

BELGEDE SAHTECİLİK SUÇLARININ KONUSU OLARAK BELGE VE ELEKTRONİK BELGE*

Arif GÖZEL*

ÖZET

Ceza adaleti sisteminde gelişen teknolojiyle birlikte bilişim sistemlerindeki elektronik belgelerin korunması daha fazla önem arz etmeye başlamıştır. Şu ana kadar bilişim sistemindeki veriler bağlamında belgede sahtecilik suçundan hüküm kurulmuş bir yargı kararı bulunmamaktadır. Uygulamada fiziki belgeler dışındaki belgelerin belgede sahtecilik suçuna konu olamayacağına dair bir pratik oluşmuştur. Buna karşılık, makalede, ayrıca bir düzenleme yapılmasına gerek olmaksızın bazı şartları taşıyan elektronik verilerin (geleneksel) belgede sahtecilik suçuna konu olabileceği savunulmaktadır. Bu bağlamda makalede, bilişim sistemindeki veriler incelenecek hangi verilerin belgede sahtecilik suçuna konu oluşturacağı, hangilerinin ise bilişim sistemindeki verileri değiştirme, tahrif etme suçunu (m.244/2) oluşturacağı incelenecektir. Güvenli elektronik imza, e-belgeler için olmazsa olmaz bir öneme sahip olduğu

* Bu makale, Gazi Üniversitesi Sosyal Bilimler Enstitüsünde yazılmakta olan “Bilişim Sistemindeki Veriler Bağlamında Belgede Sahtecilik Suçu” isimli yüksek lisans tezinden üretilmiştir.

* Gazi Üniversitesi Ceza ve Ceza Muhakemesi Hukuku Bilim Dalı Yüksek Lisans Öğrencisi

İçin bu imza türünün özellikleri ve işlevleri incelenecek ve ıslak imza ile karşılaştırılacaktır. Yine Adalet Bakanlığı tarafından hazırlanan yasa tasarısı taslağı ve özel kanunlarda düzenlenen e-belge düzenlemeleri araştırma kapsamında irdelenecektir.

Anahtar Kelimeler: *belge, elektronik veri, elektronik belge, sahtecilik, elektronik imza,*

DOCUMENT AND E-DOCUMENT AS A SUBJECT OF FORGERY CRIME

ABSTRACT

The protection of electronic documents in information systems has come into prominence through technological advancements in criminal justice system. There has not been any verdict due to forgery of electronic data so far. The forgery of other documents aside from printed ones has not generally been considered as a subject of crime in practical terms. In the article, it is claimed that the electronic data that fulfil several conditions can be subjected to the crime of forgery of documents without the need of any additional legal arrangement. In this regard, the issue that which data in information system would be subjected to the crime of forgery of documents or criminal distortion (a.244/2) is going to be analyzed. Due to the fact that secure electronic signature has a crucial importance for e-documents, the

properties and functions this type of signature are going to be explained. In addition, the types of secure electronic signature and original signature will be compared. The draft law which is prepared by the Ministry of Justice in July 2015 and the arrangements on e-documents which are prepared in special laws are going to be examined in the article.

Key Words: *document, electronic data, electronic document, forgery, electronic signature*

1. BELGE

Her suçun bir konusu bulunmaktadır. Belgede sahtecilik suçunun konusu ise belgedir.

Belge kavramı 5237 sayılı Türk Ceza Kanunu'nun (TCK) gerekçesinde tanımlanırken kanun metni içerisinde bir tanım bulunmamaktadır¹. Bu boşluk kanun koyucunun bıraktığı bilinçli bir boşluktur. Zira, Kanunun Adalet Alt Komisyonunda görüşülmesi

¹ Türk Ceza Kanunu'nda belge kavramının tanımlanmamasına karşılık İsviçre Ceza Kanunu'nda belge kavramı tanımlanmıştır. İCK'nın 110/5.maddesinde “belge, hukuksal açıdan önemli olan unsurları ispat etmek için belirlenmiş olan işaret veya bunun için belirlenmiş ve buna elverişli olan yazılardır. Aynı amaca hizmet eden bilgisayar veya bant kayıtları yazılı biçime eşit tutulur.” denilerek belge kavramı tanımlanmıştır. Tezcan, D., Erdem, M. R., Önok, R. M. (2013). *Teorik ve Pratik Ceza Özel Hukuku* (10.Baskı). Ankara: Seçkin Yayınevi, s. 732. 14 nolu dipnot. Alman Ceza Hukuku'nda ise belge “fikri bir muhtevası olup düzenleyicisi anlaşılabilen ve hukuki ilişkiler açısından delil olma özelliği taşıyan irade açıklamaları” olarak tanımlanmıştır. Gökçen, A. (2013). *Belgede Sahtecilik Suçları*. (Üçüncü Baskı). Ankara: Adalet Yayınevi. s. 72.

sırasında bu sorun gündeme gelmiş ancak yapılacak herhangi bir tanımın gelecekte uygulamaya dar gelebileceği düşüncesiyle belge kavramının tanımlanmasından vazgeçilmiştir².

Belge kavramı TDK sözlüğünde ise “bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika, doküman” olarak tanımlanmıştır³. Mülga 765 sayılı Türk Ceza Kanunu’nda “varaka” ve “evrak” tabirleri kullanılmışken, 5237 sayılı Türk Ceza Kanunu’nda ise belge kavramı tercih edilmiştir. Varak, sözlükte yazılı kâğıt olarak tanımlanırken, belge varak terimini de içine alan daha kapsamlı bir kavramdır. Bu terim değişikliğini kanun koyucunun kavramı Türkçeleştirmek için yaptığı anlaşılmaktadır. Ancak lafzi yorum yöntemiyle kanun yorumlanacak olursa kanunun kapsamı değişebilecek⁴ ve genişleyebilecektir. Gerçekten de birçok kanunda belge kavramı tanımlanırken içine yazılı kağıttan başka, film, fotoğraf, teyp ve video kaseti, elektronik ortamda kaydedilen her türlü bilgi,

² Türk Ceza Kanunu’nun TBMM Adalet Komisyonu’nda görüşülmesi sırasında belge kavramının tanımlanması tartışması yapılmıştır. Yargıtay ilgili ceza dairesi üyesi Keskin Kaylan, belgenin tanımlanmasının uygulamaya bir süre sonra dar gelebileceğini vurgulamış ve bu tanımlı uygulamanın yapmasının uygulamayı rahatlatacağını ve doğruya varmada kolaylık sağlayacağını belirtmiştir. (Yılmaz, Z. (2004). *Gereğe ve Tutanaklarla Yeni Türk Ceza Kanunu*. Ankara, Seçkin Yayıncılık. s.1012.) Gerçekten de bu yorum çok önemli ve değerlidir. Nitekim hâlihazırda kanunkoyucu da birçok maddede güvenli elektronik imza ile imzalanan bilişim sistemindeki verilerin belge hükmünde olduğunu kabul ederek belgenin kapsamını genişletme eğilimindedir.

³ http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54e896ab97eb94.07769200, Erişim Tarihi: 21.02.2015

⁴ Doğan, K. (2010). Ceza Hukukunda Belge Kavramı. *Ceza Hukuku Dergisi*. Aralık, 2010. Sayı: 14. s. 52.

haber ve veri taşıyıcıları kavramlarını da kapsadığı belirtilmiştir. O halde denilebilir ki ceza kanununda yapılan kavram değişikliği (varaka yerine belge kavramının tercih edilmesi) belgede sahtecilik suçlarının kapsamını genişletebilecektir. Burada önemli olan husus hangi “şey”lerin kanunların muteber olarak kabul ettiği “belge” olacağının belirlenmesidir.

TCK'nın 197 ila 212. maddelerinde düzenlenen kamu güvenine karşı suçların bütünüünün konularının fiziki evrak olarak ifade edilen belgelerden oluştuğu görülmektedir⁵. Fiziki evrak olarak nitelendirilen bu belgeler; para veya paraya eşit değerler, kıymetli damgalar, mühürler, resmi belgeler, resmi belge hükmündeki belgeler ve özel belgelerdir.

Türk Ceza Kanunu'nun 204. maddesinin gerekçesinde belge kavramının eski dildeki “evrak” kelimesi karşılığında kullanıldığı belirtilmiştir. Gerekçede, belgenin yazılı kâğıt anlamına geldiği, yazılı kâğıt niteliğinde olmayan “şeylerin” ispat kuvveti ne olursa olsun belge niteliği taşımadığı vurgulanmaktadır⁶.

Belge kavramı, Hukuk Muhakemeleri Kanunu'nun (HMK) 199.maddesinde “*uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya*

⁵ Arslan, Ç. Baştürk, İ. (2013). Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler, *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*. Cilt: 8 Sayı:2 2013/12. s.200.

⁶ Özgenç, İ. (2006). *Türk Ceza Kanunu Gazi Şerhi. (Genel Hükümler)*. Ankara: T.C. Adalet Bakanlığı Eğitim Dairesi Başkanlığı. s. 938.

ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları” olarak tanımlanmıştır⁷.

Bilgi Edinme Kanunu’nun 3. maddesinde ise belgenin “*kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film, fotoğraf, teyp ve video kaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını*” kapsadığı belirtilmiştir⁸.

Yargıtay Ceza Genel Kurulu ise belgeyi “*hukuki sonuç doğurmaya veyahut bir durumu belli veya ispat etmeye yarayan yazılara denir*” şeklinde tanımlanmaktadır⁹.

2. BELGE TÜRLERİ

TCK’da belge; resmi belge, özel belge ve resmi belge yerine geçen belge olmak üzere üç gruba ayrılmıştır. TCK madde 210’da emre veya hamile yazılı kambiyo senetleri, emtiayı temsil eden belgeler, hisse senetleri, tahviller ve vasiyetnameler resmi belge hükmünde belgeler olarak belirlenmiştir.

⁷ 6100 Sayılı Kanun. Yayımlandığı Resmi Gazete: Tarih: 4/2/2011, S: 27836.

⁸ 4982 Sayılı Kanun. Yayımlandığı Resmi Gazete: Tarih: 24/10/2003, S: 25269.

⁹ YCGK, 21.6.1968, 97/324; YCGK 4.4.1983, 6-13/155, www.kazanci.com.

3. BELGENİN UNSURLARI

Madde gerekçesinde belirtildiği ve doktrinin baskın şekilde kabul ettiği şekliyle belgenin 3 temel unsuru vardır. Bunlar; belgenin yazılı olması, belgenin hukuki değer taşıyan bir içeriğinin olması ve düzenleyicisinin belli olması unsurlarıdır¹⁰.

3.1. Yazılı Olma

Bir belgeden bahsedebilmek için öncelikle yazılılık koşulunun gerçekleşmesi gerekmektedir¹¹. Yazı, bir irade beyanının veya bir olayın naklinin, bunu tespit etmeye yarayan elverişli araç ve harflerle ifade olunmasıdır¹². Yazıda kullanılan dilin veya araçların bir önemi bulunmamaktadır. Ancak yazının okunabilir olması gerekmektedir. Okunamayan bir yazılı evrak belge olarak kabul edilemez¹³.

Yazılı olma şartının gerçekleşebilmesi için bir takım şartların oluşması gerekmektedir. Bunlar; bir dilin kullanılması, yazının elverişli bir cisme kaydedilmesi¹⁴ ve yazının okunabilir olmasıdır.

¹⁰ Artuk, M. E., Gökçen, A., Yenidünya, A. C. (2008). Ceza Hukuku Özel Hükümler. Ankara: Turhan Kitabevi.s. 543.

¹¹ Artuk, Gökçen, Yenidünya, 2008, s. 543.

¹² Artuk, M. E. Gökçen, A. Yenidünya, A. C. (2009). *Türk Ceza Kanunu Şerhi*. (5.Cilt). Ankara: Turhan Kitabevi.s. 543. Doğan, 2010, s.55.

¹³ Gökcan, H. T. (2010). Özel Belgede Sahtecilik Suçu. *Ankara Barosu Dergisi*. Yıl: 68. Sayı: 2010/1. s. 211.

¹⁴ Yazının sadece kağıt üzerine kaydedilmesinin belgenin varlığı için zorunlu olmadığına, herhangi bir taşınır cismin örneğinin araç plakalarında yapılan sahteciliğin de belgede sahtecilik suçunu oluşturduğuna dair Yargıtay kararı: 11. C.D. 22.2.2007, 8681-1073, nakleden Gökcan, 2010, s.212, 17 nolu dipnot.

Yazının içeriğinin herkes veya birtakım kişiler tarafından anlaşılması gerekmektedir¹⁵. Yazıyı sadece yazan kişinin anlaması durumunda evrak belge niteliği kazanamayacaktır.

