ELEKTRONİK İMZADA HUKUKSAL ALTYAPI- TÜRK, ALMAN VE AVRUPA BİRLİĞİ KANUNLARININ GENEL İNCELEMESİ

Yücel YILMAZ*

Özet:

Ticari işlemlerin günümüzde büyük oranda elektronik ortamlarda yürütülmesi, bu işlemlerin hukuki nitelikleri hakkında önemli sorunları gündeme getirmiştir. Söz konusu sorunların başında, işlemlerin bağlayıcılığı ve işlemi yürüten kişinin gerçek kimliğinin tespiti gelmektedir. Bu sorunların çözümüne yönelik olarak elektronik imza tekniği geliştirilmiş, çok sayıda ülke elektronik imza kanunlarını uygulamaya koymuştur. Elektronik imza kanunları genel olarak, elektronik ortamlardaki ticari işlemlerin ve kamu kurumlarıyla gerçekleştirilen işlemlerin güvenli bir şekilde yürütülmesini hedeflemektedir. Ülkemizde 2004 yılında yürürlüğe giren Elektronik İmza Kanunu, Avrupa Komisyonu'nun 99/93/EC sayılı Direktif'i temel alınarak hazırlanmıştır. Bununla birlikte kanunumuz, gerek yukarıda belirtilen Direktif gerekse bu çalışmada incelenen Alman İmza Kanunu ile karşılaştırıldığında önemli farklılıklar arz etmektedir.

Anahtar Kelimeler: *Elektronik imza, Açık anahtar altyapısı, Elektronik İmza Kanunu*

Abstract:

In today's world commercial operations are mostly carried out in electronic environments and this situation cause important problems about legal qualities of these operations. The mostly faced problems occur about legal bindingness and identification of the person who really carries out these operations. To overcome these problems the electronic signature technique was developed and in many countries electronic signature law took effect. These laws generally aim to secure commercial and official interactions that are applied in electronic environments. In our country the electronic signature law took effect on January 15, 2004. This law was

* Öğretim Görevlisi Dr., Marmara Üniversitesi, İ.İ.B.F., Almanca İşletme Enformatiği Bölümü

built on the base of the EU Directive 99/93/EC. Nevertheless, the Turkish Law has remarkable differences compared to EU Directive and also to German electronic signature law handled in this work.

Keywords: *Electronic signature, Public key infrastructure, Electronic Signature Code*

Giriş

Son yıllarda sıkça vurgulanan "değişim", etkisini en fazla teknolojiyle doğrudan ilgisi olan alanlarda göstermektedir. Bunun nedeni, enformasyon ve iletişim teknolojilerinin baş döndürücü bir hızla gelişmesidir. Değişim; kurallara, yapılara, süreçlere ve bunun sonucunda hukuk sistemlerine de yansımakta, böylece bizleri yeni olgular, gereksinimler ve sorunlarla karşı karşıya bırakmaktadır. Söz konusu değişim kullandığımız kavramlara da yansımaktadır. Bilgi toplumu, e-ticaret, entelektüel sermaye gibi kavramlar bundan birkaç yıl öncesine kadar çok az kişi tarafından bilinirken, günümüzde hemen herkesin kullandığı kavramlar haline gelmiştir.

Ticari işlemler de enformasyon ve iletişim teknolojilerindeki gelişmelerden önemli oranda etkilenmektedir. Günümüzde ticari işlemler büyük oranda elektronik ortamlarda gerçekleştirilmekte, özellikle farklı yerlerdeki iş ortakları veya diğer paydaşlarla yürütülen çalışmalarda, teknolojiden yoğun şekilde yararlanılmaktadır. E-ticaretin yanında e-devlet uygulamaları da gerek Türkiye'de gerekse diğer ülkelerde hızla yaygınlaşmaktadır. Vatandaşlar, vergi, pasaport, bilgi sorgulama gibi birçok işlemlerini elektronik ortamlarda gerçekleştirmektedir. Hem e-ticaret işlemlerinin hem de e-devlet uygulamalarının yaygınlaşmasında, güvenli ve tutarlı bir hukuksal altyapı en önemli faktörler arasında yer almaktadır. Elektronik imza ise söz konusu hukuksal altyapının düzenlemesi gereken temel bir unsuru ifade etmektedir.

