ELEKTRONİK İMZA KANUNUMUZ VE YENİ DÜZENLEMELER ÇERÇEVESİNDE DEĞERLENDİRİLMESİ

Electronic Signature Act and Its Assessment within the New Regulations

Prof. Dr. Yavuz KAPLAN*

ÖZET

Teknolojinin hızla geliştiği günümüz koşullarında artık ıslak imza olarak nitelendirdiğimiz imza biçimi de ihtiyaçlarımızı karşılayamaz hale gelmiştir. Teknoloji hız ve sınır tanımayan bir olgu olduğu için, bütün dünya insanları 20. yüzyılda ilk önce " internet" adı verilen dünya çapında ağ ile işlemlerini gerçekleştirmeye başlamış ve internet üzerinden ticaret, alış verişlerin yapılmaya başlanmasıyla ıslak imza yerine bilgisayar ortamında bir imzaya ihtiyaç duyulmuştur. Zaman içinde elektronik ortamda kimlik tespitini güvenli bir şekilde belirlemek için güvenilir bir mekanizmanın garanti edilmesi sağlanmıştır. Güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden söz etmek mümkün değildir. Böylece elektronik imza kavramı ortaya çıkmıştır.

Anahtar Sözcükler: Elektronik İmza, Islak İmza, Elektronik Haberleşme, Dijital İmza.

ABSTRACT

Rapid development of technology in today's wet signature is no longer sufficient to meet our needs has been described as the form of the signature. Technology is a case of speed and uninhibited, the 20th century from all over the world first century, "Internet", and started to perform operations with world-wide network called the trade on the internet, shopping, made the introduction of a computer-based wet signature instead of a signature is needed. When electronically in a secure way to determine the identification of a mechanism to ensure reliable provided. Without a secure signature of the method it is not possible to speak of a secure electronic communications. So the concept of electronic signature has emerged.

Keywords: Electronic Signature, Wet Signature, Electronic Communications, Digital Signature.

* Yeni Yüzyıl Üniversitesi Hukuk Fakültesi Özel Hukuk Bölüm Başkanı

I. GENEL OLARAK

Tarihin eski çağlarından bu yana insanlar karşılıklı ilişkilerinde imza kullanmaktadırlar. İmza, bir yandan kişinin kimliğini, diğer yandan da beyanda bulunma iradesini tespit eder. Böylece imzalayanın metni okuyup anladığı veya belgeyi bizzat hazırlayan kişi olduğu ve bağlanma iradesinin varlığı anlaşılır. İmza, bir yazının kimin tarafından yazıldığını veya içeriğinin kabul edildiğini belli etmek amacıyla metnin altına konulan isim veya işarettir[134]. Yaşanılan dönemin şartlarına göre çeşitli araçlarla örneğin tahtadan ya da metalden yapılmış mühürlerle ya da günümüzde ıslak imza olarak nitelendirilen kâğıt kalemle gerçekleştirilen imzalar kullanılmıştır. Teknolojinin hızla geliştiği günümüz koşullarında artık ıslak imza olarak nitelendirdiğimiz imza biçimi de ihtiyaçlarımızı karşılayamaz hale gelmiştir. Teknoloji hız ve sınır tanımayan bir olgu olduğu için, bütün dünya insanları 20. yüzyılda ilk önce "internet" adı verilen dünya çapında ağ ile işlemlerini gerçekleştirmeye başlamış[135] ve internet üzerinden ticaret, alış verişlerin yapılmaya başlanmasıyla ıslak imza yerine bilgisayar ortamında bir imzaya ihtiyaç duyulmuştur. Zaman içinde elektronik ortamda kimlik tespitinin güvenli bir şekilde tespitini sağlamak, diğer taraftan el yazısı ile imza yerine geçebilecek kadar güvenilir bir mekanizma kullanarak belgenin değiştirilmediğinin garanti edilmesi (bütünlük kontrolü) arayışlarına gidilmiş ve güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden söz etmek mümkün olmayacağından elektronik imza kavramı ortaya çıkmıştır.

Bankacılık, finans, sigortacılık, sanayi ve ticaret alanında artık zorunlu hale gelen elektronik imza konusu da ülke gündemine girmiş, kanun koyucular da bu konuda bir düzenleme yapma ihtiyacı hissetmişlerdir. Ve ülkemizde elektronik imzanın kullanımı için gerekli yasal çalışmalar, ilk kez 29 Haziran 2001 tarihinde Hazine Dış Ticaret Müsteşarlığı koordinasyonunda oluşturulan Hukuk Alt Çalışma Grubu tarafından başlatılmıştır. Adalet Bakanlığı, 14 Ocak 2002 tarihli yazısı yeni bir çalışma komisyonu kurarak kısa sürede *"Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı"* taslağını hazırlamış, taslak metnin hazırlanmasında 1999/93 sayılı *"Avrupa Birliği E-İmza Direktifi"*[136] ve bu Direktife göre yeniden ele alınan ve 22 Mayıs 2001'de yürürlüğe giren yeni Alman E-İmza Yasası[137] ile UNCITRAL[138] Model E-Ticaret Yasası[139]'ndan yararlanılmıştır. Söz konusu tasarı taslağı, 10 Eylül 2002 tarihli yazı ile kurumların görüşüne sunulmuş ve 19 Şubat 2003 tarihinde Başbakanlığa gönderilmiştir.

---

134 Mesut ORTA, Türkiye'de Elektronik İmza Uygulaması, Seçkin Yayınevi, Ankara 2005, s.25.

135 Yavuz KAPLAN, İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk, Seçkin Yayınevi, Ankara 2004, s.23; Leyla KESER BERBER: Şekil Ve Dijital İmza, http://www.hesy.de/sekil/SEKIL_VE_DIJITAL_IMZA.htm

136 "Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen" için bkz., http://eur-lex.europa.eu/Result.do?T1=V3&T 2=1999&T3=93&RechType=RECH_naturel&Submit=Suche, *ABl. L 13 vom 19.1.2000, S. 12–20.*

137 Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) için bkz., "Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876).

138 United Nations Commission on International Trade Law, Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu http://www.uncitral.org/uncitral/en/index.html

139 Bkz. http://translate.google.com.tr/translate?hl=tr&langpair=en|tr&u=http://cryptome.org/jya/mlec.htm&ei =4xb5UM2gOcv14QTN-4GoDA .

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiştir[140]. İkincil düzenleme çalışmaları Telekomünikasyon Kurumuna verildiğinden Kanunun verdiği altı aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır. Diğer taraftan ilk elektronik imza, 18 Temmuz 2005 tarihinde e-Dönüşüm Türkiye İcra Kurulu Başkanı Doç. Dr. Abdüllatif Şener tarafından kullanılmıştır.[141]

II. ELEKTRONİK İMZA VE DİGİTAL İMZA KAVRAMLARI

Elektronik imzanın, birçok detaylı tanımı yapılmış olsa da kısaca kişinin el yazısı ile attığı imzaya ait özellikleri elektronik ortamda gerçekleştirmek için, matematiksel formüller veya şifreleme programlar aracılığı ile yaratılan "sayısal" biçimdeki imza olarak tanımlanabilir. 13 Aralık 1999 tarihli Avrupa Birliği Direktifinde (m.2) elektronik imza, ***"başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan, kimlik teşhisine yarayan elektronik formda bulunan veriler"*** olarak tanımlanmıştır. Türk hukukunda da, elektronik imza tanımında Avrupa Birliği Direktifi esas alınarak bir tanım yapılmıştır. Buna göre, elektronik imza, ***"başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"*** şeklinde tanımlanmıştır (EİK m.3, b). Bir metni elektronik olarak imzalayabilmek için, çok basitten çok karmaşığa kadar uzanan bir seri çözüm mevcuttur. En basit çözüm kişinin kendi el yazısı ile attığı imzanın, scanner'den geçirilerek bilgisayara aktarılması ve hazırlanan metinlerin altına eklenmesidir. Ancak elektronik imza, "sayısal imza" ile sınırlı değildir. Biyometrik önlemleri içeren elektronik imzalar da vardır. Örneğin; kişilerin göz retinası, parmak izi ya da seslerinin kaydedilmesi sonucu elde edilen imzalar böyledir. Doğrudan dijital kalemle atılmış bir imza veya orijinal imzanın bir tarayıcından geçirilerek elektronik ortama aktarılmak suretiyle kullanılması da birer elektronik imza çeşididir. 5070 sayılı Elektronik İmza Kanunu'nda elektronik imzadan anlaşılması gereken ise sadece "Sayısal İmza"dır.

Bu konuda hazırlanışı en karmaşık ve fakat en güvenilir çözüm **Dijital İmza**'dır. Dijital imza, el yazısı ile atılan imzanın sahip olduğu özellikleri, elektronik belgeler bakımından da sağlamaya çalışan bir yöntemdir. Dijital ya da sayısal imza, nitelik olarak, tükenmez kalemle bir kâğıda atılan bildiğimiz imzadan farklı değildir. Yani hukuki bakımdan aynı sonucu doğururlar. Aralarındaki tek farkı, birinin kâğıt üzerinde olması, diğerinin de elektronik ortamda bulunmasıdır.

Şifreleme yöntemleri sayesinde, elektronik olarak imzalanan bir belgenin, sadece elektronik imzanın sahibi olan kimse tarafından düzenlendiği tespit edilebilmektedir. Dijital imzanın başkaları tarafından taklit edilmesi çok güçtür ve ayrıca dijital imzanın kaynağı da, yani imzanın kimin tarafından atıldığı da şüpheye yer bırakmayacak şekilde ispatlanabilmektedir. Sonuç olarak **dijital imza ≠ elektronik imza**.[142]

[140] 5070 sayılı Elektronik İmza Kanunu için bkz., RG.23 Ocak 2004-25355.

[141] www.tk.gov.tr(20.08.2005).

[142] Leyla KESER BERBER, Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi,http://www.imza.gen.tr/templates/resimler/File/makaleler/Elektronik_imzanin_Du-

Dijital imzanın kaynağının tespitinin daha kesin olduğu ve taklidinin zorluğu söylenebilse de, bu konuda kesin ifadeler kullanmaktan kaçınılmalıdır. Çünkü birçok şirketin web sayfalarının taklit edildiği, Hacker'lerin kol gezdiği internet ortamında, dijital imzanın % 100›e yakın bir garanti temin edeceğini söylemek mümkün değildir. Ancak, internetin güvenlik alt yapısının giderek daha da sağlamlaştırılması suretiyle bu konuda daha iyiye varılacağı söylenebilir.[143]

Dijital imzaya ilişkin olarak bilgi ağı üzerinde çözmemiz gereken dört sorun vardır:

1. GERÇEKLİK
2. ORİJİNALLİK
3. GÜVENİLİRLİK
4. DİJİTAL İMZANIN KAYNAĞINA İTİRAZ EDİLEMEMESİ

III. ÜLKEMİZDE ELEKTRONİK İMZAYA İLİŞKİN TEMEL DÜZENLEMELER VE YENİ GELİŞMELER

Ülkemizde elektronik imza konusunda mevcut yasal mevzuatı başta ve merkezde 5070 sayılı "Elektronik İmza Kanunu" yer almak üzere aşağıdaki şekilde sıralamak mümkündür:

1. 5070 Sayılı Elektronik İmza Kanunu
2. Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik (6 Ocak 2005 R.G. 25692)
3. Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (6 Ocak 2005 R.G. 25692)
4. Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ
5. Sertifika Mali Sorumluluk Sigortası Yönetmeliği, RG.26.08.2004-25565.
6. Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları, RG.27.01.2005-25709.
7. Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı, RG.27.01.2005-25709.
8. 2004/21 Sayılı Başbakanlık Genelgesi, RG.19.04.2006-26144,
9. Kamu Sertifikasyon Merkezine ilişkin 2006/20 sayılı Başbakanlık Genelgesi
10. Güvenli Elektronik İmza Oluşturma ve Doğrulama Uygulamaları ile Güvenli Elektronik İmza Formatlarına Dair Usul ve Esaslar, 01.06.2006 tarih ve 2006/DK-77/353 sayılı Kurul Kararı
11. Güvenli Elektronik İmza Oluşturma ve Doğrulama Uygulamaları ile Güvenli Elektronik İmza Formatlarına Dair Usul ve Esaslara İlişkin Kurul Kararında Değişiklik 02.07.2012 tarih ve 2012/DK-15/299 sayılı Kurul Kararı - Elektronik İmza Kullanım Profilleri Rehberi
12. Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Profilleri 18.04.2007 tarih ve 2007/DK-77/207 sayılı Kurul Kararı,
13. Nitelikli Elektronik Sertifika, SİL ve OCSP İstek/Cevap Profilleri Rehberi'nde Değişiklik 08.08.2012 tarih ve 2012/DK-15/374 sayılı Kurul kararı - Nitelikli

zenlenme si_Leyla_Keser .

