T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK (MEDENİ HUKUK)
ANABİLİM DALI

ELEKTRONİK İMZA

Yüksek Lisans Tezi

Ayşe Gürbüz

Tez danışmanı
Prof.Dr.M. Ali Erten

Ankara-2005

T.C.
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK (MEDENİ HUKUK)
ANABİLİM DALI

ELEKTRONİK İMZA

Yüksek Lisans Tezi

Tez danışmanı: Prof.Dr.M. Ali Erten

Tez Jürisi Üyeleri

Adı ve Soyadı	İmzası
Prof. Dr. Ali ERTEN	.....
Prof. Dr. Kudret GÜVEN	.....
Doç. Dr. Zarife SENOCAK	.....
.....	.....
.....	.....
.....	.....

Tez Sınavı Tarihi 16.09.2005

İÇİNDEKİLER

İKİNCİ BÖLÜM

ELEKTRONİK SÖZLEŞMELER

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK İMZA

DÖRDÜNCÜ BÖLÜM

DİJİTAL İMZALI ELEKTRONİK BELGELERİN TÜRK MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

KISALTMALAR

AAA : Açık Anahtar Altyapısı

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

ARPA : Advanced Research Project Agency

ARPANET : Advanced Research Projects Agency Network

Art. : Artikel

Aşa. : aşağıda

ATM : Automated Teller Machines

BATİDER : Banka ve Ticaret Hukuku Dergisi

B2C : Business to Consumer(İşletmeler-Tüketiciler arası E-Ticaret)

BGB : Bürgerliches Gesetzbuch (Alman Medeni Kanunu)

BK : Türk Borçlar Kanunu

BM : Birleşmiş Milletler

BTYK : Bilim ve Teknoloji Yüksek Kurulu

BK : Borçlar Kanunu

Bkz. : bakınız

Bs. : Bası

C : Cilt

CEFACT : Center for Facilitation of Procedures and Practices for Administration, Commerce and Transport

CONSOB : Commissione Nazionale per le Societa e la Borsa

Çev. : Çeviren

DARPA : Defense Advanced Research Projects Agency (Savunma İleri Düzey Araştırma Projeleri Kurumu)

DPT : Devlet Planlama Teşkilatı Müsteşarlığı

DTM : Dış Ticaret Müsteşarlığı

dn. : dipnot

EC : European Community (Avrupa Birliği)

e-Devlet : elektronik Devlet

EDI : Electronic Data Interchange (Elektronik Data Değişimi)

EFT : Elektronik Fon Transferi

EFTPOS : Electronic Funds Transfer from the Point of Sale

EİK : Elektronik İmza Kanunu

e-imza : elektronik imza

e-mail : electronic mail (elektronik posta)

e-sözleşme : elektronik sözleşme

e-ticaret : elektronik ticaret

ETKK : Elektronik Ticaret Koordinasyon Kurulu

f. : fıkra

ff : fortfahrend

HUMK : Hukuk Usulü Muhakemeleri Kanunu

IOSCO : International Organization of Securities Commissions

IP : Internet Protocol (Internet Protokolü)

ISS : Internet Servis Sağlayıcı

İBB : İstanbul Barosu Dergisi

İGEME : İhracatı Geliştirme Merkezi

md.	: madde
MK	: Türk Medeni Kanunu
OECD	: Organisation for Economic Co-operation and Development (Ekonomik İşbirliği ve Kalkınma Teşkilatı)
Örn.	: örneğin
par.	: paragraf
PIN	: Personal Identification Number
RG	: Resmi Gazete
sh.	: sayfa
SigG	: Signaturgesetz (Dijital İmza Kanunu)
SigRL	: Avrupa Topluluğu İmza Yönergesi
SigV	: Signaturverordnung (Dijital İmza Yönetmeliği)
TBB	: Türkiye Bankalar Birliği
TBMM	: Türkiye Büyük Millet Meclisi
TCP/IP	: Transmission Control Protocol/Internet Protocol (Transmisyon Kontrol Protokolü/ Internet Protokolü)
TKHK	: Tüketicinin Korunması Hakkında Kanun
TMK	: Türk Medeni Kanunu
TTK	: Türk Ticaret Kanunu
TUENA	: Türkiye Ulusal Enformasyon Altyapısı
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UNCTAD	: United Nations Conference in Trade and Development (Birleşmiş Milletler Ticaret ve Kalkınma Konferansı)
UNCITRAL	: United Nations Commission on International Trade Law

(Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)

UNECE : Birleşmiş Milletler Avrupa Ekonomik Komisyonu

UYAP : Adalet Bakanlığı'nın Ulusal Yargı Ağı Projesi

WTO : World Trade Organisation (Dünya Ticaret Örgütü)

vd. : ve devamı

vs : ve saire

YD : Yargıtay Dergisi

YK : Yeknesak Kurallar

yuk : yukarıda

ZPO : Alman Medeni Usul Kanunu

GİRİŞ

Geçtiğimiz yüzyılın ikinci yarısından itibaren gelişen ve halen de büyük bir ivme ile bu gelişmeyi sürdüren bilgisayar teknolojisi; insanların ve devletlerin sosyal, kültürel, ekonomik ve siyasi faaliyetlerinin dijital bir ortamda yapılmasına imkan sağlamaktadır.

Özellikle bilgisayarların birbirine bağlanması ile ortaya çıkan bir açık ağ (web) sistemi olan internet; başlangıcındaki askeri ve akademik amacının dışında, küresel düzeyde her alanı kapsayan ve ticari yönü de gittikçe artan bir özellik arzetmektedir. Internetin dünya çapında giderek artan ve yaygınlaşan bu kullanımı, daha düşük maliyetli, daha hızlı ve bilgiye dayanan yeni bir ticaret yöntemi olan elektronik ticareti de beraberinde getirmiştir.

Elektronik ticaret son on yılda büyük bir hızla gelişmiştir ve daha da artan bir hızla gelişmeye devam etmektedir. Elektronik ticaret hacmi her yıl katlanarak büyümektedir. Artık internette olmak bir tercih ya da teknolojiye ayak uydurmanın bir avantajı olmaktan çıkmış, bir zorunluluk haline gelmiştir. Kısaca, teknolojinin baş döndürücü bir hızla geliştiği ve sınırların kalktığı küresel bir dünyada elektronik ticaret mutlak hükümranlığını ilan etmek üzeredir. Çalışmamızın ilk bölümünde, elektronik ticaretin özünü teşkil eden internet ve elektronik ticaret kavramlarının gelişimi ve avantajları giriş mahiyetinde kısaca değerlendirilecektir.

Elektronik ticaretin hukuki temeli ve icra aracı, elektronik sözleşmelerdir. Elektronik sözleşmeler, internet üzerinden gerçekleştirilmesi nedeniyle, kendine özgü bazı

özellikler arz etse de, kuruluşuna ve hükümlerine, uygun düştüğü ölçüde borçlar hukukunda düzenlenen geleneksel sözleşmelere uygulanan hükümler uygulanabilecektir. Çalışmamızın ikinci bölümünde elektronik sözleşmelere ilişkin hukuki sorunlar çalışmamızın kapsamının elverdiği ölçüde incelenmeye çalışılacaktır.

Elektronik ticaretin gelişebilmesi ve kullanıcılar tarafından benimsenebilmesinin ilk şartı, internet ortamında ticariye ilişkiye giren tarafların güvenliğinin sağlanabilmesidir. Bu amaçla, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu garanti edebilen teknik ve yasal bir altyapıya dayanan elektronik imza yöntemleri kullanılmaktadır.

Çalışmamızın üçüncü bölümünde çalışmamızın ana konusunu teşkil eden elektronik imzanın teknik altyapısı, dijital imza kavramı, sistemin işleyişi ve özellikleri, elektronik imza sahibi (kullanıcı), onay kurumları ve güvenen taraf arasındaki ilişkiler, tarafların sorumlulukları ve elektronik imzalı belgelerin geçerlilik ve delil değerini düzenleyen kuralları belirleyen hukuki altyapı Türk hukuku ve yabancı hukuklar bakımından, UNCITRAL E-İmza Yeknesak Kuralları, AB düzenlemeleri ve 5070 sayılı Elektronik İmza Kanunu hükümleri çerçevesinde araştırılacak ve ilgili bölümlerde 5070 sayılı Elektronik İmza Kanunu'na ilişkin değerlendirmeler yapılacaktır.

Çalışmamızın dördüncü bölümünde, elektronik imzalı belgelerin ispat hukuku yönünden değerlendirilmesi yapılacaktır.

BİRİNCİ BÖLÜM

INTERNET VE ELEKTRONİK TİCARET

§1. INTERNET

I. TANIM

İngilizce "International Network" (Uluslararası Bilgisayar Ağı) kelimesinin kısaltılmışı olan Internet[1], teknik olarak, dünya kapsamında birçok bilgisayar sistemini TCP/IP ile birbirine bağlayan ve gittikçe büyüyen bir iletişim ağıdır[2]. TCP/IP, bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır.

Interneti dünya çapında milyonlarca bilgisayarı ve kullanıcıyı birbirine bağlayan ağların ağı [3] olarak da tanımlamak mümkündür[4].

---

[1] **Bozbel, S.:** Internet Üzerinden Yapılan Hukuki İşlemler, YD, C.27, Ocak-Nisan 2001, sh.273-303.

[2] **Orcan, S.:** T.C. Ulaştırma Bakanlığı TUENA Internet Çalışma Belgesi, Ocak 1998<http: <http://www.tuena.tub.gov.tr/rapor/cbelgeleri.htmFl.

[3] **Bryant, S.:** The Story of the Internet, Londan, 2000, sh.25; **Keeler, L.:** Cyber Marketing, USA, 1995, sh.105.

[4] Internet hakkında ayrıntılı bir araştırma için bkz. **Altınışık, U.:** Elektronik Sözleşmeler, Ankara, 2003, sh.14-24.

Internet, birden fazla haberleşme ağının (network) birlikte meydana getirdikleri bir iletişim ortamıdır. Bilgisayarlar vasıtasıyla oluşturulan bu iletişim ağları, kişilerin, birbirleri ile sınırsız amaç ve içerikte ilişki kurmalarını ve bilgi alışverişinde bulunmalarını sağlamaktadır. Internet, ABD Yüksek Mahkemesi'nin bir kararında, birbirleriyle bağlı bulunan bilgisayarlardan oluşan uluslararası ağ olarak tanımlanmıştır[5].

Internet'in ortaya çıkışı Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan DARPA vasıtasıyla olmuştur. 1969'da çeşitli bilgisayar bilimleri ve askeri araştırma projelerini desteklemek için Savunma Bakanlığı, ARPANET adındaki paket anahtarlamalı ağı oluşturmaya başlamış, bu ağ, ABD'deki üniversite ve araştırma kuruluşlarının değişik tipteki bilgisayarlarını da içererek büyümüştür[6].

Internetin, en üst düzeyde gizlilik anlayışının egemen olduğu bu merkezi ve hiyerarşik Pentagon düzeninden çıkıp, bugün ulaştığı, tamamen açık, şeffaf, yalın ve denetimden uzak bir organizmaya dönüşümü ilgi çekicidir. Bilgi iletişiminin dünya çapında, devamlı ve serbestçe yapılabileceği açık bir platform olarak tasarlanmış olan internet, iç organizasyonu bakımından ise, sınırlı birkaç uygulama için

---

[5]**Güran, S./Akünal, T./Bayraktar, K./ Yurtcan, E./ Kendigelen, A./Beller, Ö./ Sözer, B.:** Internet ve Hukuk Ortak Çalışma, Internet Hukuk Forumu, http://www.superonline.com/hukuk.

[6] Internet Society, A Brief History of Internet, http://www.isoc.org, sh.1.

tasarlanmamış, üzerinde her türlü yeni uygulamaların yapılmasına olanak verecek genel ve esnek bir altyapı olarak planlanmıştır[7].

II. AVANTAJLARI

Elektronik formatta ticari bilgi değişimi yeni bir olgu değildir. Özel ağlar üzerinden elektronik veri değişimi EDI[8] internetten daha öncesine dayanır. Ancak bu ağların yüksek kurma ve bakım maliyetleri bunların yalnızca büyük firmalar tarafından kullanılması sonucunu doğurmuştur.

Internet EDI'ye göre oldukça avantajlı koşullar sunmaktadır. Internete erişim maliyeti EDI'ninkinden çok daha azdır; elektronik pazarların kurulması ve sürdürülmesi oldukça düşük maliyetlidir; evrensel standartların kullanılması her iş kolu için bir ticaret platformu sağlayacak kadar esnek bir teknolojiyi beraberinde getirmektedir. Internet, yaygınlığı ve bağlantı kolaylığı nedeniyle bilgi değişimi için oldukça etkin bir mekanizmadır. E-ticaretin hızlı büyümesi, internetin keşfi ve bununla bağlantılı yazılım ve donanımın geliştirilmesi sayesinde gerçekleşmiştir[9].

---

[7] **Acır, B.:** Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, Sermaye Piyasası Kurulu Yeterlik Etüdü, Ankara, 2000, sh.9.

[8] EDI (Electronic Data Interchange) özel ağlar üzerinden ticari bilgi değişimi sağlayan bir iletim formatıdır (www.whatis.com).

[9] **Aydemir, İ.:** Elektronik Ticaret Alanındaki Rekabet Sorunları, Rekabet Kurumu Uzmanlık Tezi, Ankara, sh.6.

§2. ELEKTRONİK TİCARET

I.TANIMI

Internetin doğuşu ve telekomünikasyon teknolojilerinin gelişmesiyle ortaya çıkan e-ticaret, geleneksel ticareti kolaylaştıran bir yeniliktir[10]. Elektronik ticaret, tüm endüstrileri ve uygulamaları, üreticileri ve kullanıcıları, veri alışverişini ve ekonomik faaliyetleri internet olarak adlandırılan küresel bir pazarda bir araya getirmektedir.

Günümüzde bilginin ve verilerin elektronik olarak değişimi, elektronik ticareti uluslararası ticaretin en önemli bölümlerinden biri haline getirmiştir. Uluslararası ticareti düzenleyen geleneksel kuralların, bu gelişimi karşılayabilecek esneklikte olmadığı ve yeni düzenlemelere gerek duyulduğu kısa sürede kendini göstermiştir. E-ticaretin gelişim sürecinin, doğal olarak, internetin gelişimine paralel olduğu gözlenmektedir. Çünkü, e-ticaret kavramı genel olarak herkese açık elektronik ağ üzerinden gerçekleştirilen ticari faaliyetleri ifade etmektedir.

Yeni bir kavram olması dolayısıyla elektronik ticaretin değişik tanımları yapılmıştır. Kimilerine göre, elektronik araçlarla yapılan tüm ticari işlemler e-ticaret sayılırken, kimileri de sadece internet gibi açık ağlar üzerinde yapılan işlem ve ödemeleri e-ticaret saymaktadır.

---

[10]**İnce, M.:** Elektronik Ticaret: Gelişme Yolundaki Ülkeler İçin İmkanlar ve Politikalar, Devlet Planlama Teşkilatı Raporu,1999, sh. 2, 6.

Uluslararası organizasyonlar ile bu alanda faaliyet gösteren bazı uluslararası kuruluşların e-ticarete ilişkin tanımlarına bakıldığında;

WTO'nun tanımına göre; e-ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır[11].

OECD'nin tanımına göre, kurumların ve bireylerin katıldığı ve metin, ses, görsel imaj gibi sayısallaştırılmış verinin işlenerek, açık veya kapalı ağlar üzerinden iletilmesine dayanan ticaretle ilgili işlemlere elektronik ticaret denilmektedir[12].

Elektronik ticaretin yasal çerçevesinin çizilmesi için önemli çalışmalar yapan UNCITRAL'ın 1996 yılında hazırladığı Model Yasaya göre, ticari aktiviteler kapsamında her türlü veri mesajının, elektronik veri değişimi, internet, e-posta gibi gelişmiş yöntemlerin yanında, telekopi ve faks gibi daha az karmaşık yöntemler kullanılarak elektronik ortamda değişimi elektronik ticaret olarak tanımlamıştır [13].

Avrupa Komisyonunun yapmış olduğu tanıma göre e-ticaret, fiziki bağlantı veya fiziki değişimlere (değiş-tokuş) girmeksizin, tarafların elektronik olarak yaptıkları

---

[11] <http://www.wto.org/english/news-e/pr96-e.htm >.

