşı korumalıdır. Bununla birlikte, imzalanacak veri, imzalandıktan sonra değiştirilememelidir (EİK, 2004).

Güvenli elektronik imza doğrulama araçları ise imza sahibinin kimliğini, imzanın doğrulanması için kullanılan veriler ile doğrulama işlemini güvenilir ve kesin biçimde çalıştırarak sonuçları değiştirmeksizin doğrulama yapan kişiye göstermeli, aynı zamanda imzalanmış verileri güvenilir bir biçimde sunabilmelidir. Bununla birlikte, kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçları değiştirmeksizin doğrulama yapan kişiye göstermelidir (EİK, 2004).

E-imzalı belgelerin delil değerine ilişkin çeşitli hükümler HMK'da bulunmaktadır. Burada, deliller kesin ve takdiri olmak üzere ikiye ayrılmıştır. Kesin deliller, senet, yemin ve kesin hüküm; takdiri deliller ise bilirkişi, tanık, keşif, uzman görüşü ve kanunda düzenlenmemiş diğer delillerdir (HMK, 2011; Acar, 2012, s. 8-12). HMK'da 204. maddede yer alan "*yetkili memurların görevleri içinde usulüne uygun olarak düzenledikleri belgeler, aksi ispatlanıncaya kadar kesin delil sayılırlar*" (HMK, 2011) hükmünden hareketle kamu kurumlarında oluşan belgelerin kesin delil kabul edildiği anlaşılmaktadır. Burada, belgelerin usulüne uygun olarak düzenlenmesi gereği dikkat çekmektedir.

Kesin delil olarak kabul edilen kamu belgelerinin uyuşmazlık konusu vakıalara ispata elverişli olmanın yanı sıra, senetlerin sahip olması gereken özellikleri de ihtiva etmesi gerektiği anlaşılmaktadır. Senedin özellikleri, bu konuda çalışma yapan hukukçuların görüşlerinden (doktrin) öğrenilmektedir. Bunlar, somutluluk, yazılılık, bir irade beyanı içermek ve irade beyanının kimlik tespiti için bir imzanın bulunmasıdır (Berkin, 1946; Acar, 2012, s. 24-25). Ayrıca, senetler Latin harfleriyle yazılmalıdır (Yavaş, 2009, 117). Resmî senetler söz konusu olduğunda, senedin, resmî makam veya memur tarafından düzenlenmesi; düzenlemenin, düzenleyen makam veya memurun yetkisi dâhilinde olması ve usulüne uygun olarak meydana getirilmesi gerekmektedir (Yavaş, 2009, s. 150). Elektronik ortamda üretilmiş senetler için bu özelliklere veri bütünlüğünün yani verilerin değiştirilemezliğinin sağlanması da eklenmektedir (Erturgut, 2004, s. 138).

Ceza muhakemesi, maddi gerçeği araştırıp bulmayı gaye edinmiştir. Böylece, cezanın genel ve özel önleme işlevini gerçekleştirerek kişisel öç alınmasını engellemeyi amaçlar. Medeni muhakeme hukuku ise özel hukuk kurallarına aykırılık durumunda yapılacak muhakemeyi düzenleyip bireylerin kişisel haklarının sağlanmasını hedefler. Bu nedenle, medeni muhakeme hukuku ancak hakkı ihlal edilen tarafından harekete geçirilebilir. Ceza muhakemesinde maddi gerçeğin aranmasına karşılık, medeni muhakemede kural olarak biçimsel gerçeğin tespitiyle yetinilir. Bu farklılıktan dolayı ceza muhakemesinde delil serbestîsi vardır (Zafer ve Centel, 2012, s. 7).

Bireyler, özel hukuk alanındaki ilişkilerinde sorun çıkması ihtimalini düşünerek ispat vasıtalarını hazırlayabilir; fakat işleyeceği suçun delillerini hazırlayamaz. Aksine, suç delilleri yok edilmeye çalışılır. Bu nedenle, ceza muhakemesinde delillerin sınırlandırılması ispatı zorlaştırarak ceza muhakemesini işlemez hâle getirebilir. Ceza muhakemesinin bu özelliğinden kaynaklanan delil serbestîsinin sınırsız bir serbestlik olduğu düşünülmemelidir. Delil olarak kullanılacak araçların bazı özelliklere sahip olması gerekir (Zafer ve Centel, 2012, s. 196-197). Bunlar şöyle açıklanabilir (CMK, 2004; Yargıtay, 1993; Yargıtay, 2013):

- Deliller, uyuşmazlığı oluşturan olayın bir parçasını ispat edebilecek nitelikte ve beş duyu organımızla algılanabilecek maddi yapıya sahip olmalı,
- Deliller, hukuka uygun yollardan elde edilmeli,
- Delil, sağlam ve güvenilir olmalı, uydurulmamalı ve değiştirilmemeli,
- Mahkeme taraflarınca delillerin bilinmesi sağlanmalı (müştereklik) ve
- Delilin oluştuğu andan imhasına kadar geçen süreçte doğruluğu ve bütünlüğü sağlanmalı.

Bu hükümler delil olan her nesne için geçerli kabul edilmektedir. E-imzalı belgeler için bu hükümlerin bir işlem sonucunda oluşması, ekranda görünebilmesi ve çıktısının alınabilmesi, kurumun elektronik belge yönetim sisteminde kayıtlı olması, özgünlük, gerçeklik ve tamlık arz etmesi, her zaman erişilebilir ve kullanılabilir olması ile aidiyet zincirinin belgenin yaşam döngüsü boyunca korunması anlamına geldiği düşünülmektedir (Çiçek ve Sağlık, 2019, s. 151-153).

CMK'nın elektronik işlemler bölümünde e-imza ile ilgili önemli hükümler bulunmaktadır. Bu Kanun'da gösterilen istisnalar hariç olmak üzere e-imza ile UYAP üzerinden her türlü ceza muhakemesi işlemi yapılabilmektedir. Fiziki olarak hazırlanması öngörülen her türlü belge e-imza ile imzalanabilir ve e-imzalı bu belgeler, muhatabına elektronik ortamda gönderilir, gerekmedikçe fiziki olarak düzenlenmez. En dikkat çeken hüküm ise UYAP'taki e-imzalı belgenin elle atılan imzayla çelişmesi hâlinde UYAP'ta kayıtlı olan belgenin geçerli kabul edilmesidir. Bu hükmün elektronik ortamı fiziki ortama göre daha öncelediği kabul edilmektedir (CMK, 2004).

E-imzalı belgelerde, mühürleme işlemi ile kanunlarda birden fazla nüshanın düzenlenmesini öngören hükümler uygulanmamakta; zorunlu nedenlerle fiziki olarak düzenlenmiş belgeler ise yetkili kişilerce taranarak UYAP'a aktarılarak gerektiğinde ilgili birimlere elektronik ortamda gönderilmektedir (CMK, 2004). Bu hükümler, "Bölge Adliye ve Adlî Yargı İlk Derece Mahkemeleri ile Cumhuriyet Başsavcılıkları İdarî ve Yazı İşleri Hizmetlerinin Yürütülmesine dair Yönetmelik'"te de yer bulmaktadır. Ayrıca, mezkur Yönetmelik'te teknik nedenlerle fizikî olarak düzenlenen belgelerin engelin ortadan kalkmasından sonra derhâl elektronik ortama aktarılması benimsenmiştir (Bölge Adliye ve Adlî Yargı İlk Derece Mahkemeleri ile Cumhuriyet Başsavcılıkları İdarî ve Yazı İşleri Hizmetlerinin Yürütülmesine dair Yönetmelik, 2015).

Vergi hukuku, kişilerin devletler ile vatandaşlık ilişkilerinden kaynaklanan vergi ödevine ilişkin kuralları düzenler (Öner, 2019, s. 27). Vergi hukukunda, ceza hukuku ile aynı nitelikte olmasa da genel hatlarıyla benzerlik taşıyan delil serbestliği ve delillerin serbestçe değerlendirilmesi ilkeleri geçerlidir. Hukukun öngördüğü sınırlamalar dâhilinde "delil" niteliğini taşıyan her ispat aracı kullanılabilir ve hâkim tarafından serbestçe değerlendirilir. Bununla birlikte, vergi yargılamasında "kesin delil" kavramına ihtiyatlı biçimde yaklaşılmaktadır. Çünkü bir işlem uyuşmazlık konusu olduğunda, işlemin dayanaklarının ve yargılama sırasında ileri sürülen tüm ispat araçlarının "delil" olarak nitelendirilmesi; bunların doğruluğuna ve delil olarak kabulü için gerekli diğer koşulları taşıyıp taşımadığına hâkim tarafından kanaat getirilmesine bağlıdır (Gümüşkaya, 2015, s. 261, 265).

VUK'da belgelerin delil değeriyle ilgili çeşitli hükümler görülmektedir. Kanun, bir hakkın ispatında delil olarak kullanılabilecek belgelerin işlerinin icabına göre dosyasında muhafaza edilmesini gerekli kılmaktadır (VUK, 1961). Buradan, belgelerin delil değerinin korunması için sağlıklı bir dosyalama yapılması gerektiği anlaşılmaktadır. Bununla birlikte, VUK tebliğlerinde de e-belgelerle ilgili bazı hükümler görülmektedir. 509 nolu Genel Tebliğ'de, elektronik ortamda oluşturulacak belgelerin üzerinde mali mühür/nitelikli elektronik sertifika taşımaya, belge üzerinde doğrulamaya, görüntülemeye ve kâğıt baskı almaya imkân veren genel bir tanınırlığa sahip olan bir formata sahip olması gerektiği belirtilmiştir. Bununla birlikte, belgelerde üç haneli birim kodu ve 13 haneli sıra numarasından oluşan belge numarası kullanılması gerekmektedir. 13 haneli sıra numarasının ilk 4 karakteri, yılı temsil ederken 9 karakterli numara, her yıl 1'den başlayarak kullanılır. Aynı belge numarası, birden fazla kullanılmamaktadır. Yine aynı tebliğe göre, e-arşiv uygulamasını kendi sistemi üzerinden kullananlar, belgelere ait elektronik kayıtların bozulması, silinmesi, zarar görmesi, işlem görememesi halleri ile olağanüstü durumların meydana gelmesi halinde, durumu Başkanlığa on beş gün içinde bildirerek bu kayıtları nasıl tamamlayacağına ilişkin ayrıntılı bir plan sunmak zorundadır (509 Sıra No'lu VUK Genel Tebliği, 2019).