[143] Leyla KESER BERBER, Şekil Ve Dijital İmza Ankara 2001, http://www.hesy.de/sekil/SEKIL_VE DIJITAL_IMZA.htm.

Elektronik Sertifika, SİL ve OCSP İstek/Cevap Mesajları Profilleri Dökümanı,

14. İşlem Sertifikasına İlişkin Usul ve Esaslar 06.06.2012 tarih ve 2012DK-15259 sayılı Kurul Kararı.

A. TEMEL KAYNAK OLARAK 5070 SAYILI ELEKTRONİK İMZA KANUNU

Kanun yürürlük hükümleriyle birlikte 26 maddeden ve dört kısımdan oluşmuştur.

I. Kısım: Amaç, kapsam ve tanımlar
II. Kısım: Güvenli elektronik imza ve sertifika hizmetleri
III. Kısım: Denetim ve ceza hükümleri
IV. Kısım: Çeşitli hükümler

Kanunun ikinci kısmının birinci bölümünde güvenli e-imza ve güvenli e-imza araçları düzenlenmektedir. Güvenli e-imza tanımı yapılırken, e-imza tanımından hareket edilmiş ve e-imza kavramına dört unsur eklenmiştir. Bu unsurlar 1999 tarihli Avrupa Birliği direktifinden alınmıştır[144]. Kanunun getirdiği bir kısım yeni kavramlar ve elektronik imzaya yüklediği işlev ve yararların üzerinde durulmasında yarar bulunmaktadır. Nitekim bu misyon diğer temel kanunlarda da yeni bir kısım düzenlemelerin yapılması zorunluluğunu da beraberinde getiren bir önemi haizdir.

1. Güvenli Elektronik İmza ve Araçları

Türk hukukunda, "güvenli elektronik imza" kavramı tercih edilmiştir. 5070 Sayılı Elektronik İmza Kanununun 4. maddesine göre;

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 yapılıp yapılmadığının tespitini sağlayan elektronik imzalar güvenli elektronik imzadır.

Avrupa Birliği Direktifinde gelişmiş elektronik imza tanımının unsurları olan dört unsur, hukukumuzda güvenli elektronik imzanın unsurları arasında belirtilmiştir. Bu şekilde hukukumuzda gelişmiş elektronik imza şeklinde bir ayırım yapılmamıştır. Güvenli elektronik imza, Avrupa Birliği Direktifinde belirtildiği üzere el yazısıyla imzaya eşdeğer sayılacak ve yargılamada caiz delil olarak kullanılacaktır. Hukukumuz açısından bu hususların gerçekleştiği söylenmelidir. Zira Elektronik İmza Kanununda, güvenli elektronik imza, el yazısıyla imzaya eşdeğer kabul edilmiş (m. 5 ve 22) ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir (m. 23).

Güvenli elektronik imzaların önemi elle atılmış imza ile aynı sonucu doğurmalarıdır.

Yabancı mevzuatta bu hukuki etkiye sahip elektronik imzalar çeşitli adlarla (ka-

144 Halûk KONURALP, TBB tarafından 4 Mart 2004 tarihinde Düzenlenen " Elektronik İmza Kanunu " Konulu Konferans Sunumları için bkz., http://www.tbb.org.tr/turkce/konferans.htm (23.10.2007).

lifiye, üniversal e-İmza gibi) ve farklı teknik gereksinimlerle tanımlanmıştır. Ancak bütün bu imzaların ortak noktası, nitelikli sertifikaya dayanarak ve güvenli elektronik imza oluşturma aracıyla oluşturulmuş olmalarıdır. Kanunda yapılan tanım, 13 Aralık 1999 tarihli Avrupa Birliği Direktifi m.2/2-a da yer alan ileri elektronik imza tanımında belirtilen bazı gereksinimler ile m.5/1'de belirtilen gereksinimlerin birleştirilmesi sonucu oluşturulmuştur. Böylece Direktifin ortaya koyduğu elektronik imza sınıflandırılmasından (elektronik imza, ileri elektronik imza, elle atılmış imza ile aynı hukuki etkiye sahip imza [nitelikli imza]) ayrı bir sınıflandırılmaya gidilmiştir.

Genel olarak bir değerlendirme yapacak olursak; güvenlikle ilgili her endişe bilimsel bilginin boyutuna göre teknik olarak belirlenebilir. Bunun hukuki boyutu çok ayrıntılı düşünülemez. Hukuki düzenleme genel çerçeveyi ortaya koyabilir. Bilimsel bilgi birikimi düzeyinde, bilim adamları ve uzmanların görüşleri doğrultusunda yönetmelikler hazırlanacaktır. Düzenlemeler bu bilimsel veriler ışığında yapılacaktır. Güvenlik konusu da ileride ortaya bir sorun çıkması halinde yine bilimsel bilgi birikimi çözebiliyorsa buna göre düzenleme yapacaktır.

Sonuç olarak risk her zaman olacaktır. Bilimsel bilgi geliştikçe hukuk da buna uygun olarak gelişecektir.

Kanunumuzda sadece elektronik imza ve güvenli elektronik imza ayrımı vardır.[145] Kanunumuzdaki "Güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur" ifadesi AB Direktifi m.5/1'e uygundur. AB Direktifi m. 5/2'ye göre üye devletler elektronik imzanın;

a)Elektronik formda olması,

b)Nitelikli sertifikaya dayanmaması,

c)Akredite edilmiş bir sertifika hizmet sağlayıcının sağladığı sertifikaya dayanmaması,

d)Güvenli elektronik imza oluşturma aracı ile oluşturulmamış olması, nedenlerinden biriyle delil niteliğini yadsıyamazlar. Direktifin bu hükmü Kanunumuza alınmamıştır. Oysa Direktifin ve dünyadaki diğer elektronik imza kanunlarının amacı elektronik imzalara hukuki bir çerçeve çizmek ve elektronik imzanın delil değerini ortaya koymaktır. Bu sebeplerden dolayı Avusturya'da olduğu gibi hukuki sonuç kısmına yukarıda sayılan sebeplerden birinin bulunmasına rağmen elektronik imzanın delil niteliği inkâr edilemez kısmı eklenmelidir.

2. Elektronik İmzanın Hukuki İşlevi ve Yararları

İşlev olarak elektronik imza, elle atılan imzaya eşdeğer nitelikte kullanılabildiği için, elektronik ortamda her türlü resmi işlemin, kâğıt ortamına göre daha hızlı, güvenilir ve maliyet etkin biçimde yürütülmesini sağlar.

Evlenme, veraset ve intikal, gayrimenkul, oto alım satımı, teminat sözleşmeleri gibi şahit veya merasim gerektiren işlemler elektronik imza ile gerçekleştirilememektedir.

Elektronik imzanın yararlarını ise, kısaca şu başlıklar altında özetlemek mümkündür:

1- Bir kullanıcı tarafından gönderilen bilgilerin ve verilerin kesinlikle o kişi ta-

[145] Tuğrul SEVİM, Türkekul Hukuk Bürosu Teknoloji Hukuku Bölümü, II. Türkiye Bilişim Şurası Hukuk Çalışma Grubu Elektronik İmzanın Hukuksal Boyutları Mevcut Durum, Eksiklikler ve Çözüm Önerileri, 5070 Sayılı Elektronik İmza Kanunu, Avrupa Birliği 99/93/EC Sayılı Konsey Komisyon Direktifi ve Karşılaştırmalı Hukuk Çerçevesinde Bir İnceleme, Mart 2004 İstanbul.

rafından gönderildiği teyit eder. Kısacası, başkası tarafından gönderilmediğini garanti eder. Dolaysıyla, klasik imzadaki gibi taklit edilme olasılığı da ortadan kalkar. Gönderici göndermediğini, alıcı da almadığını iddia edemez.

2- Bir kullanıcı tarafından gönderilen bilgilerin veya verilerin bir başkasının eline geçmesini veya değiştirilmesini engeller.

3- Gönderilen bilgi ve verilerin içeriği, gönderici tarafından veya alıcı tarafından inkâr edilemez. Çünkü değil başkası, kendileri dahi gönderimden sonra içeriğini değiştiremez. Kaldı ki, uyuşmazlık halinde elektronik belgenin bir kopyası da onay kurumundadır.

4- Gönderilen verilerin tarih açısından tespitini sağladığı gibi, arşivleme kolaylığı sağlar.

5- Gönderilen verilen çabuk ulaşmasını sağlar, baskı, kâğıt, posta ve arşivleme maliyetlerini en aza indirir.

B. TEMEL YASALARDAKİ DEĞİŞİKLİKLERLE GETİRİLEN YENİ DÜZENLEMELER

Yeni Türk Borçlar Kanunu'nun[146](TBK) 14/I. maddesi, **"Yazılı şekilde yapılması öngörülen sözleşmelerde borç altına girenlerin imzalarının bulunması zorunludur."** ifadesiyle imza zorunluluğundan söz ettikten sonra, 14/II. maddesi **"Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer."** düzenlemesiyle güvenli elektronik imzayı yazılı şekil şartının gerçekleşmiş sayılması için yeterli görmüştür.

TBK'nun 15/I. maddesi ise, **"İmzanın, borç altına girenin el yazısıyla atılması zorunludur. Güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğurur"**[147] düzenlemesiyle güvenli elektronik imzaya vurgu yapmıştır[148]. Bu durumda, Elektronik İmza Kanununun 5. maddesindeki istisnalar dışında her türlü hukuki işlem güvenli elektronik imza ile oluşturulabilecektir. Elektronik İmza Kanunun 5. maddesinin II. fıkrası şöyledir: **"Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez"**.

TBK'nın 15/II. maddesinde yer alan **"İmzanın el yazısı dışında bir araçla atılması, ancak örf ve âdetçe kabul edilen durumlarda ve özellikle çok sayıda çıkarılan kıymetli evrakın imzalanmasında yeterli sayılır."** ifadesi ise, imzanın bir araç kullanılarak atılmasının da güvenli elektronik imzanın üretilmesi bakımından geçerli olacağını teyit etmektedir.

Yeni Hukuk Muhakemeleri Kanunu'nun[149] (HMK) "Adi senetlerin ispat gücü"

146 11.01.2011 kabul tarihli ve 6098 sayılı yeni Türk Borçlar Kanunu için bkz., RG.04.02.2011-27836.

147 5070 sayılı Elektronik İmza Kanununun 22. maddesiyle, mülga Borçlar Kanununun 14. maddesinin birinci fıkrasına eklenen benzer cümle şöyleydi: "Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir".

148 Elektronik İmza Kanunun 5. maddesinde yer alan **"Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir."** cümlesine paralel olarak, aynı Kanunun 22. Maddesi, yürürlükten kalkan 22.4.1926 tarihli ve 818 sayılı Borçlar Kanununun 14. maddesinin birinci fıkrasına da **"Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir"** cümlesinin eklenmesini öngörmüştü. Bu hüküm, önceki BK. m. 14'deki **"imza elle atılmalıdır"** şartına bir istisna getirmişti. Benzer düzenleme TBK'da da yer almıştır.