[12] http://www.oecd.org.

[13] Tübitak Bilten (Bilgi Teknolojileri Elektronik Araştırma Enstitüsü), Türkiye İçin Elektronik Ticarete Geçiş Durum Değerlendirmesi ve Pilot Uygulama Projesi Raporu, 2000, sh. 6,8; UNCITRAL Model Law on Electronic Commerce With Guide to Enactment, <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

her türlü ticari işlem olarak ifade edilmiştir[14]. T.C. Ulaştırma Bakanlığının TUENA projesinde aynı tanım esas alınmıştır[15].

ETKK'nın Mayıs 1998 tarihli Hukuk Çalışma Grubu raporunda ise, e-ticaret; bireyler ve kurumların, açık ağ ortamında (Internet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (Intranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerinin tümü olarak ifade edilmiştir.

Bu çerçevede, ticari sonuçlar doğuran ya da ticari faaliyetleri destekleyecek eğitim, kamuoyunu bilgilendirme, tanıtım-reklam vb. amaçlar için elektronik ortamlarda yapılan işlemler de e-ticaret kapsamında değerlendirilmektedir [16].

A. GENİŞ ANLAMDA ELEKTRONİK TİCARET

Yapılan tüm bu tanımlamalar dikkate alındığında, elektronik ticareti, açık veya kapalı ağlar üzerinden, fiziki temas kurmaksızın, telekomünikasyon araçları kullanarak yapılan ticari faaliyetler olarak tanımlamamız mümkündür[17].

---

[14] <http://www.europa.eu.int./ISPO/ecommerce/answers/introduction> .

[15] T.C. Ulaştırma Bakanlığı, TUENA, Türkiye Ulusal Enformasyon Altyapısı Sonuçlar Özeti,1998,<http://www.tubitak.gov.tr/rapor/pdf/sonuc-ozet>.

[16] http://www.etkk.gov.tr.

[17] **Altınışık,** sh.25.

B. DAR ANLAMDA ELEKTRONİK TİCARET

Dar anlamda elektronik ticaret, özel mülkiyette olmayan açık ağlar üzerinden, bilgisayar aracılığıyla yapılan ticari faaliyetleri ifade etmektedir. Bu anlamda internet ticareti olarak de nitelendirilmekte ve elektronik ticaretin özünü teşkil ettiği savunulmaktadır[18].

II. ELEKTRONİK TİCARETİN KATEGORİLERİ VE ARAÇLARI

Elektronik ticaret geniş anlamda ele alındığında, taraflarına göre; işletmeler arasında (Business to Business-B2B), işletme ile tüketici arasında (Business to Consumer-B2C), işletme ile Devlet arasında (Business to Administration) ve tüketici ile Devlet arasında (Consumer to Administration) olmak üzere dört kategoride yapıldığı tespit edilmektedir[19].

---

[18] **Ertaş, S.:** Elektronik Ticaret: Tanımı, Gelişimi, Avantajları, Güvenliği, Elektronik Ticaret, sh.2; **Canpolat, Ö.:** E-Ticaret ve Türkiye'deki Gelişmeler, Sanayi ve Ticaret Bakanlığı Hukuk Müşavirliği, Ankara, Mart 2001, sh.7; **Akkaya, M.:** Elektronik Ticaretin Vergilendirilmesi, Elektronikteki Gelişmeler ve Hukuk, sh.177.

[19] **Arıkan, S.:** Elektronik Ticaret, Hukuk ve Noterler, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001, s.21-22; **Bozkurt, V.:** Elektronik Ticaretin Ekonomik ve Toplumsal Boyutu, Elektronik Ticaret, sh.65-66; **Akipek Öcal, Ş.:** Elektronik Ticarette Sözleşme, Bilişim Teknolojileri ve Hukuk Semineri, http://tubitak.gov.tr/anasayfadan/toplanti/sebnemakipek.htm.

Elektronik ticaretin gerçekleşmesinde kullanılan araçlar Telefon, Faks, Televizyon, EFT, EDI ve Internet'tir. Bazı kitle iletişim araçlarının teknolojik gelişmeler karşısında tüketici/ müşteri gereksinimlerini karşılamak açısından yetersiz kalması (TV, Telefon, Faks gibi) sonucu gerek mal, gerekse hizmet alımlarının potansiyel tüketiciler tarafından da bilinmesi amacıyla daha hızlı şekilde erişimi gerçekleştiren ve daha yaygın bir alana hitap edebilen, referans olarak önem taşıyan, bilgileri daha seri bir şekilde güncelleştirebilen ve zaman, mekan kavramını alıcı lehine ortadan kaldıran bilgisayar ağları, yani internet faaliyetleri devreye girmiştir.

III. AVANTAJLARI

Alıcı ve satıcıları elektronik ortamda karşı karşıya getiren e-ticaret, zamanın ve mekanın sınırlayıcı etkilerini ve taraflar arasındaki aracıları ortadan kaldırmakta; tüketicilere, mal ve hizmetlere ilişkin bilgilere daha kolay ulaşılabilen ve daha kolay karşılaştırma yapılabilen bir ortamda, geniş bir seçenek yelpazesi içinden alışveriş yapma imkanı; satıcılara ise fiziki mekan ve personel bulundurma, stokların izlenmesi gibi hususlarda tasarruf ve ürünlerin dağıtım ve pazarlamasında hız sağlamaktadır. Satıcılar ve alıcıların, şeffaf ve tam rekabete yakın bir ortamda bir araya gelmesine imkan tanıyan e-ticaret ile, ticari işlemler daha kolay, daha hızlı daha az maliyetle gerçekleştirilebilmektedir. Böylece kaynakların daha etkin kullanım ile toplumsal refahın artmasına katkı sağlanacaktır[20].

[20] **İnce**, sh.19, <http://ekutup.dpt.gov.tr/ticaret/incem/eticaret.html>.

E-ticaret, belirtilen bu avantajlarıyla OECD, UNCTAD ve WTO gibi uluslararası organizasyonlarca oluşturulmaya çalışılan, daha kolay, uyumlu, ucuz ve hızlı bir uluslararası ticari prosedür için çıkış noktasıdır[21].

IV. ELEKTRONİK TİCARETİN GELİŞİMİ

A. E-TİCARETİN DÜNYADAKİ GELİŞİMİ

E-ticaretin, Haziran 1995'de Java[22]'nın piyasaya sürülmesi ile başlayan on yıllık kısa bir geçmişi vardır. Bu kadar kısa bir geçmişi olmasına rağmen, e-ticaret önemli boyutlara ulaşmıştır ve katlanarak büyümeye de devam etmektedir.

E-ticaretin gelişmesinde belirleyici olacak en önemli faktör internet kullanıcı sayısıdır. Halen Dünya'da 600 milyon civarında internet kullanıcısı vardır[23]. Bu sayının artması ve bunun yanında kablosuz internet erişiminin yaygınlaşması ve geniş bant erişiminin sağlanması ile internet kullanım kalitesinin de yükselmesi beklenebilir.

---

[21] **İnce**, sh.7.

[22] Internet üzerinde gelişmiş kullanıcı işlevselliği ve web sayfası ile etkileşim sağlayan, ağ ortamlarına taşınabilen bir programlama dili.

[23] http://www.hurriyetim.com.tr12/02/2002

B. TÜRKİYE'DE ELEKTRONİK TİCARET İLE İLGİLİ KONULAR, İZLENEN POLİTİKALAR

1. İLK ÇALIŞMALAR

Geniş kapsamlı e-ticaret tanımları esas alındığı takdirde, Türkiye'de e-ticaretin ilk uygulaması 1992 yılında Merkez Bankası ile bankalar arasında başlayan EFT uygulamasıdır.

1995 yılında İGEME'nin UNCTAD tarafından Ankara Ticaret Noktası[24] seçilmesi ikinci adımı oluşturur. Ağustos 1997'de toplanan Bilim ve Teknoloji Yüksek Kurulu aldığı bir kararla[25] elektronik ticaret ağının kurulmasını karara bağlamıştır. Bu çalışma çerçevesinde TÜBİTAK aynı yıl TUENA'yı başlatmıştır. Bu proje Türkiye'nin enformasyon altyapısının resmini ortaya koymaktadır ve kamunun konuya yaklaşımının başlangıç noktasını teşkil eder. Daha sonra Bilim ve Teknoloji Yüksek Kurulu Kararı çerçevesinde kamu, özel sektör ve üniversite katılımcıları ile ETKK oluşturulmuştur.

---

[24] Ticaret Noktaları Programı, az gelişmiş ve gelişmekte olan ülkelerin küçük ve orta ölçekli işletmelerinin dünyaya açılabilmelerini sağlamak amacıyla dış ticaret aktörlerini bir araya getirmeyi amaçlayan bir programdır.

[25] 25/8/1997 tarih ve 97/3 sayılı BTYK Kararı.

2. ELEKTRONİK TİCARET KOORDİNASYON KURULUNUN ÇALIŞMALARI

ETKK'nın çalışmalarının koordinatörlüğünün DTM tarafından, sekreteryasının ise TÜBİTAK tarafından yürütülmesine karar verilmiştir.

ETKK'nın ilk toplantısı, DTM başkanlığında 16 Şubat 1998 tarihinde yapılmıştır. Böylece, elektronik ticaretin geliştirilmesine ilişkin geniş katılımlı ve düzenli çalışmalar başlatılmıştır. Anılan toplantıda, çalışmaların verimli bir şekilde sürdürülebilmesi için Teknik, Hukuk ve Finans adı altında, toplantıya katılan kuruluş temsilcileri arasından üç ayrı çalışma grubu oluşturulmuştur. Çalışma gruplarının üç ay içinde bir rapor hazırlamaları kararlaştırılmıştır. ETKK'nın 16 Şubat 1998 tarihli toplantısında alınan Karar gereğince Hukuk, Teknik ve Finans çalışma grupları üç aylık raporlarını hazırlayarak 1998 Mayıs ayı içinde ETKK Değerlendirme Komisyonu'na iletmişlerdir. Değerlendirme Komisyonu bu üç raporun bir özeti olan ETKK Rapor Özeti'ni oluşturarak ETKK'nın onayına sunmuştur. Çalışma gruplarının raporlarıyla birlikte, 26 Mayıs 1998 tarihli ETKK toplantısında son şeklini alan Rapor Özeti BTYK Sekreteryası'na iletilmiştir. ETKK tarafından BTYK'ya sunulan "Özet Rapor"da ülkemizde elektronik ticaretin geliştirilebilmesi için devletin öncelikle aşağıda sıralanan dört ana görevi yerine getirmesinin gerekli olduğu vurgulanmıştır[26]:

---

[26] Bkz.Elektronik Ticaret Koordinasyon Kurulu Raporları, Dış Ticaret Müsteşarlığı, Mayıs 1998, Ankara, sh.2; http://www.foreigntrade.gov.tr; **Arıkan**, sh.48.

. Gerekli teknik ve idari alt yapının kurulmasını sağlamak,

. Hukuki yapıyı oluşturmak,

. Elektronik ticareti özendirecek önlemleri almak,

. Ulusal politika ve uygulamaların uluslararası politikalar ve uygulamalarla uyumunu sağlamak.

BTYK'nın 2 Haziran 1998 tarihli toplantısında, Ülkemizde elektronik ticaretin yaygınlaştırılması ile ilgili düzenlemeler tamamlanıncaya kadar ETKK'nun görevini sürdürmesine ve kendi önerileri doğrultusunda bir eylem planı hazırlayarak uygulamayı izlemesi, sonuçları değerlendirmesi, uygulamada ortaya çıkacak sorunları çözmeye yönelik yeni öneriler geliştirerek bunları ilgili kuruluşların ve BTYK'nun görüşüne sunmaya devam etmesine karar verilmiştir. İki yıllık bir çalışma sürecinin sonunda yapılan 26.04.2000 tarihli ETKK toplantısında; çalışma gruplarının raporları değerlendirilerek yeniden yapılanmaya gidilmiş, Proje Geliştirme, Hukuk ve Eğitim-Tanıtım Çalışma Gruplarının yeniden belirlenen üyeleri ile toplanmasına karar verilmiştir. Bu çalışmalar sonucunda, Hukuk Çalışma Grubu 01.07.2000 tarihi itibari ile hazırladığı Çalışma Sonuç Belgesi'nde; öncelikle elektronik imzanın hukuken tanınması için bir kanun taslağının hazırlanmasına ve bu konuda Adalet Bakanlığı'nın çalışmalarının beklenmesine karar verilmiştir [27].

[27] **Çamurdan, Ç.:** Elektronik İmza Kanunu Üzerine Bir Değerlendirme, TBD, sh.1, http://dergi.tbd.org.tr/yazarlar/26052003/cigdem camurdan.htm.

3. DIŞ TİCARET MÜSTEŞARLIĞININ ÇALIŞMALARI

BTYK tarafından koordinatör olarak görevlendirilen DTM, daha sonra, Başbakanlığın koordinasyonunda 30.07.2001 tarihli geniş katılımlı toplantısı ile başlatılan E-Türkiye çalışmaları kapsamında yer alan on üç ayrı çalışma grubu arasındaki "E-ticaret" grubunun koordinasyonu hususunda da görevlendirilmiştir [28].

DTM çalışma grupları ve bu çalışmalara katılan ilgili kuruluşlarla çalışmalarını koordinasyonunu sürdürmeye Başbakanlığın 27 Şubat 2003 tarih ve B.02.PPG.0.12-3120-3416 sayılı genelgesine kadar devam etmiştir. Söz konusu genelgeyle e-Dönüşüm Türkiye Projesinin koordinasyonu DPT'ye verilmiştir.

4. DIŞ TİCARET MÜSTEŞARLIĞI HUKUK ÇALIŞMA GRUBU'NUN FAALİYETLERİ

DTM koordinatörlüğündeki Hukuk Çalışma Grubu 29.06.2001 tarihli toplantısında; elektronik imza ile ilgili kanun taslağını hazırlamak üzere Adalet Bakanlığı, Gümrük Müsteşarlığı, DPT Müsteşarlığı, Merkez Bankası, PTT Genel Müdürlüğü ve Dış Ticaret Müsteşarlığı ve Telekomünikasyon Kurumu temsilcilerinden oluşan Hukuk Alt Çalışma Grubu kurulmuştur [29].

---

[28] http://www.e-ticaret.gov.tr

[29] **Çamurdan**, sh.1

Hukuk Alt Çalışma Grubu 10.07.2001 tarihinden itibaren çalışmaya başlamış, ülkemizde elektronik veri ve elektronik sözleşme konularında herhangi bir yasal düzenleme bulunmaması nedeniyle, hazırlanacak kanun taslağında bu düzenlemelere de yer verilerek çalışmanın genişletilmesi kararlaştırılmıştır. Bu çalışma sonucunda, uluslararası uygulamalar, AB mevzuatı ve 22.05.2001 tarihinde yürürlüğe giren yeni Alman Elektronik İmza Kanunu göz önünde bulundurularak ve Türk hukuk sisteminin özellikleri dikkate alınarak "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanunu Tasarısı Taslağı" hazırlanmıştır. Taslak 01.02.2002 tarihinde ETKK Hukuk Grubu üyelerine gönderilerek görüşleri alınmış, gelen görüşler üzerine Taslağa son şekli verilerek, 17.04.2002 tarihinde Başbakanlığa gönderilmiştir.

ETKK Hukuk Grubunun çalışmaları devam ederken, Adalet Bakanlığı 14.01.2002 tarihli yazısı ile çeşitli kurum ve kuruluşlardan elektronik imzanın düzenlenmesine ilişkin kanun taslağının hazırlanması için oluşturulacak komisyona temsilci bildirilmesini talep etmiş, oluşturulan komisyonun hazırladığı "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" Taslağı 10.09.2002 tarihli yazı ile kurumların görüşüne sunulmuş ve Taslak Başbakanlığa gönderilmiştir.

Adalet Bakanlığı tarafından hazırlanan taslak, daha sonra Bakanlar Kurulu tarafından kabul edilip, 09.06.2003 tarihinde TBMM'ye kanunlaşması amacıyla, kanun tasarısı olarak gönderilmiş ve Meclis komisyonlarından da geçerek Genel Kurulda 15.01.2004 tarihinde yasalaşmıştır.