Bu çalışmada öncelikle elektronik imza kavramı incelenmiştir. İkinci bölümde, elektronik imza uygulamalarındaki sorunlar ana hatlarıyla ele alınmıştır. Ardından, elektronik imza altyapısının en önemli bileşenlerinden olan açık anahtar altyapısı, sertifika sağlayıcılar ve standartlar işlenmiştir. Dördüncü bölümde e-imzanın hukuksal altyapısı; e-imza kanunları, Avrupa Birliği Direktifi, Alman İmza Kanunu ve Türk Elektronik İmza Kanunu bağlamında incelenmiştir. Çalışmanın son bölümünü ise sonuç bölümü oluşturmaktadır.

1. Elektronik İmza (E-İmza)

Elektronik imza, el yazısıyla oluşturulan imzanın elektronik ortamdaki karşılığı olarak görülebilir. Bu bağlamda, el yazısıyla oluşturulan imzanın

sahip olması gereken özellikler, elektronik imzada da bulunmalıdır. İmza, herhangi bir uzunluktaki metne yapılan ek niteliğindedir. İmza fiziksel olarak metne bağlıdır ve taklit edilemez. İmzanın doğruluğu sınanabilir olmalıdır.

Yukarıda belirtilen özelliklerin E-imzada da bulunabilmesi amacıyla asimetrik kriptografi (şifreleme) ve özetleme fonksiyonları (Hash-Function) birlikte kullanılmaktadır. Mesajı gönderen kişi, özetleme fonksiyonu aracılığıyla mesaja ait bir özet değer oluşturmakta ve bu değeri kendine ait gizli anahtarla (private key) şifrelemektedir. Şifrelenmiş özet değer, e-imza olarak adlandırılmaktadır. Gönderici mesajı ve e-imzayı alıcıya birlikte iletmektedir. Alıcı bu imzayı göndericinin açık anahtarı ile (public key) açmakta, diğer taraftan ise mesaj üzerinden kendisi bir özet değer oluşturmaktadır. İki değerin de aynı olması durumunda, imza kabul edilmektedir (Stinson, 1995).

Özetleme fonksiyonlarının kullanımı sayesinde, yukarıda belirtilen ilk iki özellik (imzanın herhangi bir uzunluktaki metne yapılan ek niteliğinde olması ve fiziksel olarak metne bağlı bulunması) sağlanmış olmaktadır. İmzanın uzunluğu, özet değerin uzunluğu kadar Bit'ten (1 ve 0 olabilen en küçük veri birimi) oluşmaktadır ve özetleme fonksiyonunun kullanımı yoluyla metne bağlı bir yapı arz etmektedir. Eğer özet değer metinden ayrılırsa, bu değer başka metinleri imzalamak için kullanılamaz çünkü bu durumda özet değer de değişecek ve normal bir süre içerisinde başka bir metne uyumlu hale getirilemeyecektir. Gizli anahtarın kullanılması ise imzanın taklit edilememesini garanti altına almaktadır çünkü bu anahtar yalnızca gönderici tarafından bilinmektedir (Wobst, 1997).

2. E-İmza Uygulamalarındaki Sorunlar

E-imza sayesinde, e-ticaret ve e-devlet işlemlerinde elektronik dokümanların imzalanmasında, teorik temelleri olan ve güvenli bir araç kullanıma sunulmuş olsa da uygulamada çeşitli sorunlarla karşılaşılmaktadır. Bu sorunlar, uygulamanın engellenmesine, verimli olmayan kullanımlara hatta güvenli olmayan çözümlerin teşvik edilmesi gibi sorunlara yol açabilmektedir. E-imzalar, elektronik sertifika hizmet sağlayıcıları tarafından üretilmekte ve sertifikalandırılmaktadır. Uygulamada, sertifikaların geçersiz kılınması gerekebilir. Sertifikaların kolayca toplanması mümkün olmadığından, geçersiz imzalar, en azından sertifikanın geçerlilik tarihine kadar, kaydedilmelidir. Geçersiz sertifikaların oluşturduğu listenin kapsamı zamanla artacağından, bu sertifikaların etkin arama yöntemleri ile işlenmesi zorunlu olacaktır.