149 12.01.2011 kabul tarihli ve 6100 sayılı HMK için bkz., RG.04.02.2011-27836.

başlığını taşıyan 205. maddesinin (2). bendi **"Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir."** demek suretiyle elektronik imzanın delil olarak kabul edildiğini ifade etmiştir[150].

Aynı maddenin (3). bendi ise, **"Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler."** demek suretiyle güvenli elektronik imzanın varlığının tespiti görevini hâkime re'sen yüklemiştir.

Güvenli elektronik imzalı belgenin inkârı başlığını taşıyan HMK'nın 210. maddesi ise, **"Güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur"** hükmünü getirmek suretiyle önceki HUMK m.308'de öncelikli yol olarak sunulan imza inkarı durumunda **"hâkim, imza incelemesi esnasında imzayı inkar eden tarafa kendi önünde yazı yazdırır veya imza attırır, daha sonra da o kişi tarafından imzalandığı kesin olan diğer belgeler ile bu imzayı karşılaştırır. Eğer bu şekilde bir sonuca varamaz ise bilirkişiye başvurur"** şeklindeki düzenlemenin elektronik imzanın incelenmesi bakımından uygulanmasının mümkün olmadığını göz önünde bulundurarak doğrudan bilirkişiye gitme yöntemini isabetli olarak benimsemiştir.

Ulusal Yargı Ağı Bilişim Sistemi (UYAP) çerçevesinde de HMK'nın "Elektronik İşlemler" başlığını taşıyan 445. maddesi ile düzenlemeler yapılmıştır. Özellikle (2). bendi ile güvenli elektronik imza ile dava açılabileceğini, belgelerin gönderilebileceğini ve bu suretle gönderilen belgelerin orijinallerinin ayrıca fiziki olarak gönderilmesine gerek bulunmadığını ifade eden maddenin tamamı aşağıdaki gibidir:

MADDE 445- (1) Ulusal Yargı Ağı Bilişim Sistemi (UYAP), adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bilişim sistemidir. Dava ve diğer yargılama işlemlerinin elektronik ortamda gerçekleştirildiği hâllerde UYAP kullanılarak veriler kaydedilir ve saklanır.

(2) Elektronik ortamda, güvenli elektronik imza kullanılarak dava açılabilir, harç ve avans ödenebilir, dava dosyaları incelenebilir. Bu Kanun kapsamında fizikî olarak hazırlanması öngörülen tutanak ve belgeler güvenli elektronik imzayla elektronik ortamda hazırlanabilir ve gönderilebilir. Güvenli elektronik imza ile oluşturulan tutanak ve belgeler ayrıca fizikî olarak gönderilmez, belge örneği aranmaz.

(3) Elektronik ortamdan fizikî örnek çıkartılması gereken hâllerde tutanak veya belgenin aslının aynı olduğu belirtilerek hâkim veya görevlendirdiği yazı işleri müdürü tarafından imzalanır ve mühürlenir.

(4) Elektronik ortamda yapılan işlemlerde süre gün sonunda biter.

(5) Mahkemelerde görülmekte olan dava, çekişmesiz yargı, geçici hukuki koruma ve diğer tüm işlemlerde UYAP'ın kullanılmasına dair usul ve esaslar yönetmelikle düzenlenir.

[150] 5070 sayılı Kanun yeni HMK yürürlüğe girmeden önce, 23. maddesiyle, elektronik imzanın usul hukukundaki yerini Hukuk Usulü Muhakemeleri Kanununun 295. maddesinden sonra getirilen 295/A maddesiyle açıklığa kavuşturmuştu. Bu maddeye göre, **"Elektronik veriler, usulüne göre güvenli elektronik imza oluşturulmuş ise senet hükmündedir ve aksi ispat edilinceye kadar kesin delil sayılırlar. Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, HUMK'un 308. maddesi kıyas yoluyla uygulanacaktır."** ibaresi eklenmişti.

IV. ELEKTRONİK İMZA PROSEDÜRÜ İÇİN GEREKLİ TEKNİK ALT YAPI

Dijital imzanın hazırlanması matematiksel olarak karmaşık bir prosedürü gerektirse de, kullanıcı için bilgisayarda hazırladığı bir mesajı imzalamak gayet basittir. Kısaca açıklamak gerekirse; göndermek istenilen mesaj hazır ise, bilgisayar ekranındaki *"imzala"* komutunu klikledikten sonra, " *imza anahtarını yerleştir* " komutu görülür ve bunun için, bir onay makamının veya sertifika kurumdan (Trust Center, Certifikation Authorities) alınmış chip kartını, kart okuyucuya soktuktan sonra işin geri kalan kısmını bilgisayarın kendisi halletmektedir.

Dijital imzanın tasdik edilmesi de karmaşık bir işlem niteliğinde değildir. Bunu da bilgisayarın kendisi otomatik olarak yapmakta ve sonucu göstermektedir. Bu işlem sırasında aynı zamanda sertifika yardımıyla açık anahtarın doğruluğu da kontrol edilmiş olmaktadır.

Bir belgeyi elektronik olarak imzalayabilmek için, kullanıcıların, bir Onay Makamının veya - daha sık kullanılan İngilizce karşılığı ile *"Trust Center"*ın hizmeti yanında teknik bir alt yapıya da sahip olması gerekir. Kullanıcının bir bilgisayarı ve kendine ait bir yazılım programının mevcut olması gerekir. Kullanıcının ayrıca bilgisayar üzerinden yapacağı işlemlerde kullanacağı bir de şifresinin olması gerekir. Bu şifre, aşağıda tekrar değineceğimiz üzere, ya yazılım (software) programları vasıtasıyla veya akıllı kart (SmartCard) olarak da adlandırılan Chip kartlar kullanılarak elde edilebilir. Chip Kartların çalınması veya kaybedilmesi durumunda, eğer kullanıcı bu durumu fark ederse, aynen kredi kartları uygulamasında olduğu gibi, Chip Kart Dağıtım Merkezine yapılacak bildirim ile, kart derhal bloke edilecektir.

Dijital imza, bir datanın üçüncü kişiler tarafından görülüp değiştirilmesi tehlikesini önlemeye yaramaktadır. Bu tür mesajı yüklemek, okumak ve değiştirebilmek, sadece şifre ve giriş kodunu (Password) kullanmak hakkına sahip olan kimseye aittir. Eğer şifre ve giriş kodu sahibi, bir başka kimseye gönderdiği mesajı okuma yetkisi vermek isterse, bu kişiye anahtar kelimeyi bildirmek zorundadır. Sistemin güvenilir bir şekilde işlemesi, her iki anahtarın uzunluğuna ve gizli şifrenin kullanıcı tarafından iyi saklanmasına bağlıdır. İmzalama aşamasında söz konusu olan karmaşık matematik işlemlere rağmen, yukarıda da değindiğimiz gibi prosedür kullanıcı için oldukça kolaydır. Kullanıcı chip kartını, gizli şifresi ile birlikte sürücüye soktuktan sonra, sadece " *imzala* " komutuna mouse ile dokunması yeterli olmaktadır. Bundan sonraki bütün işlemleri bilgisayar halletmektedir. Bir mesaj dijital imza ile tasdik edilirse, bu mesajın artık başkaları tarafından değiştirilmesi güç olacaktır. Değiştirilmesi imkânsız değildir, sadece bu tür değişiklikleri yapmak güçtür[151].

A. Şifreleme Yöntemleri

Bir metni dijital olarak imzalamak için bugün farklı yöntemler kullanılmaktadır. Bunlardan günümüzde en yaygını, şifreleme esasına dayanan yöntemlerdir.

Eski çağlarda kullanılan şifreleme yöntemleri, bugün modern bilgi teknolojisi alanında yeniden önem kazanmıştır. Kriptografik algoritmalar sadece mesajın şifrelenmesinde değil, aynı zamanda dijital imzanın hazırlanmasında ve kontrol

[151] KESER BERBER, Şekil Ve Dijital İmza, http://www.hesy.de/sekil/SEKIL_VE_DIJITAL_IMZA.htm.

edilmesinde de kullanılmaktadır.

Şifrelemenin temel amacı, herkesin okuyabileceği bir açık metinden, şifreleme yoluyla sadece istenilen bir veya birkaç kişinin okuyabileceği gizli bir metin yaratmaktır. Alıcı bu şifrelenmiş metni daha sonra ilk şekline çevirecek, yani deşifre edecektir. Şöyle ki:

(Açık Metin) - Şifreleme - (Gizli Metin)

(Gizli Metin) - Şifreleme - (Açık Metin)

Günümüzde kullanılan şifreleme yöntemlerinde farklı matematiksel metotlardan hareket edilmektedir. Dijital imza hizmeti sunan kuruluşlar ve kullanıcılar, işlemlerinde hangi yöntemi kullanacaklarını serbestçe kararlaştırabilirler.

Başlıca yöntemler arasında;

- **Data Encryption Standard (DES)**
- **International Data Encryption Algoritm (IDEA)**
- **RSA**
- **ElGamal ve DSA**

Bugün kullanılan diğer yöntemler arasında; faktör analizi, saklı logaritma ve eliptik eğriler sayılabilir . Güncel yöntemler arasında yer alan ve aşağıda ayrıntılı olarak değinilecek olan Simetrik ve Asimetrik şifreleme yöntemlerinde ise, parametrik metotlar ailesi söz konusudur. Seçilen parametre, şifre olarak da adlandırılır ve bu şifrenin birbiri ile haberleşen kişiler tarafından tamamen veya kısmen gizli tutulması gerekir. Şifrenin yetkili olmayan kişiler tarafından, bilgisayar yardımıyla kolayca bulunamaması için, parametrenin veya şifrenin yeteri kadar büyük olması gerekir. Modern şifreleme yöntemlerine; **Güvenilirlik** *(belgenin içeriği sadece bu konuda yetkili olan kimseler tarafından okunabilmelidir)*, **Orijinallik** (belgenin içeriği düzenleyen kimse fark etmeden değiştirilememelidir), **Gerçeklik** *(belgeyi düzenleyen kişinin, yani belgenin sahibinin kim olduğu tespit edilebilmelidir. Başka hiç kimse kendisini, belgeyi düzenleyen kişi olarak tanıtamamalıdır)*, **Bağlayıcılık** *(Belgeyi düzenleyen kişi, bu belgeyi düzenlemediği yolunda itirazda bulunamamalıdır)* ve bazı durumlarda **Anonimliğin** (*bu kavramla mesajın içeriğinin güvenilirliği değil, aksine haberleşme şeklinin güvenilirliği kastedilmektedir*) sağlanması yönünde talepler yöneltilmektedir.

1. Simetrik ve Asimetrik Şifreleme Yöntemleri, Gizli ve Açık Şifre

Şifreli haberleşme yapılmadan önce, bir veya bir çok şifrenin hazırlanmış olması gerekir. Şifrenin hazırlanması ise farklı tarz ve şekillerde söz konusu olabilir. Örneğin ya yazılım (software) programları vasıtasıyla veya akıllı kart (Smart Card) olarak da adlandırılan Chip Kart'lar kullanılarak şifre elde edilebilir.

a. Simetrik Şifreleme Yöntemi

Simetrik şifreleme yönteminde; şifreleme ve deşifre işlemi için, aynı şifre kullanılır. Örneğin; A ile B arasında haberleşmenin güvenli bir biçimde gerçekleşebilmesi için, şifrenin sadece birbiri ile haberleşen taraflarca bilinmesi, bunun dışındaki kimselere karşı ise mutlak bir şekilde saklı tutulması gerekir. Bir haberleşmeye ikiden çok kimse katılıyorsa, bu durumda tüm katılanlar şifreyi öğrenmiş olacaklardır. Bu durum ise, birbiri ile haberleşen tarafların, yetkili olmayan bir kimse tarafından şu ya da bu şekilde şifrenin öğrenilemeyeceğine inanarak nasıl haberleşecekleri sorununu ortaya çıkarmaktadır.