Doktrinde bir görüş, belgenin taşınabilir bir cisme kaydedilmesinin zorunluluğu fikrinden hareketle fotoğraf, video kaydı, bilişim sistemindeki program ve veriler gibi belgelerin ceza hukuku bakımından delil olarak kabul edilseler de, konumuz olan belgede sahtecilik suçları bakımından yazılı olma şartının aranması dolayısıyla bunlar üzerinde yapılan sahteciliğin belgede sahtecilik suçunu oluşturmayacağını belirtmektedir¹⁶.

Doktrin ve uygulamada üzerinde yazı olmayan ancak delil değeri olan objelerin belge olarak kabul edilemeyeceği belirtilmektedir¹⁷. Bu sava kan lekesi veya bir fotoğraf örnek olarak gösterilmektedir. Ancak özelliği itibariyle hem yazı hem de resim içeren bazı belgelerde resim unsurunda tahrifat yapılması da belgede sahtecilik suçunun oluşumuna sebebiyet verecektir. Buna örnek olarak ise bir pasaportun fotoğraf kısmının değiştirilmesi gösterilebilir¹⁸.

¹⁵ Artuk, Gökçen, Yenidünya, 2008, s. 545.

¹⁶ Üstüner, A. (2013). Resmi Belgede Sahtecilik Suçu (Yüksek Lisans Tezi, Dicle Üniversitesi, 2013). Diyarbakır. s. 12. Gökcan, 2010, s. 213, (Yazarlar, bilgisayar sistemine kayıtlı verilerde yapılan tahrifatın TCK'nın 244/2. maddesindeki suç oluşturacağını belirtmektedir.)

¹⁷ Doğan, 2010, s.54.

¹⁸ Doğan, 2010, s. 54.

Belgenin yansıttığı içeriğin delil gücüne sahip olmasından ötürü aslı gibi olmayan suretler belge sayılmayacaktır. Bu yüzden fotokopi, faks ve e-mail çıktıkları belge niteliğini haiz değildir¹⁹.

3.2. Hukuki Değer Taşıyan Bir İçeriğe Sahip Olma

Doktrinde baskın görüş, bir belgeden söz edilebilmesi için nakledilen olayın veya irade açıklamasının hukuken önem taşımamasının veya hukuki sonuçlar üretmeye elverişli olmasının gerekli olduğunu savunmaktadır. Gerçekten, belgenin içeriği tahrif edilmesi halinde cezalandırılabilen bir sahteliği oluşturmayacak nitelikte ise, fiil cezai sorumluluk doğurmayacaktır²⁰. Nitekim, Yargıtay Ceza Genel Kurulu da özel belgede sahtecilik suçunun oluşabilmesi için, belgenin doğrudan hukuki sonuç doğurucu nitelikte olması gerektiğini kabul etmiştir²¹.

Belge hukuki bir iddiaya dayanak olmalı, bir davada davalıya karşı geçerli bir delil olarak kullanılabilirdir²².

Hukuken önemli olmayan belgeler üzerinde yapılan sahtecilik herhangi bir zarar tehlikesi dahi doğurmayacağından ötürü bu fiiller

¹⁹ Gökcan, 2010, s.223.

²⁰ Toroslu, N. (2010). *Ceza Hukuku Özel Kısım*. Ankara: Savaş Yayınevi. s. 223.

²¹ YCGK, 5.11.1990. 6-246/263. Kazancı İçtihat Programı.

²² Taşdemir, K. Özkepir, R. (2009). *5237 Sayılı TCK'da Açıklamalı- İçtihatlı Sahtekarlık Suçları*. Ankara: Turhan Kitabevi. s. 11.

Yargıtay tarafından “faydasız, gereksiz sahtecilik” olarak nitelendirilmektedirler²³.

3.3. Düzenleyicisinin Belli Olması

Belgenin hukuken geçerli bir belge olabilmesi için bir düzenleyicisi olmalı ve düzenleyicinin kimliği bilinmelidir. Kimin yazdığı belli olmayan bir evrak belge vasfını kazanamayacaktır. Belgeyi düzenleyen kişinin belli olması ya da belirlenebilir olması belgenin garanti fonksiyonunu ortaya koymaktadır²⁴.

Belgeyi düzenleyen her zaman onu maddeten yazan kişi değildir. Örnek vermek gerekirse belge bir stenograf veya sekreter tarafından yazılabilir. Fakat belge, belgenin adına düzenlendiği şahsa aittir²⁵. Belgenin düzenleyicisi onu imza eden kişi olarak kabul edilir²⁶.

²³ "...Düğün eşyası (mihir senedi) cihaz hibe senedi" başlıklı suçta konu belgede tanık olarak ismi bulunan müşteki adına atılmış olan imzanın sahte iddiasından ibaret olayda; geçerli olabilmesi için her hangi bir şekil şartı öngörülme suça konu belgenin tanık olmadan düzenlenmesi halinde de geçerli olacağı, sahte olduğu kabul olunan imzanın belgenin iki tanığından birisine ait olduğu, diğer tanık ile kefile ait imzaların sahte olduğuna dair bir iddia bulunmadığı gibi belgede borçlu olarak gösterilen T Y' imzasının bulunmadığı da gözetildiğinde, tanık olarak ismi gösterilen şahıs adına sahte imza atılmasının faydasız sahtecilik olması..." 11. CD. 04.06.2012, 2011/6748- 2012/10676 (UYAP Bilgi Sistemi).

²⁴ Doğan, 2010, s. 56.

²⁵ Soyaslan, D. (2002). *Ceza Hukuku Özel Hükümler* (4. Bası). Ankara: Yetkin Yayınları. s. 476.

²⁶ Gökcan, 2010, s. 216.

Yazının özelliği sebebiyle imzalanmasına gerek duyulmayan yazılar da belge olarak kabul edilebilecektir. Nitekim, tekel bandrolleri, tiyatro ve eşya piyangosu biletleri bu tip belgelere örnek oluşturmaktadır²⁷. Yazının geçerli bir belge olması için imzanın gerekli görüldüğü durumlarda imzasız yazı belge kabul edilemez ve belgede sahtecilik suçuna konu olmaz²⁸.

Maddenin gerekçesinde de açıklandığı üzere belgenin belirli bir kişi adına düzenlenmesi yeterli olup adına belge düzenlenen bu kişinin hayali bir kişi olması durumunda dahi bir belgenin varlığından söz edilebilir. Bir olayda Yargıtay kendisini alacaklı, hayali bir kişiyi de borçlu olarak gösterip sahte bono düzenleyen failin sahtecilik suçu işlediğini kabul etmiştir²⁹.

İmza, istisnai durumlarda başka bir araçla da atılabilir. 5070 sayılı Elektronik İmza Kanunu'ndaki³⁰ (EİK) düzenlemeler bu istisnaya dahildir. EİK, 3.maddesinde elektronik imzayı tanımlamaktadır. Buna göre elektronik imza *“başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri”* olarak

²⁷ Artuk, Gökçen, Yenidünya, 2009, s. 545.

²⁸ Yar. CGK. 9.3.1987. 601/16.Artuk, Gökçen, Yenidünya, 2009, s. 546. Dipnot.122.

²⁹ 11.CD. 25.02.2009, 2008/17340 – 2009/1385. 6.CD. 25.10.1984, 5674/7520. Gökcan, 2010, s. 217. 36 nolu dipnot.

³⁰ 5070 Sayılı Kanun, Yayımlandığı Resmi Gazete Tarihi: 23/1/2004. Sayı: 25355.

tanımlanmaktadır. Bu husus aşağıda ayrıntılı olarak inceleneceğinden detaylarına bu kısımda girilmeyecektir.

4. BİLİŞİM SİSTEMİNDEKİ VERİLER VE ELEKTRONİK BELGE İLİŞKİSİ

Belgede sahtecilik suçunun konusunu oluşturan belge unsuru incelendikten sonra konumuz bağlamında elektronik verilerin ve elektronik belgelerin incelenmesi önem arz etmektedir. Bu veri ve belgelerin hukuki nitelikleri hukukun teknolojinin gerisinde kalmaması için net bir şekilde ortaya konulmalı ve muteber oldukları ölçüde hukuki korumaya mazhar olmalıdırlar. Bilişim sistemlerinin günümüzde yaygınlığı da göz önüne alındığında bilişim sistemlerinin temel yapıtaşını oluşturan “veri”lerin TCK bağlamında belgeyi oluşturup oluşturmayacağı irdelenmelidir³¹.

Veri teriminin tanımına bakıldığında “bilişimde, olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel gösterimi”³² olarak tanımlandığı görülmektedir. Kısacası bilgisayar üzerinde işlem yapılması mümkün olan her türlü değer veri olarak nitelendirilebilir³³.

³¹ Arslan, Baştürk, 2013, s. 204.

³² <http://www.dildernegi.org.tr/TR,274/turkce-sozluk-ara-bul.html>, Erişim Tarihi: 30.7.2015

³³ Arslan, Baştürk, 2013, s. 204.

TCK'da “veri” kavramı tanımlanmamış iken, 243.maddenin gerekçesinde “*sistem içindeki bütün soyut unsurlar, fikrada geçen “veri” teriminin kapsamındadır*” denilerek verinin kapsamı somutlaştırılmaya çalışılmıştır. Kişisel verileri kaydetme ve kişisel verileri hukuk aykırı olarak ele geçirme suçlarının düzenlendiği TCK'nın 135 ve 136. maddelerinde ve gerekçelerinde veri kavramı tanımlanmamıştır. CMK'nın 38/A-I maddesinde³⁴ ve HMK'nın 199.maddesinde³⁵ de veri ibaresi geçmesine rağmen bir tanım getirilmediği görülmektedir.

Buna karşılık 5070 sayılı EİK'nın 3/a maddesinde “veri”ye bir tanım getirilmiştir. Maddede elektronik veri “*elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları*” ifade eder şeklinde tanımlanmıştır. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanununun 2/1-k maddesinde ise veri, “*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri*” ifade eder şeklinde tanımlanmıştır.

³⁴ Her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılır. Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır.

³⁵ Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir.

Avrupa Siber Suçlar Sözleşmesi'nin³⁶ 1/b maddesinde ise “bilgisayar verisi”, “*bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sistemindeki işlenmeye uygun nitelikteki her türlü bilgi ve kavramı ifade eder*” şeklinde hüküm altına alınmıştır.

Elektronik verilerin yukarıdaki tanımlardan da anlaşılacağı üzere ayırt edici özellikleri bilgisayar veya makine tarafından işlenmeleri ve depolanabilmeleridir. Elektronik veriler, geleneksel olarak kabul edilen belgelerden bu özellikleri sebebiyle farklılık göstermektedir³⁷. Bu veriler fiziki bir evrak değildir. Ancak günümüzde çok yaygın olarak kullanılan bu verilerin gelecekte daha da yaygınlaşacağı ve etkin bir şekilde korunmaları gerektiği aksi kabul edilemez bir gerçektir. Bu verilerin de aynen fiziki evrakta olduğu gibi belgede sahtecilik suçlarına konu olarak kabul edilmeleri ve korunmaları düşünülmelidir.

³⁶ Avrupa Suç Sorunları Komitesi (CPDC) uzmanları tarafından hazırlanan sözleşme taslağı ve ekindeki açıklayıcı rapordan (explanatoryreport) oluşan Avrupa Konseyi Siber Suç Sözleşmesi (Convention on Cybercrimes) 23 Kasım 2001 tarihinde Budapeşte’de imzaya açılmış, 1 Temmuz 2004’te yürürlüğe girmiştir. “Siber Suç Sözleşmesi Ek Protokol” (AdditionalConventiontotheConvention on Cybercrime) ise 1 Mart 2006’da yürürlüğe girmiştir. Sözleşmeyi Türkiye Cumhuriyeti 10 Kasım 2010 tarihinde Strazburg’ta imzalamış, TBMM tarafından onaylanan sözleşme 2 Mayıs 2014 tarihinde Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Sözleşmenin metni için bkz. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>, Sözleşmenin Türkçe çevirisi ve Meclis Komisyon raporu için bkz. <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf>

³⁷ Arslan, Baştürk, 2013, s.206.

Elektronik belge, elektronik verilerin bir araya gelerek hukuken anlamlı ve önemli bir bütün oluşturmasına denilmektedir³⁸. Kağıt belgeler, üzerlerindeki yazı ve işaretlerin taşıyıcısı iken, elektronik belgeler, elektronik verilerin taşıyıcısıdır. Elektronik belgelerin geleneksel anlamdaki belgelerden farkları doğrudan algılanabilir olmamalarıdır. Elektronik verilerin algılanabilmesi için bilgisayar vb. yardımcı araçlara ihtiyaç duyulmaktadır.