Diğer tarafta, sertifikaların yenilenmesi bazı durumlarda zorunlu olacaktır. Örneğin https'nin kullanımında, sertifikaların kullanım sürelerinin dolduğu veya güvenilir olmayan kurum tarafından üretildiğine çok sık rastlanmaktadır. Sertifikaların üretilmesi ve e-imzanın kullanımı, belirli çalışmaları (kayıt, süre dolduğunda yenileme, yazılımın kurulması) ve masrafları da (kayıt, yonga kartın satın alınması) beraberinde getirmektedir. Bu yüzden, az sayıda işlem gerçekleştiren bireysel kullanıcılar e-imzayı tercih etmeyebilir. Müşterilerin bu alandaki imkânları kullanmaması, e-imzayı firmalar için de güncel bir konu olmaktan çıkaracaktır (Ordemann, Chairi, 2002).

E-imza kullanımına birden fazla tarafın katılması, tarafların ilgi alanlarının birbiriyle çatışmasına yol açabilir. Dolayısıyla sadece tek bir resmi makamda veya firmada gerçekleştirilecek olan çözümlerin uygulamaya geçirilmesi, daha başarılı şekilde yapılabilir. Ayrıca, e-imza konusundaki güvenlik bilinci, büyük firmalarda dahi yeterince gelişmemiştir. Mesajlar ve İnternet protokolleri, şifrelenmeleri mümkün olmasına rağmen, çoğunlukla şifresiz şekilde gönderilmektedir (Digital Signature Law Survey).

3. Açık Anahtar Altyapısı, Sertifika Sağlayıcılar ve Standartlar

E-imzanın önceki bölümde belirtilen özelliklerinden sonuncusu, imzanın doğruluğunun sınanabilir olması, açık anahtar altyapısının (public key infrastructure) kullanımıyla mümkün olmaktadır. Bir e-imzanın sınanabilmesi, "sertifika"lar sayesinde mümkün olmaktadır. Sertifikalar metin verilerini ifade etmektedir. Bu veriler; mesajı imzalayan kişinin açık anahtarını, imzalayanla ilgili çeşitli kişisel bilgileri, anahtarla ilgili bilgileri (Örnek: Kullanılan özetleme fonksiyonu veya geçerlilik tarihi) ve sertifikayı düzenleyen kurumla ilgili enformasyonları içermektedir (Mundy, Chadwick, 2003).

Sertifikalar, elektronik sertifika hizmeti sunan kurumlar tarafından düzenlenmektedir. Bu kurumlar, 5070 sayılı Elektronik İmza Kanunu'nda "elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler" olarak tanımlanmaktadır (Elektronik İmza Kanunu, madde 8). Söz konusu kurumlar, başvuru esnasında kimlik doğrulaması yapmakta, açık ve gizli anahtarları üretmekte, açık anahtarı sertifika aracılığıyla yayınlamakta, gizli anahtarı ise bir yonga kart ile sahibine iletmektedir. Bu kurumlar anahtarların yönetimi ve zaman damgası gibi çeşitli hizmetler de sunmaktadır.

Şifreleme ve sertifikasyon sistemlerinin standart yöntemler haline dönüştürülmesi, standardizasyon hizmeti sunan kurumlar aracılığıyla gerçekleştirilmektedir. Örneğin ABD'deki NIST (National Institute for Standards and Technology, Ulusal Standartlar ve Teknoloji Enstitüsü) adlı kurum, DES, ardından 2001 yılında AES isimli yöntemleri simetrik şifreleme standartları olarak, DSA imzalama yöntemini ise e-imza standardı olarak belirlemiştir. Uluslararası Telekomünikasyon Birliği ise X.509 isimli standardı sertifikalar için önermiştir. Bu sistemlerin ücretsiz olmaları ve kalite bağlamında yoğun şekilde sınanmalarına rağmen, e-imza alanındaki standardizasyon çalışmaları dünya çapında genel kabul gören bir yapıya dönüşmemiştir. Söz konusu sistemlerin yanında, Blowfish, RC5, IDEA veya RSA imzası da pratikte geçerliliğini ispat etmiş ve sıkça kullanılan sistemlerdir (Burnett, Pain, 2001).