509 nolu Genel Tebliğ'de e-fatura mükellefi olmayan kuruluşlara e-fatura format ve standartları kullanılarak ve faturanın basılabilir görüntüsü eklenerek faturaların elektronik ortamda gönderilebileceği belirtilmektedir (509 Sıra No'lu VUK Genel Tebliği, 2019). Bu format ve standartlar, Elektronik Arşiv Kılavuzu ve E-Fatura Entegrasyon Kılavuzunda açıklanmaktadır. Bununla birlikte, e-arşiv raporlarının ise XADES-A standardı kullanılarak e-arşiv uygulaması üzerinden Gelir İdaresi Başkanlığına (GİB)'e gönderilmesi gerekmektedir (GİB, 2018). E-arşiv uygulamasını kendi sistemlerinde kullanmak isteyen kurumlar, ISO 27001, ISO 22301 ve ISO 2000 Standartları'na sahip olmalıdır (GİB, 2018b). Oluşturulacak e-faturalar, Universal Business Language (UBL) – Türkçe (TR) olarak eXtended Markup Language (XML) dilinde, Unicode Transformation Format-8 (UTF-8) formatında, Standart Business Document Header formatındaki bir zarfta ve XML Schema Definition (XSD)'a uygun olarak üretilmelidir. UBL dilindeki faturalar, mali mühür ile onaylanmalıdır (GİB, 2018b). O hâlde, mali belgelerin belirlenen format ve standartlarda üretilmesi ile çıktısı ve elektronik ortamdaki görüntüsünün aynı olması gerektiği anlaşılmaktadır. Ayrıca, e-belgeler için bir risk planı oluşturulmalıdır.

E-faturasını kendi bilgi işlem sistemlerinde oluşturmak isteyen kurumlar, Portable Document Format (PDF) kullanıyorsa faturayı PDF Advanced Electronic Signature (PADES) standardını kullanarak mali mühür/nitelikli e-imza ile imzalamalıdır. Fatura ekine, XML yapısındaki UBL-TR ve XSD eklenmelidir (GİB, 2018). E-fatura kullanım kılavuzunda mali mühür, verinin bütünlüğü, içeriği ve düzenleyeni gösteren ve koruma altına alan nitelikli elektronik sertifika alt yapısını ifade etmektedir. Kullanım açısından e-imza ile benzerlik göstermektedir (GİB, 2013). Elektronik bilet ve elektronik yolcu listesinde mali mühür ya da e-imzanın XML Advanced Signature - Basic Electronic Signature (XADES-Bes) ile havayolu ve etkinliklerde kullanılacak e-biletlerin ise XADES-Archival (XADES-A) ile imzalanması gerekmektedir (GİB, 2016a; GİB, 2016b; GİB, 2017).

509 (509 Sıra No'lu VUK Genel Tebliği, 2019) ve 446 (446 Sıra No'lu VUK Genel Tebliği, 2015) nolu tebliğlerde e-biletlerde ve e-yolcu listelerinde bulunması gereken bilgiler açıklanmaktadır. Bununla birlikte, 509 nolu tebliğde e-bilet ve raporlarının Türkiye'de saklanması gerektiği belirtilmiştir (509 Sıra No'lu VUK Genel Tebliği, 2019). O hâlde, üretilen e-belgelerin delil değerinin korunması için belgelerin Türkiye'de saklanması gerektiğini ifade etmek mümkündür.

Kurumların elektronik ortamda hazırladığı diğer belge türleri e-defter ve beratlardır. Bu belgelerin bütünlüğü ve gerçekliği, e-imza ve mali mühür ile sağlanmaktadır. Ayrıca, e-defter ve beratlar, eksiksiz, okunabilir, anlaşılabilir ve kâğıt çıktısı alınabilir olmalıdır. Bu belgelerin Türkiye'de muhafaza edilmesi zorunludur (1 Sıra No'lu Elektronik Defter Tebliği, 2011). 509 sıra nolu Genel Tebliğ, e-defter ve e-fatura kullanımında özel entagratör kullanımını mümkün kılmakta fakat bu durumda, entagratörün donanım ve yazılımının Türkiye'de bulunması zorunluluğunu getirmiştir (509 Sıra No'lu VUK Genel Tebliği, 2019).

Bununla birlikte yazılım uyumluluk onayı kılavuzunda, eXtensible Business Reporting Language (XBRL) dili kullanılması gerekli kılınmış ve dosya boyutları, yapı gibi unsurlarla ilgili teknik

zorunluluklar belirtilmiştir. E-defterlerin XBRL Global Ledger (Küresel Defter) taksonomisine göre oluşturulması gerekmektedir (GİB, 2018c). Kılavuzda, bir dizin yapısının benimsenerek ilgili kayıtların ait olduğu dosya içerisinde bulunması yönünde bir yaklaşım benimsendiği görülmektedir (GİB, 2016). Bu noktada, bilişsel bir süreç olan dosyalama mantığının (Çiçek, 2016a) e-defterlerin yönetiminde uygulandığını ifade etmek mümkündür.

Dünyadaki fon kaynaklarının transferini sağlamak amacıyla bankacılık faaliyetleri gerçekleştirilmektedir. Bankalar, ciddi miktarda parayla finansal işlem yapmaktadır. Bu işlemlerin hilesiz yapılacağına dair bir güven ortamının tesisine ihtiyaç duyulmaktadır. Bu amaçla denetimler uygulanmakta, bankacılık kanunları düzenlenmektedir (Gündoğdu, 2019, s. 21). Bankacılık işlemleri, belgelere dayanarak gerçekleştirilmektedir. Türkiye'deki Bankacılık Kanunu ve ikincil düzenlemelerde faaliyetlerin delili olan belgelerin sahip olması gereken bazı özelliklerin ifade edildiği gözlenmektedir.

Kanun'da, "*alınan yazılar ve faaliyetler ile ilgili belgelerin asılları veya bunun mümkün olmadığı hâllerde sıhhatlerinden şüpheye mahal vermeyecek kopyaları ve yazılan yazıların makine ile alınmış, tarih ve numara sırası verilerek düzenlenecek suretleri, usûlleri çerçevesinde ilgili banka nezdinde on yıl süreyle saklanır. Bu belgelerin mikrofilm, mikrofiş şeklinde veya elektronik, manyetik veya benzeri ortamlarda saklanmaları mümkündür*" hükmü mevcuttur (Bankacılık Kanunu, 2005). Bir belgeyi asıl (orijinal) yapan özelliklerden biri ilk üretildiği haliyle mevcut olmasıdır (Çiçek, 2009, s. 208). Fakat elektronik bir belgenin aslından söz etmek pek mümkün değildir. Çünkü belge elektronik ortamdaki cihazlar arasında sürekli bir aktarım halinde olduğundan ilk üretildiği hâli korunmamaktadır (INTERPARES, 2008). Elektronik ortamın doğasına özgü bir durum olsa da, bankacılık faaliyetlerine ilişkin elektronik belgelerin delil değerinin korunması için gerekli olan bir özelliğin de sıhhatlerinden şüpheye mahal vermemek olduğu anlaşılmaktadır. Ayrıca, belgelerin evrak kayıt sistemine tarih, numara ve konusu belirtilerek kaydının zorunlu tutulduğu görülmektedir (Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2006).

Bununla birlikte, belgeler, zamanında (Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ, 2013), doğru (Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ, 2016) ve okunabilir bir şekilde denetime sunulup güvenilir bir şekilde muhafaza edilerek (Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, 2013) her zaman erişilebilir (Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik, 2014) olmalıdır. Ayrıca, belgelerin bütünlük, tutarlılık, güvenilirlik, doğruluk ve hesap verebilirlik koşullarını içermesi gerekmektedir. Bunun yanı sıra, 1 Temmuz 2020 tarihinde yürürlüğe giren "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te yer alan "*bilgi sistemlerine ilişkin işlemlerin doğruluğu ve güvenilirliği asgari olarak, yapılmak istenen işleme ait anahtar öneme sahip bilgilerin işlemin başlangıcından tamamlanışına kadar doğruluğunu yitirmemesini ve yapılmak istenen işlemin kendinden beklenen sonucu yerine getirmesini; tamlığı ise asgari olarak bütün işlemlerin hata üretmeden gerçekleşmesini ve mükerrer olamamasını gerektirir*" hükmünün, belgelerin aidiyet zincirinin korunması anlamına geldiği düşünülmektedir (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, 2020). Bahsi geçen yönetmelikte, bu konuda benimsenen yaklaşımlar şöyle belirtilebilir:

Bilgi sistemleri yönetiminin kurumsal yönetimin bir parçası olduğu ve bilgi sistemleri stratejisi ile iş hedeflerinin uyumlu olması gerektiği dile getirilmektedir. Bilgi sistemleri yönetimine ilişkin unsurların yönetsel hiyerarşi içerisinde uygun yere yerleştirilerek gerekli finans ve insan kaynağının tahsis edilmesi gerekmektedir. Bununla birlikte, bilgi sistemlerinin yönetimine ilişkin politika ve prosedürlerin hazırlanması ile risk yönetiminden bahsedilmektedir. Risk yönetiminde dikkate alınabilecek unsurlar belirtilmektedir. Bu unsurlar, teknolojik gelişmeler, hizmet alımı, işlem kayıtları, güvenilirlik ve bilgi güvenliği önlemleri şeklinde ifade edilebilir. Bilgi güvenliğinin sağlanmasında, belgelerin gizlilik, bütünlük ve ulaşılabilirliklerine dikkat edilmesiyle güvenlik hassasiyetlerine göre sınıflandırılıp uygun düzeyde güvenlik kontrollerinin tesis edilmesi ve sızma testlerinin gerçekleştirilmesi gibi yaklaşımlar önerilmektedir (Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, 2020).

E-imzalı belgelerin delil değerine ilişkin hükümlerin görüldüğü bir diğer mevzuat Elektronik Haberleşme Kanunu'dur. Bu kanun, haberleşme alt yapısı, şebeke ve hizmet alanlarında teknolojik gelişime ilişkin usul ve esasları belirlemektedir (Elektronik Haberleşme Kanunu, 2008). "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği" bu konuda önemli hükümler içermektedir (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014). Elektronik haberleşme hizmeti sunan ve/veya şebekesi sağlayan ve altyapısını işleten şirketler yani işletmeciler, bilgi güvenliği yönetim sistemi kurmakla mükellef kılınmıştır. Bu sistem, bilginin gizliliği, bütünlüğü ve erişilebilirliğini sağlamalı, bunlarla birlikte, kuralları belirlenmiş; planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, yönetimce onaylanmış ve uluslararası güvenlik standartlarına uyumlu olmalıdır. Bunun için işletmeciler, öncelikle bilgi güvenliği yönetim sistemi politikası oluşturmalıdır. Bilgi güvenliği yönetim sistemi politikasında, uygulanan güvenlik politikaları, prosedürler, kurallar, prensipler ve standartlar hakkında genel bilgiler verilir. Burada, risk değerlendirmesi yapılarak varlıklar sınıflandırılmaktadır (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014).