Elektronik verinin orijinali, veri taşıyıcısında elektronik imzalı olarak kayıtlı olanıdır. Bu verilerden kağıtlara alınan çıktılar ancak kopya olarak kabul edilir. Nitekim, bir belgenin orijinali tek olmak durumundadır. Elektronik imza, fonksiyonu gereği belge üzerinde yapılan değişiklikleri gösterdiğinden belgenin orijinalliği e-imza vasıtası ile tespit edilebilmektedir. Bu verilerin kontrolü ancak elektronik ortamda yapılabildiğinden dolayı yazılı kağıt olarak alınan çıktıları belge hüviyetinde değildir.

Elektronik belgenin ekranda temsili yahut çıktısının alınması sadece verilerin görülebilmesi için yardımcı araç niteliğindedir³⁹. Çıktılar bu anlamda belge ve delil olarak kabul edilemezler⁴⁰. Bu

³⁸ Erturgut, M. (2004). *Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi*. Ankara: Yetkin Yayınları. s. 30.

³⁹ Erturgut, 2004, s. 40.

⁴⁰ Bu çıktılar kağıt belgelerin fotokopileri olarak değerlendirilebilir.

nedenle elektronik imzalı belgelerin ibrazı elektronik ortamda yapılmalıdır⁴¹.

5. ELEKTRONİK BELGE

5.1. Tanım

Elektronik belge denildiğinde, en basit ifadeyle elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler kastedilmektedir⁴². Bu anlamda elektronik belgelerden bahsedildiğinde internet üzerinden yapılan hukuki işlemler, e-mail yoluyla gönderilen irade beyanları, çeşitli veri taşıyıcılarına kaydedilmiş ve irade açıklaması içeren elektronik veriler akla gelmektedir⁴³. Ancak ceza hukuku anlamında yukarıda belirtilen verilerden hangileri elektronik belgelerin “belge” statüsünde olacağı önem arz etmektedir.

Belge kavramının tanımının yapıldığı HMK'nın 199.maddesinde elektronik ortamdaki verilerin de belge sayılacağı hüküm altına alınmıştır. Bu tanıma ek olarak Bilgi Edinme Kanunu'nun tanımlar maddesindeki belge tanımı da gözden kaçırılmamalıdır. Bu maddede belgenin, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını da kapsadığı

⁴¹ Erturgut, 2004, s.48.

⁴² Erturgut, 2004, s. 29.

⁴³ Erturgut, M. (2003). Elektronik İmza Kanunu Bakımından E-Belge ve E-İmza, Bankacılar Dergisi. Sayı 48. s.66.

belirtilmiştir. O halde denilebilir ki, sayısal kayıt ortamında bulunan elektronik verilerin şartlar oluştuğu takdirde elektronik belge olarak kabul edileceği hukuk sistemimizde kabul görmüştür.

5.2. Elektronik Belgenin Önemi

Elektronik belgelerin kullanımı küreselleşen dünyada gittikçe daha fazla artmakta ve vazgeçilmez bir hal almaktadır. Kâğıda dayalı geleneksel iletişim modeli terk edilmekte ve modern dijital iletişim modeline doğru hızlı bir gelişim yaşanmaktadır⁴⁴. Sanal ortam, fiziksel ortam ihtiyacını ortadan kaldırmış ve maliyetleri düşürme imkânı sağlamıştır. Oluşturulan program ve ara birimler sayesinde kişilerin işlemlerini kendi kendilerine gerçekleştirmesi olanağı sağlanarak personel giderlerinde de ciddi bir azalma meydana getirmiştir. Sanal ortamın nimetlerinden öncelikle ürün pazarlayanlar, ardından finans sektörü hızla yararlanmaya başlamıştır. Hizmetlerini vatandaşlarına daha hızlı ve etkin bir şekilde iletmek isteyen devletler de bu rüzgârın etkisine girmişlerdir. Mal ve hizmet siparişleri, elektronik bankacılık ve özellikle elektronik devlet anlayışının hızlı

⁴⁴ <http://hakanalbayrak.blogspot.com.tr/2008/05/elektronik-belgelerin-delil-olarak.html>, Erişim Tarihi: 19.03.2015

bir evrim yaşaması hukuken önemli kabul edilen birçok işlemin elektronik yollarla vuku bulmasına sebep olmaktadır⁴⁵.

Söylenbilir ki belki de yakın bir gelecekte kâğıda dayalı belgeleme sistemi tamamen ortadan kaldırılacaktır. Nitekim Adalet Bakanlığı'nın amaçlarından birisi de kâğıtsız sisteme geçmektir. Ve bu planlar HMK madde 445'in gerekçesinde net bir şekilde ifade edilmektedir⁴⁶.

⁴⁵ Aslan, M. (2014). Vergilendirmede Elektronik Belgelerin Hukuki Geçerliliklerinin Değerlendirilmesi. Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi. Yıl:2. Cilt: 2. S:3

⁴⁶ Bkz: <http://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss393.pdf> “Adalet Bakanlığı e-Dönüşüm ve e-Devlet sürecinde gerekli tüm teknolojik gelişmeleri kullanarak ...e-adaleti kurmayı amaçlamaktadır. Bu çerçevede, kurumu kâğıtsız ofis ortamına taşımak, hızlı, etkin, güvenilir, adil, verimli, şeffaf ve etik değerlere uygun bir yargılama mekanizması oluşturmak, doğru ve tutarlı bilginin mevzuatın tanıdığı yetkiler çerçevesinde istenilen zamanda hızlı ve kolayca elde edilmesini ve paylaşımını, her türlü idarî faaliyetler ile denetim, teftiş ve soruşturmanın hızlı ve etkin bir şekilde yürütülebilmesini sağlamak amacıyla, üretkenliği ve verimliliği artırmak için geliştirilen; ölçeklenebilir, çoklu-kullanıcılı ve iş odaklı yönetim bilişim sistemlerinden biri olan Ulusal Yargı Ağı Bilişim Sistemini (UYAP) uygulamaya koymuştur... UYAP ile yargı birimleri ve idarî birimlerin tüm bilgi ve belgeleri doğru ve tutarlı, değişmez ve güvenli bir şekilde veritabanında saklanmakta, yetkisiz erişimlere izin verilmemektedir... Öte yandan UYAP ile diğer kamu kurum ve kuruluşlarının bilgi sistemleriyle sağlanan (Adli Sicil ve İstatistik Genel Müdürlüğü-Adli Sicil Bilgi Sisteminden sabıka kayıtları, Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü-MERNİS'ten nüfus kayıtları, Emniyet Genel Müdürlüğü- POLNET'ten ehliyet kayıtları, PTT'den tebligatların akıbetleri, Merkez Bankasından döviz kurları, KİHBİ ve POLNET'den aranan kişilerin kayıtları gibi) entegrasyonlar sayesinde mahkemelerin ihtiyaç duyduğu bilgi ve belgelere elektronik ortamda ulaşılabilmektedir.

Adil yargılama ve usul ekonomisi gibi sebeplerle elektronik belgeler hukuk dünyası için de büyük önem arz etmektedir. UYAP bu noktada çok önemli bir aşama kat etmiş bulunmaktadır.

5.3. Elektronik Belgeye Geçişteki Çekinceler

Elektronik belgelerin kullanımındaki en büyük sorun belgenin içeriğinin sonradan değiştirilip değiştirilmediği ve tahrife uğrayıp uğramadığının tespitidir⁴⁷. Bu sorun elektronik imza kanununda düzenlenen güvenli elektronik imza bakımından aşılmış görülmektedir. Nitekim güvenli elektronik imza içeriği daha sonra da ayrıntılı açıklanacağı şekliyle belgenin değiştirilip değiştirilmediğini ispatlamaya yarayan, belgenin kimin tarafından düzenlendiğini tespiti imkanı tanıyan ve kişiye sıkı sıkıya bağlanmaya çalışılan bir araçtır.

Güvenli elektronik imzanın elektronik ticaret alanındaki ilişkileri kolaylaştırma, hızlandırma ve elektronik belgeleri yasallaştırma gibi cazip özellikleri bulunmaktadır. Ancak güvenli elektronik imzanın ve elektronik işlemlerin güvenliği ne derece artırılırsa artırılırsın “insan faktörü” nedeniyle kırılganlıkları devam edecektir. Ne kadar değiştirilmesi zor matematiki şifrelere de dayansalar sanal ortamda yapılan işlemlerin, işlemin tarafları dışındaki üçüncü kişilerce kesinlikle görülemeyeceğini ve değiştirilemeyeceğini

⁴⁷ Erturgut, 2004, s. 34.

iddia etmek mümkün değildir⁴⁸. Ancak gelişen teknoloji, uluslararası ekonomik ve ticari ilişkiler, e-devlet ve e-ticaret gibi işlemleri hızlandıran, kolaylaştıran bu sistemler hemen her ülkeyi bu sistemde yer alma konusunda zorlamaktadır. Aksi halde uluslararası ilişkilerde yaşanan hıza ve teknolojiye ayak uyduramama yüzünden geçmişte karşılaşılan sorunlar gelecekte de devam edecektir.

Gelişen teknoloji ve bilişim sistemlerinden kaçınılmayacağından dolayı bilişim sistemindeki elektronik veriler niteliği gereği ceza kanunları bağlamında da bilişim güvenliği bağlamında da dikkatle ele alınmalıdır. Ceza kanunları bağlamında bu suçların konularının korunmasına ciddi önem verilmelidir. Ceza Hukuku bakımından elektronik bir kaydın hukuki nitelikte bir belge olup olmadığının tespiti cezalandırma kabiliyeti için de çok önemlidir⁴⁹.

6. ELEKTRONİK BELGENİN UNSURLARI

Elektronik belgeden bahsedebilmek için kanun gerekçesinde belirtilen belgeye ilişkin unsurlardan “kağıt ve plaka gibi taşınabilir bir cisme yazılması” unsurunun dışındaki bütün unsurlar elektronik bir belgede bulunmalıdır. Elektronik verilerin ceza hukuku anlamında

⁴⁸ Berber, L. K. (2000). “İmzalıyorum O Halde Varım” Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri. *Türkiye Barolar Birliği Dergisi*. 2000/2. s. 551.

⁴⁹ Aslan, 2014, s. 25.

belge kabul edilebilmesi için belgede sahtecilik suçunun gerekçesinden ayrılan tek unsur kağıt gibi taşınabilir cisme yazılması unsurudur. Dolayısıyla yazılı taşınabilir bir belgede aranması gereken unsurlardan yukarıdaki istisna dışındaki tüm unsurların elektronik belgede bulunması gerekmektedir.

6.1. Elektronik Belgenin Yazılılık Unsuru

Belge yukarıda da değinildiği gibi genel olarak bir eylem veya irade beyanının veya olayın yazıya geçirilmesidir. Klasik anlamda belge, yazının kâğıda geçirilmesi ile oluşturulmaktadır. Teknoloji ile birlikte elektronik ortamlarda bulunan kayıtlar da belge olarak kabul edilmeye başlanmıştır. Bir düşüncenin, olayın veya durumun fiziki dünyaya aktarılabilmesi için belgenin öncelikle yazılması, diğer bir ifade ile düzenlenmesi gerekir. Ancak, sayısal ortamda yazı kavramı da geleneksel anlamının dışına çıkmıştır. Çevre birimleri aracılığı ile kişilerin iradesinin sayısal ortamda tutulabilecek şekilde girilmesi de yazı olarak kabul edilmiştir⁵⁰.

Elektronik kayıtların fiziki ortamda bulunmaması ve sadece görme duyusu ile algılanması durumu söz konusudur. Daha sonra da değinileceği üzere güvenli elektronik imzanın göz ile görülebilme olanağı da bulunmamaktadır. Bu bağlamda bir belgenin hukuki

⁵⁰ Aslan, 2014, s.27.

anlamda bir belge olup olmadığının insan duyuları ile tespit edilmesi imkânsız hale gelmektedir⁵¹.

Bir görüşe göre belge maddi, fiziki varlığı olan bir şeyle sıkı sıkıya bağlılık içinde olmalı ve duyu organları ile algılanabilmelidir⁵². Nitekim kanunun (TCK m.204) gerekçesinde de bu unsura değinilmiştir⁵³. Makalemizde ise kanun metninin gerekçesinden ayrılarak elektronik belgeler bakımından güvenli elektronik imza unsurunun bulunması durumunda belgenin taşınabilir bir cisme kaydedilmesi unsuru bulunmadan da sahtecilik suçları bakımından konu unsurunu oluşturacağını savunmaktayız.