Elektronik ortamdaki unsurlar için standardizasyon hizmeti sunan bir diğer kurum ise IETF (Internet Engineering Task Force) isimli kurumdur. Bu kurum temel olarak İnternet protokollerinin (TCP/IP veya http) standardizasyonu konusunda faaliyet göstermektedir. Kurumun genel yapısı farklı yetkinliklerden oluşan bir birlik şeklindedir ve kurumun tavsiyeleri genel olarak takip edilmektedir. Bununla birlikte bir sistemin kabul görmesinde daha önemli olan nokta, büyük enformasyon teknolojisi firmalarının bu sistemi geliştirmesi veya en azından sistemi desteklemeleridir. Böylece SSL protokolü Netscape firması tarafından bir şifreleme protokolü olarak İnternet tarayıcılarına yerleştirilmiştir ve günümüzde dünya çapında kullanılmaktadır. Söz konusu kullanım, yukarıda adı geçen IETF'nin başka bir protokolü (s-http) tavsiye etmesine rağmen gerçekleşmektedir. Bu arada IETF, SSL'nin devamı olan TLS'yi standartlaşmıştır. Ayrıca SET sisteminin ardında da VISA ve Mastercard gibi kredi kartı firmalarının yanında büyük enformasyon teknolojisi firmalarının (Örnek: Microsoft, Netscape) desteği olduğu görülmektedir.

Herhangi bir şifreleme sisteminin seçiminde rol oynayan diğer bir önemli kıstas ise patent hukuku bağlamındaki konulardır. Örnek olarak PGP sisteminde RSA ve IDEA yöntemleri melez (hybride) bir sistem bağlamında bir araya getirilmektedir. Bununla birlikte, her iki yöntem içinde belirli bir lisanslama süreci gerekmektedir. SSL'nin ücretsiz sürümlerinde de bu yüzden IDEA'dan vazgeçilmiştir. Lisans ücretleri, çeşitli yöntemler bağlamında kullanılan rutin işlemler için de gündeme gelebilmektedir.

4. E-imzada Hukuksal Temeller

Mesajların şifrelenmesi, askeri alanlar ve gizli servis faaliyetleri yanında, e-ticaret için de büyük önem arz etmektedir. Ticari işlemlere temel

oluşturan şifrelenmiş mesajların hukuksal olarak ne şekilde değerlendirileceği konusunda, dünya çapındaki kanunlar son yıllarda önemli ölçüde serbestleştirilmiştir (Crypto Law Survey). Bununla birlikte, halen bazı ülkeler şifreleme yazılımlarının kullanımını sınırlandırmaktadır. Örneğin Çin ve Rusya'da şifrelemeye izin verilmemektedir. Ayrıca bazı Batı ülkelerinde de şifrelemeyle ilgili çeşitli sınırlandırmalar bulunmaktadır. Fransa, 2004 senesine kadar, mesajların şifrelenmesini yasaklamış ancak bu yasak daha sonra değiştirilmiştir. Fransa'da şifreleme yazılımlarının hazırlanması halen belirli kurallara bağlıdır ve talep gelmesi durumunda, şifrelenen mesajın çözülmesi de mümkün kılınmalıdır. Buna yönelik olarak Fransa'da kullanılan anahtarın bir kısmının açıklanması zorunluluğu da bulunmaktadır. Söz konusu durum ABD için de geçerlidir. ABD'de şifreleme yazılımları çeşitli değerlendirmelere tabi tutulmakta ve belli yazılımların ihracına izin verilmemektedir.