Bu konuda birçok olasılık söz konusu olabilir:

• ***Elektronik olmayan yoldan şifre değişimi:***

Taraflar, haberleşme işlemine başlamadan önce örneğin; posta yoluyla şifreyi birbirlerine gönderebilirler. Ancak bu olasılık, haberleşmek isteyen tarafların birbirini tanıması şartıyla kullanılabilir.

• **Örnek bir şifre ile elektronik yoldan şifre değişimi:**

Haberin şifreleneceği şifre, gönderilmek istenen mesaj ile birlikte, örnek bir şifre yardımıyla şifrelenmektedir. Şüphesiz bu örnek şifrenin de, haberleşmeden önce taraflar arasında değişiminin yapılması gerekir. Bu yöntem de, haberleşen tarafların birbirlerini önceden tanımalarını gerektirmektedir.

• ***Hybrid*** **yöntemi ile şifre değişimi:**

Hem simetrik hem de asimetrik şifreleme yönteminde kullanılabilen bu yönteme göre; asıl mesaj, tesadüfen yaratılan bir şifre ile şifrelenir. Bu şifre, toplantı şifresi (Session Key) olarak da adlandırılır. Daha sonra bu mesaj, alıcının açık şifresi (Public Key) yardımıyla şifrelenir. Alıcı, sadece kendisi tarafından bilinen gizli şifresi (Private Key) yardımıyla, mesajın toplantı şifresini açar ve bu şifre yardımıyla mesajı deşifre edebilir.

b. Asimetrik Şifreleme Yöntemi

Birbiri ile haberleşen iki kişi arasındaki, asimetrik şifreleme yöntemi şöyle açıklanabilir: Burada haberleşen her bir taraf, biri açık, diğeri ise gizli veya özel olmak üzere, yöndeş bir çift şifreye sahiptir. Bu durumda örneğin; A, B'ye bir mesaj yollamak isterse, bu mesajı şifrelemek için, B'nin aleni olarak ulaşılabilen açık şifresini kullanacaktır. B, şifreli mesajı aldıktan sonra, mesajı deşifre etmek için kendi gizli şifresini kullanacaktır. Tam tersi durum, yani bu sefer B'nin, A'ya mesaj yollaması da aynı şekilde gerçekleşecektir. Buna göre, asimetrik şifreleme yönteminde önemli olan herkesin kendi açık şifresini aleni olarak ulaşılabilir kılmasıdır. Asimetrik şifreleme yöntemlerinden RSA şifreleme yönteminde bir anahtar örneğin; 1024 bit'ten oluşmaktadır. Bu yaklaşık 300 haneli bir ondalık sayıya eşittir. Burada en büyük problem şüphesiz açık şifrenin belirli bir kişiye ait olup olmadığı hususudur. Bu yüzden, belirli bir açık şifrenin belirli bir kişiye yüzde yüz ait olduğunun garanti edilmesi gerekir. Bu problemle Onay Makamı veya Trustcenter veya Certification Authorities olarak adlandırılan kurumlar uğraşmaktadır. Asimetrik şifreleme yöntemlerinin güvenilirliği, her şeyden önce gizli şifrenin kullanıcı tarafından iyi saklanmasına ve anahtar uzunluğuna bağlıdır.

2. Elektronik İmza İçin Gerekli Teknik Alt Yapı

Birbiriyle dijital imzayı kullanarak haberleşmek isteyen iki tarafın bunun için iyi bir organizasyon ve sağlam bir alt yapıya sahip olması gerekmektedir.

- **Sistemin kendi içinde işleyişini sağlamak için yeknesak yöntemlerin (algoritmalar, bilgisayar programları vs.) kullanılması gerekmektedir.**

- **Elektronik haberleşmesinin hukuki açıdan bağlayıcılığını düzenleyecek Yasa, yönetmelik ve tebliğlerin düzenlenmesi gerekmektedir.**

- **Sertifika makamları, Trustcenter'lar, Kart Dağıtım Kurumları gibi merkezi görevleri yerine getirecek olan (örneğin; kullanıcıların kaydedilmesi, gizli ve açık anahtarların ve sertifikaların hazırlanması, güven zinciri adı verilen ilişkinin yürütülmesinin sağlanması gibi) üst kuruluşların oluşturulması gerekmektedir.**

a. Elektronik İmza Kapsamında Bazı Kavramlar

aa) İmza oluşturma verisi: "İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler"dir. Tanım Direktifin çevirisi şeklindedir ve yabancı mevzuatta aynı şekilde tanımlanmıştır. Bu tanım uygulamada "private key" olarak bilinen özel veya kapalı anahtarı belirtmektedir. İmza oluşturma verisinin tanımı teknoloji bağımsız bir yöntemle yapılmıştır, konuyla ilgili teknik gereksinimler [anahtar uzunluğu, hash değer, rasgele oluşturma kalitesi (random creation quality)] yönetmelikle düzenlenmelidir. Uygulamada imza oluşturma verisi hem hizmet sağlayıcı tarafından hem de sertifika sahibi tarafından oluşturulabilmektedir.

bb) İmza doğrulama verisi: "Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler" dir. Bu tanım uygulamada "public key" olarak bilinen açık anahtarı belirtmektedir. Tanım Direktifin çevirisi şeklindedir ve yabancı mevzuatta da aynı şekilde tanımlanmıştır.

cc) İmza oluşturma aracı: "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı"dır. Bu tanım da Direktifin çevirisidir ve yabancı mevzuatlarda da aynı şekilde tanımlanmıştır. Uygulamada imza oluşturma araçları smart kartlar veya bilgisayar yazılımları olarak karşımıza çıkabilmektedir. Kart teknolojisi, kart ve kart okuyucularının maliyeti sebebiyle daha masraflı olmasına rağmen bilgisayardan bağımsız çalışması nedeniyle elektronik imza kullanımını kolaylaştırmakta ve yaygınlaştırmaktadır.

Kanun gereği güvenli elektronik imza oluşturma araçları;

—Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,

—Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,

—Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,

—İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini sağlayan imza oluşturma araçlarıdır.

dd) İmza doğrulama aracı: "Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı"dır. Bu tanım da Direktif'in çevirisidir ve yabancı mevzuatlarda da aynı şekilde tanımlanmıştır. Güvenli elektronik imza doğrulama araçları ise

- İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,
- İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,
- Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,
- İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğ-

rulama yapan kişiye gösteren,

- İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,
- İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan, imza doğrulama araçlarıdır.

ee) Zaman Damgası: Kanuna göre zaman damgası "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt"tır. Direktifte zaman damgasının tanımı yapılmamıştır. Alman[152] Elektronik İmza Kanunu'nda yapılan zaman damgası tanımı Kanunumuzdaki ile örtüşmektedir. Ancak bu elektronik imza düzenlemesinde, tanımlar dışında da zaman damgasının teknik gereksinimleri ve zaman damgası hizmeti veren hizmet sağlayıcıların yükümlülükleriyle ilgili hükümler bulunmaktadır. Kanunumuzda yönetmelikle düzenlenecek hususlar belirtildiği (m.20) ve bunların içinde zaman damgası bulunmadığı için, zaman damgası yönetmelikle ayrıntılı olarak düzenlenemeyecektir. Ancak hizmet sağlayıcıların yükümlülükleri yönetmelikle düzenleneceği için bunlarla birlikte zaman damgası ile ilgili teknik gereksinimler de düzenlenebilir.

ff) Elektronik Sertifika: Kanun'a göre elektronik sertifika "İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt"tır. Bu tanım Direktifteki ve yabancı mevzuatlardaki sertifika tanımlarına uygundur. Elektronik sertifikalar, imzalama-doğrulama işlemi sırasında imzalayanın kimliğinin güvenilir üçüncü taraf (sertifika hizmet sağlayıcısı) tarafından teyit edilmesi amacıyla kullanılırlar.

gg) Elektronik İmza Ürünleri: Kanunumuzda yer almayan ama direktifte ve yabancı mevzuatta yer alan bu tanım, sertifika hizmet sağlayıcıları tarafından elektronik imza servisleri için kullanılan veya e-İmza doğrulama veya oluşturma için kullanılan donanım, yazılım ve ilgili bileşenleri belirtmektedir. Buna göre elektronik imza ürünleri Direktif Ek 2/f, 3 ve 4 de yer alan araçlardır. Ek 2/f ve 3'de hizmet sağlayıcıların sertifika hizmeti sırasında kullanacakları araçlar ile imza oluşturma araçlarının gereksinimleri sayılmıştır. Nitelikli sertifika üretmek veya güvenli elektronik imza oluşturmak için burada bahsedilen teknik gereksinimlere uyulması zorunludur. Direktifin 3/5 m.'sine göre Komisyon bu eklerde belirtilen gereksinimlerin yerine geçmek üzere genel olarak tanınmış teknik standartları referans gösterebilir, bu standartları yerine getiren sertifika hizmet sağlayıcıları eklerdeki gereksinimleri yerine getirmiş sayılır. Komisyon bu maddeye dayanarak 13 Temmuz 2003'te aldığı bir kararla bazı standartları referans göstermiştir. Bu standartlara uyan sertifika hizmet sağlayıcıları ve imza oluşturma üreticileri/dağıtıcıları Eklerdeki gereksinimleri yerine getirmiş sayılacaklardır. Komisyon, kararında Avrupa Standardizasyon Komitesinin konuyla ilgili standartlarını referans göstermiştir.

hh) İhtiyari Akreditasyon: Sertifikasyon hizmeti sunulmasıyla ilgili tüm hak ve yükümlülükleri belirleyen, ilgili sertifikasyon hizmeti sunucusunun isteği üzerine bu hak ve yükümlülüklerin geliştirilmesi ve denetimi ile ilgili kamu ya da özel nitelikli kurum tarafından verilen ve sertifikasyon hizmeti sunucusunun bu izin-

[152] Alman "SigG" m. 2/15.

den kaynaklanan haklarını kullanmasına ilgili kararın kendisine ulaşmasına dek engel olan her türlü düzenleme ve karardır.

ıı) **Öz Değeri (Hashwert):**Bilgisayar terminolojisinde *"Hash (= Öz)"*; yazılan bir mesajın, kısaltılmış şeklidir. Dijital imza, bilginin doğruluğunu korumaktadır. Teknik açıdan dijital imza, imzalanmış belgenin özünü *(Hash)* içerir. İçerikte yapılacak herhangi bir değişiklik dijital Hash'ı geçersiz kılacaktır.

V. ELEKTRONİK SERTİFİKA, ELEKTRONİK SERTİFİKA HİZMET SAĞLAYICISI

A. Elektronik Sertifika, Nitelikli Elektronik Sertifika

Nitelikli elektronik sertifikalar, kanunlar veya yönetmeliklerle belirlenmiş, bazı ek teknik gereksinimleri sağlayan ve sertifika sahibinin ek kişisel bilgilerini içeren elektronik sertifikalardır. Direktif Ek 1'de nitelikli (kalifiye) sertifikanın şartları sayılmıştır. Yabancı mevzuatta ve Kanunumuzda nitelikli elektronik sertifika tanımı Direktif Ek 1'in çevirisi şeklindedir. Ancak yabancı mevzuatta nitelikli sertifika tanımı yapılırken, sertifikanın nitelikli sertifika verme şartlarını yerine getirmiş bir sağlayıcı tarafından verilmesi zorunluluğu getirilmiştir[153]. Bizde böyle bir zorunluluk bulunmamaktadır. Bu şekilde bir ekleme, hem hangi sertifikaların nitelikli sertifika olduğunu anlamayı kolaylaştıracak, hem de normal sertifika yayınlayan sağlayıcı ile nitelikli sertifika yayınlayan sağlayıcının farklı yükümlülüklere tabi olmasını sağlayacaktır. Yabancı mevzuatlarda ve Kanunumuzda Direktiften farklı olarak, nitelikli elektronik sertifikada, varsa vekâlet yetkisine ilişkin bilginin de bulunması zorunludur. Tanımda dikkat edilmesi gereken bir başka husus ise sertifikanın varsa limitlerinin (maddi sınırlamalarının), sertifikada bulunması zorunluluğudur. Kanunun 13. maddesine göre de hizmet sağlayıcı sertifikanın kullanım ve maddi kapsamına ilişkin sınırlarının dışında, hiçbir şekilde sorumluluğunu sınırlayamaz. Uygulamada, sertifikalar imza sahibine sağlanırken sertifikanın kullanılacağı işlemlerdeki maddi sınır belirlenebilir; imza sahibi sertifikayı bu sınırların üstünde bir işlemde kullanırsa hizmet sağlayıcı, sınırın üstünde doğan zararlar için sorumlu olmayacaktır. Ayrıca sertifikanın kullanımı bazı işlemlerle de (bankacılık işlemleri, güvenli e-posta) sınırlandırılabilir. Sertifikanın bu işlemler dışında kullanılması da hizmet sağlayıcının sorumluluğu dışında kalacaktır[154].