İşletmecilerin sahip oldukları varlıkları kaydettiği varlık envanterinde, asgari olarak varlığın adı, tipi, yeri, yedekleme bilgisi, değeri, sorumlusu ve kimlik bilgileri bulunur. Bununla birlikte, varlıklar, gizlilik sınıfı, kritiklik derecesi, yasal gereksinimler ile hassasiyet kriterlerine göre etiketlenir. Ayrıca, erişim, kullanım, depolama, iletim, imha, paylaşım ve dağıtım kuralları da belirlenir (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014).

Bununla birlikte, işletmeciler, elektronik ortamda tutulan bilgilerin yetkisiz olarak erişilmesi, değiştirilmesi, silinmesi ve zarar görmesine karşı gerekli önlemleri almalıdır. Bunun için hangi yetkilinin nelere erişip erişemeyeceği belirlenerek önceden yetkilendirmeler yapılır. İmha edilmesi gereken bilgiler, geri döndürülemez şekilde silinmelidir (Güler, 2020, s. 283-288). Yönetmelik'te değişim yönetimi felsefesi benimsenmiştir. Öncelikle değişiklikler tanımlanarak kayıt altına alınır, planlanır ve test edilir. Sonrasında değişikliklerin etkileri analiz edilir ve önerilen değişiklikler onaylanır. Öngörülemeyen sonuçlarla karşılaşılması durumunda yapılacak işlemler belirlenir (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014).

İşletmeciler, felaket ya da hata durumları karşısında yedekleme yapmalıdır. Bunun için ihtiyaçlar ve sistemlerin kritiklik seviyesine uygun olarak yedekleme periyodu, yedekleme türü ve saklama zamanı belirlenir. Yedekleme aşamasında, yedek kopyaların kaydı tutulur; yedekler birbirinden farklı yerlerde saklanır ve periyodik olarak test edilir (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014).

Yönetmelikte tutulacak sistem kayıt dosyalarıyla ilişkili hükümler de bulunmaktadır. Buna göre, kullanıcı kimlikleri, oturum açma ve kapatma, veri ekleme/silme/değiştirme gibi işlemlerin tarihi, zamanı ve açıklamaları, erişimin sağlandığı teçhizatın kimliği, sistem, veri ve diğer kaynaklara başarılı ya da reddedilmiş erişim girişimleri, sistem ayarlarındaki değişiklikler, kullanılan özel izinler ve ayrıcalıklar, kullanılan sistem araçları ve uygulamaları, erişilen dosyalar ve erişim tipi, ağ adresleri, güvenlik sistemlerinin aktif ve pasif hale getirilmeleri, güvenlik ayarları ve kontrollerine ilişkin değişiklikler veya değişiklik girişimleri, sistem yöneticileri tarafından yapılan işlemler ve rapor edilen sistem hatalarını içeren log kayıtlarının en az 2 yıl süre ile saklanması gerekmektedir (Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği, 2014). Buradaki hususların, elektronik belge yönetim sistemlerinde de tutulan log kayıtları ve denetim günlüklerinde bulunması gereken özellikler için bir yol gösterici olabileceği düşünülmektedir. EBYS'lerdeki log kayıtları üzerine yapılan bir çalışmada, kurumları yönlendirici bir rehbere ihtiyaç duyulduğu dile getirilmektedir (Yalçınkaya, Gedikli ve Cibaroğlu, 2019).

İnsanların ve kurumların günlük yaşam içerisinde çeşitli risklere maruz kalması ve bu risklerin gerçekleşmesi neticesinde ciddi ekonomik zararların oluşması sigorta fikrini ortaya çıkarmış ve sigortacılık gelişmiştir (Günay, 2019, s. 17). Türkiye'de sigortacılık sektörünün güvenli ve istikrarlı bir ortamda etkin bir şekilde çalışmasını temin etmek için Sigortacılık Kanunu hazırlanmıştır. Bunun araçlarından biri olarak da denetim önemli bir fonksiyon olarak öne çıkmaktadır. Kamu kurum ve kuruluşları, birlikler ile sivil toplum kuruluşları, denetim amaçlarına uygun olarak sigortacılıkla ilgili bilgi işlem sistemlerini erişime açmalı ve verilerin güvenliğini sağlamalıdır (Sigortacılık Kanunu, 2007).

Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik'te, konuya ilişkin önemli hükümler görülmektedir. Denetimlerde, faaliyetlere ve finansal tablolara ilişkin her türlü belgenin içeriği ve kayıtlara uygunluğu ayrıntılı bir şekilde incelenmektedir. Her bir muhasebe kaydı, bir belgeye dayandırılır. Eğer kayıtlar, bilgi işlem sistemleri tarafından oluşturuluyorsa denetçiler, sistemin kayıtları nasıl oluşturduğunu, kayıtların iş süreci ile sistemde nasıl kontrollerden geçtiğini araştırır (Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik, 2008). Denetçiler, güvenilir kanıtlar derlemek zorundadır. Bunun için denetime konu olan kayıtlar, mevzuata uygun hazırlandıklarına dair güven oluşturacak bir açıklık taşımalıdır. Bununla birlikte, etkin kontrol sistemlerinin hataları azalttığı, yapısal zayıflıkların ise hataları artırdığı belirtilmektedir (Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik, 2008).

Noterlik, hukuki güvenliği sağlamak ve anlaşmazlıkları önlemek amacıyla farklı işlemler sonucunda oluşan belgelere resmiyet kazandıran kamu görevlileridir. Taraflar arasında yapılan işlemlere resmiyet kazandırmak hedeflenir (Çetin ve Ateş, 2019, s. 175). Noterler tarafından düzenlenen ve onaylanan belgeler de resmî belge olarak kabul edilmektedir.

Noterlik Kanunu ve ilişkili mevzuatta da belgelerin delil değerine ilişkin hükümler bulunduğu görülmektedir. Noterler tarafından Noterlik Kanunu'nun ikinci bölümünün hükümlerine göre düzenlenmiş olan hukuki işlemler ki neticesi belge ile somutlaşıp şekle bürünen uygulamalar, sahteliği sabit oluncaya kadar geçerlidir. Bunlar, düzenleme şeklinde yapılması zorunlu işlemlerdir (Noterlik Kanunu, 1972). Noter tarafından yapılan imza onaylaması, onaylanan imzanın ilgiliye aitliğini belgelendirme niteliğinde olup hukuki işlemlerin içeriklerini kapsamaz. Bu işlemlerde imza ve tarih, sahteliği sabit oluncaya kadar geçerlidir. Bunlar, onaylama şeklindeki işlemlerdir.

Noterlik Kanunu'nda 2014 tarihinde yapılan ekleme ile Kanun'da öngörülen işlemler, elektronik ortamda güvenli elektronik imza kullanılarak da yapılabilir (Noterlik Kanunu, 1972). Ancak, düzenleme şeklinde yapılması zorunlu tutulan işlemler ile irade beyanlarının alınmasına ilişkin işlemlerde güvenli elektronik imza kullanılabilmesi için ilgililerin noter huzurunda olmaları gerekir. Güvenli elektronik imza ile imzalanmış belgelerde, kanunlarda belirtilen mühürleme işlemi uygulanmaz ve ayrıca suret aranmaz. Güvenli elektronik imza ile oluşturulan belge, talep edilmedikçe ayrıca fiziki olarak düzenlenmez. Elektronik ortamdan fiziki örnek çıkartılması gereken hâllerde, belge, aslının aynı olduğu belirtilerek noterlikçe imzalanır ve mühürlenir. Güvenli elektronik imza ile imzalanmış belgenin elle atılan imzalı suretiyle çelişmesi hâlinde noterlerin kullandığı bilişim sisteminde kayıtlı olan güvenli elektronik imzalı belge esas alınır (Noterlik Kanunu, 1972).

Noterlere ait belgelerin korunması ve saklanması için ortak tedbirler almak Noterler Birliğinin görevleri arasındadır. Noterler tarafından elektronik ortamda yapılan tüm işlemlere dair bilgi ve belgeler, Türkiye Noterler Birliğinin Bilişim Sisteminde (TNBBS) kaydedilir ve saklanır. Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik ile güvenli elektronik imza ile yapılan tüm noterlik işlemlerinde zaman damgası kullanılması hüküm altına alınmıştır. Noterler, elektronik ortamda tespit işlemleri de yapmaktadır. Bir donanımdaki veya internet ortamındaki verinin tespiti işlemi ile o verinin belirli bir anda ya da zaman aralığında o anki veya zaman aralığındaki hâlinin değişmez olarak belirlenmesi, tekrar edilebilir hâlde tutulması ve saklanması anlaşılmaktadır (Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik, 2015).

Türkiye Noterler Birliği, elektronik ortamda güvenli elektronik imza ile işlem yapılmasına imkân sağlayacak altyapıyı kurmak ve işletmekten sorumludur. Bunun için gerekli standartlar ve şartları belirler. Noterlerdeki işleme katılanların tamamının güvenli elektronik imzası ile elektronik ortamda yapılan bir işlem için talep edilmedikçe fizikî olarak belge düzenlenmez ve bu işleme ilişkin olarak elektronik ortam dışında bir saklama yapılmaz. Bu kayıtlar, iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak yedekli ve güvenli bir şekilde saklanır. Sistem tarafından tutulacak iz bilgilerinin kapsamı, Birlik tarafından belirlenir. İz bilgilerinin güvenliği, gizliliği ve bütünlüğü sağlanır. Bu Yönetmelik gereğince elektronik ortamda yapılan işlemlere ilişkin bilgi ve belgeler Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik hükümlerine, iş sürekliliği ve bilgi güvenliğine ilişkin uluslararası kabul görmüş standartlara uygun olarak yedekli ve güvenli bir şekilde TNBBS'de saklanır (Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik, 2015). Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik'te, noterler, ellerinde bulunan arşiv

malzemesi ve arşivlik malzemeyi, her türlü zararlı tesir ve unsurlardan korumak, mevcut asli düzenleri içerisinde tasnif edip saklamakla yükümlü kılınmıştır (Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik, 1990). Buradan noterlik belgelerinin doğal afetlere karşı önlem alınıp tasnif edilerek saklanmaları gerektiği anlaşılmaktadır.