Güvenli elektronik imzalı olmayan veriler ise mevzuatımıza göre belge olarak kabul edilemeyecek ve ancak bilişim sistemindeki verileri değiştirme suçu (TCK 244/2) kapsamında değerlendirilecektir. Önemle belirtmek gerekir ki Adalet Bakanlığı Kanunlar Genel Müdürlüğü tarafından hazırlanan yeni tasarı taslağıyla bu suçun cezası ağırlaştırılmaktadır⁵⁴.

⁵¹ Aslan, 2014, s.27.

⁵² Arslan, Baştürk, 2013, S. 201.Tezcan, Erdem, Önok, 2013, s. 691

⁵³ *Ayrıca belirtilmelidir ki, her ne kadar, belgeden söz edilen durumlarda yazılı bir kağıdın varlığı gerekli ise de; bazı durumlarda belgenin varlığını kabul için, yazının kağıt üzerinde bulunması gerekmez. Bir metal levha üzerine yazı yazılması hâlinde de belgenin varlığını kabul etmek gerekir. Bu itibarla, araç plakaları da resmi belge olarak kabul edilmek gerekir.*TCK madde 204'ün gerekçesinden.

⁵⁴ Taslağa Ulaşmak İçin: <http://www.kgm.adalet.gov.tr/DUYURULAR/TASARI-alternatif%20%C3%A7%C3%B6z%C3%BCm%20y%C3%B6ntemleri.pdf>, Erişim Tarihi: 19.08.2015.

6.2. Elektronik Belgenin İmza Unsuru

Hukuki bir belgenin en önemli unsuru imzadır. Bir belgenin hukuk aleminde sonuç doğurabilmesi için düzenleyenin belli olması gerekmektedir. Kimin düzenlediği bilinmeyen yazı ve verilerin belge niteliği bulunmamaktadır⁵⁵. İmza, bir belgenin düzenleyeni gösteren eşsiz bir araçtır.

Elektronik imzaya ihtiyacın ortaya çıkmasındaki en önemli sebep gelişen teknolojik koşullarda elektronik ortamda yapılan hukuki işlemlerin güvenliğini sağlama, belgelerin düzenleyeni tespit etme ve imzaların inkâr edilmemesini sağlamaktır⁵⁶.

Elektronik bir belgenin hukuki anlamda bir belge olabilmesi için de belli bir kişiye izafe edilebilmesi gerekir. Mevzuatımızda muteber kabul edilen elektronik imza çeşidi güvenli elektronik imzadır. Ancak güvenli elektronik imza kullanılarak oluşturulan belgelerin kişilere izafe edilmesi şartı gerçekleşmektedir. Güvenli elektronik imza dışındaki dijital imzalarla imzalanmış belgeler hukuk düzenimiz bağlamında belge vasfını kazanamamaktadır.

Elektronik imza birçok ülkenin mevzuatında ve Avrupa Parlamentosunun 1993/93/AT sayılı direktifinde tanımlanmıştır. Direktifte elektronik imza “*başka bir elektronik veriye eklenen veya*

⁵⁵ Aslan, 2014, s. 28.

⁵⁶ Erturgut, 2003, s. 68.

onunla mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri” şeklinde tanımlanmaktadır.

Türk kanun koyucusu da EİK’da Avrupa Birliği Direktifini esas alarak elektronik imzayı “*başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri”* olarak tanımlamıştır⁵⁷.

Bu başlık altında güvenli elektronik imzanın unsurları ve işlevleri ehemmiyeti gereği ayrıntılı olarak açıklanacaktır.

6.2.1. Elektronik İmza Çeşitleri

Elektronik imzanın çeşitli şekillerde ortaya çıktığı görülmektedir. Bunların başlıcaları şunlardır: Kişilerin biyometrik özelliklerine dayalı yöntemler (bunlar ses, göz retinası ve parmak izi taraması gibi yöntemlerdir), PIN kodları, elle atılmış imzanın tarayıcıdan geçirilerek elektronik ortama aktarılmış hali, bilgisayar ekranlarına bu amaçla yapılmış özel kalemlerle atılan imza veya çift anahtarlı kriptografiyle oluşturulan dijital imzalar⁵⁸.

Elektronik imza uygulamalarına bakıldığında e-imzanın farklı çeşitlerde ortaya çıktığı görülmektedir⁵⁹. Bunlardan başlıcaları basit

⁵⁷ Elektronik İmza Kanunu, madde 3/b.

⁵⁸ Erturgut, 2004, s.61.

⁵⁹ Erturgut, 2004, s.61-68.

elektronik imza, gelişmiş elektronik imza, güvenli elektronik imza ve akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilen imzadır. Mevzuatımızda muteber kabul edilen elektronik imza çeşidi ise güvenli elektronik imzadır. Güvenli elektronik imza, basit elektronik imzadan çeşitli yönleriyle ayrılmaktadır. Basit elektronik imza çeşitlerinin bazı unsurları eksik olduğu için mevzuatımızda bu imzalar muteber kabul edilmemektedir. Elektronik imza çeşitleri kapsamında basit elektronik imza ve güvenli elektronik imzaya değinilecektir.

6.2.2. Basit Elektronik İmza

Basit elektronik imza hukuki geçerlilik, bağlayıcılık ve güvenlik gereksinimleri bakımından bir imzanın taşınması gereken bütün şartların tamamlanmadığı elektronik imza türüdür⁶⁰. Basit elektronik imza ile kimlik doğrulama ve elektronik belge ile bağlantı kurma işlevleri sağlanabilirken basit elektronik imzalı belgelerde bu işlevler her zaman doğru sonuçlar vermemektedir.

Basit elektronik imza türlerine bilgisayar ekranına özel kalem ile atılan imza, biyometrik imza, dijital imza, ıslak imzanın tarayıcıdan geçirilerek e-belgelere eklenmesi durumları örnek olarak verilebilir⁶¹.

⁶⁰ <http://hakanalbayrak.blogspot.com.tr/2008/05/elektronik-belgelerin-delil-olarak.html>, Erişim Tarihi: 19.03.2015

⁶¹ <http://hakanalbayrak.blogspot.com.tr/2008/05/elektronik-belgelerin-delil-olarak.html>, Erişim Tarihi: 19.03.2015

Biyometrik imzalar farklı türlerde görülmektedir. Bunlar; retina taraması, imza tanımlaması, yüz tanımlama, parmak izi ya da ses gibi biyolojik özelliklerin kullanıldığı imzalardır. Bu yöntemleri sınırlayıcı bir şekilde tanımlamak mümkün değildir. Zira her geçen gün bu yöntemler farklı şekillerde gelişebilmektedir⁶². Basit elektronik imza kapsamında değerlendirilen bu yöntemler, elektronik imzadan beklenen belgenin bütünlüğünün korunması, imza sahibinin kimliğinin tespiti gibi birtakım işlevleri sağlamak bakımından yetersiz kalmaktadır⁶³.

HMK'ya göre (m.205/2) basit elektronik imza kapsamında bulunan elektronik imza türleri hukuken korunmadıkları gibi yargılamada delil olarak kullanılamazlar. Zira sadece güvenli elektronik imzalar hukuki işlemlerde “güvenlilik şartını” yerine getirir ve yargılamada senet delili olarak kullanılabilirler.

Buna karşılık, Avrupa Birliği 1999/93 sayılı elektronik imzaların düzenlenmesi hakkındaki direktifinin 5.maddesinde sadece bazı özelliklerinin eksik olması nedeniyle basit elektronik imzaların yargılamada kullanılmasının önüne geçilmemesi gerektiğini belirtmektedir. Bu özellikler:

- bir imzanın elektronik olması
- akredite edilmiş sertifikaya dayanmaması

⁶² Acar, A. E. (2013). Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Değeri, İstanbul: XII Levha Yayınları. s. 78.

⁶³ Acar, 2013, s.79.

- akredite edilmemiş bir sertifika sağlayıcıdan temin edilmiş olması

- güvenli elektronik imza oluşturma aracı ile oluşturulmamasıdır.

Yukarıdaki durumlarda bu imzaların sadece bu özellikleri nedeniyle hukuki etki doğurmasına veya yargılamada caiz delil olmasına engel olunmaması gerektiğini belirtilmektedir⁶⁴.

6.2.3. Güvenli Elektronik İmza

Elektronik imza, kısaca elektronik veriye eklenen ya da mantıksal bağlantısı bulunan, kimlik doğrulama amacıyla kullanılan elektronik bir veri anlamına gelmektedir⁶⁵. Islak imza nasıl bir kağıda atılan imzanın atan kişiye ait olduğunu ispatlamaktaysa, elektronik imza da herhangi bir elektronik dokümana eklenen imzalama verisinin yetkili kişiye ait olup olmadığını ispatlamaktadır. Bazı kaynaklarda dijital imza olarak da geçen güvenli elektronik imzanın

⁶⁴ “Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is

- in electronic form, or

- not based upon a qualified certificate, or

- not based upon a qualified certificate issued by an accredited certification-service-provider, or

- not created by a secure signature-creation device.”

<http://www.columbia.edu/~mr2651/ecommerce3/2nd/statutes/ElectronicSignaturesDirective.pdf>, Erişim Tarihi: 23.3.2015. S. 256.

⁶⁵ <https://eteydeb.tubitak.gov.tr/eimzabilgisayfasi.htm>. Erişim Tarihi: 1.10.2015.

mevzuatımızda bu isimle tanımlanmasının sebebi karşılaştırmalı hukuktaki mevzuatla uyum içinde olma çabasıdır⁶⁶. Güvenli elektronik imza AB Direktifindeki “*nitelikli elektronik imzaya*” karşılık gelmektedir⁶⁷.

Güvenli elektronik imzanın unsurları EİK madde 4’te belirlenmiştir.

Madde 4- Güvenli elektronik imza;

a. Münhasıran imza sahibine bağlı olan,

b. Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c. Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d. İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan, elektronik imzadır.

6.2.3.1. Güvenli Elektronik İmzanın Unsurları

AB Direktifi’nde tanımlanan güvenli elektronik imza, Direktifin 5.maddesinde üye ülkeler tarafından ıslak imzaya eşdeğer

⁶⁶ Belgin, D. (2009). Elektronik İmzalı Belgelerin Delil Değeri. *Ankara Barosu Hukuk Gündemi Dergisi*. 2009-2. S.39.

⁶⁷ <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31999L0093&from=EN>. Erişim Tarihi: 6.10.2015

kabul edilmektedir. Ayrıca güvenli elektronik imzanın yargılamada caiz delil olarak kullanılabilmesi de bu maddede düzenlenmektedir⁶⁸.

Güvenli elektronik imza, Direktif'e göre gelişmiş elektronik imzanın unsurlarını taşımaları, nitelikli sertifikaya sahip olmaları ve güvenli imza oluşturma araçları ile oluşturulma şartını taşımalarıdır. Gelişmiş elektronik imza mevzuatımızda düzenlenmemiştir. Direktifin ikinci maddesinde gelişmiş elektronik imzanın unsurları belirtilmiştir.

Bunlar;

- münhasıran imza sahibine bağlı olma,
- imza sahibini tanımlayabilme,
- imza sahibinin tasarrufunda bulunan araçlarla oluşturulma,
- veride sonradan yapılan değişiklikleri gösterme

unsurlarıdır⁶⁹.

⁶⁸ Bu durum 1999/93/EC sayılı direktifin beşinci maddesinde şu şekilde açıklanmıştır:

Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31999L0093&from=EN>, Erişim Tarihi: 26.5.2015.

⁶⁹ Bu unsurlar 1999/93/EC sayılı direktifin tanımlar başlıklı ikinci maddesinde şu şekilde açıklanmıştır: "Advanced electronic signature" means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

Hukukumuzda bu unsurlar güvenli elektronik imzanın unsurları olarak EİK madde 4'te kabul edilmiştir⁷⁰. AB Direktifi ile uyumlu olarak hukukumuzda güvenli elektronik imza, ıslak imza ile eş değer sayılmış ve bunlar çeşitli kanunlarımızda yer almıştır⁷¹. Yine Direktif doğrultusunda güvenli elektronik imzalı belgeler hukukumuzda muteber kabul edilip yargılamada delil olarak kullanılabilir. Bu durum da mevzuatımızda kayıt altına alınmıştır⁷².

6.2.3.1.1. Münhasıran İmza Sahibine Bağlılık

Güvenli elektronik imzanın ilk unsuru olan münhasıran imza sahibine bağlılık, imza oluşturma verisinin⁷³ yalnızca imza sahibine has olduğu anlamına gelmektedir. Kişiyeye has imza oluşturma verisi ile oluşturulmuş bir elektronik imza elektronik imza sahibi tarafından atılmış kabul edilir. “İmza sahibi” kavramı EİK'nın tanımlar

(c) it is created using means that the signatory can maintain under his sole control; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.”