Adalet Bakanlığı tarafından hazırlanarak 23.01.2004 tarih ve 25355 sayılı RG'de yayımlanmış olan Elektronik İmzanın Düzenlenmesi Hakkında Kanun, yayımı tarihinden altı ay sonra 23.07.2004 tarihinde yürürlüğe girmiştir. Kanunun uygulanmasına yönelik ikincil düzenlemeler ise, Kanunun yürürlük tarihinden itibaren altı ay içerisinde yani 23.01.2005 tarihine kadar Telekomünikasyon Kurumu tarafından yapılacaktır.

İKİNCİ BÖLÜM

ELEKTRONİK SÖZLEŞMELER

§3. ELEKTRONİK SÖZLEŞME KAVRAMI VE TANIMI

Ticaretin hukuk altyapısı ve icra aracı sözleşme kurumudur. Bu bağlamda, elektronik ticaret de, elektronik sözleşmeler vasıtasıyla yapılır[30]. Elektronik ticaretin hukuki altyapısı, esas olarak "elektronik sözleşme" kavramına dayanır. Elektronik sözleşme genel anlamda, elektronik iletişim araç ve yöntemleriyle kurulan sözleşmeleri ifade etmektedir.

Elektronik sözleşme kavramı, Avrupa Parlamentosu ve Konseyi'nin 8.6.2000 tarih ve 2000/31/EC sayılı Elektronik Ticaret Direktifi'nin "Amaç ve Kapsam"a ilişkin 1. maddesinin 2. bendinde Direktif kapsamındaki işlemler arasında düzenlenmiştir. Direktifte, e-sözleşmelerin, kağıda dayanan, geleneksel usul ve araçlarla yapılan sözleşmelerle eşit hukuki statüde olması amaçlanmaktadır. Direktifte e-sözleşme tanımı yapılmamış olmakla beraber, sözleşmelere ilişkin 9. maddenin 1. bendi uyarınca, Üye Devletlerin, hukuk sistemlerinin, elektronik araçlarla sonuçlandırılan sözleşmelere izin vermesini ve özellikle sözleşme usulüne uygulanacak hukuki şartların, e-sözleşmelerin kullanılmasında engel yaratmayacak ve bu sözleşmelerin,

---

[30] **Sözer, B.:**Elektronik Ticaret/Elektronik Sözleşmeler, TÜSİAV İstanbul Sohbetlerinde Sunulan Tebliğ, İstanbul, (Tebliğ); sh.3, **Sözer, B.:** Elektronik Sözleşmeler, İstanbul, 2002, (Sözleşme), sh.89.

elektronik araçlarla yapılmış olmaları nedeniyle hukuki etkinlik ve geçerlilikten yoksunlukla sonuçlanmayacak şekilde olmasını sağlamaları gerektiği öngörülmüştür. Bu hükümden hareketle, e-sözleşmeler, elektronik araçlarla yapılmış olan ve/veya elektronik araçlarla tamamlanan sözleşmeler olarak tanımlanabilir[31].

Elektronik sözleşme, genellikle EDI, e-mail, web sayfası ve usenet kullanılarak yapılan sözleşmeler olarak tanımlanmaktadır[32]. Ancak bazı yazarlarca, e-sözleşme, elektronik iletişim tekniği kullanılarak, internet üzerinden yapılan sözleşmeler olarak tanımlanmakta ve standart bir yapıda, kapalı özel ağlar üzerinden bilgisayardan bilgisayara belge ve bilgi değişimini sağlayan bir sistem olarak tanımlanabilecek EDI, bir sözleşmenin kuruluşunda değil, daha önce yapılmış bir sözleşmenin ifası aşamasında kullanılan bir yöntem olduğu gerekçesiyle e-sözleşme kapsamına dahil edilmemektedir[33].

SÖZER, e-mail ile yapılan sözleşmelerin de, e-mailin, işin hukuki yönü bakımından, teleteks veya fax haberleşmesinden farklı olmadığı gerekçesiyle e-sözleşme kapsamında sayılmayacağı görüşündedir[34]. Ancak bizim de katıldığımız görüşe

---

[31] **Acır**, sh.11.

[32] **Hance and Balz:** Business ans and Law on the Internet, 1996 (translated from French by S.D.Balz), 151 ff., 164.

[33]**Güran/Akünal/Bayraktar/Yurtcan/Kendigelen/Beller/Sözer,** Bölüm II, Par. 3, **Sözer,** (Tebliğ), sh.3, 4.

[34] **Sözer,** (Tebliğ), sh. 4.

göre[35], e-mail ile yapılan sözleşmeler de, taraflar arasındaki sözleşmenin hukuki geçerliliği ve hükümlerini doğurması bakımından büyük önem taşıyan, tarafların kimlikleri, bilginin (iradenin ve sözleşme şartlarının) bütünlüğü ve doğruluğu vs. hususlarda e-imzayı gerektirdiğinden, elektronik sözleşmeler kapsamında değerlendirilebilir.

Ticaret yapma şeklinde yaşanan değişikliğe rağmen, elektronik ticarette ortaya çıkan elektronik sözleşmelerin hukuki niteliği ve konusu klasik araç ve yöntemlerle yapılan sözleşmelerle aynıdır [36]. Mevcut hukuk kuralları tarafından dolaylı veya doğrudan tanımlanmamış bir unsurun konu edilmediği elektronik sözleşmeler, alışılmış ortamda meydana gelen sözleşmelerden tarafların hak ve yükümlülükleri bakımından farklılık göstermez[37].

Sözleşme hukukunun geneli bakımından, elektronik sözleşmeler içerikten ziyade kuruluş yöntemi ile bağlantılıdırlar. Bu bağlamda, elektronik sözleşme mevcut

---

[35] **Acır,** sh.12.

[36] Aynı görüş için bkz. **Kidd/Daugtrey:** Adapting Contract Law to Accomodate Electronic Contracts: Overview and Suggestions, rutgers Computer&Tech.L.J., 2000/26, sh.240; **Stone, P.:** The Treatment of Electronic Contracts and Torts in Private International Law under European Community Legislation, Information&Communication Technology Law, 2002/11 S.2, sh.122; **Falcıoğlu, M.Ö.:** Karşılaştırmalı Hukuk ve Türk Hukukunda Elektronik Satım Sözleşmesi ve Kuruluşu, Ankara, 2004, sh.61.

[37] **Falcıoğlu,** sh.62

sözleşmelerden bağımsız bir tip sözleşme olarak değerlendirilmemeli, bu nedenle tarafların hak ve yükümlülükleri bakımından özel hükümlere bağlanmamalıdır. Nitekim, Amerikan ve AB kanun koyucuları, elektronik sözleşmeye tip sözleşme olarak değil klasik şekillerde meydana gelen sözleşmelerle eşit geçerlik ve ispat tanınmaları açısından yaklaşmaktadırlar [38].

§4. E-SÖZLEŞMELERİN HUKUKİ NİTELİĞİ

E-ticarette, özellikle web siteleri vasıtasıyla gerçekleştirilen e-sözleşmelerde, sözleşmenin şartlarını satıcı belirler. Alıcının bu şartlar üzerinde müzakere imkanı yoktur. Çünkü elektronik ortamda belirmiş olan mesajda çizilmiş olan sınırların dışına çıkılması ve belirtilen usul ve aşamaların aynen izlenmemesi işlemin başarısızlıkla sonuçlanmasına yol açacaktır[39].

İltihaki sözleşme; sözleşme şartlarını, sözleşmenin taraflarından bir tanesinin, örneğin satıcının, sözleşme kurulmadan önce, ileride kuracağı tüm satış sözleşmelerinde kullanmak amacı ile ve karşı tarafın yani alıcının, herhangi bir müzakere yetkisi olmadan aynen kabul edeceği (veya red edeceği) surette, tek yanlı olarak hazırladığı sözleşme türüdür. İltihaki sözleşmenin en belirgin özelliği, diğer akidin sözleşme şartlarını müzakere etme şansına sahip olmamasıdır. Bu tür

---

[38] **Winn/Haubold:** Electronic Promises: Contract Law Reformand ECommerce In A Comparative Perspective, E.L., Rev., 2000/27, S.5, sh.568.

[39]**Güran/Akünal/Bayraktar/Yurtcan/Kendigelen/Beller/Sözer,** Bölüm II, E-Contract, Sözleşmenin Kurulması, İcap-Kabul, son par.

sözleşmeler, bir tarafın hazırladığı şartları diğer tarafın aynen kabul etmesi ile kurulurlar[40].

İltihaki sözleşmeler genel işlem şartlarını içerirler. İltihaki sözleşmelerin içeriklerini oluşturan genel işlem şartlarını tanımlamak için şu unsurların bulunmasına dikkat edilmelidir: Bir tarafça hazırlanmıştır; İlgili olduğu bütün sözleşmelerde kullanılmak üzere, standart ve objektif olarak hazırlanmıştır; Hazırlanmasında diğer tarafın hiçbir müdahalesi olmamıştır; Sözleşmenin kurulması aşamasında müzakere imkanı yoktur, ya aynen kabul edilir veya akit hiç kurulmaz[41].

İltihaki sözleşmelerde satıcının kendi icabına karşı kabul beyanında bulunan tarafın kabul beyanını reddetme hakkı yoktur. Bu tür sözleşmelerde icap kamuya yapılmış sayılır ve ilgilenen herkes kabul beyanında bulunarak icabı yapanla sözleşme kurma hakkına sahiptir[42]. Bu sebeple bu sözleşme türünde icaba davet söz konusu değildir.

Kanaatimize göre, web üzerinden kurulan sözleşmeler iltihaki sözleşmelerin belirgin özelliklerini göstermektedirler. Zira, elektronik sözleşmeler de genel işlem şartları içermektedirler. Bu genel işlem şartları ve/veya diğer sözleşme hükümleri, satıcı tarafından önceden ve tamamen kendi tercihleri doğrultusunda saptanmış, bütün sözleşmelerde kullanılmak amacı ile hazırlanmış, objektif hükümler içeren

---

[40] **Sözer,** (Sözleşme), sh. 112.

[41] **Sözer,** (Sözleşme), sh. 114; **Atamer,Y.:** Sözleşme Özgürlüğünün Sınırlandırılması Çerçevesinde Genel İşlem Şartlarının Denetlenmesi, İstanbul, 1999, sh.45, 62-73.

[42] **Sözer,** (Tebliğ), sh.6.

maddelerdir[43]. Bu hükümlerin, bireysel işlemlerle değiştirilmesi söz konusu değildir. Bu sebeple sözleşmenin diğer tarafı, sözleşmeyi ya kendisine sunulan şartlarda kabul edecek veya sözleşmeyi yapmaktan vazgeçecektir[44].

Bu noktada, tüketiciyi koruma düzenlemeleri de gözönünde bulundurularak, tüm standart şartların alıcının dikkatine yeterli olarak sunulması ve tüm şartların açıkça görülebilecek bir şekilde web sitesinde yer alması gerekmektedir.[45]

§5. E-SÖZLEŞMELERDE İRADE BEYANLARININ HUKUKİ AÇIDAN DEĞERLENDİRİMESİ

Elektronik irade beyanlarıyla da sözleşme kurmak mümkündür [46]. Şöyle ki;

Türk Hukukunda sözleşmelerin kuruluşu BK'nun 1 ila 10. maddeleri arasında düzenlenmiştir. Elektronik sözleşmeler her ne kadar klasik haberleşme araçları dışında, elektronik iletişim tekniği kullanılarak yapılsa da, sözleşmenin kurulması,

---

[43] **Sözer,** (Sözleşme), sh. 115.

[44] **Eren,** (1991), sh. 277.

[45] **Acır,** sh.17.

[46]**Zanger, L. M.:** Electronic Contracts: Some of the Basics http://www.mbc.com/ecommrce/Itecpubs.asp; **Zammit, J.P./Galant, F.B.:** Electronic Sözleşme, (Çeviren: **Çeliktaş, İ.**), İBD, 1999, C.73, sh.4; **Delta, G. B./Matsuura, J.H.:** Law of the Internet, Newyork, 2000, s.22 vd.; **Bozbel,** sh.8; **Altınışık,** sh.37.

BK'nun akdin in'ikadına (sözleşmenin kurulması) ilişkin bu genel mahiyetteki hükümler çerçevesinde değerlendirilebilecektir. BK 1. md'ye göre, "iki taraf karşılıklı ve birbirine uygun surette rızalarını beyan ettikleri taktirde akit tamam olur". Bu hükme göre, sözleşmenin kurulabilmesi için tarafların irade beyanlarının birbirine uygunluğu şarttır. İrade beyanlarındaki uygunluk, sözleşmenin içeriğini oluşturan bütün esaslı noktaları kapsamalıdır[47].

Sözleşmenin kurulması için birbirine uygun olması gereken taraf iradelerine "icap" ve "kabul" adı verilir. Sözleşmenin bütün esaslı noktalarını kapsaması gereken icap, zaman bakımından yapılan ilk irade beyanıdır. Kabul ise icaba uygun olarak akdin meydana gelmesine imkan sağlayan varması gerekli tek taraflı irade açıklamasıdır.[48]

Web siteleri ile yapılan e-sözleşmelerde, satıcının, web sitesinde yer verdiği yazı, görüntü ve veritabanının ve e-mail yolu ile yapılan e-sözleşmelerde gönderilen mailin icap mı, yoksa icaba davet mi olduğunun tespiti de önemlidir. Zira, bu websiteleri ve mailler ile icapta bulunulduğu kabul edildiği taktirde, yazılı halde yapılması geçerlik veya ispat koşulu olan sözleşmeler ile, finansal hizmetlere ilişkin

---

[47] **Eren, F.:** Borçlar Hukuku Genel Hükümler, C.I, 4. Bası, Ankara 1991, sh. 290, (1991); **Tekinay, S.S./Akman, S./Burcuoğlu, H./Altop, A.:** Borçlar Hukuku, Genel Hükümler, 6. Bası, İstanbul 1988, sh.99.

[48] Elektronik sözleşmelerin ve özel olarak Internet Aracılığıyla Yapılan Satım Sözleşmesinin Kuruluşu ve Düzenleniş Biçimi hakkında ayrıntılı bir çalışma için bkz. **Altınışık,** sh.37-68.

sözleşmeler gibi, satıcı tarafından kesin ve yazılı bilgi verilmesini gerektiren sözleşmelerde önemli problemler doğacaktır[49].

Bu bağlamda icaba davete kısaca değinilecek olursa, icapta, sözleşmenin yapılması için gerekli bütün unsurlar, irade beyanıyla kesin olarak saptanmakta ve karşı tarafın kabul beyanıyla sözleşme kurulmaktadır. Buna karşılık icaba davet ile, icaptan farklı olarak, muhatabın kabul beyanıyla akdin kurulması değil, karşı tarafın icapta bulunması amaçlanır. Diğer bir ifadeyle icaba davette bulunan, karşı tarafa, belirli bir sözleşmeyi yapmaya hazır olduğunu bildirir. BK md. 7/I'de icapta bulunanın beyanına icabın bağlayıcı olmadığını belirli şekilde gösteren bir kayıt koyması veya icapta bulunanın icabıyla bağlı olmak istemediğinin hal ve durumun özelliğinden anlaşıldığı hallerde icaba davetin söz konusu olduğu ifade edilmiştir. Hükmün ikinci fıkrasında, "Tarife ve cari fiyat gönderilmesi icap teşkil etmez." denilmektedir. BK md. 7/III'de ise, üzerinde fiyatı gösterilmek suretiyle herkesin görebileceği yerlerde özellikle bir mağaza, satış yeri vs.'de mal sergilenmesinin icap teşkil ettiği öngörülmektedir.