4.1 E-imza Kanunları

Birçok ülkede ve Avrupa Birliği'nde, farklı isimlerle de olsa e-imza kanunları bulunmaktadır. Bu kanunlarda özellikle, e-imza ile el yazısına dayanan imzanın eşit statüde değerlendirilmesi, imzanın kalitesiyle ilgili gereklilikler, elektronik sertifika hizmet sağlayıcılarının rolü ve kötüye kullanım durumundaki cezalar düzenlenmektedir. Söz konusu kanunlar farklı terminolojiler kullanmaktadır. Örneğin Alman İmza Kanunu, mesajların gizli anahtarla "imzalandığını", açık anahtarla ise "onaylandığını" belirtmektedir. Avrupa Biriliği'ndeki imza kanunu ise daha geniş kapsamlıdır. Bu kanun biyometrik sistemleri ve simetrik şifrelemeye dayanan sistemleri de e-imza olarak tanımaktadır.

Sertifikalarla ilgili temel sorumluluk, tüm kanunlarda, elektronik sertifika hizmet sağlayıcısına verilmiştir. İmzanın veya anahtarların sahipleri aracılığıyla kötüye kullanımı hakkındaki detaylar, kanunlarda değişik tanımlarla ve yorumlarla ifade edilmektedir. Avrupa İmza Direktifi, Alman Kanunu'nun üstünde yer almaktadır. Bu yüzden Alman İmza Kanunu, Avrupa'daki Direktifin 1999'da yürürlüğe girmesinin ardından yeniden şekillendirilmiştir. Vurgulanması gereken bir diğer önemli husus da imza kanunları bağlamında diğer kanunlar veya yönetmeliklerde de çeşitli değişikliklerin yapılmasının gündeme gelebileceğidir. Örnek olarak, kullanılan şifreleme yöntemleri temelde haberlerin şifrelenmesiyle ilgilidir ve burada iletişim hakkındaki kanunlar gündeme gelmektedir.

Alman Devleti konuyla ilgili kanunu, 16 Mayıs 2001 tarihinde yürürlüğe koymuştur. Bu kanun, "Gesetz über Rahmenbedingungen für elektronische Signaturen" (Elektronik İmzalar için Çerçeve Koşullar Hakkında Kanun)

olarak adlandırılmıştır. Ülkemizdeki kanun ise 15 Ocak 2004 tarihinde yürürlüğe girmiş ve Elektronik İmza Kanunu olarak adlandırılmıştır. Her iki kanun da Avrupa Komisyonu'nun 99/93/EC sayılı, Elektronik İmzalara İlişkin Direktif'ini temel almaktadır.

4.2 Avrupa Komisyonu'nun "Elektronik İmzalara İlişkin Direktifi"nin ve Türk "Elektronik İmza Kanunu"nun Genel Karşılaştırması

Ülkemizdeki Elektronik İmza Kanunu'nda yer alan tanım ve tespitler, genel olarak Avrupa Komisyonu'nun konuyla ilgili direktifine uyum göstermektedir. Bununla birlikte, söz konusu kanun ve direktif arasında bazı farklılıklar da bulunmaktadır. Bu farklılıklardan başlıcaları şöyle belirtilebilir: (Keser, vd. 2004; Varas, 2002; Berber)

- Direktifte yer alan "gelişmiş elektronik imza"y (advanced electronic signature, 99/93/EC, md.2/2-b), Türk Kanununda değinilmemektedir. Direktif, elektronik imza çeşitlerini, elektronik imza ve gelişmiş elektronik imza olarak tanımlarken, Kanunumuzda elektronik imza ve güvenli elektronik imza ayrımı yapılmıştır.

- Direktifte "elektronik veri" kavramının tanımı yapılmamıştır. Türk Kanununda ise elektronik veri "Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar" şeklinde tanımlanmaktadır.

- Direktifte yer alan ancak Türk Kanununda belirtilmemiş tanımlar da mevcuttur. Bunların başlıcaları, "elektronik imza ürünleri" ve "ihtiyari akreditasyon" kavramlarıdır. Elektronik imza ürünleri, sertifika hizmeti sunan kurumlar tarafından elektronik imza servisleri için kullanılan ya da elektronik imzanın doğrulanmasında veya oluşturulmasında yararlanılan donanım, yazılım bileşenlerini ifade etmektedir. İhtiyari akreditasyon ise yönetsel, prosedürle veya sunulan hizmetlerle ilgili olarak, kanunda belirtilenlere ek olarak ortaya çıkabilecek unsurların tanımlandığı ve akredite edilen kurumların akredite edenlerin verdiği onaya dayanarak, bu onay çerçevesinde ifade edilen hak ve yetkilerin kullanılmasına imkân tanıyan bir sistemdir.