<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31999L0093&from=EN>, Erişim Tarihi: 26.5.2015.

⁷⁰ Acar, 2013, S.101.

⁷¹ EİK m.5, 818 s. BK m.14, 6095 s. BK. M.15/1.

⁷² HMK madde 205/2, HUMK m. 295/A.

⁷³ İmza oluşturma verisi, EİK'nın tanımları düzenleyen maddesinde, imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler şeklinde tanımlanmaktadır.

maddesinde, “*elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi*” olarak tanımlanmaktadır. Görüldüğü üzere kanunda imza sahibi olarak elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan “gerçek kişi” kabul edilmiştir. O halde, mevcut yasal düzenleme çerçevesinde elektronik bir belge ancak, gerçek bir kişi tarafından oluşturulabilecektir⁷⁴.

Elektronik imza oluşturma verisini içeren elektronik imza oluşturma araçları⁷⁵ Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) tarafından kişilere teslim edilmektedir. Bunlar kart şeklinde olabildikleri gibi çubuk olarak adlandırılan bir usb bellek şeklinde de olabilmektedir. Bu şekilde her imza sahibinin imza oluşturma verisi ayrı olur ve teslim edilmesi ile imza sahibine bağlanır⁷⁶.

ESHS’ler imza oluşturma verisinin kopyasını ellerinde bulunduramayacaklardır⁷⁷. Yine ESHS’ler güvenlik gereği bu verileri 3. kişilerin bulunduğu ortamda bulunduramayacaklardır⁷⁸.

⁷⁴ Aslan, 2014, s.35.

⁷⁵ Elektronik imza aracı, EİK’nın tanımları düzenleyen 3.maddesinde, elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını ifade eder şeklinde tanımlanmaktadır.

⁷⁶ Acar, 2013, s.103.

⁷⁷ EİK madde 10/son: Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

⁷⁸ EİK madde 12/b: Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz.

6.2.3.1.2. Yalnızca İmza Sahibinin Tasarrufunda Bulunan Güvenli Elektronik İmza Oluşturma Aracı İle Oluşturulma

Güvenli elektronik imza sahibi olan gerçek kişi elektronik imzasını başkasına kullandırmamakla ve bu konuda gerekli önlemleri almakla yükümlüdür. Ayrıca imza sahibi, imza oluşturma verisinin gizliliğinden veya güvenliğinden şüphe etmesi durumunda ESHS'yi derhal bilgilendirmekle yükümlüdür. Elektronik imza sağlayıcılarının imza sahiplerini bu konuda bilgilendirmesi gerektiği ise EİK'nın 10.maddesinde belirtilmiştir⁷⁹.

Kanunda imza oluşturma verisinin imza oluşturma aracının dışına çıkarılmayacağı belirtilerek gizliliğin korunması amaçlanmıştır. Nitekim, yetkisiz olarak imza oluşturma verisine ulaşmaya çalışıldığı takdirde kapalı anahtar olarak da adlandırılan bu veri kendisini bloke etmektedir⁸⁰.

İmza oluşturma verisinin gizliliğinin yanı sıra güvenli elektronik imza atabilmek için imza sahibinin oluşturduğu PIN kodu da imzanın kişiye münhasır olmasını sağlamaktadır. PIN kodunun arka arkaya yanlış girilmesi durumunda PUK kodu devreye girmekte

⁷⁹ f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle,

⁸⁰ Acar, 2013, s. 104.

ve yanlışlık bu şifrede de tekrar edildiği takdirde güvenlik gereği elektronik imza oluşturma aracı bloke olmaktadır⁸¹.

Bu önlemlerle elektronik imza oluşturma aracı, imza sahibi dışındaki üçüncü kişilerin kullanımına kapalı kalmaktadır.

6.2.3.1.3. Nitelikli Elektronik Sertifikaya Dayanarak İmza Sahibinin Kimliğinin Tespitini Sağlama

Elektronik İmza Kanunu, güvenli elektronik imzanın geçerli olabilmesi için nitelikli elektronik sertifikaya dayanması gerektiğini şart koşmaktadır. Kanunun 9.maddesinde nitelikli elektronik sertifika düzenlenmiştir. Elektronik sertifikanın tanımı ise, kanunun 3.maddesinde yapılmıştır. Tanıma göre elektronik sertifika, *“imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı”* ifade etmektedir.

ESHS’lerden temin edilen elektronik sertifikalar ile imza sahibinin kimliği tespit edilmektedir. Sertifikalar üzerindeki ESHS’nin elektronik imzası vasıtasıyla sertifikanın bütünlüğü ve doğruluğu garanti altına alınmaktadır⁸².

Nitelikli elektronik sertifikanın şartları Kanunun 9.maddesinde belirtilmiştir. Bunlar;

⁸¹ Acar, 2013, s. 104.

⁸² Acar, 2013, s.105.

- “Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare,
- Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adı,
- İmza sahibinin teşhis edilebileceği kimlik bilgileri,
- Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi,
- Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri,
- Sertifikanın seri numarası,
- Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi,
- Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri,
- Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgileri,
- Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası” dır.

Yukarıda sayılan nitelikleri taşıyan sertifikalara sahip güvenli elektronik imzalar sertifika sağlayıcılar tarafından tescil edilmiş olurlar. Nitelikli elektronik sertifikalar Bilişim Teknolojileri Kurulu’na (BTK) bildirimde bulunmuş ESHS’ler tarafından verilmektedir. Türkiye’de BTK tarafından kabul edilen ESHS’ler ise

şunlardır: E-Güven, TürkTrust, E-Tuğra, E-imzaTR'dir. Ayrıca kamu kurumları için TUBİTAK-UEKAE ve Emniyet Genel Müdürlüğü Sertifikasyon Merkezi (EGMSM) bulunmaktadır⁸³.

Güvenli elektronik imzaların, Türkiye'de yetkilendirilmiş olan ESHS'ler tarafından sağlanmış sertifikalarla atılması gerekmektedir. Bu durumda yabancı ESHS'ler tarafından verilmiş sertifikalarla atılan elektronik imzalı belgeler hukuki anlamda belge hüviyetini kazanamayacaktır.

Bu noktada uyumsuzluğa konu olmuş bir davayı incelemek faydalı olacaktır. Yargıtay Ceza Genel Kurulu'nda görülen bir davada sanığın okuduğu üniversitedeki öğrenci işlerinde görevli olan memurla anlaşıp kendi notlarını üniversitenin bilişim sisteminde değiştirtmesi işleminde yerel mahkeme TCK madde 244/2'den yani bilişim sistemindeki verileri değiştirmek suçundan hüküm kurmuştur. Yargıtay 11. Ceza Dairesi ise söz konusu suçun evrakta sahtecilik kapsamında değerlendirilebileceğini ve bunun değerlendirmesinin ağır ceza mahkemesince yapılması gerektiğini belirterek asliye ceza mahkemesince verilen hükmü bozmuştur. Yargıtay Ceza Genel Kurulu ise iddianamede atılı suçun bilişim sistemindeki verileri değiştirme suçunun olduğunu dolayısıyla iddianameye konu edilmeyen bir fiilden dolayı (davasız yargılama olmaz ilkesi)

⁸³ http://www.tk.gov.tr/bilgi_teknolojileri/elektronik_imza/eshs.php,
Zamanı: 6.4.2015.

yargılama yapılamayacağını belirterek yerel mahkemeyi haklı görmüştür⁸⁴.

Karardan anlaşılacağı üzere Yargıtay 11. Ceza Dairesi söz konusu elektronik verileri değiştirme işleminin belgede sahtecilik suçunu oluşturabileceğini belirtmiştir. Yargıtay Ceza Genel Kurulu ise bu eylemin belgede sahtecilik suçunu oluşturmayacağını savunmaktadır.

Söz konusu olayda tartışılması gereken husus ise bilgisayar sistemine girilerek notların değiştirildiği verilerin hukuki anlamda belge olarak kabul edilip edilemeyeceğidir. Konumuz olan imza unsuru bağlamında değerlendirilecek olursa, bilişim sistemindeki bu veriler bir şahsa izafe edilebiliyorsa yani düzenleyen olarak belli bir kişinin görüldüğü verilerse bu verilere hukuki anlamda belge demek mümkün olacaktır. Ancak elektronik verilerdeki tespit ve irade beyanları herhangi bir kişiye izafe edilemiyorsa bu verilere hukuki anlamda belge denilemez.

Örnek vermek gerekirse bir odaya birden fazla kapıdan girilip odanın içinde yapılan değişikliklerin hangi kapıdan giren kişi tarafından yapıldığı belli olmuyorsa burada hukuk tekniği bağlamında belgeden bahsedilemeyecektir. Dolayısıyla bu nitelikteki bilişim sistemlerinde yapılan sahtecilikler belgede sahtecilik suçunu değil

⁸⁴ YCGK E. 2007/11-44 K. 2007/200 T. 9.10.2007.

<http://www.kararara.com/forum/viewtopic.php?f=44&t=19762>, Erişim Tarihi: 15.4.2015

bilişim sistemindeki verileri değiştirme suçu olan TCK 244/2'deki suçu oluşturacaktır. Nitekim, bir belgeden bahsedilebilmesi için söz konusu verilerin düzenleyicisinin belli olması ve elektronik belge bağlamında bu düzenleyicinin güvenli elektronik imza ile tespit edilir olması gerekmektedir.

Ancak yukarıdaki olayla ilgili olarak Adalet Bakanlığı Kanunlar Genel Müdürlüğü'nün hazırladığı kanun tasarısı taslağı yasalırsa bu fiil için ayrıca belgede sahtecilik hükümlerinden de cezalandırma yapılacaktır. Nitekim tasarı taslağına göre 244. maddeye eklenmesi planlanan 5. Fıkra yeni bir içtima hükmü getirmektedir ve şu şekildedir:

“İkinci ve üçüncü fıkralarda tanımlanan fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca belgede sahtecilik suçlarına ilişkin hükümler uygulanır.”

6.2.4. Güvenli Elektronik İmzanın İşlevleri

Elektronik imzanın ıslak imzayı ikame edebilmesi için, ıslak imzanın yerine getirdiği işlevlerin elektronik imza tarafından da yerine getirilmesi gerekir (işlev eşitliği)⁸⁵. Tüm fonksiyonlar bakımından elektronik imzanın ıslak imza ile aynı olması ise, her iki şekil

⁸⁵ Keser Berber,L.*Şekil ve Dijital İmza*.http://enoter_hukuk.tripod.com/leyla-keser_berber.htm. Erişim Tarihi: 27.04.2015.

arasındaki yapısal farklılıklar yüzünden pek mümkün gözükmemektedir. Bazı fonksiyonlar elektronik imza tarafından daha iyi bir şekilde yerine getirilirken, diğer bazılarına ise ıslak imza ile daha iyi ulaşılabilmektedir. El yazısı ile imzanın, kimliği tespit işlevi, gerçeklik işlevi, sonuçlandırma işlevi, uyarı işlevi, devamlılık işlevi ve ispat işlevi vardır⁸⁶.

6.2.4.1. Kimlik Tespiti ve Gerçeklik

İmza, yer aldığı belgede düzenleyen kişinin kimliğini tespit etmeye yarayan bir araçtır. Nitekim el yazısı ile atılmış olan imza kişinin kişisel özelliğini yansıtır ve biriciktir.

Güvenli elektronik imza, imzalama işlemi sırasında imzalayan kişinin kimliğinin doğrulanmasını sağlamaktadır. ESHS'lerin bir görevi de, kullanıldığı anda elektronik imzanın geçerli olup olmadığını doğrulamaktır⁸⁷. Sertifika hizmet sağlayıcısının önemi asıl olarak bu noktada yani kimliğin tespiti bakımından ortaya çıkmaktadır. Zira kendisine elektronik imzalı bir metin gönderilen kişi, bu imzanın bir kişiye özgülenmiş olduğunu, açık anahtar vasıtasıyla tespit edebilecektir. Elektronik sertifikaya dayanan bu şekildeki özgülenme, gönderilen kişi tarafından kişinin kimliğini tespit etmeye yarayacaktır. Kimliği tespit işlevi, kişinin elektronik sertifikası

⁸⁶ Acar, 2014, s.96, 97, 98, 99.

⁸⁷ Aslan, 2014, s.39.

sayesinde gerçekleşmektedir. Bu durumda, sertifika hizmet sağlayıcısının en önemli fonksiyonunun, elektronik imza sahibinin kimliğini tespit etmek olduğu söylenmelidir. Böylece, el yazısı ile imzanın sağladığı kimliği tespit işlevi elektronik imza ile de sağlanmış olacaktır⁸⁸.