Elektronik sözleşmeler, BK'nun genel hükümlere ilişkin bu bilgiler ışığında değerlendirilecek olursa, bir web sitesinde, satılmak üzere sunulan mal veya hizmetle ilgili olarak, icapta yer alması gereken esaslı noktaları içeren yeterli bilgilere yer verilmişse ve fiyatları da belirtilmişse, BK md. 7/III gereğince, bu web sitesinde

---

[49] **Rowe H./Haftke, M.:** A Practitioner's Guide to The Regulation of the Internet, 1999/2000 Ed., sh.80.

icapta bulunulduğu kabul edilebilir[50]. Buna göre alıcının, web sitesindeki adım ve usullere uyarak sipariş vermesi kabul beyanı sayılır. Satıcının bu beyana karşılık gönderdiği beyan, alıcının kabul beyanının satıcı tarafından alınmış olduğunu ve sözleşmenin kurulmuş olduğunu ifade eden bir teyit mesajıdır. Öte yandan, mal veya hizmetin bir web sitesinde satılmak üzere sergilenmesinin icap mı icaba davet mi olduğunun, yapılacak sözleşmenin konusuna göre belirlenmesi gerektiği, bilgi vermeyle ilgili sözleşmeler gibi sözleşmelerde web sitesinde icapta bulunulduğu, bu sözleşmelerde alıcıya elektronik formda bir sipariş formu gönderildiği, alıcının bu formu doldurarak göndermesinin ise kabul anlamına geldiği; maddi varlığı olan malların satımına ilişkin sözleşmelerde ise, web sitesinde satılmak üzere mal sergilenmesinin ise icaba davet olduğu yönünde görüşler de bulunmaktadır[51].

I. E-SÖZLEŞMELERİN KURULDUĞU AN

Sözleşmelerin kurulduğu anı açıklayan birçok teori bulunmaktadır[52] . Bu konuda BK'nun kabul ettiği teoriye göre, sözleşmenin kurulduğu anın tespitinde, icabın

---

[50] Bkz. aynı görüşte **Güran/Akünal/Bayraktar/Yurtcan/Kendigelen/Beller/Sözer,** Bölüm II, E-Contract, Sözleşmenin Kurulması; **Sözer,** (Tebliğ), sh. 5.

[51] **Özsunay, E.:** Elektronik Sözleşmeler, AB'de, Bazı Üye Devletlerde ve Türkiye'de Elektronik Ticaretin Hukuksal Sorunları-Elektronik Sözleşmeler Seminerinde sunulan tebliğ, 12.5.2000, İstanbul Ticaret Odası AB Şubesi, İstanbul.

[52] **Tekinay/Akman/Burcuoğlu/Altop,** sh.95; **Esener, T.:** Turkish Business Law, Law of Obligations-Contracts and Torts, C.I, İstanbul, 2000 (**Çeviren: Yarsuvat, Ö.**).

hazırlar arasında mı gaipler arasında (hazır olmayanlar arasında) mı olduğu hususunda bir ayrım yapılmaktadır. Taraflar arasında doğrudan doğruya bir iletişim ve çok yakın bir konuşma imkanı var ise hazırlar arasındaki icaptan bahsedilir[53]. BK, md. 4/I hükmünde, hazırlar arasındaki icaba derhal kabul cevabı vermeyi öngördüğü için, icap beyanından sonra muhatabın kabul beyanında bulunduğu anda sözleşme kurulmuş olur. Taraflar arasında bu şekilde, anında müzakere yapma imkanının olduğu chat ve internet üzerinden sesli mesajlarla gerçekleştirilen sözleşmeler de hazırlararası sözleşmelere benzetilebilir. Zira BK md. 4/II'de telefonda müzakere edilmek suretiyle yapılan sözleşmelerin hazırlar arasında olacağı ifade edilmiştir. Buradan hareketle, bu sözleşmeler, muhatabın kabul ettiğine dair mesajını gönderdiği anda kurulmuş olur[54].

Bir sözleşmenin kurulmasına yönelik icap ve kabulün yapıldığı taraflar arasında yer ve zaman unsurlarının bulunması halinde hazır olmayanlar arasındaki (gaipler arasındaki) sözleşmelerden bahsedilir[55]. Örneğin, mektup, telgraf, teleks ve faks ile yapılan beyanlar, hazır olmayanlar arasında yapılmış sayılır[56]. BK. md. 5 uyarınca,

---

[53] **Eren,** (1991), sh. 313; **Oğuzman, K./Öz, M. T.:** Borçlar Hukuku Genel Hükümler, İstanbul, 2000, sh.55; **Keser Berber, L.:** Şekil ve Dijital İmza, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001 (Şekil), sh.216; **Kırca, Ç.:** Internette Sözleşme Kurulması, Banka ve Ticaret Dergisi (BATİDER) C.XX, sh.4.

[54] **Acır,** sh.15.

[55] **Tekinay/Akman/Burcuoğlu/Altop,** s.88; **Kırca,** sh.107.

[56] **Oğuzman/Öz,** sh.55; **Eren, F.:** Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş 6.Bası, C.I, İstanbul, 1998, (1998)sh.233.

kabul beyanı icapta bulunanın hakimiyet alanına ulaştığı anda sözleşme kurulmuş olur. E-mail yoluyla yapılan icap ve kabullerde de e-sözleşmeler gaipler arasında kurulmuş sayılmakla beraber, e-sözleşmelerde kabul beyanına dair "bilgi"nin ISS aracılığıyla iletilmesi ve bu aracıların ise tarafların müstahdemi olmaması sebebiyle tarafların hakimiyet alanı olarak kabul edilemeyeceği görüşü mevcuttur. Bilginin, icapta bulunan tarafından ISS'nın mail server'ından alınması anında sözleşmenin kurulacağının kabulü halinde ise, BK'nun benimsediği ulaşma teorisinden farklı olan öğrenme teorisinin kabulü söz konusu olur[57].

II. E-SÖZLEŞMELERİN HÜKÜM VE SONUÇLARINI DOĞURMAYA BAŞLADIĞI AN

Hazırlar arasındaki sözleşmeler, hüküm ve sonuçlarını kabul iradesinin açıklandığı, diğer bir ifadeyle akdin kurulduğu anda doğurur[58]. Bu nedenle hazırlar arasındaki sözleşme hükümlerine tabi sayılan chat ve internet üzerinden sesli mesajlarla gerçekleştirilen e-sözleşmeler ile ilgili olarak sözleşmenin kurulmasına ilişkin yukarıda belirtilen tartışmalar, sözleşmenin hüküm ve sonuçlarını doğurması bakımından da mevcuttur.

Hazır olmayanlar arasındaki sözleşmelerin hüküm ve sonuçlarını doğurduğu an bakımından, İngiliz hukukunda olduğu gibi gönderme teorisi kabul edilmektedir. BK. md.10 hükmüne göre, kabul haberi icap sahibine gönderildiği anda sözleşme

---

[57] **Sözer,** (Tebliğ), s.7; **Acır,** sh.15.

[58] **Eren,** (1998), sh.242; **Oğuzman/Öz,** sh.67.

hükümlerini doğurmaya başlar. Ancak bu noktada, özellikle e-mail yoluyla kurulan sözleşmelerde, internetin doğasından kaynaklanan nedenlerle, (örneğin gönderilen bir e-mail networkdeki arızalar nedeniyle muhatabına ulaşamayabilir veya muhatabın mesaj kutusuna ulaştığı halde burada açılmadan - okunmadan -kalabilir), geleneksel posta hizmetlerindeki, gönderilmiş ve açılmamış olarak geri dönmemiş olan bir iletinin teslim edilmiş olduğunu varsayan kuralları dikkate alan genel karinelerden yararlanılamamaktadır[59].

Öte yandan, gönderildiği zaman okunaklı olan bir e-mail, muhataba ulaştığında bozulmuş veya okunaksız hale gelmiş olabilir. Bu sebeple e-mailin güvenilirliğinin yetersizliği dikkate alınarak, bu şekilde gönderilen beyanları, yalnızca alındığında tam (bütün halde) olarak varsaymaktadır.

UNCITRAL tarafından hazırlanan Elektronik Ticaret Model Kanunu'nda (Model Law on Electronic Commerce), haberin gönderildiği an, verinin, göndericinin denetim ve kontrolünden çıktığı an olarak kabul edilmektedir. Mesajın gönderilene ulaşması anı ise, mesajın gönderilenin egemenlik alanı içine girdiği an olarak görülmektedir. Bu an, muhatap belli bir bilgi sistemine sahip ise verinin bu bilgi sistemine vardığı an; veri başka bir sisteme gönderilmiş ise bunun muhatap tarafından ele geçirildiği andır[60].

---

[59] **Acır,** sh.16.

[60] Nakleden **Sözer,** (Tebliğ), sh.8.

AB'nin 08.06.2000 tarih ve 2000/31/EC sayılı Elektronik Ticaret Direktifi'nin 11. md.'sine göre; bir hizmet alıcısının, teknolojik araçlarla sipariş vermesi halinde, servis sağlayıcının, alıcı tarafından verilen siparişin alındığını, gecikmeksizin teyit etmek zorunluluğunda olduğu öngörülmüştür. Sipariş ve siparişin alındığına dair onay (alındı onayı) ise, muhatabın bunlara erişebildiği zaman alınmış sayılır.

Ancak maddenin 3. bendinde, e-mail yoluyla kurulan sözleşmelerde, servis sağlayıcının, 1 nolu bendin, alıcının verdiği siparişin alındığını onaylama zorunluluğuna dair ilk paragrafının uygulanmayacağı öngörülmüştür[61].

§6. ELEKTRONİK SÖZLEŞMELERİN TARAFLARINDAN BİRİNİN TÜKETİCİ OLMASI DURUMUNDA TÜKETİCİ HUKUKU BAKIMINDAN İNCELENMESİ

I. MESAFELİ SÖZLEŞMELER

A. AVRUPA BİRLİĞİ DÜZENLEMELERİ

Elektronik ticareti oluşturan dört kategoriden sadece ikisinde tüketiciler de taraflardan biri konumunda bulunmaktadır. Ancak, özellikle işletmeler ile tüketiciler

[61] **Acır,** sh.17.

arasında gerçekleştirilen işlemler ve elektronik ticaret kapsamında kurulan sözleşmeler bakımından tüketicinin korunması büyük önem taşımaktadır[62].

Konuya AB açısından bakıldığında, elektronik ticarete büyük önem verildiği, 20 Mayıs 1997 tarihinde çıkarılan "97/7/EC sayılı Mesafeli Sözleşmelerde Tüketicinin Korunması" isimli bir Yönerge[63] kapsamında konunun düzenlendiği, bununla yetinilmeyerek 8 Haziran 2000 tarihli 2000/31 sayılı "Elektronik Ticaret Hakkında Direktif"[64] ile bazı hususların daha ayrıntılı olarak ortaya konulduğu görülmektedir.

Yönerge gereğince; mesafeli sözleşme, satıcı veya hizmet sunan ile tüketicinin sözleşmenin kurulması anında karşı karşıya gelmedikleri tüm sözleşmeler olarak tanımlanmıştır. Dolayısıyla internet aracılığıyla gerçekleştirilen tüm sözleşmelerin mesafeli sözleşme olarak nitelendirilmesi mümkündür. Bu Yönerge ile satıcı veya hizmet sunan, mesafeli sözleşme kurulmadan önce belli konularda tüketiciye ayrıntılı

---

[62] **Akipek Öcal, Ş.:** Mesafeli Sözleşmelere İlişkin AB Direktifleri Çerçevesinde Elektronik Ticarette Sözleşme, Bilişim Teknolojileri ve Hukuk Konulu Seminerde sunulan tebliğ, 16.03.2001

[63] Directive 97/7/EC of The European Parliament and of The Council of 20 May 1997on the Protection of Consumers in Respect of Distance Contracts, Official Journal of the European Communities L. 178/1.

[64] Directive 2000/31/EC of the European Parliament and of the Council of 8 June on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, (Directive on Electronic Commerce) Bkz. Official Journal of the European Communities L. 178/1.

olarak bilgi vermek ve bunu yazılı olarak göndermekle yükümlüdür. Verilecek bilgiler arasında; satılan malların ya da sağlanan hizmetin niteliği, ödeme miktarı ve koşulları, satıcı veya hizmet sunanın açık kimliği ile adresi, yaptığı icap ve belirlediği fiyatın geçerli olacağı süre, ürün teslimatının nasıl yapılacağı ve tüketici tarafından ödenecekse posta bedeli, tüketicinin sözleşmeyi feshetme koşulları gibi bilgiler sayılabilir. Bu Yönerge ile tüketiciye tanınan önemli bir olanak da, herhangi bir neden ileri sürmesi ve cezai şart ödemesi gerekmeksizin, 7 iş günü içinde sözleşme yapma konusundaki iradesini geri alma hakkının tanınmış olmasıdır. Ayrıca tüketici bakımından bir diğer olumlu düzenleme de, malın ya da hizmetin, sözleşme yapıldıktan sonra en geç 30 gün içinde tüketiciye ulaştırılması gereğidir[65].

8 Haziran 2000 tarihli Elektronik Ticaret Hakkındaki Direktif ile Mesafeli Sözleşmelerde Tüketicinin Korunmasına İlişkin Yönerge hükümlerinin geçerliliğini koruduğu vurgulanmış, ancak elektronik ticaretin Topluluk içinde daha kolay uygulanabilmesini ve yaygınlaşmasını sağlamak amacıyla bazı hususların bu Direktif ile daha ayrıntılı düzenlendiği belirtilmiştir. Üye Devletler, bu Direktif gereğince, Topluluk içinde bilgi iletişiminin serbest dolaşımını sağlamakla yükümlüdür. Ayrıca bu Direktif gereğince, Internet hizmet sağlayıcıların faaliyete başlayabilmesi için, o üye Devletten mutlaka ön izin alması gerekir.

Elektronik Ticaret Hakkındaki Direktif ile getirilen en önemli düzenleme, tüm üye ülkelerin hukuk sistemlerini elektronik yollarla sözleşme kurulmasına izin verecek şekilde değiştirme yükümlülüğü altına sokan düzenlemedir. Ancak üye ülkelere

[65] **Akipek Öcal,** (tebliğ)

istedikleri takdirde belli bazı konulardaki sözleşmelerin, elektronik yolla yapımını yasaklama yetkisi tanınmıştır. Kira hariç, gayrimenkuller üzerinde ayni ya da şahsi hakların kurulması veya devrine ilişkin sözleşmeler; yapımında bazı kamu makamlarının katılımını gerektiren sözleşmeler; aile hukuku ve miras hukukuna ilişkin sözleşmeler örnek olarak verilebilir.

Bu Direktif gereğince ayrıca satıcı veya hizmet sunanın, sözleşmenin yapılmasına ilişkin aşamalar hakkında da tüketiciye açık bir şekilde bilgi vermesi gerekmektedir.

B. TÜRK HUKUKUNDA MESAFELİ SÖZLEŞME

4822 sayılı TKHK'da Değişiklik Yapılmasına Dair Kanun'un[66] 14. md. ile 4077 sayılı TKHK'a "Mesafeli Sözleşmeler" başlığı altında 9/A md. eklenmiştir. Sanayi ve Ticaret Bakanlığı tarafından, mesafeli sözleşmeler hakkında uygulama usul ve esaslarını düzenlemek üzere Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmelik[67] (Mesafeli Sözleşmeler Yönetmeliği) çıkarılmıştır.

Mesafeli sözleşme, Türk Hukukunda elektronik sözleşme kavramının tanımlanması bakımından öncelikle ele alınması gereken bir kavramdır. Buna göre, mesafeli sözleşmeler; "yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya

---

[66] 4822 sayılı Tüketicinin Korunması Hakkında Kanun'da Değişiklik Yapılmasına Dair Kanun RG No. 25048, 14.03.2003.

[67] RG No.25137, 13.06.2003.

hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan" sözleşmelerdir. Tanım uyarınca, mesafeli sözleşmeler satıcı veya sağlayıcı ile tüketicinin karşı karşıya gelmeksizin iletişim araçlarıyla kurdukları sözleşmelerdir[68]. TKHK md.9/A f.1'da tanımlanan mesafeli sözleşme olgusu bir sözleşme tipini hedef almaktan ziyade sözleşmelerin kurulma şeklini ifade etmektedir[69]. Mesafeli sözleşme, bir tüketici işlemi olarak TKHK'da tanımlanan her türlü mal veya hizmeti konu edinebilir[70].

Mesafeli sözleşmelerin TKHK bakımından kavramsal içeriği md. 9/A f.1 hükmü ile sınırlıdır. TKHK md.9/A hükmü elektronik ortam kavramına atıfta bulunmasına rağmen, bu kavrama ilişkin olarak madde hükmünde veya Mesafeli Sözleşmeler Yönetmeliğinde bir tanım bulunmamaktadır[71]. Bununla birlikte, Mesafeli Sözleşmeler Yönetmeliğinin kapsam dışı sözleşmeler başlığını taşıyan md.11'de, Yönetmelik hükümlerinin uygulanmayacağı sözleşmeler belirlenmiştir. Buna göre,

---

[68] **Aslan, Y.:** Tüketici Hukuku (En Son Değişiklikler ve Yargıtay Kararları Işığında), 2004, sh.410.