2018 yılında çıkarılan Elektronik Tebligat Yönetmeliği, pek çok kamu ve özel kuruma tebligatın elektronik yollarla yapılmasını bir zorunluluk hâline getirmiştir. E-tebligat işlemlerinin yürütülmesi amacıyla Posta Telgraf Telefon Anonim Şirketi (PTT) tarafından Ulusal Elektronik Tebligat Sistemi (UETS) kurulmuştur. Tebligat oluşturmaya yetkili makam ve merciler, oluşturdukları tebligatı UETS'ye yükler ve UETS, bu mesajı zaman damgasıyla ilişkilendirerek muhatabın adresine iletir. Hem mesajın UETS'ye yüklenmesi hem de muhatabın mesajı aldığına dair kayıtlar, UETS'de saklanır. Yönetmelikte, tebligatın UETS tarafından teslim alındığı, muhatabına gönderildiği, muhatap tarafından okunduğu ve usulen tebliğ edilmiş olduğuna dair üretilen ve e-sertifika ile imzalanan kayıtlar delil kaydı olarak tanımlanmaktadır. Bu kayıtlar, aksi ispat edilmedikçe kesin delil sayılırlar. Bu işlem ve delil kayıtlarının erişilebilir, güvenli ve gizli bir şekilde ve bütünlük içerisinde saklanması gerekmektedir. Delil kayıtları, 30 yıl saklanmalıdır (Elektronik Tebligat Yönetmeliği, 2018).

UETS'yi kurmak, işletmek, sistemin güvenliğini ve sistemde kayıtlı verilerin muhafazasını sağlamak PTT'nin görevidir. E-tebligata ilişkin ana ve yedek sistemler, Türkiye'de bulunmalıdır. PTT, e-tebligatların imzalanmasında kendisi için oluşturulan nitelikli sertifikayı kullanmalı ve delil kayıtlarının doğrulanması hizmetini sunmalıdır. PTT'nin UETS'nin yukarıda belirtilen kriterler ışığında çalışması için gerekli önlemleri alması benimsenmişse de bu konuda bir teknik rehberin hazırlandığı henüz görülememektedir (Elektronik Tebligat Yönetmeliği, 2018).

Kamu kurumlarında oluşan yazışmaların hangi usullere göre üretileceğinin ifade edildiği Resmî Yazışma Yönetmeliği'ne göre e-imzalı bir belge format ve ilişkisel özelliklerini koruyarak aidiyet zincirini muhafaza etmeli, güvenli e-imza ile imzalanmalı ve kurumsal belge yönetim sisteminde kayıt altına alınmalıdır. Bununla birlikte, Yönetmelik'te zorunlu hâl ve olağanüstü durum belirlenmiştir. Zorunlu hâl, belgenin mevzuat gereği fiziksel ortamda bulunması gereken hâli, olağanüstü durum ise donanım ve yazılımdan kaynaklı sorunlar nedeniyle EBYS'lerin uzun süreli çalışamamasından dolayı belgenin fiziksel ortamda hazırlanması gereken durumları ifade etmektedir. Olağanüstü durumdan sonra belgenin üstverileriyle birlikte EBYS'ye kaydedilmesi gerekmektedir. Ayrıca, Resmî Yazışma Yönetmeliği'ne göre kurumda oluşan tüm belgeler için Elektronik Yazışma Paketi (EYP) oluşturulmalıdır (Resmî Yazışma Yönetmeliği, 2020). EYP, resmî bir yazışmaya ait belge ve üstveri gibi bileşenleri tanımlanan kurallar neticesinde tek bir elektronik dosyaya dönüştürür. Bu dosya, teknoloji ve platformdan bağımsız bir paket yapısına sahiptir (Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2020).

Bununla birlikte, ekonomik ve sosyal yaşamı düzenleyen mevzuatta da belgelerin delil değeriyle ilgili hükümler görülmektedir. Bu noktada toplum içerisindeki alacak ve verecek gibi edimleri düzenleyen TBK öne çıkmaktadır (Cansel ve Özel, 2017, s. 26, 37). TBK'da belgelerin sahip olması gereken niteliklere ilişkin hükümler görülmektedir. Aşağıda, bu hükümlerin açıklanmasına gayret edilmiştir.

TBK'da taraflar, hukuk tabiriyle "edinim" olarak tarif edilen mal mülk edinmekle alakalı işlemlerin hukuki geçerliliği için sözleşme düzenlerler. Bu sözleşmelerden bazılarının geçerliliği Kanun tarafından belirlenen şekle bağlanmıştır. Kanuni olarak adlandırılan bu şekil, 5 sınıfta değerlendirilmektedir. Bunlar, sözlü şekil, nitelikli yazılı şekil, resmi şekil, tescil ve ilandır (Kavak, 2015, s. 33). Sözlü şekilde bir hukuki işlemin ya da akdin kurulabilmesi için sözlü olarak irade beyanına ihtiyaç duyulur. Buna evlilik akdi örnek verilebilir.

Yazılı şekilde ise kanun, bazı sözleşmelerin geçerliliğini yazılı olarak yapılmaları şartına bağlamıştır. Sözleşmede bir irade beyanı bulunması ve bu irade beyanını ortaya koyanların imzasının varlığı gereklidir. Yazılı şekil ise metin ve imzadan oluşmaktadır. Metnin, sözleşmenin mahiyetini gösterebilmesi gereklidir (Doğan, Şahan ve Atamulu, 2019, s. 117,118).

TBK'da şirketlerin düzenleyeceği belgelere ilişkin hükümler de yer almaktadır. Türk şirketlerin her türlü hukuki işlem, sözleşme ve ticari defterlerini Türkçe olarak düzenlemeleri zorunludur. Türkiye'de faaliyet gösteren yurt dışı kaynaklı şirketlerin de Türkiye'deki resmi makamlara ibraz edecekleri belgeler ve hukuki işlemlerde kullanacakları belgeler Türkçe olmalıdır (Kavak, 2015, s. 84). O hâlde,

TBK'ya göre bir belgenin delil değerinden bahsedebilmek için belgenin Türkçe olması ve imzalanması gereklidir.

Bu noktada güvenli e-imza ile oluşturulan metinlerin de yazılı şekil şartı taşıyıp taşımadığı akla gelmektedir. TBK'da güvenli e-imza ile gönderilen metinlerin de yazılı şekil şartını taşıdığı kabul edilmiştir (TBK, 2011). Bu noktada irade beyanının borçlar hukukunda sahip olması gereken özelliklerinin incelenmesi gerekli görülmektedir. Bir irade beyanının yazılı kabul edilebilmesi için istenildiğinde ibraz edilmesi ve değiştirilemezliğinin temin edilmiş olması gerekir. E-imza, elektronik ortamda yapılacak sözleşmelerde tarafların kimliklerinin doğruluğunu, sözleşmenin bütünlüğünü ve doğruluğunu sağlayacak bir çözüm olarak kullanılmaktadır (Ber, 2018, s. 64).

Bir diğer kanuni şekil ise tescildir. TBK, bazı hukuki işlemlerin geçerliliğini, yasa gereği tutulan resmi sicillere kayıt düşürülmesine bağlamıştır. Vakıfların vakıf siciline, şirketlerin de ticaret siciline kaydedilmesi tescil şartına örnek verilebilir. Bununla birlikte, Kanun, bazı hukuki işlemlerin ilan edilmesini öngörmüş ve işlemin geçerliliğini bu ilana bağlamıştır. Vakıflar Genel Müdürlüğü tarafından merkezi sicile kaydedilen vakıf, Resmî Gazete ile ilan olunur. Medeni Kanun'a göre vasi tayini, gaiplik, hacir ve kazai rüşt kararlarının da ilan edilmesi gereklidir (Kavak, 2015, s. 39, 43-44). O hâlde bu işlemler elektronik ortamda yapılırsa belgelerin delil değerinin korunması için Ticaret Odaları ve Borsalar Birliği ile Vakıflar Genel Müdürlüğünün oluşturduğu prosedürlerdeki şekil özelliklerinin incelenmesi gerekmektedir. Çünkü bu prosedürler, belgenin delil değerini etkileyen şekil özelliklerine ilişkin hükümler içermektedir.

İnsanlar, mal ve hizmet üretip bunları tüketerek ticari faaliyetlerde bulunur. Bu faaliyetler aynı zamanda ekonomik sermayeyi oluşturur. Ticaret hukuku buradaki faaliyetleri düzenlemektedir (Kayar, 2018, s. 45). Bireyler oluşturdukları ekonomik sermayeden ayırdıkları paylar ile devletin gerçekleştirdiği hizmetlerin finansmanını sağlar. Ticaret hukukunda işlemler, belgelere dayalı yürütülür. TTK'da belgelerin delil değerine ilişkin önemli yaklaşımlar görülmektedir.

TTK'da ticari defterlere yazımlar ve kayıtların eksiksiz, doğru, zamanında ve düzenli yapılması gerektiği belirtilmiştir. Bu kavramların tanımı ise kanunun gerekçesinde bulunmaktadır. Tamlık, iş ve işlemlerin eksiksiz olarak muhasebeleştirilmesi anlamına gelmektedir. Bununla birlikte, ticari kayıtların doğruluk arz etmesi gerekir. Kaydın gerçeğe uygun bir biçimde iş ve işlemi yansıtması, işlemin gerçeğe uygun şekilde muhasebeleştirilmesi doğruluk anlamına gelmektedir. Bunun yanı sıra, zamanındalık ve düzenlilik ilkeleri ile karşılaşılmaktadır. Bu ilke, muhasebe kayıtlarının en geç 10 gün içerisinde kaydedilmesini, düzenlilik ise kayıtların zaman akışına göre tarih ve belge numarası esas alınarak yapılmasını ifade etmektedir (Öner, 2019, s. 228-230).

Bununla birlikte, TTK'nın 82. maddesinde tacirlerin, ticari faaliyetler sonucu oluşan belgeleri sınıflandırarak saklaması gerektiği belirtilmiş; e-belgelerin her an erişilebilir olması istenmiştir (TTK, 2011). O hâlde, TTK'ya konu olan faaliyetler kapsamında üretilen belgelerin delil değerinin korunması için belgeler, erişilebilir olmalı, tamlık ve gerçeklik arz etmeli, zamanında ve düzenli bir şekilde oluşturulmalı ve sınıflandırılarak saklanmalıdır. Bu noktada, belgelerin sınıflandırılarak saklanması gerekliliği dikkat çekmektedir. Belgelerin ait oldukları faaliyetle ilişki kurularak önceden hazırlanmış bir dosya planına göre dosyalanması gerektiği anlaşılmaktadır.