- Direktifte "zaman damgası" kavramının tanımı yapılmamıştır. Türk Kanununa göre ise zaman damgası, "Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydını" ifade etmektedir.

- Kanunumuzun 23. maddesi, 18.6.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanununa 295 inci maddeden sonra gelmek üzere 295/A maddesinin eklenmesini öngörmektedir. Bu madde, usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olduğunu, söz konusu verilerin aksi ispat edilinceye kadar kesin delil sayılacaklarını belirtmektedir. Direktifte ise elektronik imzanın delil niteliğinin inkâr edilememesiyle ilgili geniş açıklamalarda bulunulmuştur. Kanun'umuza dahil edilmeyen bu maddelere göre elektronik imzanın delil niteliği üye devletlerce;
  - o Elektronik şekilde olması,
  - o Nitelikli sertifikaya dayanmaması,
  - o Akreditasyon almış bir sertifika hizmet sağlayıcının sunduğu sertifikaya dayanmaması ve
  - o Güvenli elektronik imza oluşturma aracı ile oluşturulmamış olması nedenlerinden biri sebebiyle yadsınamaz.
- Direktifte, nitelikli elektronik sertifikaların ancak "nitelikli sertifika verme" yeterliliğine sahip kurumlarca verilebileceği belirtilmekte, 5070 sayılı kanunda ise böyle bir hüküm bulunmamaktadır. Ayrıca Direktifte nitelikli hizmet sağlayıcılar için öngörülen hükümler kanunumuzda ilk bakışta tüm servis sağlayıcılar için geçerliymiş gibi görünmektedir.
- Kanunumuzda, elektronik sertifika hizmet sağlayıcılarının denetimine ilişkin hükümler, Avrupa Komisyonu Direktif'ine göre oldukça belirsiz durumdadır. Direktif, üye devletlerin kendi sınırları içerisinde, nitelikli elektronik sertifika sunan kurumların denetimini yapmak üzere yetkili bir sistem oluşturmalarını öngörmektedir. Türkiye'de, elektronik sertifika hizmet sağlayıcılarının denetimi yetkisi Telekomünikasyon Kurumu'na verilmiştir.

Avrupa Komisyonu Elektronik İmzalara İlişkin Direktifi ile Türk Elektronik İmza Kanunu arasındaki bu farkların yanında, vurgulanması gereken diğer bir nokta, ABD kanunları ve kanunumuz arasındaki "elektronik imzanın kullanılması yasak olan" durumlara ilişkin farklılıktır. 5070 sayılı kanunun 5. maddesi 2. fıkrasında "Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez" hükmü bulunmaktadır. Bu hükümden, vasiyet işlemleri, tapu kayıtlarında değişikliğe yol açacak işlemler gibi çeşitli işlemlerde elektronik imzanın kullanılamayacağı anlaşılmaktadır. Benzer hükümler diğer ülkelerdeki kanunlarda bulunsa da bazı ülkeler bu konuda daha esnek bir anlayış benimsemişlerdir. Örneğin, ABD'deki Eyaletlerarası veya Dış Ticarette Elektronik Kayıtların ve İmzaların Kullanılmasını Kolaylaştıracak Kanun Bölüm 103'de, belirlenen

alanlarda, elektronik imzanın üç yıllık süre için kullanılamayacağını, üç yıllık süre içinde Ticaret Bakanlığının bu yasaklamanın tüketicilerin korunması için gerekli olmaya devam edip etmediğini kontrol edeceğini hükme bağlamıştır. 5070 sayılı kanun ise elektronik imzanın kullanılamayacağı alanlar konusunda mutlak bir yasaklama getirmiştir (Berber, 2006).