Elektronik sertifikalarda temel olarak aşağıdaki alanlar bulunur:

Sertifika sahibi bilgileri (isim, şirket, çalışılan birim, yer, ülke, e-posta vb.)
Sunucu sertifikalarında sunucu bilgileri (alan adı, sunucu adı, şirket adı vb.)
Ülke adı TR (Türkiye) olmak üzere ESHS bilgileri
Sertifika geçerlilik süresinin başlangıç ve bitiş zamanı

- **Kullanılan elektronik imza oluşturma algoritmaları**
- **Sertifika sahibi imza doğrulama verisi**
- **Sertifika seri numarası**
- **ESHS'nin imzası.**

Nitelikli elektronik sertifikalarda, Kanun gereği aşağıdaki bilgiler de yer alır:

- **Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare**

153 Avusturya Elektronik İmza Kanunu "SigG" m. 2/3-7.
Almanya Elektronik İmza Kanunu "SigG" m. 7.

154 ORTA, s.112.

- 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 sertifika kullanımına yönelik maddi işlem sınırı.

Nitelikli elektronik sertifikanın gereksinimlerini sıralayan m. 9'un j bendine göre "sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının" sertifikada bulunması zorunludur. Kanunda Yer alan güvenli elektronik imza ve imza sahibi tanımları uyarınca imza sahibi ancak gerçek kişi olabilecektir. Bu durumda hizmet sağlayıcı sadece gerçek kişi olabilir gibi bir sonuç ortaya çıkarmaktadır. Bu sorunun giderilmesi için "imza sahibi" tanımına Avusturya'da[155] olduğu gibi "sertifika hizmetlerini sağlamak üzere sertifika sağlayan hizmet sağlayıcıları"nın da eklenmesi gerekmektedir[156].

Nitelikli sertifikalarla ilgili gereksinimler Direktifte, yabancı mevzuatlarda ve Kanunumuzda sayılmıştır ancak bu şartlar yeterli değildir. Bu sebeple pek çok ülke, e-İmza yönetmeliklerinde uluslararası standartları referans göstermişlerdir (x.509, ETSI).

B. Elektronik Sertifika Hizmet Sağlayıcısı

Kanuna göre elektronik sertifika hizmet sağlayıcıları "Elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir". Kanunda yapılan tanım Direktife uygundur ancak hizmet sağlayıcının yüklendiği sorumluluklar düşünüldüğünde oldukça geniş bir tanımdır. Sertifika hizmeti sağlamak, Kanunda yapılan tanımın da desteklediği şekilde, sadece bilgisayarlar aracılığıyla yapılan bir işlemdir. Açık anahtarlı altyapı sistemiyle çalışan bir bilgisayar ağında, bilgisayar kullanıcıları iletişimlerini güvenli hale getirmek için sertifikalar kullanabilirler ve bu durumda sistemdeki güvenlik sunucusu (server) sertifika ve zaman damgası hizmeti sağlar. Kanuna göre bu sunucunun operatörü veya sunucunun sahibi olan kişi veya kurum "sertifika hizmet sağlayıcısı" olacak ve sağlayıcıya ait yükümlülüklere (kuruma bildirim, denetim, yönetmelikle getirilecek ek yükümlülükler) tâbi olacaktır. Böyle bir durumun oluşmaması için ya Kanundaki tanımın daraltılması gerekir ya da Kanuna ayrıca "nitelikli sertifika sağlayan hizmet sağlayıcı" tanımı ve yükümlülükleri eklenmelidir[157].

Kanun'a göre "hizmet sağlayıcı Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer". Direktif m.3/1'e göre hizmet sağlayıcıların kurulması izne tabi tutulamaz. Bu hükme yabancı mevzuatta da yer verilmiştir. Kanunumuzda bu tür bir izin yasağından bahsedilmemesine rağmen sağlayıcının bildirimle faaliyete geçeceğinin belirtilmiş olmasından, faaliyet için izin prosedürünün kullanılmayacağı anlaşılmaktadır. Bildirim zorunluluğu, yabancı ülkelerde farklı uygulamalarla karşımıza çıkmaktadır. Kimi ülkelerde tüm sağlayıcılar bildirimde bulunmak zorundayken, kimilerinde sadece nitelikli sertifika sağlayanlar bildirimde bulunmak zorundadırlar. Bazı ülkelerde ise akredite olmak isteyen sağlayıcılar ayrıca bildirimde bulunmak zorundadırlar. Bildirim bedelleriyle ilgili uygulamada da farklı-

155 Avusturya Elektronik İmza Kanunu "SigG" m. 2/2.

156 ORTA, s.111.

157 ORTA, s.117-118.

lıklar bulunmaktadır. Bedeller sertifika başına veya senelik olarak çeşitli kıstaslara göre belirlenebilmektedir.

Kanun'a göre "Elektronik sertifika hizmet sağlayıcıları, Kurumun belirleyeceği ücret alt ve üst sınırlarına uymak zorundadır." Bu sistemde sertifika fiyatlarını belirleme yetkisi Telekomünikasyon Kurumu'na bırakılmış gibi gözükmektedir; eğer Kurumun kendisi veya devlete ait bir başka kurum sertifika hizmet sağlayıcı olarak görev yapacak olursa, bu durum haksız rekabete yol açabilecektir. Yabancı mevzuatlarda buna benzer bir düzenleme bulunmamaktadır.

Ülkemizde de elektronik sertifika hizmet sağlayıcısı olarak görev yapan kuruluşlar bulunmaktadır. Bunlardan bazıları,

• Elektronik Bilgi Güvenliği A.Ş 24.06.2005'te hizmet vermeye başlamıştır ve satışını yaptıkları elektronik imza sertifikasının adı E-Güven dir.

• TÜBİTAK Kamu Sertifikasyon Merkezi 30.06.2005 tarihinde hizmet vermeye başlamıştır.

• Türk Trust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş 16.07.2005 tarihinde hizmet vermeye başlamıştır.

• EBG Bilişim Teknolojileri ve Hizmetleri A.Ş 31.09.2006 tarihinde hizmet vermeye başlamıştır ve satışını yaptıkları elektronik imza sertifikasının adı E-Tuğra 'dır.

C. Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri ve Hukukî Sorumluluğu

1. Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri

5070 sayılı Elektronik İmza Kanunu'nun 10. maddesinde sertifika hizmet sağlayıcının yükümlülükleri belirtilmiştir; madde, Direktifin nitelikli sertifika sağlayan sertifika sağlayıcılarla ilgili gereksinimleri sıralayan Ek 2 ile uyumludur. Ancak, Ek'in isminden de anlaşılacağı üzere burada belirtilen yükümlülükler nitelikli sertifika sağlayan sağlayıcılara ilişkindir[158]. Oysa Kanunumuzda bu yükümlülükler tüm hizmet sağlayıcılar için öngörülmüştür. Madde 10'a göre, elektronik sertifika hizmet sağlayıcısı;

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle yükümlüdür:

Burada bahsedilen personelin niteliği iki aşamalıdır. Personel, hem e-İmza ve sertifikasyon konusunda yeterli teknik bilgiye sahip olmalı ve hatta bu bilgisini kanıtlayabilmeli, hem de güvenilir bir kişiliğe sahip olmalıdır. Çalışma sırasında personel, sertifika sahipleriyle ilgili kişisel bilgileri öğrenebilir; personelin bu bilgileri daima saklı tutabilecek kapasitede olması gerekmektedir.

b) Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle yükümlüdür:

Hizmet sağlayıcı nitelikli sertifika talebinde bulunan kişiye sertifika sağlamadan önce bu kişinin beyan ettiği kimlik bilgilerinin gerçekliğini tespit etmekle yükümlüdür. Yanlış kimlik bilgileri sebebiyle sertifika kullanımından zarar doğması sonucunda (üçüncü kişilerin gördüğü zararlar da dahil olmak üzere) hizmet sağlayıcı zararı tazminle yükümlüdür. Ancak elinde olmayan sebeplerle kişinin kimliğinin yanlış tespit edilmesi sonucunda bu yükümlülüğünden kurtulur. Bazı ülkelerde sertifika talebi ve kaydı sırasında fotoğrafla başvuru veya kişisel başvuru zorunlu

[158] ORTA, s.121 vd.

kabul edilmektedir.

c) Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisinin, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle yükümlüdür:

Burada bahsedilen vekâletin veya sertifika sahibinin sertifikada belirtmek istediği kişisel ve mesleki bilgilerinin de (avukatlık, doktorluk vb.) sağlayıcı tarafından teyit edilme zorunluluğudur.

d) İmza oluşturma verisinin sertifika hizmet sağlayıcısı veya sertifika talep eden kişi tarafından sertifika hizmet sağlayıcısına ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamak; sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamakla yükümlüdür:

İmza oluşturma verisi, iki şekilde üretilebilir. Veri hizmet sağlayıcı tarafından, sağlayıcıya ait araçlarla üretilir ve sertifika sahibine teslim edilir veya veri doğrudan sertifika sahibine ait araçla üretilir ve üretilen veri sağlayıcı tarafından tasdik edilir. Burada bahsedilen yükümlülükte verinin sağlayıcı, tarafından üretilmesi halinde sağlayıcı, bu işlemin gizliliğini sağlamakla yükümlüdür, çünkü işlem sırasında veri başkaları tarafından kopyalanabilir. İkinci durumda veri, sağlayıcının sağladığı araçlarla üretilirse, bu işleyişin güvenliğini sağlamak yükümlülüğü hizmet sağlayıcıya aittir. Uygulamada sağlayıcı bu sorumluluğunu, ancak kalitesi ispatlanmış güvenli araçları sertifika sahiplerine temin ederek yerine getirecektir.

e) Sertifikanın kullanımına ilişkin özellikler ve uyuşmazlıkların çözüm yolları ile ilgili şartlar ve kanunlarda 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 yükümlüdür:

Burada bahsedilen bilgi verme zorunluluğudur. Sağlayıcı, sertifika sahiplerine sertifikanın kullanımıyla ilgili her türlü teknik ve hukuki bilgiyi vermek zorundadır. Ayrıca güvenli elektronik imzanın hukuki değeri de sertifika sahiplerine bildirilmelidir. Yabancı mevzuatlarda sağlayıcıya; konuyla ilgili bütün hukuki düzenlemeleri, sertifikasyon işlemleri ile ilgili uluslararası standartları ve kullanılacak güvenli araçları, sertifika sahibine bildirme zorunluluğu getirilmiştir.