Türk Muhasebe Standartları'nda da belgelerin delil değeriyle ilişkilendirilebilecek özellikler görülmektedir. Buna göre, defter ve kayıtların Türkçe'den başka bir dilde tutulmayıp Türk Muhasebe Standartları ve IFRS'ye uyumlu bir şekilde düzenlenmesi gereklidir (Kayar, 2018, s. 227). Türk Muhasebe Standartları'na göre finansal bilgi, ihtiyaca ve gerçeğe uygun olmalıdır. İhtiyaca uygunluk, bilginin karar verme süreçlerine etki etmesi olarak tanımlanabilir. Gerçeğe uygunluk ise sunulan bilginin meselenin özünü anlatabilme kapasitesi olarak ifade edilebilir. Bilgi, ihtiyaca ve gerçeğe uygun olmak için karşılaştırılabilir, tam, doğrulanabilir, anlaşılabilir olmalı ve zamanında sunulmalıdır. Tamlık, bilginin ve sunumun bir olayın anlaşılması için gerekli olan tanımlamalar ve açıklamalar içermesi olarak ifade edilmektedir (Finansal Raporlamaya İlişkin Kavramsal Çerçeve, 2018).

Bununla birlikte, bilginin anlaşılabilir olması da bir diğer gerekliliktir. Bunun için bilgi, sınıflandırılmalı, tanımlanmalı ve sunulmalıdır. Finansal bilgilerin sınıflandırılmasında birimin yapısı ve işletmenin yürüttüğü faaliyetlerdeki rolünün açıklanmasına gayret edilir (Finansal Raporlamaya İlişkin Kavramsal Çerçeve, 2018). Hazırlanan bilgiler, işletmenin sürekliliğine hizmet etmelidir

(Emeklilik Fayda Planlarında Muhasebeleştirme ve Raporlama, 2006). Bu noktada, bilginin güvenilir olması da gerekir (Finansal Tabloların Sunuluşu, 2018). Aksi takdirde, ciddi sorunlara sebep olacak hatalarla karşılaşılabilir (Muhasebe Politikaları, Muhasebe Tahminlerinde Değişiklikler ve Hatalar, 2018). O hâlde, üretilen belgeler, doğru, tam, erişilebilir, anlaşılabilir ve tanımlanabilir olmalı; ait olduğu faaliyetle ilişkisi kurularak dosyalanmalıdır.

Defter ve belgelerin yükümlü lehine delil olabilmesi için, bunların birbirleriyle ve kayıt düzeniyle uyumlu olmaları gerekir. Aksi durumda defter ve belgelerin "güvenilir" olma niteliği ortadan kalkmaktadır. Defter ve belgelerin yükümlü lehine delil olabilmesi, defter ve belgelerin yasada belirlenen şekilde tutulup yasaya uygun düzenlenmelerine bağlıdır. Ticari defterlerin ispat gücüne ilişkin hükümlerin düzenlendiği HMK madde 222'ye göre ticari defterlerin ticari davalarda delil olarak kabul edilebilmesi için yasaya göre eksiksiz ve usulüne uygun olarak tutulması, açılış ve kapanış onaylarının yaptırılıp defter kayıtlarının birbirini doğrulamış olması gerekir (Gümüşkaya, 2015, s. 277).

Türk Ticaret Kanunu ile tacirler arasında, diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarlar veya ihtarlar, noter aracılığıyla, taahhütlü mektupla, telgrafla veya güvenli elektronik imza kullanılarak kayıtlı elektronik posta sistemi ile yapılabilmektedir. Kayıtlı elektronik posta (KEP) sistemi hakkındaki hususların düzenlenmesi Bilgi Teknolojileri ve İletişim Kurumunun uhdesine verilmiştir (TTK, 2011). Kayıtlı elektronik posta hizmet sağlayıcıların (KEPHS), KEP ile ilgili ürettiği kayıtların aksi ispat edilmedikçe kesin delil olduğu kabul edilmektedir. KEP ile ilgili kayıtlar, güvenli olmalı, gizlilik ve bütünlük içermelidir. Söz konusu kayıtlar, bu özellikleri korunarak en az 20 yıl saklanmalıdır. Bununla birlikte, KEP iletileri ve delilleri anlaşılabilir ve okunabilir olmalı, kullanılan sistem arayüzlerinin de engelli dostu olması gerekmektedir. Ayrıca, KEP'teki imzalama süreçlerinde KEPHS'ler için üretilmiş sertifikalar kullanılmalıdır (Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik, 2011).

KEP işlemlerinin nasıl yönetileceğine ilişkin de teknik bir tebliğ hazırlanmıştır (Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 2011). Bununla birlikte imzalama süreçlerinde Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e de uyumlu hareket edilmesi gerekir (Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ, 2020). KEP iletisi, paketleri ve işlem loglarının CMS Archival Electronic Signature (CMS Arşiv Elektronik İmza [CADES-A), kep delillerinin ise XML Archival Signature (XML Arşiv Elektronik İmza [XADES-A]) ile imzalanması önerilmektedir. Söz konusu imzaların "Elektronik İmza Kullanım Profilleri Rehberinde" (Bilgi Teknolojileri Kurumu [BTK], 2012) de yer alan en uzun ömürlü imza türü olarak adlandırılan profilde imzalanması gerekir. Bu imzalama işlemlerinde zaman damgası da kullanılır. Uygulama işlem kayıtları ise 20 yıl saklanmalıdır. Bununla birlikte, işlem kayıtlarında tutulması gereken asgari bilgiler de belirtilmektedir (BTK, 2012).

EBYS'lerde kayıt altına alınan elektronik imzalı bir belgenin delil değeri taşıması, öncelikle e-imza oluşturma ve doğrulama araçlarının tasarlandığı gibi çalışmasına bağlıdır. Sahada bu araçlarda yaşanabilecek olası bir aksaklığın nasıl giderilebileceği, bu aksaklığı gidermek amacıyla belgelerin delil değerinin nasıl güçlendirilebileceği yönünde bir yaklaşım pek görülememektedir. E-imzalı belgelerin mevzuattaki özelliklere uyumlu üretilip üretilmediğini değerlendirme imkânı sunabilecek bir kontrol listesinin bu konuda yardımcı olabileceği düşünülmektedir.

4. E-imzalı Belgelerin Delil Değerinin Korunmasında Kullanılabilecek Kontrol Listesi

E-imzalı belgelerin delil değerinin korunması amacıyla onun mevzuatta öngörülen özelliklere uyumlu olup olmadığının incelenebileceği düşünülmektedir. Bunun için aşağıda e-belge özelliklerinin topluca gösterildiği bir tablo oluşturulmuştur. Tabloda verilen kriterler, birden fazla mevzuatta yer alabilir, fakat mevzuat kısmı bu kriterlerin ilk görüldüğü yeri belirtmektedir. Tablo'daki kriterlerin özellikle hangi tür belgeler için kullanılabileceğinin belirtilmesine çalışılmıştır. Bununla birlikte, kriterler sıralanırken herhangi bir önem sırası benimsenmemiş, kanun, yönetmelik, tebliğ, Yargıtay kararları ve kılavuzlar şeklinde genelden özele doğru hareket edilmiştir.

Kriter	Belge Türü	Mevzuat
Güvenli e-imza ile imzalanmış olmak	E-imzalı tüm belgeler	Elektronik İmza Kanunu

Zaman damgası	E-imzalı tüm belgeler	Elektronik İmza Kanunu
Usulüne uygun düzenlenmiş olmak	Resmî yazışmalar	Türk Ceza Kanunu
Güvenilirlik	E-imzalı tüm belgeler	Türk Ceza Kanunu
Doğrulanabilirlik	E-imzalı tüm belgeler	Türk Ceza Kanunu
Gerçeklik	E-imzalı tüm belgeler	Türk Ceza Kanunu
Doğruluk ve bütünlük	E-imzalı tüm belgeler	Ceza Muhakemesi Kanunu
Uyuşmazlık konusu vakıalara ispata elverişli olmak	Medeni muhakeme hukukunda kullanılacak e-imzalı belgeler	Hukuk Muhakemeleri Kanunu
Metin	E-imzalı tüm belgeler	Borçlar Kanunu
Türkçe olmak	E-imzalı tüm belgeler	Borçlar Kanunu
Tamlık	E-imzalı tüm belgeler	Türk Ticaret Kanunu
Zamanındalık ve düzenlilik	Tacirlerin gerçekleştirdiği faaliyetler sonucunda oluşan e-imzalı belgeler	Türk Ticaret Kanunu
Sınıflandırmak	E-imzalı tüm belgeler	Türk Ticaret Kanunu
Dosyalama	E-imzalı tüm belgeler	Vergi Usul Kanunu
Bir işlemin yerine getirilmesi için oluşturulması	E-imzalı tüm belgeler	Resmî Yazışma Yönetmeliği
Aidiyet zincirini muhafaza etmek	E-imzalı tüm belgeler	Resmî Yazışma Yönetmeliği
EBYS'de kayıt altına alınmış olmak	E-imzalı tüm belgeler	Resmî Yazışma Yönetmeliği
EYP'ye sahip olmak	Resmî yazışmalar	Resmî Yazışma Yönetmeliği
Yedekleme	E-imzalı tüm belgeler	Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik
Doğal afetlere karşı önlem almak	E-imzalı tüm belgeler	Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik
UETS ve KEP kayıtlarının bütünlük içermesi	Resmî yazışmalar	Elektronik Tebligat Yönetmeliği, Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik
Politika ve prosedürlerin hazırlanması	E-imzalı tüm belgeler	Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik

Finans ve insan kaynağı tahsisi	E-imzalı tüm belgeler	Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik
Risk yönetimi	E-imzalı tüm belgeler	Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik
Belgelerin güvenlik hassasiyetlerine göre sınıflandırılıp uygun düzeyde güvenlik kontrollerinin tesis edilmesi ve sızma testlerinin gerçekleştirilmesi	E-imzalı tüm belgeler	Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik
Uluslararası güvenlik standartlarına uyumluluk	E-imzalı tüm belgeler	Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
Varlık envanteri	E-imzalı tüm belgeler	Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
Erişim, kullanım, depolama, iletim, dağıtım, paylaşım ve imha kuralları	E-imzalı tüm belgeler	Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
Değişim yönetimi planı uygulamak	E-imzalı tüm belgeler	Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
Log kayıtları	E-imzalı tüm belgeler	Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği
Doğrulamaya, görüntülemeye ve kâğıt baskı almaya imkân veren genel bir tanınırlığa sahip bir formata sahip olması	E-imzalı tüm belgeler	509 nolu Genel Tebliğ
E-fatura ve e-deftere ilişkin özelliklerin bulunması	E-fatura ve e-defter	509 nolu Genel Tebliğ
Belgelerin Türkiye'de saklanması	E-imzalı tüm belgeler	509 nolu Genel Tebliğ
Yazılı olmak	E-imzalı tüm belgeler	Yargıtay
Dil ve alfabenin kullanılması	E-imzalı tüm belgeler	Yargıtay
Bir cisme kaydedilebilirlik	E-imzalı tüm belgeler	Yargıtay
Okunabilirlik ve anlaşılabilirlik	E-imzalı tüm belgeler	Yargıtay
Hukuki sonuç doğurmaya elverişli içerik	E-imzalı tüm belgeler	Yargıtay
Hukuki ilişkinin varlığını ya da yokluğunu gösterecek irade beyanı	E-imzalı tüm belgeler	Yargıtay
Risk planı	E-imzalı tüm belgeler	Gelir İdaresi Başkanlığı Kılavuzu

Tablo 1. Delil Değeri Kontrol Listesi

E-imzalı belgelerin delil değeri analiz edilirken genelden özele bir süreç takip edilebilir. Bu sürece en başta kanunlarda geçen hükümlerle başlamak yerinde bir karar olacaktır. Sonrasında yönetmelik, tebliğler, Yargıtay kararları ve yönerge ile kılavuzlar şeklinde sıralanabilir. Bu sıralamaya rağmen, duruma özgü olarak bir vakanın değerlendirilmesinde kanunun ardından bir Yargıtay kararının öncelikle göz önünde bulundurulması gerekebilir.