4.3 Alman "Elektronik İmzalar için Çerçeve Koşullar Hakkında Kanunu" ve "Türk Elektronik İmza Kanunu"nun Genel Karşılaştırması

Alman İmza Kanunu ile Türk E-imza Kanunu arasındaki önemli farklardan biri, zaman damgası konusundaki hükümlerdir. Alman Kanunu zaman damgasının taşıması gereken teknik özellikler ve zaman damgası hizmeti sunan kurumların uyması gereken yükümlülükler ile ilgili hükümlere yer verirken, Türk Kanununda böyle bir hüküm bulunmamaktadır. Kanunumuzun 20. maddesinde yönetmelikle düzenlenecek hükümler belirlenirken, zaman damgasına değinilmemiştir. Ayrıca Alman Kanunu ihtiyari akreditasyon ile ilgili hükümlere yer verirken, kanunumuzda böyle bir hüküm bulunmamaktadır (Keser, vd. 2004).

Söz konusu kanunlar arasındaki diğer bir önemli farklılık ise elektronik sertifika hizmet sağlayıcılarının yatırmaları gereken teminatla ilgilidir. Alman Kanunu 13. maddesinde, faaliyete geçmek için kanunun ve yönetmeliğin aradığı koşulları yerine getiren sertifika hizmet sağlayıcılarının, 250.000 Euro değerinde teminat tedbiri göstermeleri gerektiği belirtilmektedir. Bunun nedeni, söz konusu kurumların Kanununun ve Yönetmeliğin aradığı şartları ihlal etmeleri ya da nitelikli elektronik imza veya kullanılan diğer teknik araçlar bakımından ürünlerinin yetersiz olması durumunda, ortaya çıkabilecek zararın giderilmesine yöneliktir. Türk Kanununda ise teminat tedbiri ile ilgili herhangi bir hüküm bulunmamaktadır (Berber, 2006).

Elektronik imzanın hangi alanlarda kullanılamayacağı konusunda, Alman Kanunu ve Türk Kanunu arasında çeşitli farklar bulunmaktadır. Türk Elektronik İmza Kanunu'nda, elektronik imzanın kullanılamayacağı alanlar "kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile teminat sözleşmeler" olarak tanımlanmaktadır. Alman Kanunu'nda ise çeşitli resmi belgeler (Örnek: Üniversite diploması), işten çıkılacağının veya çıkarılacağının bildirilmesi, kefalet gibi konular, elektronik imzanın kullanılamayacağı alanlar olarak belirtilmektedir.

4.4 Kanunlar Arasındaki Farklılıkların Genel Değerlendirmesi

E-imza kanunları, çok sayıda ülkede yürürlüğe girmiştir. Bu ülkelerin çoğunda, e-imza el yazısıyla oluşturulan imzaya eşit statüde değerlendirilmektedir. E-imza kanunlarının giderek daha serbestleştiği ve esnek bir hale geldiği görülmektedir. Bu durumun ortaya çıkmasında, teknolojideki ilerlemeler önemli rol oynamaktadır. Kanunlarda kullanılan tanımlar, yapılan yorumlar ve kanunların kapsamı, ülkeden ülkeye farklılık göstermektedir. Bununla birlikte, tüm kanunların ortak noktası, e-imza uygulamalarının güvenli şekilde gerçekleştirilmesini amaçlayan hükümlerin ifade edilmiş olmasıdır.

Gerek Alman Kanunu gerekse Türk Kanunu, Avrupa Komisyonu tarafından yayınlanan 99/93/EC sayılı, Elektronik İmzalara İlişkin Direktif çerçevesinde oluşturulmuştur. Bununla birlikte, Direktifte yer alan çeşitli tanımların kanunumuzda yer almadığı veya Alman ve Türk Kanunlarında farklı şekillerde yorumlandığı görülmektedir. Diğer ülkelerde veya birliklerde oluşturulan kanunlar karşılaştırmalı hukuk olarak kullanılırken, bu kanunların hangi şartlarda ve hangi çalışmalar / araştırmalar sonucunda oluşturulduğu da göz önünde bulundurulmalıdır. Böylece kanunlar arasındaki farklılıklar en aza indirilmiş olacaktır.