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

Bu hüküm de bilgilendirme yükümlülüğü içerisindedir. Sağlayıcı, oluşturma verisini başkasına kullandırmaması konusunda sertifika sahibini bilgilendirdikten sonra bu konuyla ilgili sorumluluğundan kurtulur; yani sertifika sahibi kendi isteğiyle oluşturma verisini başkasına kullandırırsa ve bu durum sonucunda bir zarar meydana gelirse sağlayıcı bu zararı tazminle yükümlü tutulamaz.

g)Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla yükümlüdür:

Kayıtları saklama koşulları ile ilgili pek çok uluslararası standart bulunmaktadır. Yabancı uygulamada da bu standartlar referans gösterilmekte ve kayıt saklama süreleri farklılık arz etmektedir. Konuyla ilgili yönetmelik düzenlenirken süreler kadar, kayıt tutma koşulları da göz önüne alınmalı ve bunlarla ilgili şartlar ortaya

konulmalıdır.

h) Faaliyetine son vereceği tarihten en az üç ay önce durumu Kuruma ve elektronik sertifika sahibine bildirmekle yükümlüdür:

Burada bahsedilen bildirimin amacı, sağlayıcının hizmetleri sona erdikten sonra hizmetleri geçici olarak Kurumun veya başka bir sağlayıcının üstlenmesini sağlamak içindir.

Yabancı uygulamada sağlayıcılara hizmetlerini durduktan belli bir süre sonra dahi dizin (directory) ve iptal listesi (revocation list) hizmetlerini sunma zorunluluğu getirilmektedir.

ı) Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz:

Burada bahsedilen işlem anahtar kurtarma (key backup) işlemidir. Bu işlemde sertifika sahibi anahtarını kaybettiği takdirde sağlayıcı da bulunan yedek anahtarını kullanmaktadır. Ancak Kanunumuzda ve bazı yabancı mevzuatta yedekleme işlemi yasaklanmıştır.

2. Elektronik Sertifika Hizmet Sağlayıcısının Hukukî Sorumluluğu

Elektronik İmza Kanunu'nun 13. maddesinin 1. ve 2. bentlerine göre "*Elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tâbidir. Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz.*" Burada dikkat edilmesi gereken husus servis sağlayıcının sorumluluktan kurtulabilmesi için kusurunun bulunmadığını ispat etmesi gerektiğidir. İspat yükü böylece iddiada bulunan taraftan karşı tarafa geçmiştir. Ters ispat yükü Direktifte de belirtilmiştir ayrıca yabancı mevzuatların da çoğu düzenleme bu sistemi benimsemiştir[159].

13. maddenin 3. bendine göre ise "Elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, BK'nun 66. maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz." Burada hizmet sağlayıcıların, istihdam ettikleri personelin fiillerinden kusurları bulunmasa dahi sorumlu olacakları belirtilmiştir. Bu konu Borçlar Kanunu'nun 66. maddesinde belirtilen *adam çalıştıranın sorumluluğu* müessesesidir. Burada kusursuz sorumluluk mevcuttur, yani istihdam edenin zararı tazmin etmesi için kendi kusurunun bulunması zorunluluğu yoktur. Ancak, BK 66. maddesine göre "Adam çalıştıran, çalışanını seçerken, işiyle ilgili talimat verirken, gözetimve denetimde bulunurken, zararın doğmasını engellemek için gerekli özeni gösterdiğini ispat ederse, sorumlu olmaz." Elektronik İmza Kanunu'nun 13. maddesine göre ise, bu kurtuluş kanıtı sertifika sağlayıcının sorumluluğunda kullanılamaz; 13. maddede ağırlaştırılmış kusursuz sorumluluk vardır.

13. maddenin 4. bendine göre; *"Nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir".* Buna göre

[159] ORTA, s.127.

sertifika sağlayıcı ile sertifika sahibi arasında yapılacak, sağlayıcının sorumluluğunu kısıtlamaya yönelik antlaşmalar geçersiz olacaktır. Sorumluluk kısıtlaması ancak sertifikayla yapılacak işlemlerin niteliğine ve sertifikanın kullanıldığı işlemin mali değerine yönelik olacaktır.

13. maddede belirtilen bir başka sorumluluk ise sertifika sağlayıcının sertifika mali sorumluluk sigortası yaptırma zorunluluğudur. Sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle[160] belirlenecektir. Ancak burada Kanunun kurgusuyla ilgili bir hata bulunmaktadır. Sigortaya ilişkin usul ve esasların yönetmelikle belirleneceği maddede belirtilmiştir fakat yönetmelikle belirlenecek hususların belirtildiği 20. maddede 13. maddeden bahsedilmemiştir.

3. Nitelikli Elektronik Sertifikaların İptal Edilmesi

Elektronik İmza Kanunu'nun 11. maddesine göre elektronik sertifika hizmet sağlayıcısı;

a) Nitelikli elektronik sertifika sahibinin talebi,

b) Sağladığı nitelikli elektronik sertifikaya ilişkin veri tabanında bulunan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi,

c) Nitelikli elektronik sertifika sahibinin fiil ehliyetinin sınırlandığının, iflâsının veya gaipliğinin ya da ölümünün öğrenilmesi, durumunda vermiş olduğu nitelikli elektronik sertifikaları derhâl iptal eder.

Burada belirilen koşullar yabancı mevzuatla da uyumludur.

Madde 11/2'ye göre *"Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikaların iptal edildiği zamanın tam olarak tespit edilmesine imkân veren ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir kayıt oluşturur"* Burada bahsedilen sertifika iptal listesidir (revocation list). Sertifika iptal listeleri, bir sertifika iptal edildiğinde bunun otomatik ve eşzamanlı olarak "sertifika kayıt veri tabanına" işlenmesi ve imzanın doğrulanması sırasında sertifikanın iptal edildiğinin belirlenebilmesi amacıyla kullanılırlar. Maddede belirtilen gereksinimler sertifika iptal işlemi için yeterli değildir, fakat madde 20'ye göre bu işlemin uygulanmasına ilişkin usul ve esaslar yönetmelikle[161] belirlenecektir. Yönetmelikte sertifika iptal işlemi ile ilgili uluslararası standartlara atıf yapılması faydalı olacaktır.

11. maddenin son fıkrasına göre *"Elektronik sertifika hizmet sağlayıcısı geçmişe yönelik olarak nitelikli elektronik sertifika iptal edemez"* Bu işleme retroaktif iptal yasağı denmektedir ve çoğu yabancı mevzuatta da bu hükümle karşılaşılmaktadır. Buna göre sağlayıcılar iptal işlemini, işlemin yapıldığı günden önceki bir tarihten itibaren başlatamazlar.

Maddede belirtilen bir başka husus ise, sertifika hizmet sağlayıcının faaliyetine Kurum tarafından son verildiğinde, sağlayıcının elindeki sertifikaların başka bir sağlayıcıya teslim edilmesine yine Kurumun karar verecek olmasıdır. Sağlayıcı hizmetine kendisi son verirse, elindeki sertifikaları bir başka sağlayıcıya teslim etmelidir, bunu başaramazsa elindeki sertifikaları derhal iptal etmelidir.

Kanunumuzda hiç bahsedilmeyen servis sağlayıcının sertifikası konusu, ser-

[160] 26 Ağustos 2004 Tarihli R.G. S: 25565, Sertifika Mali Sorumluluk Sigortası Yönetmeliği.

[161] Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik için bkz., R.G. 06.01.2005-25692.

tifikaların iptal prosedüründe de önem kazanmaktadır. Konuyla ilgili Avusturya Elektronik İmza Kanunu'nun 9/5 maddesine göre servis sağlayıcının hizmetleri yetkili kurum tarafından yasaklandığında yetkili kurum, servis sağlayıcının sertifikasını iptal eder[162].

4. Bilgilerin Korunması

Kanunun 12. maddesine göre elektronik sertifika hizmet sağlayıcısı;

a) Elektronik sertifika talep eden kişiden elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez,

b) Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,

c) Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz.

Maddedeki hükümler, Direktif ve yabancı mevzuatla uyumludur. Direktif'in 8. maddesi bilgilerin korunmasıyla ilgilidir ve Kanunumuzda belirtilenlerle benzer yükümlülükler içermektedir. Ancak Direktif m.8, ek olarak kişisel verilerin korunması ile ilgili 95/46/EC sayılı Direktif'e atıf yapmıştır. Yabancı mevzuatların konuyla ilgili hükümlerinde de kişisel verilerin korunması ile ilgili kanunlara atıflar bulunmaktadır. Ülkemizde bu konuyla ilgili bir kanun tasarısı mevcuttur. Tasarı yasalaştığı takdirde yabancı mevzuatlardaki gibi, 12. maddeye bu kanunla ilgili bir atıf konmalıdır[163].

5. Yabancı Elektronik Sertifikalar

Kanunun 14. maddesine göre yabancı bir ülkede kurulu bulunan sertifika sağlayıcının sağladığı sertifikaların Türkiye'deki hukuki değerleri iki yolla belirlenebilir.

i) yabancı sertifikaların hukuki statüsü milletlerarası antlaşmalarla belirlenebilir. (Yönetmelik m.32/1)

ii) yabancı sertifikalara Türkiye'de mukim bir hizmet sağlayıcının garanti vermesi ile yabancı sertifikalar Türkiye'de geçerli nitelikli sertifika ile aynı hukuki statüye sahip olurlar. Burada dikkat edilmesi gereken husus Türkiye'deki sağlayıcı tarafından garanti edilen yabancı sertifikaların kendi ülkelerinde nitelikli olup olmadıklarına bakılmaksızın, Türkiye'de nitelikli sertifika ile aynı hükme sahip olacak olmalarıdır. Garanti edilen sertifikanın doğuracağı zararlardan garanti eden sağlayıcı da sorumlu olacağı için nitelikli-niteliksiz ayrımı yapmadan bütün sertifikaların nitelikli sertifika sayılması, garantör sağlayıcıya geniş sorumluluklar yükleyecektir. Yabancı sertifikaya garanti verilmesi ve karşılıklı antlaşmalarla sertifikanın hukuki etkisinin belirlenmesi Direktife uygun düzenlemelerdir.

6. Denetim

Yönetmelik'in 22. maddesine göre, sertifika hizmet sağlayıcıların faaliyetlerinin ve işlemlerinin denetimini yapmaya yetkili kurum Telekomünikasyon Kurumudur. Denetleme sırasında Kurumun yetkilendirdiği kişiler her türlü defter ve kayıtları inceleyebilir, sertifika sağlayıcının binalarına ve eklentilerine girebilirler; sağlayıcı bu duruma rıza göstermek zorundadır. Denetim gerekli görülen zamanlarda yapılabileceği gibi, şikayet üzerine de yapılabilecektir.

162 ORTA, s.115.
163 ORTA, s.134.

Kanunumuzda denetlemeye ilişkin hükümler yabancı mevzuata göre çok daha belirsiz durumdadır. Direktifin denetlemeyle ilgili 3.3 maddesine göre üye devletler kendi sınırları içerisindeki nitelikli sertifika sağlayan hizmet sağlayıcıların denetimini yapmak üzere gerekli sistemi kurmak zorundadır.

Yönetmelik'in 23. maddesine göre, denetim görevlileri denetimle ilgili özeni göstermek, tarafsız davranmak ve dürüstlük kuralına aykırı bir müdahaleye imkan tanımamak zorundadırlar. Denetim sonunda hazırlanan denetim raporunun en geç otuz gün içinde Telekomünikasyon Kurulu'na iletilmesi gerekir. Yönetmelik'in 28. maddesine göre, Kurul raporları değerlendirdiğinde aykırı bir durum varsa, mevzuatın öngördüğü yaptırım ve cezaların uygulanmasına karar verir[164].

7. Ceza Hükümleri

Kanunda ceza hükümleri, suçlar ve idari para cezaları olarak ikiye ayrılmıştır. Madde 16 ve 17'de imza oluşturma verilerinin izinsiz kullanımı ve sertifikalarda sahtekârlık hükümleri düzenlenmiştir.