E-imzalı bir belgenin delil değeri kritiğinde öncelikle e-imza sertifikası doğrulaması yapılmalı ve zaman damgası içerip içermediği incelenmelidir. Bu durum EİK'e göre ön koşuldur. Bu sorgulama neticesinde başarılı sonuç alınsa dahi diğer hususların kritik edilmesiyle belgelerin delil değerinde yaşanabilecek olası bir sorunun önüne geçilebileceği düşünebilmektedir. Her ne kadar Yargıtay kararlarının yönetmelik ve yönergeden sonra göz önünde bulundurulabileceği düşünülse de, daha önce de belirtildiği gibi söz konusu kararların temel düzeyde özellikler belirtmesinden dolayı e-imza kontrolünden sonra buradaki kriterler incelenebilir.

Söz konusu sorgulamadan sonra e-imzalı belgelerin yazılı bir metne ve dile sahip olup alfabenin kullanılıp kullanılmadığı incelenmelidir. Öğretiye göre kullanılan dilin Türkçe olması gerekir (Yavaş, 2009). Bununla birlikte, belge genel tanınırlığa sahip bir formata sahip olup bir cisme kaydedilebilmelidir. Kritik edilecek bir diğer husus ise belgenin okunabilir ve anlaşılabilir olup hukuki sonuç doğurmaya elverişli olduğudur. Bir belgede e-imzanın bulunması irade beyanı eden ile belge arasında hukuki ilişkinin varlığı ya da yokluğunu açıklamak için kimlik tespiti yapmaya imkân verir.

Bununla birlikte, güvenilir, doğrulanabilir ve gerçek olması ile doğruluk ve bütünlük arz etmesi e-imzalı belgeler için aranan diğer özelliklerdendir. Bu özelliklerin korunup korunmadığının incelenmesi için belgelerin EBYS'de kayıt altına alınması gerekir. EBYS'de kayıt altına alınan belgeler, bir işlemin yerine getirilmesi için oluşturulup aidiyet zincirini muhafaza etmelidir. Söz konusu belgeler, medeni muhakeme hukukunda kullanılacaksa uyuşmazlık konusu vakıaları ispatlayacak nitelikte olmalıdır.

Belirtilen bu hususiyetler, e-imzalı belgeler için genel kabul gören hususiyetler olurken, belgenin kullanıldığı sektöre göre de özel nitelikler aranabildiği görülmüştür. Örneğin TTK'ya göre tacirlerin evraklarını sınıflandırması, Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'e göre risk yönetiminin bulunması e-imzalı belgeler için bir kriter olarak belirtilmiştir. Dolayısıyla e-belgelerin delil değeri sorgulanırken üretildiği ve kullanıldığı sektörün iş ve işlemlerini düzenleyen ve e-belge özelliklerini açıklayan prosedürleri de ayrıca göz önünde bulundurmak gerektiği anlaşılmaktadır. Sektöre göre daha özel kriterler aranabildiği gözden uzak tutulmamalıdır.

E-imzalı belgelerin delil değeri kritik edilirken üretildiği kurumdaki politika ve prosedürler, tahsis edilen finans ve insan kaynağı, oluşturulan risk planı ve risk yönetimi, değişim planı yönetimi, yedekleme planı, doğal afetlere karşı alınan önlemler, hazırlanan varlık envanteri, belgelerin güvenlik hassasiyetlerine göre sınıflandırılıp uygun güvenlik kontrollerinin tesis edilerek gerçekleştirilen sızma testleri, belgelerin Türkiye'de saklandığı, uluslararası güvenlik standartlarına uygunluk, oluşturulan erişim, kullanım, depolama, iletim, dağıtım, paylaşım ve imha kuralları ve log kayıtları incelenmelidir. Bu hususların e-imzalı belgeler için hangi hususları içereceğine ilişkin rehberlerin hazırlanmasına ihtiyaç duyulmaktadır.

Resmî yazışmalar söz konusu olduğunda ise e-imzalı belgelerin usulüne uygun düzenlenmesi ve üretildiği EBYS'nin EYP'ye sahip olması gerekir. Bununla birlikte, UETS ve KEP kayıtlarının bütünlük içerip içermediği incelenmelidir. Tacirlerin faaliyetleri sonucunda oluşan e-imzalı belgeler söz konusu olduğunda ise bunların prosedürlerin uygun gördüğü düzen içerisinde ve zamanında üretilip üretilmediğinin, bir dosya planı neticesinde sınıflandırılarak dosyalama pratiklerinin incelenmesi gerekli görülmektedir. Kurumlarda oluşan e-imzalı belgeler bir işlemin sonucunda meydana geldiğinden dosyalama pratiklerinin tüm belgeler için incelenmesi gereken bir husus olduğu düşünülmektedir.

E-belgenin kullanıldığı sektör örneğinde olduğu gibi belge türüne göre de izlenecek adımlar değişebilmektedir. Mesela, e-fatura ve e-defter için 509 nolu Genel Tebliğ'de bulunan hususların incelenmesi gerekir. Bu hususlara, kullanılan uygulama dili, belgelerin Türkiye'de saklanması ve benimsenen taksonomi ile atılan e-imza türü örnek verilebilir.

5. Sonuç

EBYS'lerde kayıt altına alınan e-imzalı belgelerin delil değeri sorgulanırken e-imza oluşturma ve doğrulama araçları üzerinden hareket edilmektedir. E-imza sertifikalarının doğrulanamaması gibi bir ihtimal karşısında e-imzalı belgelerin delil olarak kullanılamaması riski ortaya çıkmaktadır. Bunu engellemek için bu belgelerin mevzuatta belirlenen diğer delil özelliklerine uyumlu üretilip üretilmediğini değerlendirme imkânı sunacak bir kontrol listesinden yararlanılabilir.

TTK'nın 82. maddesinde tacirlerin, ticari faaliyetler sonucu oluşan belgeleri sınıflandırarak saklaması gerektiği belirtilmiş; e-belgelerin her an erişilebilir olması istenmiştir. Aynı şekilde, VUK da bir hakkın ispatında delil olarak kullanılabilecek belgelerin işlerinin icabına göre dosyasında muhafaza edilmesini gerekli kılmaktadır. Dosyalamaya ilişkin ifadelerin görüldüğü bir diğer mevzuat Türk Muhasebe Standartlarıdır. Buna göre bilgi anlaşılabilir olmalı; bunun için sınıflandırılmalı, tanımlanmalı ve sunulmalıdır. Usulüne uygun dosyalamanın e-imzalı belgelerin delil değerini güçlendirdiği bilinmektedir. Fakat, çeşitli çalışmalardan kurumlarda dosyalamaya yeteri kadar ehemmiyet verilmediği öğrenilmektedir.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik'te bilgi sistemlerinin yönetimine ilişkin politika ve prosedürlerin hazırlanması ile risk yönetiminden bahsedilmektedir. Risk yönetiminde dikkate alınabilecek unsurlar belirtilmektedir. Bu unsurlar, teknolojik gelişmeler, hizmet alımı, işlem kayıtları, güvenilirlik ve bilgi güvenliği önlemleri şeklinde ifade edilebilir. Bilgi güvenliğinin sağlanmasında, belgelerin gizlilik, bütünlük ve ulaşılabilirliklerine dikkat edilmesiyle güvenlik hassasiyetlerine göre sınıflandırılıp uygun düzeyde güvenlik kontrollerinin tesis edilmesi ve sızma testlerinin gerçekleştirilmesi gibi ciddi yaklaşımlar önerilmektedir. Belge yönetimi sürecini şekillendiren Devlet Arşivleri Başkanlığının, söz konusu yaklaşımların uygulanıp uygulanmadığını denetlemesi e-imzalı belgelerin delil değerini güçlendirebilir.

E-imzalı belgelerin delil değerine ilişkin hükümlerin görüldüğü bir diğer mevzuat Elektronik Haberleşme Kanunu'dur. "Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği" bu konuda önemli hükümler içermektedir. İşletmecilerin kurmakla mükellef kılındığı bilgi güvenliği yönetim sistemine ilişkin çeşitli kriterler geliştirilmiş, bilgi güvenliği yönetim sistemi politikası hazırlanmasına vurgu yapılmıştır. Bu politikada, risk değerlendirmesi yapılarak varlıkların sınıflandırılması, erişim, dağıtım ve kullanımla ilgili kuralların belirlenmesi gerekmektedir. Burada, risk değerlendirmesiyle varlıklar sınıflandırılmaktadır. EBYS'lerde kayıt altına alınan e-imzalı belgeler için de bir varlık envanterinin oluşturulması delil değerini güçlendirebilecek bir unsur olarak kabul edilmektedir. Fakat mevzuatta belirtilen kriterlerin geliştirilmesi gerekli görülmektedir. Bu konuda Devlet Arşivlerinin çalışmalar başlatmasına ihtiyaç duyulduğu düşünülmektedir.

Bununla birlikte, elektronik ortamda saklanan bilgilerin yetkisiz olarak erişilmesi, değiştirilmesi, silinmesi ve zarar görmesine karşı gerekli önlemler alınmalıdır. Bunun için hangi yetkilinin nelere erişip erişemeyeceği belirlenir. İmha edilmesi gereken bilgiler, geri döndürülemez şekilde silinmelidir. Bu konuda Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından Bilgi ve İletişim Güvenliği Rehberi oluşturulsa da elektronik belgelerin imhasıyla ilgili bir yaklaşıma ihtiyaç duyulmaktadır.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği'nde değişim yönetimi felsefesinin benimsendiği görülmektedir. Burada öncelikle değişiklikler tanımlanarak kayıt altına alınır, planlanır ve test edilir. Sonrasında değişikliklerin etkileri analiz edilir ve önerilen değişiklikler onaylanır. Öngörülemeyen sonuçlarla karşılaşılması durumunda yapılacak işlemler belirlenir. Bununla birlikte, yedeklemeye ilişkin hükümler görülmektedir. Bunun için ihtiyaçlar ve sistemlerin kritiklik seviyesine uygun olarak yedekleme periyodu, yedekleme türü ve saklama zamanı belirlenir. Yedekleme aşamasında, yedek kopyaların kaydı tutulur; yedekler birbirinden farklı yerlerde saklanır ve periyodik olarak test edilir. Söz konusu adımların e-imzalı belgeler için de benimsenebileceği düşünülmektedir. Böylece, delil değerinin değerlendirilmesinde bir karine ortaya konulabilir.