[69] **Bozbel, S.:** Türk Hukukunda Mesafeli Sözleşmeler, AÜEHFD, 2003, C. VII, S.3-4, sh.784; **Gezder, Ü.:** Mukayeseli Hukuk Açısından İnternette Aktedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, 2004, sh.49-50.

[70] **Falcıoğlu,** sh.75.

[71] Madde hükmünde geçen yazılı, görsel ve elektronik ortam ifadelerinin bir araç örneği olarak belirtildiklerini savunan görüş için bkz. **Özdemir Kocasakal, H.:** Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, İstanbul, 2003, sh.44.

Yönetmelik hükümleri banka, sigorta ile ilgili, otomatik satış makinaları vasıtasıyla akdedilen, halka açık jetonlu telefonlar vasıtasıyla akdedilen, gıda, içecek ve günlük tüketim için tüketicinin evine veya işyerine düzenli olarak sağlanan malların tedariki ile ilgili ve sağlayıcının üstlendiği, barınma, ulaşım, yemek tedariki, sportif ve kültürel faaliyetler ve eğlence hizmetlerini özel bir günde veya sürede tedarik etmesine ilişkin hükümler içeren sözleşmelere uygulanmamaktadır.

Bizim de katıldığımız görüşe göre, Mesafeli Sözleşmeler Yönetmeliğinin kapsam dışı sözleşmeler başlığını taşıyan md. 11'de konu ve kurulma şekilleri bakımından belirlenen sözleşmelerin dışında kalan ve tüketicilerle biraraya gelinmeksizin yapılan sözleşmelerin mesafeli sözleşme olarak tanımlanması gerekir. Diğer bir ifadeyle, genel anlamda uzaktan pazarlama araç ve yöntemleri olan katolog gönderme, telefonla arama, televizyondan pazarlama araç ve yöntemleri ve kanundaki ifadesiyle, elektronik ortamda kurulan sözleşmeler mesafeli sözleşme olarak değerlendirilmelidir[72].

4822 sayılı Kanunun madde gerekçesinde[73], TKHK md.9/A hükmünün getirilme amacı, "Madde ile satıcının birbirleriyle doğrudan temas halinde olmadığı televizyon, gazete, ilan ve internet aracılığıyla yapılan her türlü alışverişlerde

---

[72] **Bozbel,** sh.785; **Falcıoğlu,** sh.76; **Özdemir Kocasakal ise,** mesafeli sözleşme kavramında tek belirleyici unsurun tarafların sözleşmeyi fiziksel ortamda bir arada olmadan kurmaları olduğunu savunmaktadır.

[73] 4822 sayılı Tüketicinin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanunun gerekçesi için bkz. http://www2.tbmm.gov.tr/d22/1/1-0477.pdf

yaşanan sorunların yasal çerçevede çözümlenmesi amaçlanmaktadır" şeklinde ortaya konulmaktadır. Gerekçede geçen internet aracılığıyla yapılan her türlü alışveriş ifadesinden, başta web ve elektronik posta gelmek üzere genel olarak internete elektronik iletişimde kullanılan araç ve yöntemlerle kurulan elektronik sözleşmelerin mesafeli sözleşme olarak tanımlandıkları sonucu çıkarılabilir[74].

Sonuç olarak, TKHK md.9/A'da ifadesini bulan ve mesafeli sözleşme çerçeve kavramının içinde değerlendirilen elektronik sözleşmeler, tüketici ve satıcı/sağlayıcıların fiziken bir araya gelmeksizin internette kullanılan iletişim araç ve yöntemleriyle kurdukları, mal veya hizmetin tüketiciye anında veya sonradan teslimi ve ifası kararlaştırılan sözleşmeleri ifade etmektedir.

Türk Hukukunda mesafeli sözleşmelerde, sözleşmenin tüketici ile bir araya gelmeksizin kurulması yeterli görülmektedir. AB'nin Mesafeli Sözleşmeler Yönergesinde aranan organize bir mesafeli satım veya hizmet sistemini kullanma şartı md.9/A hükmünde yer almamaktadır. Bu nedenle, bizim de katıldığımız görüşe göre[75], Türk Hukuku bakımından satıcı veya sağlayıcının sürekli bir sistem çerçevesinde gerçekleştirmediği uzaktan pazarlama yöntemleriyle kurulan sözleşmeler de mesafeli sözleşme olarak değerlendirilmelidir.

Bir satıcı veya sağlayıcı, bir web sitesi işletmek veya elektronik posta adresini kamuya duyurmak suretiyle bu araç ve yöntemlerle sipariş verilmesine olanak

---

[74] Aynı yönde bkz. **Bozbel**, sh.785; **Aslan,** sh.415; **Falcıoğlu,** sh.76

[75] **Falcıoğlu,** sh.76-77.

sağlaması halinde tüketicilerle mesafeli sözleşme ilişkisine girmiş olacaktır. Bu durum, Mesafeli Sözleşmeler Yönergesi ile kıyaslandığı takdirde, TKHK bakımından tüketicilerin lehinedir ve daha ileri bir koruma sağlamaktadır. Zira, satıcı ve sağlayıcının kendi iç işleyişini ilgilendiren konulara girilmeksizin, her türlü mesafeli sözleşme bakımından getirilmiş olan ön bilgi ve sözleşmede bulunması gereken bilgilere ilişkin yükümlülüklerin yerine getirilmesi gerekecektir[76].

II. MESAFELİ SÖZLEŞME NİTELİĞİNE BAĞLANAN SONUÇLAR VE INTERNET ORTAMINDA KURULAN SÖZLEŞMELERDE TÜKETİCİNİN KORUNMASI

A. TÜKETİCİNİN KORUNMASI GEREĞİ VE ELEKTRONİK SÖZLEŞMELERDE TÜKETİCİ AÇISINDAN KORUYUCU HÜKÜMLER GETİRİLMESİ

Gelişen teknolojinin, özellikle bilgisayar teknolojisinin bir ürünü olan internet ve elektronik ticaret hayatımızın vazgeçilemez bir parçası haline gelmiştir. Elektronik ticaretin geleneksel ticaret usullerini değiştiren sayısız faydayı beraberinde getirdiği ve hayatımızda yeni bir çığır açtığı yadsınamaz bir gerçektir. Etkili ve hızlı bir yöntem olması, masrafları azaltması, rekabeti arttırması, ulusal ve uluslararası pazara rahat erişim olanağı sağlaması, tüketicilere daha çok seçenek sunması gibi sayısız yararının yanı sıra, elektronik ticaret pek çok sorunu da bünyesinde barındırmaktadır. Bu sorunlar arasında, toplumdaki herkesin bilgisayar ve/veya internet erişimi sahibi

[76] **Falcıoğlu,** sh. 77.

olmaması, bu konudaki eğitim ve bilgi eksikliği, özel bilgiler bakımından gizliliğin sağlanamayacağı yönünde duyulan korku, tüketicilerin korunmasına ilişkin karşılaşılan sorunlar sayılabilir. Bu alanda karşılaşılan en önemli sorunlardan bir tanesi de, çok hızlı gelişen teknolojiye, hukuk düzeninin aynı hızla ayak uyduramamasıdır.

Klasik ticaretteki tüketici hakları elektronik ticaret için de geçerli olmakla birlikte, elektronik ortam sebebi ile satıcı ve tüketicinin mesafeli olması, alışveriş, sözleşme ve ödeme işlemlerinin hızlı yapılması ve özellikle gayrımaddi mallarda alışverişin tamamen gıyabta gerçekleşmesi gibi özellikler tüketiciye ilave korunma sağlanmasını gerektirmektedir.

Elektronik ticarette tüketicinin korunmasını zorlaştıran önemli bir noktanın da ortamın sınır ötesi niteliği olduğu anlaşılmaktadır. Bu konuda ülke sınırları içinde yapılan elektronik ticarette karşılaşılan tüketici sorunlarının klasik ticarette karşılaşılan sorunlara benzer yöntemlerle önemli ölçüde çözülebileceği, ancak, tüketici ile satıcının farklı ülkelerde bulunduğu durumlarda tüketicinin ciddi problemlerle karşılaşabileceği belirtilmektedir.

Bu alandaki tüketici sorunları; aldatıcı reklam ve hileli işlemlerden korunma, ödeme kartlarının suistimalinin engellenmesi, tüketici mahremiyeti anlamında alışveriş esnasında toplanan müşteri bilgilerinin korunması, mal ve hizmetteki ayıpların tazmini şeklinde özetlenebilir. Elektronik ticarette bu konularda karşılaşacakları

sorunlar karşısında tüketicilere sağlanacak hukuki korumanın klasik ticarette sağlanandan daha aşağı olmaması öngörülmektedir.

Diğer bir husus olarak, genel tüketici hukukunun önemli bir konusu olan sözleşme yapılması sırasında sözleşmenin kuvvetli tarafının öne sürdüğü genel işlem şartlarının; elektronik ticaret tüketicisi yönünden özel öneme sahip bir sorun alanı olarak değerlendirilmesi gereğidir.

Tüketici önceden tek taraflı olarak belirlenmiş olan sözleşme şartlarına müdahale edememekte, çoğu zaman sistem müşterinin şartları onaylamaması halinde işlem akamete uğrayacak şekilde yapılandırılmaktadır. Uluslararası normlara göre internet üzerinden yapılacak hukuki işlemlerde genel işlem şartlarının kullanımı halinde açıkça genel işlem şartları kullanımına dikkat çekilmiş olması, kavram ve ifadelerin müşteri tarafından anlaşılabilecek tarzda izah edilmiş olması ve nihayet uyuşmazlık halinde genel işlem şartlarının yorumlanmasında muhtemel yorum sonuçlarından müşterinin lehine olanın tercih edilmesi kabul edilmektedir.

Abartılı içerik ve reklamlar ile hileli işlemlerden önleyici korunma bağlamında, satıcının dokümalarda kullandığı dilin sade ve anlaşılabilir bir anlatımla oluşturulması ve özel bir terminoloji gerekli ise burada yer alan terimlerin tanımların da sunulması ve talep halinde soruların cevaplanmasını sağlayan bir yapı sağlanması gereğine işaret edilmektedir.

B.BİLGİ VERME YÜKÜMLÜLÜĞÜ

1. GENEL OLARAK

Mesafeli sözleşmenin kuruluşu esnasında taraflar farklı yerlerde bulunduklarından, tarafların birbirlerini görme ve gerek kişisel, gerekse ticari işletmeleri ile ilgili özellikleri açısından yeterince tanıma imkanına sahip olamamaktadırlar. Dolayısıyla, bu tür sözleşmelerde, sipariş edilen bir ürünün teslim edilmemesi veya çok geç teslim edilmesi, teslim edilen malın istenilen özelliklere uymaması, ödenen paranın çok geç iade edilmesi gibi riskler her zaman için mevcuttur[77].

Oysa, elektronik ticaretin gelişimindeki en büyük engellerden biri olarak görülen güven unsurunun ve kişilerin, özellikle tüketicilerin elektronik ticarete daha aktif katılabilmelerinin sağlanabilmesi için, mal veya hizmet sağlayan kişilerin kimliklerinin ve onların teşhisine yarayacak diğer bilgilerin önceden bilinmesi gerekmektedir. Bu durum, özellikle tüketici konumunda olan kişiler açısından, bir sözleşme ilişkisine girdiklerinde, mal veya hizmet sağlama taahhütlerini yerine getirip getirmeyecekleri, yerine getirmedikleri takdirde, onlara nasıl başvurabilecekleri konularında endişe duyulmasına yol açmaktadır. Bu endişelerin giderilmesi, bireylerin elektronik ticarete daha aktif şekilde katılmalarını sağlayacaktır. Diğer yandan, sözleşme konusu mal veya hizmetten yararlanacak olan kişiler, sözleşmenin kurulmasından önceki aşamada, bu mal veya hizmetleri görme

[77] **Özdemir Kocasakal,** sh. 47.

ve tecrübe etme imkanına sahip olmadıklarından, bunların nitelikleri hakkında da yeterince bilgi sahibi olamamaktadırlar[78].

Bu sakıncaları gidermek amacıyla, mesafeli sözleşmelerde, gerek mal veya hizmet sağlayan tarafın teşhisine yarayacak, gerekse sözleşme konusu mal veya hizmetin niteliklerini belirlemeye yönelik bazı bilgilerin, sözleşmenin kurulmasından önce muhataba bildirilmesi gerekmektedir.

Bu ihtiyaç, mal veya hizmetten yararlanacak olan tarafın tüketici sıfatıyla hareket ettiği durumlarda, zayıf taraf olarak tüketicinin korunması açısından da bir zorunluluk olarak kendini göstermektedir. Bunun yanında, internetin henüz ticari işlemler açısından çok yaygın olarak kullanılmaması, teknik birtakım özelliklerin herkes tarafından yeterince bilinmemesi, özellikle tüketicilerin internet teknolojisine uzak kalmaları, internet ortamında yapılan beyanların yazılı bir belgede yer almaması, dolayısıyla, bunların sonradan incelenme imkanının olmaması gibi hususlar bu koruma ihtiyacını artırmaktadırlar[79].

2. TÜRK HUKUKU AÇISINDAN

Genel olarak, TMK md.2'de yer alan dürüstlük kuralına dayandırılan bu yükümlülük, tüketici sözleşmeleri açısından, bu sözleşmelerin zayıf tarafını oluşturan tüketiciyi korumak amacıyla, özel olarak düzenlenmiştir.

---

[78] **Özdemir Kocasakal,** sh. 47.

[79] **Özdemir Kocasakal,** sh. 48.

Gerçekten de, 4077 sayılı TKHK'un mesafeli sözleşmelerle ilgili md.9/A'da, mesafeli satış sözleşmesinin akdinden önce, birtakım bilgilerin tüketiciye verilmesinin zorunlu olduğu belirtilmiştir.

Tüketicinin bu bilgileri, sözleşmenin kurulmasından önceki bir aşamada edinmiş olması o kadar önemlidir ki, tüketici bu bilgileri doğru ve eksiksiz olarak edindiğini yazılı olarak (elektronik ortamda yapılan sözleşmelerde elektronik ortamda) teyit etmedikçe sözleşmenin kurulması mümkün değildir.

Sanayi ve Ticaret Bakanlığı, Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmelik[80]'te bu bilgilerin içeriğini belirlemiştir. Bu bağlamda, tüketiciye verilmesi gereken bilgiler, Yönetmeliğin "Ön Bilgiler" başlığını taşıyan md.5'te hükme bağlanmıştır. Buna göre;

ba) Satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,
bb) Sözleşme konusu mal ya da hizmetin temel özellikleri,
bc) Sözleşme konusu mal ya da hizmetin tüm vergiler dahil satış fiyatı,
bd) Satıcı veya sağlayıcının fiyat dahil tüm vaatlerinin geçerlilik süresi,
be) Tüketicinin ödemelerinin nasıl yapılacağına dair bilgiler,
bf) Teslimat ve ifanın nasıl yapılacağına ve varsa buna ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,
bg) Cayma hakkı ve bu hakkın nasıl kullanılacağına dair bilgiler,

[80] RG 13.06.2003-25137.

bh) Tüketiciye bir maliyeti varsa kullanılan iletişim yollarının ücreti,

bı) Sözleşme konusu mal ya da hizmetin, teslim ve ifa tarihlerine ilişkin program,

bi) Tüketicinin talep ve şikayetlerini iletebileceği satıcı veya sağlayıcının açık adres, telefon ve varsa diğer erişim bilgilerinin,

mesafeli sözleşmenin akdinden önce tüketiciye verilmesi zorunludur.

Mesafeli sözleşmenin akdinden önce tüketiciye verilmesi gereken bilgiler ile AB'nin Mesafeli Sözleşmeler Yönergesi 4. md. uyarınca tüketiciye bildirilmesi gereken bilgiler arasında paralellik olduğu gözlenmektedir.

Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmeliğin "Ön Bilgilerin Doğruluğunun Yazılı Olarak Kanıtlanması" başlığını taşıyan 6.md., "Tüketici, ön bilgileri doğru ve eksiksiz olarak edindiğini yazılı olarak teyit etmedikçe sözleşme akdedilemez. Elektronik ortamda yapılan sözleşmelerde bu teyit işlemi yine elektronik ortamda yapılır. Tüketici, mallar için sözleşme konusu mal kendisine ulaşmadan, hizmetler için de en geç sözleşmenin ifasından önce ön bilgileri içeren yazılı onayı almalıdır." hükmünü ihtiva etmektedir.

TKHK md.9/A f.2 ve Yönetmeliği 6. md. ön bilgiler teyit edilmeden sözleşmenin akdedilemeyeceğini öngörmektedir. Bu konuya ilişkin olarak doktrinde Aslan, TKHK md.9/A f.2 ve Yönetmeliğin 6.md.'nin mesafeli sözleşmenin geçersiz olacağı

şeklinde anlaşılmaması gerektiğini, zira, sözleşmenin zorunlu içeriği ve şeklinin başka bir maddede düzenlendiğini belirtmektedir[81].

Bizim de katıldığımız görüşe göre, aynı sonuca farklı bir gerekçeyle de ulaşılabilir. TKHK'nun "Kapıdan Satışlarda Satıcının ve Sağlayıcının Yükümlülüğü" başlığını taşıyan 9. md. son paragrafında; "Bu madde hükümlerine göre düzenlenmiş bir sözleşmenin veya malın tüketiciye teslim edildiğini ispat satıcı veya sağlayıcıya aittir. Aksi takdirde, tüketici cayma hakkını kullanmak için yedi günlük süre ile bağlı değildir." hükmü yer almaktadır. Bu hüküm TKHK md.9/A f.5 hükmü uyarınca mesafeli sözleşmelere de uygulanmaktadır. Buna göre, sözleşmenin aslının teslim edilmemesinin dahi sözleşmenin geçersizliği sonucuna bağlanmadığı bir durumda, mesafeli sözleşmeye ilişkin ön bilgilerin teyit edilmemesinin ilgili sözleşmeyi geçersiz kılması şeklinde bir sonuca varılmaması gerekir. Nitekim, ön bilgilerin tüketici tarafından teyit edilmemesi halinde taraflar arasında bir elektronik satım sözleşmesinin kurulmadığının kabulü özellikle tüketicilerin aleyhine olan sonuçlar doğuracaktır[82].

Ön bilgi verme yükümlülüğüne aykırılıktan dolayı tüketicilerin uğrayacakları olası zararların giderilmesine yönelik olarak farklı görüşler ileri sürülmektedir. Özdemir Kocasakal, bilgilendirme yükümünün ihlalinin edimin ayıplı mal veya hizmet olarak nitelendirilmesine yol açması halinde, tüketicinin TKHK'nun bu konuya ilişkin düzenlemeleri (md. 4 ve 4/A) ile kendine sağlanan haklardan yararlanabileceğini

---

[81] **Aslan,** sh.419.

[82] **Falcıoğlu,** sh. 223-224.

belirtmektedir[83]. Buna karşılık, Aslan, gerekli bilgileri vermeyen satıcıya TKHK md. 25'te getirilen para cezasının uygulanabileceğini ve bilgilendirilmemekten dolayı tüketicinin uğrayacağı zararların tazmin edilmesinin gerekeceğini saptamaktadır[84].

C. MESAFELİ SÖZLEŞMEDE TÜKETİCİYE TANINAN CAYMA HAKKI

Web üzerinden kurulan bir elektronik satım sözleşmesinin alıcı tarafında bir tüketicinin bulunması halinde tüketiciye bir cayma hakkı tanınmıştır[85]. Bu bağlamda, TKHK md.9/A f.5 hükmü uyarınca, "Cayma hakkı süresince sözleşmeye konu olan mal veya hizmet karşılığında tüketiciden herhangi bir isim altında ödeme yapmasının veya borç altına sokan herhangi bir belge vermesinin istenemeyeceğine ilişkin hükümler dışında kapıdan satışlara ilişkin hükümler mesafeli sözleşmelere de uygulanır". Hüküm uyarınca, mesafeli sözleşmeler kapıdan satışlarda söz konusu olan cayma hakkının kapsamına alınmışlardır. Mesafeli sözleşmelerde tüketiciye tanınan cayma hakkı doktrinde oldukça tartışmalara neden olmuş bir konudur[86].

---

[83] **Özdemir Kocasakal,** sh.49.

[84] **Aslan,** sh.420.

[85] **Özel, Ç.:** Mukayeseli Hukuk Işığında Tüketiciyi Koruyan Geri Alma Hakkı, Ankara,1998, sh.168-169.

[86] **Gonzenbach, R.:** "Pacta sunt servanda" oder neues Licht auf alten Grundsatz-Notizen zu einem Konsumentenschutzproblem, ZSR, 1987 I, sh.462; **Honsell, Heinrich/ Pietruszak, Thomas:** Der Vernehmlassungsentwurf zu einem Bundesgesetz über den elektronischen Geschaftsverkehr, AJP, 7/2001, sh.779; **Roth, Birgit/ Schulze, Götz:** Verbraucherschutz im Electronic Commerce- Schutz-

Buna göre, kapıdan satışları düzenleyen, TKHK md.8 f.3 uyarınca, "tüketici, teslim aldığı tarihten itibaren yedi gün içinde malı kabul etmekte veya hiçbir gerekçe göstermeden ve hiçbir yükümlülük altına girmeden reddetmekte serbesttir". Tüketici bu süre içinde caymazsa, sözleşme kurulması anından itibaren hüküm ve sonuçlarını doğurmaya başlar, bununla birlikte, sözleşmeden cayılması halinde başlangıçtan itibaren hüküm doğurmayacaktır[87]. Tüketiciye tanınan cayma hakkı çerçevesinde yapılan cayma bildirimi yenilik doğuran haklardandır[88].

Web üzerinden kurulan bir elektronik satım sözleşmesi, alıcının cayma hakkı süresi boyunca hüküm ve sonuçlarını doğurmayacaktır. AB'nin Mesafeli Sözleşmeler Yönergesi ise mesafeli sözleşmelerde cayma hakkının kullanımını yedi iş günü ile sınırlandırmıştır.

Mesafeli sözleşmeler bakımından tüketiciye tanınmış olan cayma hakkının konu ve kapsam açılarından elektronik satım sözleşmesi ile ilgili iki istisnası bulunmaktadır. TKHK md.9/A f.5 metninde saptandığı üzere, kapıdan satışlarda tüketicinin cayma hakkı süresince ödeme yapmamasına ilişkin kural, genel olarak mesafeli

---

mechanismen un grenzüberschreitende Geschaefte nach dem Referentenent- wurf eines Fernabsatzgesetzes, RIW, 1999, sh. 927 (Nakleden **Bozbel,** sh. 206, 207).

[87] **Zevkliler, A.:** Tüketicinin Korunması Hakkında Kanun, Ankara, 2001, sh.129; **Aslan,** sh.395; **Özel,** sh.168.

[88] **Aslan,** sh.395; **Özel,** sh.100; **Falcıoğlu,** sh.233; Cayma bildiriminin genel olarak bozucu bir yenilik doğuran hak olduğu görüşü için bkz. **Zevkliler,** sh.129.

sözleşmelerde ve dolayısıyla web üzerinden kurulan elektronik satım sözleşmelerinde uygulanmamaktadır.

Mesafeli sözleşmelerde cayma hakkına ilişkin olarak getirilmiş olan ikinci istisna ise sözleşmenin konusuna ilişindir. Mesafeli Sözleşme Yönetmeliği md.8 f.2 uyarınca, "Elektronik ortamda anında ifa edilen hizmetler ve tüketiciye anında teslim edilen mallara ilişkin sözleşmeler cayma hakkı ve kullanımına ilişkin hükümlere dahil değildir". Mesafeli Sözleşme Yönetmeliği çerçevesinde, tüketiciye anında teslim edilen mallara ilişkin olarak yapılan mesafeli sözleşmelerde tüketicinin cayma hakkı bulunmamaktadır. Hükmün elektronik satım sözleşmeleri bakımından etkisi, özellikle maddi olmayan malların satımında ortaya çıkmaktadır. Elektronik satım sözleşmesinin kurulmasını takiben, satıcı tarafından alıcıya anında teslim edilen mallar olan maddi olmayan mallar ilişkin sözleşmelerde tüketicinin cayma hakkı bulunmamaktadır[89].

[89] **Falcıoğlu,** sh.234.

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK İMZA

§7. DİJİTAL İMZA-ELEKRONİK İMZA

I. TANIM

E-ticaretin gelişebilmesi ve kullanıcılar tarafından benimsenebilmesinin ilk şartı, açık ağ sistemine güven duyulmasının sağlanmasıdır[90]. Bu amaçla, e-ticaretin gerçekleştiği ortamda, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu, kurulacak teknik ve hukuki bir altyapı ile garanti edilebilmesi ihtiyacı duyulmaktadır. İşte e-imza, bu ihtiyacın karşılanması amacıyla kullanılan bir teknolojidir[91].

E-imza, kimliğini ve mesaj içeriğine onay verildiğini göstermek amacıyla bir kimse tarafından (veya onun namına) mesaja eklenen veya mantıksal olarak mesaja bağlı

---

[90] **Konuralp, H.:** Genel Hatlarıyla Elektronik İmza Kanunu, Bankacılık Açısından Elektronik İmza Konferansı, 04.03.2004, İstanbul, www.tbb.org.tr/eklenenler/eklenenler-ocak04.htm, sh.2

[91] **Acır,** sh.22; 5070 sayılı Elektronik İmza Kanununun Genel Gerekçesi için bkz. <http://www.basbakanlik.gov.tr/tasarilar/Tasari-9.htm

olan elektronik bilgidir. Başka bir tanımda[92] e-imza, bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir set olarak tanımlanmaktadır.

E-imza, birçok ulusal ve uluslararası düzenlemelere konu olduğundan bu düzenlemelerde yapılan e-imza tanımlarına da değinilmesinde yarar vardır.

15.01.2004 tarihinde kabul edilen ve 23.01.2004 tarih ve 25355 sayılı RG'de yayınlanan ve 23.07.2004 tarihinde yürürlüğe giren 5070 sayılı EİK'nun "Tanımlar" başlıklı 3. maddesinin b bendine göre, elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi ifade eder. Bu tanım oldukça geniş bir tanımlamadır. Türk hukukunda da, elektronik imza tanımında AB Direktifi esas alınarak bir tanım yapılmıştır[93] .

---

[92]ElektronikTicaretHukukAltyapısı,Etkk,<http://www.igeme.org.tr/tur/etrade/etkk/huk uk/h altyapi.htm> (par.2).

[93] **Erturgut, M.:** Elektronik İmza Kanunu Bakımından e-Belge ve e-İmza(Hukuki Açıdan Tanıtım ve Değerlendirme), Bankacılık Açısından Elektronik İmza Konferansı, 04.03.2004, İstanbul, www.tbb.org.tr/eklenenler/eklenenler-ocak04.htm, sh.3.

ETKK Hukuk Çalışma Grubu raporlarında, elektronik imza şu şekilde tanımlanmıştır: Bir bilginin, üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir seti ifade eder[94].

UNCITRAL Elektronik Ticaret Çalışma Grubu'nun 14-25 Şubat 2000 tarihlerinde yapılan 36. toplantısında hazırlanan ve e-imza konusunda düzenleme yapacak ülkelere yol gösterme ve bu alanda, uluslararası ticaretin gelişimine yönelik olarak paralel düzenlemeler yapılmasını teşvik etmek amacıyla hazırlanan "Draft Uniform Rules on Electronic Signatures[95] (Elektronik İmza Yeknesak Kurallar Taslağı)" nın 2 nci maddesinin (a) bendinde, e-imza, imza sahibinin kimliğini tanımlamak ve veri mesajının içeriğindeki bilginin imza sahibince onaylandığını göstermek için, elektronik formdaki bir veriye eklenmiş olan veya mantıksal olarak o veri mesajı ile bağlantısı kurulabilen, elektronik bilgi veya yöntem olarak tanımlanmıştır.

AB'nin 13 Aralık 1999'da tarihinde kabul edilen ve 19.1.2000 tarihinde yürürlüğe giren "Directive 1999/93/EC of the European Parliament and of the Council of 13

---

[94] http://www.etkk.gov.tr/hukuk.htm>

[95] Recent Documents of UNCITRAL and its Working Groups, Working Group on Electronic Commerce, <http://www.uncitral.org/english/sessions/wg_ec/index.htm>

December 1999 on a Community Framework for Electronic Signatures"[96] (Elektronik İmzalar için Ortak Altyapıya Dair Avrupa Parlamentosu ve Konseyi Direktifi)'nin 2. maddesinin 1. bendinde e-imza, eklendiği veya mantıksal olarak ilişkili olduğu elektronik formdaki bilgiye, bir kimlik belirleme (doğrulama) yöntemi olarak hizmet eden, (a) münhasıran imza sahibine bağlanan, (b) imza sahibini tanımlayabilen, (c) imza sahibinin münhasır kontrolü altında muhafaza edilen araçlarla yaratılan, (d) veride sonradan meydana gelen değişiklikleri gösterecek (ortaya çıkaran) şekilde veriye eklenen elektronik formdaki bilgi şeklinde tanımlanmıştır.

ABD'nde 30 Haziran 2000 tarihinde kabul edilerek 1 Ekim 2000 tarihinde yürürlüğe giren "Electronic Signatures In Global and National Commerce Act"[97] (E-SIGN ACT: E-İmza Kanunu)'nun SEC.301/6-B hükmüne göre e-imza, bir elektronik kayda eklenen veya mantıksal olarak onunla bağlantılı olan ve bir kimse veya onun elektronik temsilcisi tarafından bir sözleşmeyi, anlaşmayı veya kaydı imzalamak niyetiyle, icra edilen veya kabul edilen elektronik biçimdeki bilgi veya veridir.

---

[96] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures (Official Journal L 13, 19.01.2000). <http://www.ispo.cec.be/eif/policy/policy.html>.

[97] List of Enacted Statutes and Regulations, McBride Baker&Coles <http://www.mbc.com/ecommerce/legis/congress.html>

II. KAVRAM

Görüldüğü üzere, elektronik imza, konuyla ilgili birçok çalışmada ve Avrupa Birliği Direktifi ve pek çok ülkelerin kanunlarında tanımlanmıştır. Bütün bunlar dikkate alınarak kavramı açıklamak gerekirse, elektronik imzanın, kişilerin biyometrik özelliklerine dayalı (ses, göz retinası taraması, parmak izi taraması gibi) biyometrik yöntemler, kredi kartlarında kullanılan PIN kodları, elle atılmış imzanın tarayıcıdan geçirilerek elektronik ortama aktarılmış hali, bilgisayar ekranında bu amaçla yapılmış bir kalemle atılan imza tekniği veya çift anahtarlı kriptografiyle oluşturulan dijital (sayısal) imzayı da içeren bir üst kavram olarak karşımıza çıktığı görülmektedir[98].

Elektronik imza tanımlarında herhangi bir teknolojiye üstünlük tanınmadan, sadece ondan beklenen fonksiyonlar dikkate alınarak tanım yapılması "teknolojik tarafsızlık" kavramıyla açıklanabilir. Böylece elektronik imza alanında gerçekleşen değişikliklerin kanun değişikliğine gerek kalmaksızın uygulanabilmesi sağlanmış olmaktadır. Kanuni düzenlemeler, bu anlamda teknolojinin gerisinde kalmamış ve her değişikliğe uygulanabilir bir duruma getirilmiştir. Elektronik imza, şimdiye kadar

---

[98] **Erturgut,** sh.2; www.tk.gov.tr; **Ford, M. D.:** Identitiy Authentication and E-Commerce, http://www.law.worwick.ac.uk/jilt/98-3/ford.html>; **Arıkan,** sh.23, dp.32; **Sevimli, A.:** Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası, Prof.Dr. Hayri Domaniç'e 80.Yaş Günü Armağanı, C.II, İstanbul, 2001, sh.1029; **Reed, C.:** What is a signature? http://www.elj.warwick.ac.uk/jilt/00-37reed.httm>.

imzalamada kullanılan ve ileride kullanılabilecek tüm yöntemleri kapsar bir şekilde hukuki düzenlemeye kavuşmuştur[99].