Güvenli elektronik imza ile imzalanmış belgelerde ise belgeyi gönderenin kimliği belge ile birlikte gönderilen elektronik imza sertifikasından tespit edilmektedir⁸⁹. ESHS'ler tarafından verilmiş bulunan sertifikalarda imzalayan kişinin bilgileri bulunmaktadır. Bu sertifikaların incelenmesi ile imza sahibinin kimliğinin tespiti mümkün olmaktadır. Güvenli elektronik imzalar vasıtasıyla imza sahibinin tespiti güvenilir bir şekilde sağlanabilmektedir⁹⁰.

Ancak elektronik imzanın başkası tarafından kullanılmış olma ihtimali burada değerlendirilmelidir. Zira, bunun tespiti çok mümkün değildir. Nitekim el yazısı ile imzalanmış belgelerde imza imzalayanın karakteristik özelliğini göstermekte iken güvenli elektronik imzada bu karakteristik özellik, imza oluşturma verisinin teklüğünden kaynaklanmaktadır⁹¹. Bu nedenle güvenli elektronik imzalı belgelerde ulaşılabilen veri sadece imza sahibinin bilgileridir. Her bir imza oluşturma verisi her imza sahibi için farklı olduğundan dolayı bir belgenin elektronik imza ile imzalanması durumunda o belge artık

⁸⁸ Erturgut, 2004, s. 113

⁸⁹ Acar, 2013, s.96.

⁹⁰ Acar, 2013, s.96.

⁹¹ Acar, 2013, s.97.

ilgili imzanın sahibi tarafından imzalanmış olarak kabul edilmektedir. Nitekim elektronik imza kanununun 16.maddesinde elektronik imza verilerini içeren araçların kişilere özgü olduğu vurgulanarak izinsiz kullanımları hapis ve adli para cezaları ile yaptırıma bağlanmıştır.

Güvenli elektronik imzaların kural olarak inkar edilemez olmaları da gerçeklik işlevinin bir sonucudur.

6.2.4.2. Sonuçlandırma

Bir belgeye el yazısı ile imza atılması imzalayan kişinin belgenin oluşturulmasında iradesinin olduğunu ve son halini kabul ettiği anlamına gelmektedir⁹². Bu nedenle belgenin oluşturulmasından sonra yapılan eklemeler ve değişiklikler imza sahibinin iradesini yansıtmayacak ve imza sahibini bağlamayacaktır. Yani imzalayan kişi belgenin yalnızca altına imza attığı durumundaki içerikten sorumlu olacaktır.

Bir belgenin güvenli elektronik imza ile imzalanması durumunda da sonuçlandırma işlevi yerine gelmektedir. Zira değinildiği üzere güvenli elektronik imzalı belgede yapılan herhangi bir değişiklik belgenin hash değeri⁹³nin değişmesine sebep olmakta ve belgenin elektronik imzasının kaldırılmasına yol açmaktadır⁹⁴.

⁹² Acar, 2013, s.96.

⁹³ Hash değeri, dosyaların parmak izi gibidir. Dosyalar, karmaşık algoritmalarla taranır ve dosyanın benzersiz bir parmak izi, yığını

6.2.4.3. Uyarı İşlevi

Atılan imzanın en önemli işlevi olarak uyarı işlevi kabul edilebilir⁹⁵. İmza atılması bir şekil kuralı olup, imza atan kişinin bir yükümlülük altına girdiğinin uyarılması işlevini görmektedir. İmza sayesinde beyanda bulunan kişi, acele hareket etmekten korunmuş olacaktır. İmza atmak kişinin imza attığı belgedeki ifade ve olgularla bağlanması anlamına gelmektedir. Kişi imza ile bu ifade ve olguları kabul edip hukuki sonuçlarını üstlendiğini belirtmektedir.

Güvenli elektronik imza ile bir belgeyi imzalamak isteyen kişi imza çubuğunu veya kartını bilgisayara adapte edip, gerekli olan PIN kodunu girmelidir. Ayrıca kapalı anahtar denilen metni belgeyi kripteye eden şifre girilmeden önce sertifika hizmet sağlayıcılarının imzanın ıslak imza ile aynı hukuki değere sahip olduğu uyarısı yapması gerekmektedir⁹⁶. Nitekim EİK madde 10'da bu durum açıkça ifade edilmektedir;

Elektronik sertifika hizmet sağlayıcısı;

“ ...

e) Sertifikanın kullanımına ilişkin özelliklerin ve uyumsuzlukların çözüm yolları ile ilgili şartların ve kanunlarda

çıkartılır.<https://www.technopat.net/sosyal/konu/hash-nedir.3551/>, Erişim Tarihi: 30.08.2015

⁹⁴ Tamer, S. (2006). Teknik ve Hukuki Açından Elektronik İmza, *Legal Hukuk Dergisi*, Mart 2006, Sayı: 39. (s. 697-733).

⁹⁵ Tamer, 2006, s. 697-733.

⁹⁶ Tamer, 2006, s. 697-733.

öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle,

f) Sertifikada bulunan imza doğrulama verisine karşılık gelen imza oluşturma verisini başkasına kullandırmaması konusunda, sertifika sahibini yazılı olarak uyarmak ve bilgilendirmekle

yükümlüdür.”

Elektronik imza kanunundaki düzenlemelerle birlikte değerlendirildiğinde güvenli elektronik imzanın uyarı işlevini yerine getirdiği görülmektedir. Hatta denilebilir ki elektronik imza ile imza atmak ıslak imzaya nazaran daha çok işlem gerektirmekte ve uyarı işlevini yerine getirmektedir⁹⁷.

6.2.4.4. Devamlılık İşlevi

Devamlılık işlevi, imzalanan metnin istenildiğinde okunabilmesi ve gerektiğinde incelenebilmesini ifade etmektedir⁹⁸.

Islak imzalı belgeler mahiyetleri gereği fiziki ortamda bulunmaktadır ve el ile algılanma yeteneğine sahiptirler. Buna karşılık güvenli elektronik imzalı belgeler ancak elektronik ortamda

⁹⁷ Erturgut, 2004, s. 122-123.

⁹⁸ Acar, 2013, s.99.

görülebilmekte ve imzaların gerçekliği ancak elektronik ortamda test edilebilmektedir.

Yazılı şekil zorunluluğu, imzanın ve imzalanacak metnin sürekli bir kontrole elverişli olması hususunu da gerektirir. Elektronik ortamda imzalanan belgeler de bilgisayar hafızasında veya diğer harici disklerde saklanabilir⁹⁹. Bu durumda devamlılık işlevinin sağlandığı kabul edilmelidir.

6.2.4.5. İspat İşlevi

Bir belgenin imzalanmasının önemli hukuki sonuçlarından birisi de ispat işlevidir. El yazısı ile imzalanan metin bir uyumsuzluk durumunda yazılı şeklin varlığına ve taraflar arasında kurulan sözleşme ilişkisine kanıt sağlar. Elektronik imza kanunu ve diğer mevzuatımızdaki düzenlemeler gereğince ise geçerli olarak imza edilen belgeler de bu manada ispat şartını haiz olacaklardır. HMK'da güvenli elektronik imza ile imzalanan belgelerin senet hükmünde olacağı belirtilmektedir. Borçlar Kanunu'nda ise güvenli elektronik imzanın elle atılan imza ile aynı ispat gücüne sahip olduğu belirtilmiştir. Yine CMK'nın 38/A maddesinin 5.fıkrasında elektronik imzalı belgenin elle atılan imzalı belgeyle çelişmesi halinde UYAP'ta kayıtlı olan güvenli elektronik imzalı belgenin geçerli kabul edileceği

⁹⁹ Tamer, 2006,s. 697-733.

belirtilmiştir. Dolayısıyla güvenli elektronik imza ispat işlevini yerine getirmektedir denilebilir.

Güvenli elektronik imza ile imzalanmamış bir elektronik belge ise medeni usul yargılamasında ancak delil başlangıcı teşkil edecektir¹⁰⁰.

6.3. Elektronik Belgenin Zaman Unsuru

Bir belgenin hukuki sonuç doğurabilmesi için belgenin hukuki sonuç doğurmaya yönelik olarak daha önceden düzenlenmiş olması gerekmektedir. Güvenli elektronik imza, imzalanan belgenin oluşturulduğu zamanın bilgisini de tutmaktadır. Belgenin oluşturulma zamanını tespit etmek imzanın tespit edilmesiyle mümkün hale gelecektir.

EİK'nın 3.maddesi, elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı, veya kaydedildiği zamanın tespiti amacıyla ESHS tarafından sağlanan aracı "zaman damgası" olarak adlandırmaktadır. EİK, düzenlenme zamanının tespiti güvenli elektronik imza ile mümkünken belgenin geçerliliği adına ayrıca zaman damgasını da zorunlu tutmaktadır. Zaman damgası bulunmayan güvenli elektronik imza ile imzalanmış belgelerde yer alan tarih/zaman bilgisinin belgenin düzenleme zamanı olarak kabul

¹⁰⁰ Acar, 2013, s.100.

edilip edilmeyeceği bu konuda ileride ortaya çıkacak yargı içtihatları ile şekillenecektir¹⁰¹.

7. ELEKTRONİK BELGELERDE SAHTECİLİK VE KANUNİLİK UNSURU

Avrupa Siber Suçları Sözleşmesi'nin¹⁰² 7.maddesinde elektronik verilerde sahtecilik fiili düzenlenmiştir¹⁰³. Sözleşmenin açıklayıcı raporunda ise bu maddenin amacının fiziki belgelerde sahteciliğe paralel bir suç ihdas etmek olduğu belirtilmektedir¹⁰⁴.

¹⁰¹ Aslan, 2014, s.34.

Sözleşmenin metni için bkz. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>, Sözleşmenin Türkçe çevirisi ve Meclis Komisyon raporu için bkz. <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf>

¹⁰³ *Taraflardan her biri, özgün olmayan verilerle sonuçlanan yeni veri girme, verileri değiştirme, silme veya engelleme eylemlerinin, söz konusu verilerin yasal açıdan özgün verilmiş gibi kabul edilmesi, veya işlem görmesi niyetiyle, kasten ve haksız yere gerçekleştirildiği zaman, verilerin doğrudan okunabilir ve anlaşılabilir olup olmadığına bakılmaksızın, bu eylemlerin kendi iç hukukunda cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan her biri, cezai yükümlülüğün doğması için, eylemin hile veya benzer bir sahtekarlık niyetiyle gerçekleştirilmiş olmasını şart koşabilir.* <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf>, Erişim Tarihi: 31.7.2015. Not: Türkiye Cumhuriyeti anlaşmayı onaylarken bu maddedeki suç tanımının gerçekleşmesi için dolandırma ve hileli davranış kastı gerektirdiğini beyan etmiştir. <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf>, Erişim Tarihi: 31.7.2015.

¹⁰⁴ Koca, M. (2003). Avrupa Konseyi Siber Suç Sözleşmesi, *Bilgi Toplumunda Hukuk Ünal Tekinalp'e Armağan, Cilt: III*. İstanbul: Beta Yayınevi. S. 803.

Mevzuatımızda elektronik verilerde yapılan sahteciliğin belgede sahtecilik suçları bağlamında değerlendirileceğine yönelik açık bir hüküm bulunmamaktadır.

Bir görüş, kanunilik ilkesi gereği elektronik veriler bakımından ayrı ve açık bir düzenleme yapılmadığı sürece bu verilerin geleneksel sahtecilik suçlarına konu olamayacağını belirtmektedir. Bu görüş elektronik verilerin sahtecilik suçları bağlamında değerlendirilebilmesi için bu verilere ceza kanunlarında belge vasfı verilmesinin zorunlu olduğunu vurgulamaktadır¹⁰⁵.

Diğer bir görüş ise belgede sahtecilik suçlarının niteliği gereği sadece maddi varlığa sahip belgeler bakımından söz konusu olabileceğini belirtmektedir¹⁰⁶. Dolayısıyla bu görüş elektronik belgelerin belgede sahtecilik suçlarına konu olamayacağını savunmaktadır.

Elektronik belgelerde sahtecilik fiilleriyle ilgili olarak müstakil bir düzenleme yapılmadığı bir gerçektir. Ancak savunduğumuz görüşe göre bazı elektronik verilerde yapılacak sahteciliklerin yeni bir düzenleme yapılması gerekmeksizin geleneksel belgede sahtecilik suçlarına konu olacaktır. Nitekim, ceza kanunundaki sahtecilik

¹⁰⁵ Bilindiği üzere kanunilik ilkesi kanunda açıkça suç olarak tanımlanmamış bir fiil için kimsenin cezalandırılmayacağını ifade eden ceza hukukunun temel ilkelerinden birisidir. Arslan, Baştürk, 2013, s. 208.