Bununla birlikte, bahsi geçen Yönetmelik'te tutulacak log kayıtlarıyla ilişkili hükümler de bulunmaktadır. Buna göre, kullanıcı kimlikleri, oturum açma ve kapatma, veri ekleme/silme/değiştirme gibi işlemlerin tarihi, zamanı ve açıklamaları, erişimin sağlandığı teçhizatın kimliği, sistem, veri ve diğer kaynaklara başarılı ya da reddedilmiş erişim girişimleri, sistem ayarlarındaki değişiklikler, kullanılan özel izinler ve ayrıcalıklar, kullanılan sistem araçları ve uygulamaları, erişilen dosyalar ve erişim tipi,

ağ adresleri, güvenlik sistemlerinin aktif ve pasif hale getirilmeleri, güvenlik ayarları ve kontrollerine ilişkin değişiklikler veya değişiklik girişimleri, sistem yöneticileri tarafından yapılan işlemler ve rapor edilen sistem hatalarını içeren log kayıtlarının en az 2 yıl süre ile saklanması gerekmektedir. Buradaki hususların, elektronik belge yönetim sistemlerinde de tutulan log kayıtlarında bulunması gereken özellikler için bir yol gösterici olabileceği düşünülmektedir. Türkiye'deki EBYS'lerde tutulacak log kayıtlarına ilişkin bir rehberin hazırlanmasına ihtiyaç duyulmaktadır. Bu rehberin belgelerin delil değerinin korunmasına ciddi katkı sunacağı kabul edilmektedir.

EBYS'lerde kayıt altına alınan e-imzalı belgeler mevzuattaki delil özelliklerine uygun olarak hazırlansa da zaman içerisinde özgünlüklerini kaybedebilme, içeriğe ulaşamama gibi tehditlerle karşı karşıya kalmaktadır. Böyle bir ihtimalin gerçekleşmesi durumunda, HMK 203. maddesi gereği tanık dinlenecek ya da 210. madde gereği bilirkişiye danışmak söz konusu olacaktır. EBYS'lerde kayıt altınan alınan e-imzalı belgelerin delil değerinin zaman içerisinde korunduğu ortaya konulamazsa hangi yöntemler uygulanacaktır sorusunun araştırılmasına ihtiyaç duyulduğu düşünülmektedir. Bu çalışma, söz konusu araştırmaların artmasına küçük de olsa bir katkı sunarsa amacına ulaşmış olur.

Kaynakça

Acar, A. E. (2012). *Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği.* İstanbul: On İki Levha Yayıncılık.

Bankacılık Kanunu. Kanun No: 5411, Resmî Gazete [*R.G]*., S 25983 Mükerrer, tar. 01.11.2005. Erişim Adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf.

Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik.*R.G.,* S 31069, tar. 15.03.2020. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm.

Bankaların Muhasebe Uygulamalarına ve Belgelerin Saklanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik. *R.G.*, S 26333, tar. 01.11.2006. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2006/11/20061101.htm.

Ber, A. S. (2018). *Elektronik Konişmento.* Ankara: Seçkin Yayınları.

Berkin, N. (1946). İspat Hukukunda Senet Delili ve Yazılı Şekil. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 12(4), 1175-1192.

Bilgi Alışverişi, Takas ve Mahsuplaşma Kuruluşlarında Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler ile İş Süreçleri ve Bilgi Sistemlerinin Denetimine İlişkin Tebliğ. *R.G.*, S 28841, tar. 04.12.2013. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2013/12/20131204.htm.

Bilgi Edinme Hakkı Kanunu. Kanun No: 4982, *R.G.*, S 25269, tar. 24.10.2003. Erişim Adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.4982.pdf.

Bilgi Teknolojileri Kurumu [BTK]. (2012).*Elektronik İmza Kullanım Profilleri Rehberi*. Erişim Adresi: https://www.btk.gov.tr/uploads/pages/elektronik-imza-kullanim-profilleri-rehberi-5a33ff5b59f93.pdf.

Boudrez, P. (2007). Digital Signatures and Electronic Records.*Archival Science*, 7(2), 180-191.

Bölge Adliye ve Adlî Yargı İlk Derece Mahkemeleri ile Cumhuriyet Başsavcılıkları İdarî ve Yazı İşleri Hizmetlerinin Yürütülmesine Dair Yönetmelik.*R.G.*, S 29437, tar. 06.08.2015. Erişim Adresi: //www.resmigazete.gov.tr/eskiler/2015/08/20150806-3.htm.

Bralic, V., Kules, M. ve Stancic, H. Vladamir Bralic (2017). A Model for Long-term Preservation of Digital Signature Validity: TrustChain. *InFuture 2017*, Zagreb, 8-10 Kasım 2017, Yayına Hazırlayanlar: Iana Atassova, Wajdi Zaghouani, Bruno Kragic, Kuldar Aas, Hrvoje Stancic ve Sanja Seljan, 89-103.

BTK. Kayıtlı Elektronik Posta Hizmet Sağlayıcılarının Birlikte Çalışabilirliğine İlişkin Usul ve Esaslar. Erişim Adresi:https://www.btk.gov.tr/uploads/pages/kephsbirliktecalisabilirlikusulesas-5a3406e891d77.pdf.

Cansel, E. ve Özel, Ç (2017). *Borçlar Hukuku Genel Hükümler Cilt: 1.* 2.bs. Ankara: Seçkin Yayıncılık.

Centel, N. (2012). *Ceza Muhakemesi Hukuku*, 9. bs.İstanbul: Beta Basım Yayınları.

Ceza Muhakemesi Kanunu. Kanun No: 5271, *R.G.*, S 25673, tar. 17.12.2004. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2004/12/20041217.htm#1.

Çetin, S. ve Ateş, D. (2019). *Avukatlık ve Noterlik Hukuku*, 2. baskı. Ankara: Seçkin Yayıncılık.

Çiçek, N. (2009). *Modern Belgelerin Diplomatiği*. İstanbul: Derlem Yayınları.

Çiçek, N. (2016). Elektronik Belge Yönetimi Uygulamalarında Dosya Bütünlüğü Problemi.*Kurumsal Belleklerin Geleceği: Dijitalleştirme-Elektronik Arşiv-Elektronik Belge Yönetimi*. E-Beyas 2015 Sempozyumu, 21-22 Ekim 2015, Yayına Hazırlayanlar: Fahrettin Özdemirci, Nevzat Özel, Tolga Çakmak, Zeynep Akdoğan, Bahattin Yalçınkaya. Ankara: Ankara Üniversitesi, 163-172.

Çiçek, N. (2016a). Elektronik Belge Yönetimi Uygulamalarında Bir Alt Sistem Olarak Dosya Yönetimi.*Türk Kütüphaneciliği*, 30(3), 434-448.

Çiçek, N. ve Sağlık, Ö. (2017). E-Belgelerin Arşivsel Bağının Elektronik Delil Elde Etme Yöntemlerine Etkisi: Belge Yönetimi Literatürü Bağlamında Bir İnceleme.*Bilgi Sistemleri ve Bilişim Yönetimi: Beklentiler ve Yeni Yaklaşımlar*, Yayına Hazırlayanlar: Fahrettin Özdemirci, Zeynep Akdoğan, Ankara: Ankara Üniversitesi, 257-276.

Çiçek, N. ve Sağlık, Ö. (2019). Blokzincir Teknolojisinin Elektronik Belgelerin Güvenilirliğinin Korunmasında Başarıya Katkısı. Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ, Yayına Hazırlayanlar: Bahattin Yalçınkaya, M. Altay Ünal, Burcu Yılmaz, Fahrettin Özdemirci, Ankara: Ankara Üniversitesi, 141-170.

Damga Vergisi Kanunu. Kanun No: 488, *R.G.*, S 11751, tar. 11.07.1964 (Çevrimiçi) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.488.pdf.

Danıştay. (2018). *12. Daire Tarih:13.12.2018, Esas:2018/3591 sayılı karar.*

Danıştay. (2019).*2. Daire Tarih:14.11.2019, Esas:2019/3223 sayılı karar.*

Doğan, M., Şahan G. ve Atamulu, İ. (2019). *Borçlar Hukuku Genel Hükümler Ders Kitabı*. Ankara: Seçkin Yayıncılık.

Elektronik Haberleşme Kanunu. Kanun No: 5809, *R.G.*, S 27050 Mükerrer, tar. 10.11.2008. Erişim Adresi:https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5809.pdf.

Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği.*R.G.*, S 29059, tar. 13.07.2014. Erişim Adresi:https://www.resmigazete.gov.tr/eskiler/2014/07/20140713-4.htm.

Elektronik İmza Kanunu. Kanun No: 5070, *R.G.*, S 25355, tar. 23.01.2004. Erişim Adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf.

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğde Değişiklik Yapılmasına Dair Tebliğ.*R. G.*, S 31078, tar. 24.03.2020.

Elektronik Tebligat Yönetmeliği.*R.G.*, 30617, tar. 06.12.2018. Erişim Adresi:http://www.resmigazete.gov.tr/eskiler/2018/12/20181206-2.htm.

Emeklilik Fayda Planlarında Muhasebeleştirme ve Raporlama. *R.G.*, S 26095, tar. 01.03.2006. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2006/03/20060301-20.htm.

Erturgut, M. (2004). *Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi* (Yayınlanmamış Doktora Tezi). İzmir: Dokuz Eylül Üniversitesi.

Finansal Raporlamaya İlişkin Kavramsal Çerçeve. *R.G.*, S 30578, tar. 27.10.2018. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2018/10/20181027-16.pdf.

Finansal Tabloların Sunuluşu. *R.G.*, S 30430, tar. 24.05.2018. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2018/05/20180524-14.pdf.

Gelir İdaresi Başkanlığı [GİB]. (2013). *E-Fatura Portalı Kullanım Kılavuzu*. Erişim Adresi: http:/ebelge.gib.gov.tr/dosyalar/kilavuzlar/e-FaturaPortaliKullanimKilavuzu-v1.5.pdf.