Elektronik imzaya ihtiyaç duyulmasının en önemli sebebi, hukuki işlemlerde güvenlik, kimlik tespiti, inkar edilmeme gibi özelliklerin sağlanmak istenmesidir.

III. DİJİTAL İMZA İLE ELEKTRONİK İMZANIN KARŞILAŞTIRILMASI

A. GENEL OLARAK DİJİTAL İMZA (SAYISAL İMZA)

20. yüzyılda teknoloji hız ve sınır tanımayan bir olgu olduğu için, bütün dünya insanlarını ilk önce "internet" adı verilen global ağ ile, daha sonra ise bu ağ üzerinden kendisinden kilometrelerce uzakta bulunan diğer bir kişi ile haberleşmek veya sözleşme yapmak için can atan kişilerin, bu işlemlerini bağlayıcı kılmalarını sağlayacak, kimliklerini ispata yarayacak "dijital imza" adı verilen bir imza türü ile tanıştırmıştır[100].

Teknoloji, bu yenilikleri bizlere sunma görevini yerine getirdikten sonra, şimdilik devreden çıkmış ve bu yenilikler konusunda yasal düzenlemeler yapılması, bu yeniliklerin ortaya çıkarabileceği hukuki sorunlara çözümler bulunması için sahneyi hukukçulara bırakmıştır. Bugün, hukukçulara düşen görev, teknolojinin hepimize hazırlayacağı bir sonraki sürprize kadar, karşı karşıya bulunduğumuz " Dijital İmza

---

[99] **Erturgut,** sh.3

[100] **Keser Berber,** (Şekil), sh.54.

ve Ortaya Çıkarabileceği Sorunlar, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri" gibi konularda yasal bir çerçeve oluşturmaktır. Ancak burada dikkat edilmesi gereken önemli bir nokta vardır: Yarıştığımız şey, başka bir ülkenin hukuku değil, teknolojidir. Teknoloji, ortaya çıkardığı her yeniliğe yasal bir elbise giydiren hukuktan daha hızlı gelişen ve değişen bir yapıya sahiptir. Şu an biz dijital imzayı ve sorunlarını tartışırken, aynı anda teknoloji uzmanları belki halihazırda tartıştığımız konuları çözümleyecek veya bu tartışmaları gereksiz bırakacak tamamen yeni bir yöntemle karşımıza çıkmaya hazırlanıyor olabilirler [101].

Türkiye gibi toplumlarda "dijital imza", yalnız elektronik ticaret ve özel hukuku değil, "e-devlet"e geçiş ve bilgi-okuryazarlığını teşvik açısından kamu hukukunu da ilgilendiren bir konudur[102]. Bu bir bakıma devletin ve bireylerinin kimliklerini elektronik ortama taşıyıp, birbirleriyle yeni bir düzlemde iletişim kurması olacağı için, önemli bir dönüşümün anahtarı demektir[103].

---

[101] **Keser Berber,** (Şekil), sh.54

[102] Bkz. Kamu Hukuku ve Bilişim İletişim Teknolojileri, **A. Tansuğ-Ö. Uçkan,** TBS Hukuk Çalışma Grubu Arşivi http://www.bilisimsurasi.org.tr (Hukuk Çalışma Grubu Dosyaları)

[103] Dijital İmza ve Yasal Düzenleme Yaklaşımları, Bilişim Şurası Hukuk Çalışma Grubu Raporu, Şubat 2002.

B. TANIM VE KAVRAM

Elektronik imzaların bir türü olan dijital imza, asimetrik kriptografinin kullanılması suretiyle, elektronik mesajların doğruluğunu teyit ve bu mesajların içeriğinin bütünlüğünü garanti eden, açık anahtarlı kriptografi (şifreleme) sistemleri ile yapılan teknolojik uygulamaların adıdır[104]. Bir başka tanımda, dijital imza, başka bir dijital dokümana[105] eklenmiş ya da mantıken ilişkilendirilmiş bitlerden oluşan bir seriyi ifade eder. Başka bir deyişle, alıcıya, gönderenin kimliğini ve mesajın iletişim sırasında değiştirilip değiştirilmediğini belirleme imkanı tanıyan bir mühür olarak da tanımlamak mümkündür[106].

Elektronik ortamda yaratılan kimlik bilgisi olarak tanımlayabileceğimiz elektronik imza ve dijital imza (sayısal imza) terimleri birbirlerinin yerine geçer şekilde kullanılmaktadır Ancak, elektronik imza her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız bir terim olduğundan bir üst kavram olarak kabul edilebilir.

---

[104] **Acır,** sh.26

[105] Doküman: Bir verinin üzerine kaydedildiği, insan ya da makina tarafından okunabilen, (değişmez) veri taşıyıcı. Elektronik Ticaret Terimler Sözlüğü?" http://www.etkk.gov.tr/ETKKsozluk.htm>.

[106] **Keser Berber,** (Şekil), sh.72-73; **Keser Berber, L.:** İmzalıyorum O Halde Varım, Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri, TBDD, S.2000/2 (İmza), sh.506; **Kırçova, İ./Öztürk, P.:** Internette Ticaret ve Hukuki Sorunlar, İstanbul, 2000, sh.69; **Arıkan,** sh.23.

Dijital imza (sayısal imza), elektronik imza çeşitlerinden sadece birisidir. Elektronik imza, günümüz teknolojisinde çeşitli şekillerde olabilmektedir. Halen kullanılan imza dosyaları, biyometri tekniği (kullanıcının parmak ya da el izi, göz retinası vb. kişiye has özellikler) ile oluşturulan imzalar ve sayısal imzalar en çok bilinen ve tartışılan elektronik imza çeşitleridir. Hatta, çoğu kişi ve kurumların, fiziki ortamda imzaladıkları belgeleri tarayıp bilgisayara aktarmak ve sonra da karşı tarafa göndermek şeklinde elektronik imza uygulaması yaptıkları da sıkça görülmektedir[107].

DTM bünyesinde kurulmuş ETKK Hukuk Raporu'na göre sayısal imza; "Elektronik imzanın özel bir çeşidi olup, bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür. Sayısal imzalar göndericinin kimliğinin açık ve net bir biçimde teyidini, elektronik dokümanın orijinalliğini ve güvenilirliğini mümkün kılar. Gönderici için ve mesajın gönderildiği taraf için tek olan sayısal imzalar doğrulanabilir ve inkar edilemez." diye tanımlanmaktadır.

---

[107] Diğer elektronik imzalara parmak izi, retina, yüz veya ses taraması gibi biometrik yöntemlerle oluşturulan veya PIN (Personal Identification Number) numarası verilerek oluşturulan elektronik imzalar örnek verilebilir. Bkz. **Ekşi, N.:** Elektronik İmzalara İlişkin UNCITRAL Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme, Yasa Hukuk Dergisi, S.3, Mart, 2001, sh.336; **Ahi, G. M.:** Hukuki Bakımdan Dijital İmza (Sayısal İmza), gokhan@hukukcu.com, sh.2

Avrupa'da e-imza alanında ilk yasal düzenleme yapan ülkelerden biri olan Almanya'nın Dijital İmza Kanunu[108]'nun 2/1 hükmünde dijital imza şu şekilde tanımlanmıştır: Dijital imza, dijital (sayısal) veri üzerinde, bir özel imza anahtarı ile yaratılan bir mühür anlamına gelir. Bu mühür, ilgili açık anahtarların kullanımı ile, bir onaylayıcının veya bu kanunda belirtilen Kurum'un imza anahtar sertifikasına eklenmek suretiyle, imza anahtarının sahibinin ve verinin doğruluğunun anlaşılmasını sağlar[109].

Öte yandan e-imzaya ilişkin bazı uluslararası düzenlemelerde[110], gerek farklı devletlerin yasal düzenlemelerinde, elle atılan imzanın yerine kullanılabilen bir e-imza olarak benimsenmiş olan farklı e-imza (kimlik tespiti) teknolojilerine, gerek kimlik tespiti hususunda bilim ve teknoloji alanında her geçen gün geliştirilmekte olan yeni teknolojilere karşı, bu teknolojilerin, elle atılan imzanın işlevlerini yerine getirebilmesi ve böylece elle atılan imza yerine geçebilmesi koşuluyla, ayrım ve sınırlayıcı düzenlemeler yapılmaması ve bu özelliklere sahip tüm e-imzalara aynı hukuki değerin tanınması gerektiği hükmü öngörülmektedir. Bu suretle e-ticaretin küresel boyutu bağlamında, farklı devletlerdeki farklı düzenlemeler nedeniyle meydana gelebilecek hukuksal güvensizlik ve mevcut teknolojiler çerçevesinde

---

[108] Digital Signature Law (Signaturgesetz) Translated from German by **C. Kuner**) <http://www.kuner.com/data/reg/multimd3.htm> (par.3).

[109] **Acır,** sh.26

[110] UNCITRAL Draft Uniform Rules on Electronic Signatures, md.3.; Directive of the European Parliament and Council on a Community Framework for E-signatures, Recital par.21.

yapılmış bulunan düzenlemelerin, zaman içinde gelişen e-imza teknolojilerinden yararlanamaması tehlikesi karşısında, mevcut düzenlemelerin sık sık güncellenmesi ihtiyacı bertaraf edilmeye çalışılmaktadır[111].

C. DİJİTAL İMZA-ELEKTRONİK İMZA İKİLEMİ

Çeşitli ülkelerde yürürlüğe girmiş bulunan ya da girmek üzere olan yasa metinleri incelendiğinde "dijital imza" ve "elektronik imza" terimlerinden birinin seçildiği görülmektedir. İlk bakışta bu bir terminoloji tercihi meselesi gibi durmakla birlikte, bu iki terim birbirinden farklıdır ve birbirleriyle karıştırılmamalıdır.

Bir "dijital imza", aynı zamanda "elektronik" olmakla birlikte, "elektronik imza" çok daha geniş bir alanı kapsamaktadır. Bu geniş alanın içinde, el yazısı (ıslak) imzanın yerini elektronik ortamda alabilecek bütün teknolojiler girmektedir. El yazısı imzanın orijinalinin taranarak dönüştürüldüğü bir görüntü dosyası, PIN kodu ve dijital kalemle atılmış imza gibi.

İmza, "kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir kimse tarafından veya onun namına kullanılan herhangi bir işaret veya kabul edilen herhangi bir güvenlik usulüdür[112]. Genel olarak elektronik imza; elektronik ortamda oluşturulan, iletilen ve saklanabilen özel bir elektronik belgeyi ifade etmektedir[113].

---

[111] **Acır,** sh.26-27

[112] **Çanga, T.M.:** Elektronik İmza Ve Elektronik İmza Yasa Çalışmaları, www.etkk.gov.tr/hukuk.htm

Dijital imza ise bir bilginin, üçüncü kişilerin erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir settir[114]. Dijital imza el yazısı ile atılan imzanın sahip olduğu özelliklerini ve fonksiyonlarını, elektronik ortamda yapılan hukuki işlemler için de sağlamak amacıyla geliştirilmiş olan bir tekniktir[115]. Dijital imza; metnin, belgenin yazarı tarafından düzenlendiğini belirtmek kadar, başkası tarafından bozulmadığını da göstermek amacını güder ve dolayısıyla esasında metnin tamamı dijital imzaya dönüşmüş olur[116]. İmzayı atanın iradesinin yönünü ortaya koyması imzanın asıl fonksiyonudur[117]. Sözleşmeye taraf olma ve sözleşmenin getirdiği hak ve yükümlülükleri kabul etme iradesinde olma imzanın önemli bir fonksiyonudur. Aynı zamanda imzadan, imzalayanın; imzaladığı metni okuduğu ve anladığı ya da belgeyi bizzat hazırlayan kişi olduğu sonucuna da varılabilir. İrade beyanında bulunan kişinin tespiti ve beyan ettiği iradenin bütün ve değişmeksizin ulaştığına dair güvenin sağlanması yine imzanın sağladığı diğer

---

[113] **Sevimli,** sh.1029.

[114] www.etkk.gov.tr/hukuk.htm: Elektronik Ticaret Koordinasyon Kurulu Raporları, Hukuk Çalışma Gurubu Raporu, s.8; Diğer bir tanım: Elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletim sırasında bozulmadığını kanıtlamaya yarayan bölüm. Bkz. Elektronik Ticaret Terimler Sözlüğü, (TÜBİTAK-BİLTEN), http://www.etkk.gov.tr

[115] **Sözer,** (Sözleşme), sh.127.

[116] **Sözer,** (Sözleşme), sh.127

[117] **Sevimli,** sh.1028.

güvencelerdir[118]. Dijital imza; el ile imzanın tüm bu fonksiyonlarını yerine getirebilmek için geliştirilmiş bir teknolojidir[119]. Dijital imzanın işlevi, elektronik ortamda aslından ayrılması güç olan sahte imzayı önlemek ve orijinal dokümanların olduğu şekilde herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır[120]. Ancak bunun için dijital imzanın belli vasıflara sahip olmasının aranacağı kuşkusuzdur. Elektronik imzaların el ile atılan imzalarla eşdeğer kabul edilebilmesi için bir takım hukuki şartlar gerek Avrupa Topluluğu İmza Yönergesinde (SigRL)[121] gerekse ABD'de kanunlaşan "E-Sign Act[122]" da yer almaktadır[123]. Internet bilindiği üzere belli bir ülkeye ait değildir, dolayısıyla bu iletişim ağının tamamında ve her konuda geçerli bir hukuk düzeninin sağlanması mümkün değildir[124]. AB

---

[118] **Sevimli,** sh.1028.

[119] **Pekcanıtez, H.:** Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, Uluslararası Internet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002, sh.395.

[120] **Keser Berber,** (İmza), sh.503.

[121] Signaturrichtlinie(SigRL): İmza Yönergesi; 19 Ocak 2000 tarihinde yürürlüğe girmiştir. Üye ülkelerde 19.7.2001 tarihine kadar iç hukuka alınacağı öngörülmüştür.

[122] 1 Ekim 2000 tarihinde yürürlüğe girmiştir.

[123] **Bilgili, F.:** Özel Hukukta Elektronik İmza ve Elektronik Ticaret, Prof.Dr. Ömer Teoman'a 55. Yaş Günü Armağanı, C.II, Beta Yayınları, İstanbul, 2002, sh.991 vd.

[124] **Nomer, N. F.:** Internet Alan Adının (Domain Name) Hukuki Niteliği Ve Marka Ve Ticaret Unvanı Gibi Ayırt Edici Ad Ve İşaretler İle Arasında Benzerlik

çerçevesinde yapılan düzenlemeler ve hazırlanan model kanun bu hususta yeknesaklığı sağlamaya yöneliktir. Diğer bazı ülkelerde de internet ve dijital imza ile ilgili kanuni düzenlemeler yapılmakta ancak bunların yürürlük alanı o ülke ile sınırlı kalmaktadır.

Elektronik imza günümüzde, kişinin elektronik ortamda tanınmasına olanak veren en basitten en karmaşığa kadar her türlü teknik çözüm için kullanılan bir üst kavramdır. Örneğin; kişinin kendi el yazısı ile attığı imzanın bir tarayıcıdan (scanner) geçirilerek bilgisayara aktarılması ve hazırlanan metinlerin, mesajların altına (copy paste edilerek) eklenmesi en basit bir elektronik imza tekniğidir. Sanal ortamda bağlayıcı işlem yapma olanağını bugün sağlamaya çalışan diğer bir elektronik imza tekniği ise; sayısal imza veya dijital imzadır. Dijital imza ise, kişinin el yazısı ile attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştirmeye çalışan matematiksel formüllere veya şifreleme programlarına verilen bir isimdir. Bugün için dijital imza, internette işlem güvenliğini sağlamak için en çok tercih edilen bir elektronik imza çeşididir.