¹⁰⁶ Güngör, D. (2010). *Resmi Belgelerde Sahtecilik Suçu*. Ankara: Yetkin Yayınevi, s. 50.

suçlarını düzenleyen maddelerin elektronik belgelere uygulanamayacağını gösteren bir düzenleme de bulunmamaktadır¹⁰⁷.

Gerçekten, daha önce de belirtildiği gibi ceza kanununda belgenin tanımı yapılmamıştır. Güvenli elektronik imza ile imzalanmış elektronik belgeler ıslak imzalı belgelere nazaran - yukarıda açıklandığı üzere- daha iyi korunmaktadırlar. Dolayısıyla elektronik belgelerin bu suçlar bağlamında değerlendirilmesi kıyas yasağı ve kanunilik ilkelerine ters düşmemektedir¹⁰⁸.

Diğer yandan, elektronik imza kanununun beşinci maddesinde düzenlenen “*güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*” hükmü belgelerin yalnızca fiziki evrakların “belge” olarak kabul edileceği fikrini yanlışlamaktadır. Nitekim ıslak imza unsuru dışındaki tüm unsurları taşıyan güvenli elektronik imzalı e-belgeler geleneksel anlamda belge ile aynı hukuki korumaya sahiptir.

7.1. 765 Sayılı ve 5237 Sayılı TCK’larda Durum

765 sayılı mülga TCK’nın 525/c maddesinde “*hukuk alanında delil olarak kullanılmak amacıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları*

¹⁰⁷ Tekin, N. (2014). Resmi Belgede Sahtecilik Suçunda Bazı Özel Durumlar, *TAAD*, Yıl:5 Sayı 19, Ekim 2014. s. 935

¹⁰⁸ Tekin, 2014, s. 935.

tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir” hükmü düzenlenerek elektronik veriler bakımından ayrı bir düzenleme yapılmıştı.

Ancak 5237 sayılı yeni TCK böyle bir hükme yer vermemiştir. Yukarıda değinilen görüş kanunilik ilkesi gereği yeni TCK’ya göre elektronik verilerin belgede sahtecilik suçuna konu oluşturmayacağını, yalnızca 244/2.maddede düzenlenen verileri değiştirme veya yok etme suçunu oluşturacağını belirtmektedir¹⁰⁹.

Bu makalede savunulan düşünce, herhangi bir düzenleme yapılmasa dahi yeni TCK’nın güvenli elektronik imza ile imzalanmış elektronik verilerin sahtecilik suçlarına konu oluşturacağıdır. EİK’da düzenlenmiş olan güvenli elektronik imzalı belgelerin madde 5/1 uyarınca¹¹⁰ ıslak imzalı belgelerle aynı değerde olduğunu kabul etmek zorunludur. Nitekim ıslak imza ile gerçekleştirilebilecek her türlü işlem elektronik ortamda güvenli elektronik imza ile yapılabilecektir¹¹¹. Bu belgelerin hukukumuzun itibar ettiği belgeler olması sebebiyle bu belgelerde yapılan tahrifatlar, ceza kanunları

¹⁰⁹ Bu yorum kabul edilecek olursa failer ödüllendirilmiş olacaktır. Nitekim birçok elektronik verinin hukuki anlamda büyük değerleri vardır. Yazıcıoğlu, R.Y. (2005). Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirilmesi, *Yeni Türk Ceza Kanunu Sempozyumu*, İstanbul, s.107.

¹¹⁰ EİK madde 5/1: Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur. Borçlar Kanunu madde 15: Güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur.

¹¹¹ Tekin, 2014, s. 932.

bağlamında belgede sahtecilik suçlarına da sebep verebilecektir. Bu sahteciliklerin belgede sahtecilik kapsamında değerlendirilmesi kıyas anlamına gelmeyecek ve suç ve cezada kanunilik ilkesine aykırılık da teşkil etmeyecektir. Zira güvenli elektronik imza ile imzalanmış ve nitelikli sertifikayla onaylanmış her elektronik veri belge kavramının tüm unsurlarına sahiptir¹¹².

7.2. Yeni Kanun Tasarısı Taslağı

Temmuz 2015 tarihli bir bildirgeyle Adalet Bakanlığı Kanunlar Genel Müdürlüğünün duyurduğu yasa tasarısı taslağı bu konu ile ilgili olarak özel bir düzenleme yapılacağını göstermektedir¹¹³.

Hazırlanan taslakta TCK 244/2’de düzenlenen verileri değiştirme, bozma suçunun cezası arttırılmaktadır¹¹⁴. Eski halinde “6

¹¹² Tekin, 2014, s. 935.

¹¹³ <http://www.kgm.adalet.gov.tr/DUYURULAR/TASARI-alternatif%20%C3%A7%C3%B6z%C3%BCm%20y%C3%B6ntemleri.pdf>, Erişim Tarihi: 1.8.2015

¹¹⁴ Tasarı taslağındaki madde gerekçesi şu şekildedir:

“Maddeyle, Türk Ceza Kanununun 244 üncü maddesinde değişikli yapılarak, sistemi engelleme, bozma, verileri yok etme veya değiştirme eylemleriyle ilgili cezalar caydırıcılığın sağlanması ve bu suçlarla etkin mücadele edilebilmesi amacıyla arttırılmaktadır.

Diğer yandan, Sözleşmenin 7 nci maddesinde, klasik anlamdaki evrakta sahtecilik suçuna paralel bir şekilde bilişim ortamında saklanan verilerde sahtecilik yapılmasının dacezalandırılması öngörülmektedir. Bu doğrultuda maddeye beşinci fıkra eklenerek, ikinci ve üçüncü fıkralarda tanımlanan fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca belgede sahtecilik suçlarına ilişkin hükümlerin uygulanacağı öngörülmektedir.

aydan 3 yıla kadar” olan hapis cezası taslakta “1 yıldan 5 yıla kadar” olarak düzenlenmiştir.

Taslak, önemli bir değişiklik olarak, maddeye yeni bir fıkranın daha eklenmesini de öngörmektedir. Yapılacak düzenlemede değiştirilen, bozulan, yok edilen vb. elektronik verilere dayalı olarak sahte belge düzenlenmesi durumunda ayrıca belgede sahtecilik suçlarından da cezaya hükmedileceği kayıt altına alınmıştır¹¹⁵.

Tam bu noktada Yargıtay’ın bir kararını hatırlamakta fayda bulunmaktadır¹¹⁶. Yargıtay Ceza Genel Kurulu öğrenci işleri bilgi sistemine girilerek kalmış derslerin hukuka aykırı olarak geçilmiş olarak gösterilmesi eyleminde TCK 244/2’den hüküm kurmuş, belgede sahtecilik kapsamında değerlendirmemiştir. Ancak yazılan karşı oylarda bilişim sisteminde değiştirilen verilerin sahte belge (diploma/mezuniyet belgesi) oluşturmak amacıyla yapıldığı belirtilerek belgede sahtecilik kapsamında değerlendirilmesi gerektiği belirtilmiştir. Karşı oy yazısında fikri içtimanın tartışılması gerektiği

Düzenlemeyle hukuki işlem ve belgeleri de kapsayan hukuki ilişkiler açısından önemliolabilecek dijital verilerin güvenliği ve güvenilirliği sağlanmak istenmektedir. Bu suretleSözleşme hükümleriyle uyum sağlanmaktadır.”
<http://www.kgm.adalet.gov.tr/DUYURULAR/TASARI-alternatif%20%C3%A7%C3%B6z%C3%BCm%20y%C3%B6ntemleri.pdf>, Erişim Tarihi: 21.08.2015

¹¹⁵ Tasarı taslağı ile maddeye eklenmesi planlanan fıkra şu şekildedir: “(5) İkinci ve üçüncü fıkralarda tanımlanan fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca belgede sahtecilik suçlarına ilişkin hükümler uygulanır.”

¹¹⁶ T.C. Yargıtay Ceza Genel Kurulu, E. 2007/11-44 K. 2007/200 T. 9.10.2007. Erişim: www.legalbank.net.

belirtilmiştir. Yasa tasarısı taslağı bu noktadaki tartışmayı bitirmeye yönelik önemli bir gelişme olarak değerlendirilebilir.

7.2.1. Yeni Tasarıya İhtiyaç Var mı?

Bu makalede savunulan düşünceye göre hiçbir değişiklik yapılmassa dahi güvenli e-imza ile imzalanan elektronik belgeler klasik belgede sahtecilik suçunun konusunu oluşturabilir. Ancak uygulamada klasik anlamda evrak olarak adlandırılan fiziki belgeler haricindeki belgelerde yapılan sahteciliklerin bu suçlara konu edilmediği ve sadece bilişim sistemindeki verileri değiştirme suçuna konu edildiği görülmektedir. Bu durum da ceza adaletini sağlamada olumsuz sonuçlar ortaya çıkarmaktadır.

Yapılması planlanan düzenleme birkaç açıdan faydalı olacaktır. İlk olarak uygulamada e-imzalı olan belgelerde yapılan sahteciliklerin geleneksel anlamda belgede sahtecilik suçları kapsamında değerlendirmesinde bulunulan çekince kaldırılmış olacak ve kanundaki özel düzenleme uygulayıcıları rahatlatacaktır.

Diğer yandan TCK 244/2'de düzenlenen bilişim sistemindeki verilerde yapılan sahtecilik suçlarının cezası –yaptırım açısından- uygulamada bir ödüllendirme olarak kabul edilmektedir¹¹⁷. Tasarıyla cezaların üst sınırının yükseltilmesi ve alt sınırla üst sınır arasındaki

¹¹⁷ Arslan, Baştürk, 2013, s. 210.

marjın açılması ceza adaleti açısından daha adil sonuçlar doğuracak ve hakimlerin takdir yetkisi daha önemli hale gelecektir.

7.3. Özel Kanunlarda Elektronik Belge ile İlgili Yapılan Düzenlemeler

Yukarıda değinildiği gibi Elektronik İmza Kanunu'nda elektronik belge düzenlenerek güvenli elektronik imza ile imzalanmış belgelerin elle atılan imza ile aynı sonucu doğuracağı düzenlenmiştir.

HMK madde 199'da "belge", uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcılar olarak tanımlanmıştır. Görüldüğü üzere maddede elektronik veriler belge olarak kabul edilmiştir. HMK 205/2.maddede ise güvenli elektronik imzalı belgelerin senet olarak kabul edildiği belirtilmiştir. Dolayısıyla senet olarak kabul edilen bu belgelerde yapılan sahtecilikler, TCK'nın 207 ve 208.¹¹⁸ maddelerinde düzenlenen özel belgede sahtecilik suçlarını oluşturacaktır¹¹⁹. Yine HMK'nın 445/2.maddesinde UYAP

¹¹⁸ TCK'nın 210.maddesinde düzenlenen resmi belge hükmündeki belgeler TTK madde 1526 ve EİK 5/2 uyarınca elektronik imza ile düzenlenememektedirler.

¹¹⁹ Dülger, M. V. (2014). Türk Borçlar Kanunu, Türk Ticaret Kanunu ve Hukuk Muhakemeleri Kanunu'ndaki Bilişim Alanına İlişkin Düzenlemelerin Ceza Hukukuna Yansımaları. Ankara Barosu Dergisi. 2014/1. s. 141.

işlemleri düzenlenmiş ve güvenli elektronik imza ile imzalanmış belgelerin fiziki belge ile aynı değerde olduğu vurgulanmıştır.

Ceza Muhakemesi Kanunu'nun (CMK) 38/A maddesine “*kanunlarda gösterilen istisnalar hariç olmak üzere, dosyalar güvenli elektronik imza kullanılarak UYAP'tan incelenebilir ve her türlü ceza muhakemesi işlemi yapılabilir*” hükmü getirilerek kanunun güvenli elektronik imzalı belgelere verdiği değer gösterilmiştir. Maddenin 5.fikrasında elektronik imzalı belgenin elle atılan imzalı belgeyle çelişmesi durumunda güvenli elektronik imzalı belge geçerli kabul edilir, denilerek elektronik imzalı belgelere üstünlük tanınmıştır¹²⁰.

İcra İflas Kanunu'nun (İİK), 8/A maddesinde güvenli elektronik imzalı belgelerin elle atılan imzalı belgeler gibi olduğu düzenlenmiştir.