GİB. (2016). *E-Defter Uygulaması Yazılım Uyumluluk Onayı Versiyon 1.6*. Ankara. Erişim Adresi: http://edefter.gov.tr/dosyalar/kilavuzlar/e-DefterYazilimUyumlulukOnayKilavuz.pdf.

GİB. (2016a). *Elektronik Yolcu Listesi Raporu*. Ankaraa. Erişim Adresi: https://ebelge.gib.gov.tr/dosyalar/ebilet/e-Yolcu_Listesi_Raporu_Teknik_Kilavuzu.pdf.

GİB. (2016b). *Havayolu Elektronik Bilet Raporu.* Ankara. Erişim Adresi: https://ebelge.gib.gov.tr/dosyalar/ebilet/e-Bilet_Raporu_Havayollari_Teknik_Kilavuzu.pdf.

GİB. (2017). *Etkinlik E-Bileti Rapor Kılavuzu*. Ankara. Erişim Adresi: http://www.efatura.gov.tr/dosyalar/ebilet/Etkinlik_e-Bilet_Raporu_Kilavuzu.pdf.

GİB. (2018). *Elektronik Arşiv Kılavuzu.* Ankara. Erişim Adresi: http://ebelge.gib.gov.tr/dosyalar/kilavuzlar/e-ArsivTeknikKilavuzu1.9.pdf.

GİB. (2018a). *Elektronik Arşiv Başvuru Kılavuzu*, Ankara. Erişim Adresi: http://ebelge.gib.gov.tr/dosyalar/kilavuzlar/e-ArsivBasvuruKilavuzu.v1.4.08.01.2018.pdf.

GİB. (2018b). *E-Fatura Uygulaması Entegrasyon Kılavuzu*. Ankara. Erişim Adresi: http://ebelge.gib.gov.tr/dosyalar/kilavuzlar/e-FaturaUygulamasiEntegrasyonKilavuzu-v1.10.pdf.

GİB. (2018c). *E-Defter Uygulama Kılavuzu V. 1.6*, Ankara. Erişim Adresi: http://edefter.gov.tr/dosyalar/kilavuzlar/e-DefterUygulamaKilavuzu_(V_1.6)_03.01.2018.pdf.

Göksoy, R. (2019). C*eza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması.* Ankara: Seçkin Yayınevi.

Göksu, M. (2010). *Hukuk Yargılamasında Elektronik Delil* (Yayınlanmamış Doktora Tezi). Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

Gümüşkaya, G. (2015). *Vergi Hukukunda İspat*(Yayınlanmamış Doktora Tezi). İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Güler, C. (2020). Elektronik Belgelerin İmhası: Teori ve Uygulama. İstanbul: Hiperyayın.

Günay, B. (2019). *Sigorta Hukuku*. Ankara: Seçkin Yayıncılık.

Gündoğdu, A. (2019).*Bankacılık Hukuku*, 6. baskı, Ankara: Seçkin Yayıncılık.

Hukuk Muhakemeleri Kanunu [HMK]. Kanun No: 6100, *R.G.*, S 28736, tar. 04.02.2011. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2011/02/20110204-2.htm.

International Research on Permanent Authentic Records in Electronic Systems [INTERPARES]. (2002). *The Long-term Preservation of Authentic Electronic Records: Findings of the INTERPARES Project*.

INTERPARES. (2008). *INTERPARES 2: Experiential, Interactive and Dynamic Records*.Yayına Hazırlayanlar: Luciana Duranti ve Randy Preston. Padova: Associazione Nazionale Archivistica Italiana.

Kamu Sertifikasyon Merkezi [KAMU SM]. (2015). *Elektronik Belgeleri Açık Anahtar Altyapısı Kullanarak Güvenli İşleme Rehberi*, Sürüm 1.4. Erişim Adresi: http://kamusm.bilgem.tubitak.gov.tr/dosyalar/rehberler/REHB-001.001_1.4.pdf.

Kayar, İ. (2018). *6102 Sayılı Türk Ticaret Kanunu'na göre Ticaret Hukuku*, 5. baskı. Ankara: Seçkin Yayıncılık.

Kayıtlı Elektronik Posta Sistemi ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ. *R.G.*, S 28036, tar. 25.08.2011. Erişim Adresi:http://www.resmigazete.gov.tr/eskiler/2011/08/20110825-21.htm.

Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik.*R.G.*, S 28036, tar. 25.08.2011. Erişim Adresi:http://www.resmigazete.gov.tr/eskiler/2011/08/20110825-7.htm, 10 Mart 2019.

Kavak, Y. (2015). *Borçlar Hukukunda Yazılı Şekil* (Yayınlanmamış Doktora Tezi). İstanbul: İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Külcü, Ö. ve Turan, M. (2013). Kamu Hukukunda Geleneksel ve Elektronik İletişim, Bilgi ve Belge Yönetimi Uygulamaları. *Türk Kütüphaneciliği*, 27(2), 266-300.

Leroux, O. (2004). Legal Admissibility of Electronic Evidence. *International Review of Law, Computers&Technology*, 18(2),193-220.

Muhasebe Politikaları, Muhasebe Tahminlerinde Değişiklikler ve Hatalar. *R.G.*, S 30450, tar. 13.06.2018. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2018/06/20180613-14.pdf.

Noterlik Daireleri Arşiv Hizmetleri Hakkında Yönetmelik.*R.G.*, S 20639, tar. 18.09.1990. Erişim Adresi: http://www.resmigazete.gov.tr/arsiv/20639.pdf.

Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik.*R.G.*, S 29413, tar. 11.07.2015. Erişim Adresi:http://www.resmigazete.gov.tr/eskiler/2015/07/20150711-19.htm.

Noterlik Kanunu. *R.G*. S 14090, tar. 05.02.1972. Erişim Adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.1512.pdf.

Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik.*R.G.*, S 29043, tar. 27.06.2014. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2014/06/20140627.htm.

Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun.*R.G.*, S 28690, tar. 27.06.2013. Erişim Adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6493.pdf.

Ödeme ve Menkul Kıymet Mutabakat Sistemlerinde Kullanılan Bilgi Sistemleri Hakkında Tebliğ. *R.G.*, S 29588, tar. 09.01.2016. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2016/01/20160109.htm, 18 Şubat 2019.

Öner, E. (2019). *Vergi Hukuku*. 11. baskı. Ankara: Seçkin Yayıncılık.

Özbek, M. S. (2016). Elektronik Ortamda Düzenlenen Noter Senetleri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 22(3), 2213-2282.

Pekcanıtez, H., Atalay, O. ve Özekes, M. (2011). *Hukuk Muhakemeleri Kanunu Hükümlerine Göre Medeni Usul Hukuku*, 11. bs., Ankara: Yetkin Yayınları.

Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik.*R.G.*, S 31151, tar. 10.06.2020. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2020/06/20200610-8.pdf.

Sigortacılık Bağımsız Denetim İlkelerine İlişkin Yönetmelik.*R.G.*, S 26934, tar. 12.07.2008. Erişim Adresi:https://www.resmigazete.gov.tr/eskiler/2008/07/20080712-7.htm.

Sigortacılık Kanunu. Kanun No: 5684, *R.G.*, S 26552, tar. 14.06.2007. Erişim Adresi:https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5684.pdf.

Türkiye Büyük Millet Meclisi [TBMM]. (2003). Türk Ceza Kanunu Gerekçesi. Erişim Adresi: http://www2.tbmm.gov.tr/d22/1/1-0593.pdf.

TBMM. (2011). *HMK Gerekçesi*. Erişim Adresi: https://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss393.pdf.

Türk Borçlar Kanunu. Kanun No: 6098, R.G., S 27836, tar. 04.02.2011. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2011/02/20110204-1.htm.

Türk Ceza Kanunu. Kanun No: 5237, *R.G.*, S 25611, tar. 12.10.2004. Erişim Adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf.

Türk Ticaret Kanunu. Kanun No: 6102, *R.G.*, S 27846, tar. 14.02.2011. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2011/02/20110214.htm.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020).*e-Yazışma Projesi.* Erişim Adresi:https://cbddo.gov.tr/projeler/e-yazisma/.

Vergi Usul Kanunu [VUK]. Kanun No: 213, *R.G.*, S 10703-10705, tar. 10.01.1961-12.01.1961. Erişim Adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.4.213.pdf.

Yalçınkaya, B., Gedikli, M. E., Cibaroğlu, M. O. (2019). Elektronik Belge Yönetim Sisteminde Log Analizi: İstatistiksel Bir Değerlendirme. Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zekâ, Yayına Hazırlayanlar: Bahattin Yalçınkaya, M. Altay Ünal, Burcu Yılmaz, Fahrettin Özdemirci, Ankara: Ankara Üniversitesi, 61-77.

Yardım, E. (2013). Medeni Usul Hukuku Çerçevesinde Güvenli Elektronik İmzalı Belgelerin Delil Niteliği ve Unsurları. *Prof.Dr. Mustafa Dural'a Armağan*, Yayına hazırlayanlar: Tufan Öğüz. İstanbul: Seçkin Yayıncılık, 1290-1315.

Yargıtay. (1993). *Ceza Genel Kurulu Kararı, Esas No: 1993/108, Karar No: 1993/6-79.*

Yargıtay. (2013). *9. Ceza Dairesi Kararı, Esas No: 2013/9110, Karar No: 2013/12351.*

Yargıtay. (2017). *Yargıtay Ceza Genel Kurulu Kararı, Esas No: 2016/1065, Karar No: 2017/27.*

Yargıtay. (2020). *11. Ceza Dairesi Kararı, Esas No: 2020/166, Karar No: 2020/3034.*

Yargıtay. (2020a). *8. Ceza Dairesi Kararı, Esas No: 2019/22599, Karar No: 2020/11575.*

Yavaş, M. (2009). *Senetle İspat ve Senede Karşı İspat Kuralları ile Bu Kuralların İstisnaları*. Ankara: Seçkin Yayıncılık.

Yıldırım, A. ve Şimşek, H. (2016).*Nitel Araştırma Yöntemleri: Sosyal Bilimlerde*.Ankara: Seçkin Yayıncılık.

Yılmaz, M. (2016). Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta ve İdari Yargılama Hukukunda Delil Niteliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 22(3), 3413-3464.

Zafer, H. ve Centel, N. (2012). *Ceza Muhakemesi Hukuku*. 9. bs., İstanbul: Beta Basım Yayım.

446 Sıra No'lu VUK Genel Tebliği, *R.G.*, S 29316, tar. 04.04.2015. Erişim Adresi: http://www.resmigazete.gov.tr/eskiler/2015/04/20150404.htm.

509 Sıra No'lu VUKGenel Tebliği, *R.G.*, S 30923, tar. 19.10.2019. Erişim Adresi: https://www.resmigazete.gov.tr/eskiler/2019/10/20191019-5.pdf.