5. Sonuç

Enformasyon ve iletişim teknolojilerinde kaydedilen ilerlemeler, e-ticaret ve e-devlet işlemlerinin kapsamını genişletmekte, bu işlemleri daha da yaygınlaştırmaktadır. Bu gelişmenin etkin ve sürekli olarak devam etmesinde, kullanıcıların elektronik sistemlere olan güveni belirleyici rol oynamaktadır. Geliştirilen çeşitli teknikler ile verilerin güvenliği sağlanmaya çalışılmaktadır. Bu tekniklerden başlıcaları, asimetrik şifreleme teknikleri, özetleme fonksiyonları ve e-imzadır.

E-imzanın taşıması gereken özellikler, el yazısıyla oluşturulan imza ile aynıdır. Uygulamada e-imzanın kullanımında çeşitli sorunlar görülmektedir. Söz konusu sorunların çözümünde, e-imza işlemlerinin gerek teknik açıdan gerekse hukuksal açıdan güvenilir bir altyapıya kavuşturulması önemli rol oynayacaktır. Hukuksal altyapı ve kullanılan teknikler arasındaki uyum, bu tekniklerden etkin ve verimli şekilde yararlanılmasında büyük önem taşımaktadır.

Birçok ülke, son yıllarda e-imza kanunları yayınlamış ve bu kanunlarda e-imzanın ve el yazısıyla oluşturulan imzanın aynı hükümde olduğunu belirtmiştir. Avrupa Biriliği ve Birlik üyeliğine aday ülkelerdeki kanunlar, Avrupa Komisyonunun 99/93/EC sayılı Direktif'ine uygun olmak

durumundadır. Ülkemizde bu alandaki Kanun 2004 yılında yürürlüğe girmiştir. Kanunumuz genel olarak, yukarıda belirtilen Direktife uyumlu olsa da arada bazı tanım ve yorum farkları bulunmaktadır. Kanunumuz Alman Kanunu ile karşılaştırıldığında ise Alman Kanununun söz konusu Direktife daha uygun olduğu değerlendirilmektedir.

Kaynakça:

Berber, L.K. (2006). Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi. Erişim: 01.10.2006, www.e-imza.gen.tr/templates/resimler/File/makaleler/Elektronik_imzanin_Duzenlenmesi_Leyla_Keser.doc.

Burnett, S., Paine, S. (2001). *RSA Security's Official Guide to Cryptography*. Berkeley: McGraw-Hill.

Keser, L., Beceni, Y., Sevim, T. (2004). *Hukuk Çalışma Grubu, İlerleme ve Sonuç Raporu*. İstanbul: Elektronik Ulusal Koordinasyon Kurulu.

Mundy, D.P., Chadwick, D.W. (2003). Security issues in the electronic transmission of prescriptions. *Medical Informatics & the Internet in Medicine*. 28 (4), 253-277.

Ordemann, D., Chairi, Y. (2002). Elektronische Signaturen – Sicherheitsgarant im Zeitalter digitaler Transaktionen?, *Zeitschrift für Information Management & Consulting*. 17 (2), 33-38.

Stinson, D. (1995). *Cryptography: Theory and Practice*, Boca Raton, Florida: CRC Press.

Varas, M. (2002). 'E-imza Paneli Notları'. *VII.Türkiye'de Internet Konferansı 19-21 Aralık*. İstanbul.

Wobst, R. (1997). *Abenteuer Kryptologie: Methoden, Risiken und Nutzen der Datenverschlüsselung*, Bonn u.a.: Addison Wesley Longman Verlag GmbH.

Alman İmza Kanunu. Erişim: 01.10.2006, http://www.e-imza.gen.tr/index.php?Page=Mevzuat&HukukiAltYapiNo=26.

Crypto Law Survey. Erişim: 01.10.2006, rechten.uvt.nl/koops/cryptolaw.

Digital Signature Law Survey. Erişim: 01.10.2006, dsls.law.uvt.nl.

Elektronik İmza Kanunu. Erişim: 01.10.2006, http://www.hukuki.net/kanun/5070.15.text.asp.