Türk Ticaret Kanunu'nda (TTK) tacirler arasındaki bazı işlemlerin güvenli elektronik imza vasıtasıyla kayıtlı elektronik posta (KEP) sistemiyle yapılacağı düzenlenmiş ve bu verilere belge vasfı verilmiştir¹²¹. Yine TTK'ya göre tacirler güvenli elektronik imza

¹²⁰ Ünver, Y. (2013). Üçüncü Yargı Paketinin Değerlendirilmesi. *Marmara Üniversitesi Hukuk Araştırmaları Dergisi*. Cilt: 19 Sayı: 2. s. 420.

¹²¹ Arslan, Baştürk, 2013, S. 213. Yeni TTK 1526/1 uyarınca poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetler güvenli elektronik imza ile düzenlenemez. Ancak maddenin ikinci fıkrasına göre konişmento, taşıma senedi ve sigorta poliçesi elle imzalanabileceği gibi imza, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla da atılabilir denilmiştir. Orel, G. (2011). *Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu*, Ankara: Adalet Yayınevi, s. 55.

vasıtasıyla e-fatura düzenleyebilmektedirler¹²². Diğer yandan tacirler güvenli elektronik imza ve zaman damgası vasıtasıyla e-defter tutmakta ve bu defterler denetlenmektedir. Yine elektronik ortamda şirket toplantısı yapılabilmesi de yeni TTK'nın güvenli elektronik imzaya verdiği değeri gösteren faktörlerden birisidir. Nitekim e-toplantıya katılan üyeler güvenli elektronik imza vasıtasıyla oylamalara katılmaktadırlar.

Vergi Usul Kanunu'nda ise elektronik defter ve elektronik faturalarla ilgili düzenleme yapılmış olup Maliye Bakanlığı'nın çıkarmış olduğu tebliğlerde bu belgelerin güvenli elektronik imza ile imzalanmaları düzenlenmiştir.

6572 sayılı kanunla Aralık 2014'te Noterlik Kanunu'na eklenen 198/A maddesiyle noterlik işlemlerinin güvenli elektronik imza kullanılarak elektronik ortamda da yapılabileceği düzenlenmiştir.

Yukarıda değinilen mevzuatlarda güvenli elektronik imza ön plana çıkarılarak elektronik ortamdaki bu verilere kanunlarla belge niteliği verilmiştir. Dolayısıyla bu verilerde yapılan değişiklikler ve tahrifatlar mevzuatta bir değişiklik yapılmaksızın geleneksel belgede sahtecilik suçuna konu olabileceklerdir. Güvenli elektronik imzalı olmayan elektronik belgeler TCK 244'teki suçu oluştururken güvenli

¹²² Keser Berber, L. (2011). Dijital Şirkete Geçmek İçin Sekiz Yasal Gerekçe, *Regesta Dergisi*. İstanbul Ticaret Odası. s.60.

e-imzalı belgelerde yapılan sahtecilikler TCK 204 vd. düzenlenen belgede sahtecilik suçlarını oluşturacaktır.

Buna karşılık Aile Hekimleri Kanunu'nun (AHK), 5.maddenin 3.fikrasında elektronik ortamda tutulan kayıtlar resmi evrak niteliğindedir denilmiş ancak güvenli elektronik imzadan hiç bahsedilmemiştir. Bu düzenleme doktrinde haklı olarak eleştirilmiştir¹²³. Nitekim güvenli elektronik imza ile imzalanmamış verilerin bütünlüğünün sağlanması noktası sorunludur. Böyle verilere resmi belge niteliği tanımak ise uygun değildir.

8. SONUÇ VE DEĞERLENDİRME

Bilişim sistemindeki veriler bakımından belgede sahtecilik hükümlerinin uygulanması halihazırdaki mevzuatla sadece güvenli elektronik imzalı e-belgeler bakımından mümkündür. Nitekim yukarıda değinildiği üzere birçok özel kanunda güvenli elektronik imzalar muteber kabul edilerek ıslak imzalı belgelerle çelişmeleri durumunda bu belgelerin geçerli kabul edilecekleri vurgulanmıştır. Diğer yandan güvenli elektronik imzalı olmayan elektronik verilerde yapılan sahtecilikler ancak TCK 244/2'de düzenlenen bilişim sistemindeki verileri tahrif etme suçuna sebebiyet verecektir. Bu duruma örnek verilecek olursa, failin nüfus kayıtlarının tutulduğu sisteme girerek gerçeğe aykırı verileri sisteme eklemesi veya

¹²³ Arslan, Baştürk, 2013, s. 215.

sistemdeki verileri tahrif etmesi halinde TCK 244/2’de düzenlenen bilişim sistemindeki verileri deęiştirme suçı oluşmuş olacaktır. Buradaki veriler eęer düzenleyeni belli olan (güvenli elektronik imzalı) bir e-belgede yapılan sahtecilikle tahrif edilmiş ise ancak o zaman ayrıca TCK 204 ve devamında düzenlenen belgede sahtecilik hükümlerine başvurulabilecektir.

Dięer yandan güvenli elektronik imza ile imzalanmamış bir elektronik veride yapılan sahteciliğin bir belge düzenlenmesine dayanak yapılması durumunda halihazırda belgede sahtecilik suçlarına gidilemeyecektir. Buna karşılık Adalet Bakanlığı Kanunlar Genel Müdürlüğü’nün hazırladığı yasa taslağı olumlu bir düzenleme yaparak ceza adaletinin sağlanmasına yönelik önemli bir adım atmıştır. Düzenlemeye göre elektronik ortamdaki bir veri güvenli elektronik imza ile imzalanmasa dahi sahte bir belge oluşumuna dayanak yapılmışsa bu verileri tahrif edenler hakkında ayrıca belgede sahtecilik hükümlerinden cezalandırma yapılabilecektir. Belirtmek gerekir ki ceza adaletinin sağlanması bakımından bu düzenlemenin yasalaşması ile uygulamacıların tereddütleri de giderilmiş olacak ve uygulamadaki önemli bir eksiklik kapanmış olacaktır.

Yasa tasarısı taslağı ile TCK 244’de düzenlenen bilişim sistemindeki verileri tahrif etme suçunun cezasının arttırılması ise doktrinin de üzerinde durduğu önemli bir adımdır. Gerçekten bilişim sistemindeki verilerin gelişen çağda önemine bakıldığı zaman bu

verileri tahrif edenler bakımından verilen cezalar adeta ödüllendirme olarak kabul edilmekteydi. Adalet Bakanlığı'nın hazırladığı tasarı taslağı bu sorunu çözmeye önemli bir adım olarak değerlendirilebilir.

KAYNAKÇA

- ACAR, A. E. (2013). Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Değeri, İstanbul: XII Levha Yayınları.
- ARSLAN, Ç. Baştürk, İ. (2013). Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler. Erciyes Üniversitesi Hukuk Fakültesi Dergisi. Cilt: 8 Sayı:2 2013/12.
- ARTUK, M. E., Gökçen, A., Yenidünya, A. C. (2008). Ceza Hukuku Özel Hükümler. Ankara: Turhan Kitabevi.
- ARTUK, M. E. Gökçen, A. Yenidünya, A. C. (2009). Türk Ceza Kanunu Şerhi. (5.Cilt). Ankara: Turhan Kitabevi.
- ASLAN, M. (2014). Vergilendirmede Elektronik Belgelerin Hukuki Geçerliliklerinin Değerlendirilmesi. Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi. Yıl:2. Cilt: 2. S:3
- BELGİN, D. (2009). Elektronik İmzalı Belgelerin Delil Değeri. Ankara Barosu Hukuk Gündemi Dergisi. 2009-2.
- DOĞAN, K. (2010). Ceza Hukukunda Belge Kavramı. Ceza Hukuku Dergisi. Aralık, 2010. Sayı: 14.
- DÜLGER, M. V. (2014). Türk Borçlar Kanunu, Türk Ticaret Kanunu ve Hukuk Muhakemeleri Kanunu'ndaki Bilişim Alanına İlişkin Düzenlemelerin Ceza Hukukuna Yansımaları. Ankara Barosu Dergisi. 2014/1.
- ERTURGUT, M. (2004). Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi. Ankara: Yetkin Yayınları.
- ERTURGUT, M. (2003). Elektronik İmza Kanunu Bakımından E-Belge ve E-İmza, Bankacılar Dergisi. Sayı 48.
- GÖKCAN, H. T. (2010). Özel Belgede Sahtecilik Suçu. Ankara Barosu Dergisi. Yıl: 68. Sayı: 2010/1.
- GÖKCEN, A. (2013). Belgede Sahtecilik Suçları. (Üçüncü Baskı). Ankara: Adalet Yayınevi.
- GÜNGÖR, D. (2010). Resmi Belgelerde Sahtecilik Suçu. Ankara: Yetkin Yayınevi.

- KESER Berber, L. (2000). “İmzalıyorum 0 Halde Varım” Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri. Türkiye Barolar Birliği Dergisi. 2000/2.
- KESER Berber, L. (2011). Dijital Şirkete Geçmek İçin Sekiz Yasal Gerekçe, Regesta Dergisi. İstanbul Ticaret Odası.
- KOCA, M. (2003). Avrupa Konseyi Siber Suç Sözleşmesi, Bilgi Toplumunda Hukuk Ünal Tekinalp’e Armağan, Cilt: III. İstanbul: Beta Yayınevi.
- OREL, G. (2011). Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezaî Sorumluluğu, Ankara: Adalet Yayınevi.
- ÖZGENÇ, İ. (2006). Türk Ceza Kanunu Gazi Şerhi. (Genel Hükümler). Ankara: T.C. Adalet Bakanlığı Eğitim Dairesi Başkanlığı.
- SOYASLAN, D. (2002). Ceza Hukuku Özel Hükümler (4. Bası). Ankara: Yetkin Yayınları
- TAMER, S. (2006). Teknik ve Hukuki Açından Elektronik İmza, Legal Hukuk Dergisi, Mart 2006, Sayı: 39
- TAŞDEMİR, K. Özkepir, R. (2009). 5237 Sayılı TCK’da Açıklamalı- İçtihatlı Sahtekarlık Suçları. Ankara: Turhan Kitabevi.
- TEKİN, N. (2014). Resmi Belgede Sahtecilik Suçunda Bazı Özel Durumlar, TAAD, Yıl:5 Sayı 19, Ekim 2014.
- TEZCAN, D., Erdem, M. R., Önok, R. M. (2013). Teorik ve Pratik Ceza Özel Hukuku (10.Baskı). Ankara: Seçkin Yayınevi.
- TOROSLU, N. (2010). Ceza Hukuku Özel Kısım. Ankara: Savaş Yayınevi.
- ÜNVER, Y. (2013). Üçüncü Yargı Paketinin Değerlendirilmesi. Marmara Üniversitesi Hukuk Araştırmaları Dergisi. Cilt: 19 Sayı: 2.
- ÜSTÜNER, A. (2013). Resmi Belgede Sahtecilik Suçu (Yüksek Lisans Tezi, Dicle Üniversitesi, 2013). Diyarbakır. s. 12. Gökcan, 2010.
- YILMAZ, Z. (2004). Gerekçe ve Tutanaklarla Yeni Türk Ceza Kanunu. Ankara, Seçkin Yayıncılık.

İnternet Kaynakları

www.kazanci.com

http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.54e896ab97eb94.07769200, Erişim Tarihi: 21.02.2015

UYAP Bilgi Sistemi

Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge

- <http://www.dildernegi.org.tr/TR,274/turkce-sozluk-ara-bul.html>, Erişim Tarihi: 30.7.2015
- <http://www.kgm.adalet.gov.tr/DUYURULAR/TASARI-alternatif%20%C3%A7%C3%B6z%C3%BCm%20y%C3%B6ntemleri.pdf>, Erişim Tarihi: 19.08.2015.
- <http://hakanalbayrak.blogspot.com.tr/2008/05/elektronik-belgelerin-delil-olarak.html>, Erişim Tarihi: 19.03.2015
- http://www.tk.gov.tr/bilgi_teknolojileri/elektronik_imza/eshs.php, Erişim Zamanı: 6.4.2015.
- <http://www.kararara.com/forum/viewtopic.php?f=44&t=19762>, Erişim Tarihi: 15.4.2015
- Keser Berber, L. Şekil ve Dijital İmza. http://enoter_hukuk.tripod.com/leyla-keser_berber.htm, Erişim Tarihi: 27.04.2015.
- <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
- <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf>
- <http://www.kgm.adalet.gov.tr/DUYURULAR/TASARI-alternatif%20%C3%A7%C3%B6z%C3%BCm%20y%C3%B6ntemleri.pdf>, Erişim Tarihi: 1.8.2015
- www.legalbank.net.
- <https://www.technopat.net/sosyal/konu/hash-nedir.3551/>, Erişim Tarihi: 30.08.2015