Madde 16'ya göre güvenli elektronik imza oluşturma araçlarını ve verilerini sahibinden izinsiz olarak elde edenler, kullananlar, verileri kopyalayanlar ve araçları yeniden oluşturanlarla izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar, hapis ve para cezasıyla cezalandırılacaklardır. Bu hükümde açıklanması gereken nokta "izinsiz elde edilen imza oluşturma aracı" bahsindeki iznin araç sahibinden mi yoksa Denetleme Kurumu veya benzer bir kurumdan mı alınacağı sorusudur. Eğer hükümde bahsedilen izin Kurumdan alınacaksa, bu durumda imza oluşturma aracı elde etmek veya kullanmak için Kurumdan izin alınması gerektiği gibi bir sonuç ortaya çıkacaktır. Oysa bu araçlar mevcut bilgisayar ağ sistemlerinde güvenli iletişim sağlanması için zaten kullanılmaktadırlar. Bu sebeple bunları elde etmek veya kullanmak için Kurumdan izin alınması gerekliliği uygulamada kullanılamayacak bir hükümdür.

Madde 17'de ise sahte sertifikalar, geçerli sertifikaların tahribatı ve yetkisiz sertifika oluşturma ve bunları kullanma ile ilgili hükümler yer almaktadır. Burada problem yaratacak husus yetkisiz sertifika yaratma ve bunları kullanma ile ilgili olan hükümdür. Kanunda yetkisiz sertifika yaratma fiili ile ilgili bir açıklama bulunmamaktadır. Maddeden anlaşıldığı üzere sertifika yaratmak için ayrıca yetkili olmak gerekmektedir. Kanunda sertifika yaratma ile ilgili yetkilendirilmeden bahsedilmemekle birlikte Direktifin en çok önem verdiği husus da sertifika hizmet sağlayıcıların herhangi bir izin veya yetkilendirme prosedürüne bağlı kalmadan faaliyetlerini yürütebilmesidir. Kanunda yetkiyle bağdaştırılabilecek tek hüküm Denetleme Kurumuna yapılan hizmete başlama ile ilgili ihbardır. Bu durumda maddeden çıkarılabilecek sonuç denetleme kurumuna ihbar yapmadan sertifika hizmeti sağlayan sağlayıcıların yetkisiz kabul edileceğidir. Ancak daha öncede belirttiğimiz gibi elektronik sertifikalar sadece elektronik imza oluşturmak için kullanılmamakta bunun yanı sıra bilgisayar ağlarında güvenli iletişimin sağlanması için de kullanılmaktadır. Hâlihazırda kullanılmakta olan ağ iletişim sistemlerinin çoğunda sertifika ve açık anahtarlı altyapı kullanılmaktadır. Kanunun yetkisiz sertifika oluşturma ve bunları kullanmayla ilgili hükümlerine göre, mevcut sistem-

[164] Avrupa'da "Avrupa Elektronik İmza Denetim Kurumları Forumu" (FESA), konuyla ilgili denetim kurumları arasında işbirliğini sağlamakla görevlidir ve Telekomünikasyon Kurulu da Türkiye adına FESA'ya üyedir.

lerde bu teknolojik altyapıyı kullanan operatörler, sistem kullanıcıları ve sistemi mülkiyetinde bulunduranlar suçlu durumunda olacaklardır. Bu sebeplerden dolayı yetkisiz sertifika oluşturanlar ve bunları kullananlar ile ilgili hüküm kanundan çıkartılmalıdır. İmza oluşturma verilerinin ve araçlarının izinsiz kullanımı ile sertifikalarda sahtekârlık ile ilgili suçları sertifika sağlayıcının personelinin işlemesi durumunda cezalar ağırlaştırılacaktır.

Kanunun 18. maddesinde ise idari para cezalarına konu olan fiiller düzenlenmiştir. Kanunda fiiller sıralanmamış fakat bunun yerine ihlali halinde para cezası verilecek hükümler sayılmıştır. Buna göre sertifika hizmet sağlayıcı; sertifika iptal hizmetini Kanunda belirtildiği şekilde yapmadığı halde (m.11), Kanunla kendisine verilen yükümlülükleri yerine getirmediği halde (m.10), sigorta ile ilgili hükümleri ihlali halinde (m.13), denetimle ilgili hükümleri ihlali halinde (m. 15) idari para cezasına çarptırılacaktır.

VI. ELEKTRONİK İMZA KANUNUMUZ HAKKINDA BİR DEĞERLENDİRME VE DİĞER KANUNLARDAKİ DÜZENLEMELER

A. Elektronik İmza Kanunumuz Hakkında Bir Değerlendirme

1. Yapı itibariyle birbirinden tamamen farklı olan dijital imza ile biyometrik yöntemlerin, elektronik imza üst kavramı altında, aynı kanunda aynı hüküm ve sonuçlara bağlı olarak düzenlenmesi kanun yapma tekniği açısından sakıncalı olmuştur. Biyometrik yöntemlerin teknik yapısı ve hukuki sorunlarının mutlaka ayrı bir kanunda düzenlenmesi gerekmektedir. Zaten Tasarıdaki hükümler dikkate alındığında, bu hükümler ile kanun koyucunun sadece dijital imza ile ilgili olarak düzenleme yaptığı anlaşılmaktadır. Dolayısıyla bu kanunun adının ***"TÜRK DİJİTAL İMZA KANUNU"*** olması yerinde olacaktır.

2. Kanunun *"Tanımlar"* kenar başlıklı 3. maddesinde yer verilmeyen veya yanlış tanımlanan bazı kavramlar mevcuttur. Bu konudaki kavramlar listesi ve tanımları bakımından Örneğin; elektronik veri (3a) şeklinde bir kavram kullanılması kavram karışıklığı yaratmaktadır. Buna sadece veri denilmesi ve yapılan tanımlama da elektronik, optik veya benzeri yollarla hazırlanan (üretilen değil), taşınan veya saklanan bilgiler, denilmesi gerekmektedir. **Elektronik imza** (3b) kavramı Tasarıda *"başka bir* ***elektronik veriye eklenen*** *veya* ***elektronik veriyle mantıksal bağlantısı bulunan*** *ve kimlik doğrulama amacıyla kullanılan* ***elektronik veriyi****"* ifade edecek şekilde tanımlanmıştır. Bu tanımın dijital imza çeşitleri için kullanılması mümkün ise de; biyometrik yöntemlerin bu şekilde tanımlanması ve bu kapsamda değerlendirilmesi mümkün değildir. Yine bu tanım karşısında elektronik veri ile elektronik imza arasındaki farkın ne olduğu anlaşılamamaktadır[165]. Dijital imza bu Tasarıda belirtildiği şekilde bir elektronik veri değildir. Dijital imza bir şifreleme programıdır. Ayrıca veriyle mantıksal bağlantının neyi ifade ettiği anlaşılamamaktadır.

3. Kanun m. 3'te elektronik imzanın genel olarak tanımı yapılmış, m. 4'te ise dijital imza çeşitlerinden sadece güvenli elektronik imza tanımlanmış ve m. 5/f.1'de de bu imza kullanımının doğuracağı sonuç hükme bağlanmıştır. Kanundaki gü-

[165] Leyla KESER BERBER, Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi, http://www.imza.gen.tr/templates/resimler/File/makaleler/Elektronik_imzanin_Duzen lenmesi_Leyla_Keser (21.10.2007).

venli elektronik imza tanımı, Alman Dijital İmza Kanunundaki nitelikli elektronik imza kavramını karşılamaktadır. Oysa kanunda gelişmiş elektronik imzanın ne olduğu tanımlanmamıştır. Bu durumda ise örneğin; bir Türk vatandaşının Almanya'daki bir sertifika kurumundan **gelişmiş** elektronik imza alması ve kullanması sorunu bizim kanunda çözüme kavuşturulmadığı için, bu açıdan kanunda boşluk bulunmaktadır.

4. Madde 5/f.1'e göre; güvenli elektronik imza, elle atılan imza ile aynı hukuki doğuracaktır. 2. Fıkrada ise; elektronik imza kullanımının mümkün olmadığı işlemler sayılmıştır. Ancak bu fıkradaki yasaklama bütün gelecek için midir? Yani sayılan işlemler bakımından getirilen yasak, teknoloji ileride dijital imza bakımından bugün mevcut olan belirsizlikleri giderdiği zaman da mı devam edecektir? Kanun m. 5/f.2 hükmünün lafzından çıkan sonuç bu işlemlerde elektronik imzanın mutlak olarak kullanılamayacağıdır. Oysa ABD'deki uygulamalara paralel olarak mutlak bir yasaklama getirilmeyip, belirli bir sürenin sonunda tekrar koşulların değerlendirileceği hükme bağlanmalıydı.

5. Kanun m. 6 (a,b,c,d)'da tanımlanmaya çalışılan güvenli imza oluşturma araçlarından maksat, maddede sayılan amaçları yerine getirmeye elverişli yazılım, özellikle şifreleme programlarıdır; bu araçlardan neyin kastedildiğinin açıkça belirtilmesi isabetli olacak ve bu araçların da gelişen teknoloji ile değişeceği hüküm altına alınmalıydı.

6. İkinci Bölümün Başlığında ve 8. maddenin kenar başlığında *"elektronik sertifika hizmet sağlayıcısı"* kavramının kullanılması uygun değildir. Bunun *"güvenli elektronik sertifika hizmet sağlayıcısı"* olarak değiştirilmesi gerekmektedir. Çünkü Kanun elektronik imzanın her bir çeşidi bakımından değil, sadece güvenli elektronik imza bakımından hükümler ihtiva ettiği için, bu alanda faaliyet gösterecek sertifika kurumlarının da ilgililere vereceği sertifika ancak, güvenli elektronik imza sertifikası olabilecektir.

7. Kanunun 10/d maddesi hükmünün ne ifade ettiği, bu hükümle kanun koyucunun neyi düzenlemek istediğinin anlaşılması mümkün değildir. İmza oluşturma verisinin (yani dijital imzaya esas teşkil eden şifrelerin veya şifreleme programlarının) sertifika talep eden kişi tarafından, sertifika hizmet sağlayıcısına ait yerlerde üretilmesi neyi ifade etmektedir? Normal olarak dijital imza almak isteyen kişiler, bunun için onay makamı veya sertifika kurumu olarak görev yapan yerlere müracaat ederler. Sertifika kurumu ise, hangi şifreleme programını tercih etmişse, bu programa göre hazırlanan dijital imzayı bir karta kopyalayarak talep sahibi kişilere verecektir. Dolayısıyla dijital imza sertifikası almak isteyen kişilerin, sertifika hizmet sağlayıcılarının faaliyet gösterdikleri binalarında, onların iş yerlerinde kendi başlarına dijital imza üretmeleri mümkün değildir. Ancak Kanun hükmünün lafzından çıkan sonuç bunun mümkün olduğu şeklindedir.

B. Diğer Bazı Kanunlardaki Elektronik İmzaya İlişkin Düzenlemeler

1. Yeni TBK'nun 14 ve 15. Maddesiyle yapılan değişikliklere yukarıdaki açıklamalarda yer verildiğinden tekrar üzerinde durulmayacaktır.

2. Kanun, mülga HUMK'da değişiklik yaparak 295/A hükmü ile; *usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler* ***senet*** hükmündedir. Bu veriler aksi ispat edilinceye kadar ***kesin delil*** *sayılırlar"* düzenlemesini getirmişti. Bu

düzenleme yeni HMK m.205/(2)'de aynen yer almıştır. Ancak isabetli olarak aynı maddenin (3). bendine hâkimin mahkemeye sunulan elektronik imzalı belgelerin güvenli elektronik imza ile oluşturulmuş olup olmadığını re'sen inceleme görevini yüklemek suretiyle bu konudaki sahtekarlıkların önlenmesi konusunda önleyici tedbir alınması yoluna gidilmiştir[166].

3. Kanun ile yürürlükten kalkan HUMK'a 295/A maddesi ile *"dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun yani HUMK'un 308. maddesi kıyas yoluyla uygulanır"* şeklinde bir hüküm getirilmişti. Halbuki HUMK m. 308 vd. hükümlerinin, elektronik bir belgede yer alan dijital imzanın inkârı halinde aynen uygulanabilmesi mümkün değildi. Dijital imzanın inkarı halinde hakimin,inkar eden tarafa kendi önünde yazdırdığı yazı ve attırdığı imza ile dijital imzayı karşılaştırabilmesi mümkün değildir. Dijital imzanın inkarı halinde izlenecek tek yol hakim için, doğrudan doğruya bilirkişiye yani dijital imza sertifikası veren kuruma müracaat etmek ve imzanın o kişi tarafından atılıp atılmadığının tespitini istemek olmalıydı[167]. Dolayısıyla Kanunun tasarısında[168] HUMK m. 308 vd. hükümlerine doğrudan atıf yapmak yerine, dijital imzanın inkarı halinde hakimin bilirkişiye, yani dijital imza sertifikası veren kuruma müracaat etmesi gerektiğini belirlemek yeterli olacaktı. Nitekim yeni HMK'nın 210. maddesi ile, **"Güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur."** hükmü getirilmek suretiyle bu konuda gerekli değişiklik yapılmıştır.

4. Elektronik imzalı belgenin İİK[169] bakımından senet niteliği kabul edildiği takdirde, senedi imzalayan kişi tarafından imzanın ikrar edilmesi durumunda bu elektronik belge 68. madde anlamında belge olarak değerlendirilebilir. Buna karşılık, imzası ikrar edilmiş elektronik belgenin, senet özelliklerini taşımaması sebebiyle itirazın kaldırılmasında sınırlı inceleme yetkisi olan icra mahkemesi tarafından incelenmesi mümkün olamayacaktır. Çünkü elektronik formda ibraz edilen, elektronik belgenin icra mahkemesince görülüp algılanabilmesi ve itirazın kaldırılması konusunda kanaat edinilebilmesi için bilirkişinin yardımı zorunludur. Bu sebeple hangi çeşit imzayla imzalanmış olursa olsun, imzası ikrar edilmiş elektronik imzalı belge icra mahkemesinin sınırlı inceleme yetkisi sebebiyle itirazın kesin kaldırılması aşamasında 68/I anlamında belge olarak nitelendirilemez.

Bundan başka, alacaklı takip talebi ile senedin aslını vermemişse itirazın kaldırılmasında, senedin aslını vermelidir. Fotokopi veya faks senet olmadığı için alacaklının itirazın kaldırılmasında bu belgelere dayanması mümkün değildir. Aynı

[166] Detaylı açıklamalar için bkz., Leyla KESER BERBER, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Yetkin Yayınları, Ankara 2002, s. 229 vd.

[167] Sinem Pelin CİVELEK, 5070 Sayılı Elektronik İmza Kanunu Doğrultusunda Elektronik İmza Kullanımı, http://www.turkhukuksitesi.com/makale_208.htm (19.10.2007).

[168] Elektronik İmza Kanunu Tasarısı Madde 23- 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere aşağıdaki 295/A maddesi eklenmişti.
"Madde 295/A- Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar."Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkar ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır." http://www.nvi.gov.tr/attached/NVI/sayisalimza/kanun.doc (20.10.2007)

[169] 2004 sayılı İcra İflas Kanunu için bkz., RG. 19.06.1932 S**:** 2128.

şekilde senedin mikro filmi de tek başına itirazın kaldırılması için yeterli değildir.

Buna karşılık, alacaklının senet fotokopisini ibrazı halinde, fotokopinin borçlu tarafından kabul edilmemesi durumunda icra mahkemesi tarafından fotokopinin değerlendirilemeyeceği görüşü dikkate alındığında borçlu tarafından fotokopinin kabul edilebileceği sonucu çıkmaktadır. Elektronik imzalı belge çıktısının bu anlamda itirazın kaldırılmasına yarar bir belge olduğu düşünülebilir. Çünkü elektronik belgenin çıktısı, icra mahkemesi tarafından, görülüp algılanabileceği için, incelenebilecektir. Belgenin çıktısının, senedin özelliklerinden olan *cisim bulma* ve *yazılılık niteliklerini* karşıladığı söylenmelidir. Senedin diğer özelliği olan, imzanın bulunması unsurunun ise borçlu tarafından elektronik belgedeki imzanın ikrar edilmesi sonucu karşılanmış olduğu düşünülebilir. Ancak bütün bu söylenenler bakımından, takibin dayanağının itirazın kaldırılması duruşmasında ibraz edilen elektronik belge olması gerektiği belirtilmelidir.

Elektronik imzalı belgedeki imza inkârı durumunda ise icra mahkemesinin bu imzayı İİK' nın 68/a maddesine göre itirazın geçici kaldırılması açısından incelemesi mümkündür.

5. Tüketicinin Korunması Hakkında Kanun 6.3.2003 tarihinde 4822 sayılı Kanun[170] ile değiştirilmeden önce, mal, ticaret konusu taşınır eşya olarak tanımlanmıştı. Kanun değişikliğinde elektronik ticaret dikkate alınarak mal, *"alış-verişe konu olan taşınır eşyayı, konut ve tatil amaçlı taşınmaz malları ve elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları"*, kapsayacak şekilde tanımlanmıştır. Tüketicinin korunması bakımından kanun koyucunun elektronik ortamda artan alış verişi göz ardı etmemesi olumlu karşılanmalıdır.

Bundan başka, 4822 sayılı Kanunun 14. maddesi ile 4077 sayılı Kanuna[171] 9. maddeden sonra gelmek üzere 9/A maddesi eklenmiştir. Bu maddede mesafeli sözleşmelere ilişkin düzenleme yapılmıştır. Kanuna göre, mesafeli sözleşmeler, *yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmelerdir* (TKK m.9/A/I).

Bu hükümle, elektronik ortamda ve tüketici ile karşı karşıya gelinmeksizin yapılan sözleşmeler Kanunun kapsamına alınmıştır. Ancak mesafeli satış sözleşmesinin elektronik ortamda yapılması durumunda da sözleşmenin yapılmasından önce, ayrıntıları Bakanlıkça çıkarılacak tebliğle belirlenecek bilgilerin tüketiciye verilmesi zorunludur. Sözleşmenin akdedilmesi için tüketicinin, bu bilgileri edindiğini yazılı olarak teyit etmesi gerekir. Elektronik ortamda yapılan sözleşmelerde teyit işleminin, yine elektronik ortamda yapılması mümkündür (TKK m.9/A/II). Elektronik ortamda yapılan mesafeli sözleşmeler bakımından, satıcı veya sağlayıcının elektronik ortamda tüketiciye teslim edilen gayri maddî malların veya sunulan hizmetlerin teslimatının ayıpsız olarak yapıldığını ispatla yükümlü olacağı belirtilmiştir (TKK m.9/A/IV). Aslında tüketicinin kendisine teslim edilen malın veya sunulan hizmetin ayıplı olduğunu ispat etmesi, genel kuraldan hareketle vakıadan lehine hak çıkaran (MK m.6) kişi olarak tüketiciye aitken, bu hüküm sonucunda,

[170] R.G. 14.3.2003 S: 25048, http://www.hukuki.net/kanun/4822.15.text.asp.

[171] 4077 Sayılı Tüketicinin Korunması Hakkında Kanun 23 Şubat 1995 tarihinde kabul edilmiştir. Bkz., RG.08.03.1995-22221.

elektronik ortamda malın veya hizmetin ayıpsız teslim edildiğini ispatla yükümlü olan kişi satıcı ve sağlayıcı olacaktır. Böylece kanun tarafından ispat yükünün belirlendiği bir durum söz konusudur.

SONUÇ

Türkiye'de ilk elektronik imzanın kullanıldığı 18 Temmuz 2005 tarihinden beri yaklaşık sekiz yıl geride kaldı. Türkiye'de elektronik imza konusunda yapılan yasal düzenlemeler oldukça iyi bir hale getirilmiş ve yeni TBK ile HMK'da da eksikliği görülen hususlarda gerekli düzenlemeler yapılmıştır. Elektronik imzanın kullanılması, kamudaki dönüşümün, yeniden yapılanmanın, verimliliği sağlamanın ve e-devlet olmanın bir fırsatı olarak görülüp iyi değerlendirilmesi gerektiği açıktır.

Elektronik İmza Kanunu'nun yürürlüğe girdiği andan itibaren kamu kurum ve kuruluşları arasında da bilgilerin elektronik ortamda değişimi mümkün hale gelmiştir. Hantal ve ağır işleyen bürokrasinin önüne geçilmesi ve evrak akışının hızlandırılması bakımından da elektronik imzanın işlevi ve yararı yadsınamaz bir gerçektir.

Örneğin, halen uygulanmakta olan ve yargıda kullanılan "Ulusal Yargı Ağı İletişim Sistemi" önemli bir e-devlet uygulamasıdır. Yine Adalet Bakanlığı tarafından bilgi güvenliğinin sağlanması, kişisel verilerin korunması, birlikte çalışabilirlik, hizmet kalitesinin sağlanması ve uluslar arası standartların yakalanması amaçlarıyla yeni uygulamaya konulan Elektronik Tebligat Yönetmeliği güncel ve son gelişmeler arasında yer almaktadır. Uygulamayla tebligatların kısa sürede, ucuz ve güvenli olarak yapılabilmesi ve trafik cezalarından dava dilekçelerine kadar bir çok tebligatın elektronik posta yoluyla tebliğ edilmesinin sağlanması amaçlanmıştır.

E-devlet uygulamalarının birçoğunda öncelikle uygulanması gerekli olan elektronik imza kullanımı, elektronik ortamda güvenli iletişim ve işlemler için günümüzde vazgeçilmez yöntem olarak işlevini artırmakla birlikte, isteyen herkes el yazısı ile de işlemlerini yapabilecektir. Bir başka deyişle fotoğrafa karşın günümüzde nasıl resim yapılmaya devam ediliyorsa, elektronik haberleşme ve sayısal imzanın yanı sıra kâğıt dokümanlar, el yazıları ve el yazısı ile atılan ıslak imza da var olmaya devam edecektir.

Elektronik imzaya olan güvenin sarsılmaması adına elektronik sertifika hizmet sağlayıcılarına önemli bir rol düşmektedir. Özellikle kimlik bilgilerinin düzgün tutulması son derece önemlidir. Telekomünikasyon Kuruluna bu bakımdan verilen denetleme yetkisinin gerektiği şekilde kullanılmasına da saygı gösterilmeli ve her türlü kolaylık sağlanmalıdır.

İnternet kullanıcıları sadece kendi ülkelerindeki değil, aksine dünyanın her bir köşesindeki web sayfalarında dolaştıkları için, dijital imza konusunda her bir ülkenin ulusal düzenlemeler yapmak yerine, bu konuda tüm dünya ülkelerinde uygulanacak yeknesak kurallar konulması ve uluslararası sözleşmelerin uygulama

alanının tüm dünyaya yayılması konuyla ilgili doğal bir amaçtır.

Elektronik imza biz internet ve bilgisayar kullanıcılarına kolaylıklar sağlayarak bilgisayar başından her türlü işlemimizi yapmamıza yardımcı olmaktadır. Ancak, elektronik imzanın gerçekleştirildiği şifreleme yöntemlerinin de birileri tarafından deşifre edilebileceği ve hackerların bu konudaki gayretleri de gözden uzak tutulmamalıdır. Bu tür olumsuzluklar internetin ve elektronik işlemlerin teknik ve hukuki alt yapısının açık vermeksizin sağlam hale getirilmesi ile minimize edilebilir.

Nihayet elektronik imzanın e-ticaret gibi farklı e-devlet uygulamaları ile de yakından ilgili olduğu düşünüldüğünde gerekli hukuki ve cezaî düzenlemelerin spesifik bazı yasal düzenlemelerde de yapılması gerektiği ve bundan sonra da halin icabına göre yapılmaya devam edeceği açıktır. Nitekim Elektronik İmza Kanunu bu noktadaki ana düzenleme olmasına karşılık yeni TBK ve HMK gibi düzenlemelerde yer alan hükümleri de bu çerçevede değerlendirmek gerekir.