Elektronik imza kapsamına giren diğer bir grup ise; biyometrik yöntemlerdir. Biyometrik yöntemler, kişinin kendi vücut özelliklerinin gerek bilgisayara girişte gerek internette yapılacak işlemlerde güvenliği sağlamak amacıyla kullanılmasıdır. Örneğin; çok yaygın olarak kullanılan parmak izi, avuç içi izi, ses, retina ve DNA kopyalama sistemleri, günümüzde internette yapılacak işlemlerin güvenliği

---

Bulunması Sebebiyle Doğabilecek Hukuki Sorunlar, Prof.Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı, C.1, Beta Yayınları, İstanbul, 2001, sh.398.

bakımından değil, daha çok bilgisayar sistemine girişte güvenliği sağlamak amacıyla kullanılmaktadır. Şüphesiz yakın bir tarihte biyometrik yöntemler sanal ortamda işlem güvenliği bakımından belki dijital imza yerine daha çok kullanılacak olan yöntemlerdir. Ancak, kişilerin söz konusu özelliklerinin dijital imzadaki gibi bir sertifika kurumu tarafından kopyalanması ve sistemin bu tür kurum veya kurumlar aracılığı ile işletilmesi, dijital imzadakinden daha farklı bir alt yapıyı ve güvenliği gerektirmektedir. Bu nedenle her ne kadar 5070 sayılı EİK'nun Genel Gerekçe bölümünde elektronik imza kavramının, sayısal imza veya biyometrik tanımlama yöntemlerinin kullanımına olanak veren bir üst kavram olduğu ve bu nedenle tercih edildiği belirtilmişse de; bilgisayar tekniği ve hazırlanış ve kullanılış (işleyiş) şekilleri bakımından dijital imza kullanımı ile biyometrik yöntemler arasında oldukça büyük farklar mevcuttur. 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 mümkün değildir. Biyometrik yöntemlerin teknik yapısı ve hukuki sorunlarının mutlaka ayrı bir kanunda düzenlenmesi gerekmektedir. Zaten Kanundaki hükümler dikkate alındığında, bu hükümler ile kanun koyucunun sadece dijital imza ile ilgili olarak düzenleme yaptığı anlaşılmaktadır.

Dolayısıyla, kanaatimize göre bu Kanunun adının "TÜRK DİJİTAL İMZA KANUNU" olması ve böylece Kanundaki hükümler ile Kanunun adı arasındaki çelişkinin giderilmesi yerinde olacaktır.

IV. DİJİTAL İMZA TEKNİĞİ

A. DİJİTAL İMZANIN TEKNİK ALTYAPISI VE SİSTEMİN İŞLEYİŞİ

1. GENEL OLARAK

Dijital imza teknik olarak bir yazılımdır (Software)[125]. İnternet üzerinden yapılan veri alışverişinde şu üç unsurun sağlanmasına yönelik işlev görür. Bunlardan birincisi gizliliktir yani iletilen verilerin alıcıya varana kadar başkalarının bu verilere vakıf olamaması yani tamamıyla gizli kalmasıdır[126]. Teknik açıdan öncelikle alıcının bu hususta emin olması sağlanmalıdır. İkinci unsur bütünlüktür. Verilerin bozulmadan, başkaları tarafından değiştirilmeden, üzerine eklemeler veya silintiler yapılmadan alıcıya ulaşmasıdır[127]. Üçüncü unsur gerçekliktir yani verilerin görünüşe

---

[125] **Keser Berber,** (İmza), sh.514; **Sözer,** (Sözleşme), sh.127; Dijital imzanın bir donanım (Hardware) şeklinde hazırlanması da mümkündür. Ancak yazılımın pratik yönü nedeniyle yazılım şeklinde dijital imzadan bahsedilmektedir. Nitekim 1997 tarihli eski Alman Elektronik İmza Kanununda donanıma dayanan bir sistem benimsenmişken sonradan 2001 tarihli yeni Elektronik İmza Kanununda , Avrupa Birliği İmza Yönergesine (SigRL) paralel olarak, kart okuyucusuna gerek olmayan, bu nedenle de ucuza mal olan, yazılıma dayalı imza sistemini de caiz kılan bir düzenleme getirilmiş gibi gözükmektedir. (**Şenocak,** sh. 112'den naklen).

[126] **Sözer,** (Sözleşme), sh.127.

[127] **Sözer,** (Sözleşme), sh.123.

göre onu göndermiş olan kişiden gelmiş olduğunun tespitidir[128]. Nasıl imzanın kimden sadır olduğu yani kimin tarafından atıldığının tespiti hususunda zorluk çekmiyorsak aynı kolaylık dijital imzada da sağlanabilmelidir. Bu hususların sağlanması için şifreleme yöntemine başvurulmaktadır. Şifreleme, yetkisi olmayan kişilerin gönderilen verileri elde etmesini, okumasını önleyecektir. Şifreleme anahtar vasıtasıyla yapılır. Anahtar, verilerin işleme tabi tutularak anlaşılmaz hale getirildiği sonrada yine anlaşılabilir hale sokulduğu yani deşifre edildiği algoritmaya dayanan formüldür. Şifreleme için tek bir anahtar kullanılabildiği gibi çift anahtar da kullanılabilmektedir[129].

2. ŞİFRELEME YÖNTEMLERİ

a. GENEL OLARAK

Bir metni dijital olarak imzalamak için bugün farklı yöntemler kullanılmaktadır. Bunlardan günümüzde en yaygını, şifreleme esasına dayanan yöntemlerdir[130].

---

[128] **Sözer,** (Sözleşme), sh.123; Dijital imzalar tek yani birbirinden farklı olmalıdır. İmzaların güvenilirde olması yani elektronik imzayı kullanan olarak kimliği tespit edilen kişinin gerçekten mesajı görüp imzalamış olması gerekir. Mesaj değiştiğinde elektronik imza geçersiz hale gelmelidir. **Pekcanıtez,** sh.396.

[129] **Özgü, M. E.:** İnternette Hukuki Güvenlik Ve Dijital İmza.

[130] **Keser Berber,** (Şekil), sh.84; **Keser Berber** (İmza), sh.519

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 edilmesinde de kullanılmaktadır [131].

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)[132]

Günümüzde kullanılan şifreleme yöntemlerinde farklı matematiksel metotlardan hareket edilmektedir. Çalışmamızda genel kabul görmüş başlıca iki şifreleme yöntemi olan Simetrik ve Asimetrik şifreleme yöntemleri üzerinde durulacaktır.

b. SİMETRİK ŞİFRELEME YÖNTEMİ

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

[131] **Keser Berber**, (Şekil), sh.84-85

[132] **Keser Berber**, (Şekil), sh.85

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[133]. Güvenli olarak şifrenin iletilmesi genel anahtar şifrelemesi yolu ile aşılmaya çalışılmıştır[134].

c. ASİMETRİK ŞİFRELEME YÖNTEMİ

Bu şifreleme yönteminde, haberleşen her bir taraf, biri açık (genel), 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[135] .

---

[133] **Keser Berber**, (Şekil), sh.87; **Keser Berber**, (İmza), sh.521; **Hassler, V./Biely, H.:** Digital Signature Management, Internet Research: Electronic Networking Applications and Policy, Volume 9, Number 4, 1999, sh.262.

[134] **Kırçova /Öztürk,** sh.69

[135] **Keser Berber**, (Şekil), sh.89-90; **Keser Berber**, (İmza), sh.523; **Ersoy, Z.:** Elektronik Ticaret ve Ticaret Noktaları, İGEME, Ekim 1999, sh.51; **Orta, M.:**

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 adlandırılan kurumlar uğraşmaktadır[136].

Asimetrik şifreleme yöntemlerinin güvenilirliği, her şeyden önce gizli şifrenin kullanıcı tarafından iyi saklanmasına ve anahtar uzunluğuna bağlıdır [137].

Asimetrik şifreleme yönteminde deşifre etme süreci, simetrik şifreleme yöntemine göre daha uzun sürmektedir. Özellikle uzun mesajlarda, mesajlar müdahaleye de maruz kalabilmektedirler. Bunun üstesinden gelebilmek amacıyla Rivest tarafından hash fonksiyonu geliştirilmiştir[138]. 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 [139].

Ulusal Yargı Ağı Projesinde Elektronik İmza, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001, sh. 167 vd.; **Kırçova /Öztürk,** sh.69

[136] **Keser Berber**, (Şekil), sh.91

[137] **Keser Berber**, (Şekil), sh.91.

[138] **Kırçova/Öztürk**, sh.70; **Altınışık,** 2003, sh.83,

[139] **Keser Berber**, (Şekil), sh.91

Hash fonksiyonları, dijital imzanın hazırlanması için son derece önemlidir. Hash fonksiyonu matematiksel bir algoritmadır[140]. Asimetrik şifreleme yönteminde birbiri ile haberleşen her bir taraf, biri açık (imza doğrulama verisi) diğeri ise gizli (imza oluşturma verisi) olmak üzere iki şifreye sahiptir. Hazırladığı mesajı imza etmek isteyen kimse, mesajının hash değerini hesaplamak için, bir hash fonksiyonu kullanacaktır. Bu şekilde hash değeri, gizli şifre ile şifrelenmiş olacaktır. Bir belgenin hash değeri belli olduğu için, alıcı bunu mesajı gönderenin açık şifresi yardımıyla tespit edebilir. Alıcı hash fonksiyonunu bu defa deşifre edilen mesaja da uygulayabilir ve her iki değeri birbiri ile karşılaştırabilir. Her iki değer birbirine uyuyorsa, alıcı, bu belgenin göndericinin orijinal belgesi olduğundan ve mesajın sonradan değiştirilmediğinden emin olabilir. Mesaj sonradan değiştirilmiş olsaydı, bu durumda elde edilen hash değerleri birbirinden farklı olacaktı[141]. Çünkü her mesajın farklı bir hash değeri vardır[142].

Değerler aynı ise, aksi ispat edilene kadar şu karineler geçerli olur:

a. Dijital imza mesaja eklendiği andan itibaren mesaj değişmemiştir.
b. Dijital imza gönderene aittir.
c. Dijital imza mesajı imzalamak amacıyla mesaja eklenmiştir.

---

[140]**Prosise, J.:** Dijital Signatures: How They Work? http://www.zdnet.com./ccmag/issues/107/pcm.htm>

[141]**Keser Berber,** (Şekil), sh.92

[142]**Keser Berber**, (Şekil), sh.91 vd., **Keser Berber,** (İmza), sh.524-525; **Kırçova/Öztürk,** sh.70; **Orta,** sh.166

3. DİJİTAL İMZANIN ATILMASI

Dijital imzanın atılmasında kullanılacak anahtar çifti elde edildikten sonra artık dijital imza ile gönderilecek verilerin şifrelenmesi ve sonrasında bu şifrenin çözülmesinin nasıl olacağına değinmek uygun olacaktır. Gizli anahtar ile verilerin tamamının şifrelenmesi halinde gönderilecek mesajın boyutu iki katına kadar artabilmektedir. Algoritma yapısından dolayı böyle bir şifreleme uzun sürede gerçekleşecektir. Aynı şekilde şifrelenmiş mesajın çözülmesi de zaman alacaktır. İşte hiçte pratik olmayan bu işlemi kolaylaştıracak bir yöntem geliştirilmiştir. Buna göre gönderilecek verilerin hash değeri alınır yani bir anlamda özeti çıkarılır. Metnin hash değerinin alınması demek metne hash algoritmasının tatbik edilerek, metni harf ve rakamlardan oluşan bir özet haline getirmek demektir[143]. Ortaya çıkan değer gizli anahtar kullanılarak şifrelenir ve alıcıya gönderilir. Bu yönteme "message digest" yöntemi denilmektedir. Böylece zaman ve bilgi yükünden tasarruf edildiği gibi mesajın alıcıya değişmeden gittiğinin de onaylanması sağlanır. Elde edilen değer, tamamen bilgisayarda seçilen ve işaretlenen metne özgü olup, bu metinde yapılacak bir değişiklik, elde edilen hash değerini değiştirecektir[144]. Çünkü bu yöntemde kullanılan mesajın hash değerinin alınması, mesaj uzunluğu ne olursa olsun 160 veya 128 bit'lik bir çıktı verir ve bu çıktı tamamen o mesaja özgüdür. Mesajdaki 1 bit'lik değişiklik bile message digest sonunda tamamen farklı bir değer çıkmasına neden olur ki alıcı gelen mesajda aynı işlemi yaptığında eğer mesaj değişmişse göndericinin yolladığı değerden farklı bir değer elde edecektir. Alıcının yapacağı işlem kendisine

---

[143] **Şenocak,** sh.100; **Keser Berber,** (İmza), sh.524.

[144] **Şenocak,** sh.100; **Sözer,** (Sözleşme), sh.127.

gelen mesajın hash değerini almaktır. Daha sonra, kendisine daha önceden bildirilmiş olan gönderenin açık anahtarını kullanarak mesajı deşifre edecektir. Böylece orijinal metnin hash değerine ulaşmış olacaktır. Artık iş gönderilen mesajın ilk alınan hash değeri ile açık anahtar kullanıldıktan sonraki hash değerinin birbirini tutup tutmadığına bakmaya kalacaktır. Eğer bu iki değer birbirini tutuyorsa alıcı belgenin hiçbir değişime uğramadan, güvenli bir şekilde kendisine ulaştığına emin olur[145].

B. DİJİTAL İMZA İÇİN GEREKLİ ALT YAPI

1. ZAMAN KAŞESİ

Elektronik ortamda yapılan işlemlerin yapıldıkları zamanın tespiti, işlem güvenliği açısından önemlidir. Elektronik bir belgenin ispat gücünü artırmak için, diğer koşulların yanı sıra belgenin düzenlendiği zamanın şüpheye yer bırakmayacak bir şekilde tespit edilmesi gerekir. Bu yüzden şifreleme ve kimlik teşhis etmenin yanı sıra, zaman kaşesi fonksiyonu da önemli bir role sahiptir[146].

Özellikle dijital imzanın hangi tarihte oluşturulduğu, imzanın doğrulanması ve mesaj bütünlüğünün denetlenebilmesi açısından vazgeçilmez bir unsurdur. Mesajı alan taraf aldığı mesajın geçerli olup olmadığını denetleyebilmek için imzanın atıldığı tarihe ihtiyaç duyar. Eğer kulanım süresi dolmuş ya da kullanımı askıya alınmış, iptal

---

[145] **Şenocak,** sh.100 vd.; **Sözer,** (Sözleşme), sh.128.

[146] **Keser Berber**, (Şekil), sh.94.

edilmiş bir imza sertifikasına dayanıyorsa, bunu onay kurumu aracılıyla öğrenebilir. İmzanın hukuken geçersiz olduğunu ve sahibinin kimliğini doğrulamadığını kolayca anlar[147]. Diğer taraftan, iletişim sürecinde mesaja müdahale yapılmışsa, en son yapılan işlemin tarihi görüneceğinden, bu da anlaşılabilecektir. Bu yüzden onay kurumları, talep üzerine dijital tarihleri zaman kaşesi ile belirtmek zorundadır[148].

Türk Kanun koyucusu 15.01.2004 tarihinde kabul edilen ve 23.01.2004 tarih ve 25355 sayılı RG'de yayınlanan ve 23.07.2004 tarihinde yürürlüğe giren 5070 sayılı EİK'nun "Tanımlar" başlıklı 3. maddesinin h bendi ile zaman damgasını tanımlamıştır. Bu tanımla, bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydın zaman damgası olduğu düzenlenmiştir. Bu düzenleme ile elektronik veriyle ilgili olarak yapılan işlemlerin zamanının doğrulanması amaçlanmıştır[149].

---

[147] **Altınışık,** sh.88'den naklen.

[148] **Keser Berber**, (Şekil), sh.95 , **Keser Berber,** (İmza), sh.526.

[149] Bkz. 5070 sayılı Elektronik İmza Kanununun Madde Gerekçeleri, http://www.basbakanlik.gov.tr./tasarilar/Tasari9.htm

2. ONAY MAKAMI- SERTİFİKA HİZMET SAĞLAYICILARI (TRUSTCENTER- CERTIFICATION AUTHORITIES)

a. KAVRAM

Algoritmaların, anahtarların ve anahtar hazırlama yöntemlerinin güvenilirliği konusunda birçok araştırma yapılmıştır. Ancak bugün ulaşılan matematiksel güvenlik şüphesiz tek başına yeterli değildir. Burada önemli olan şey, açık imza anahtarının kullanıcıya kesin bir şekilde tahsis edilmesidir. Çünkü anahtar hazırlama yöntemleri genel olarak bilindiği için, kötü niyetli bir kişi imza atmakta kullanılacak bir çift imza anahtarı oluşturabilir, açık anahtarı kullanıma açar ve böylece sahte bir kimlik yaratmış olur. Bu yüzden dijital imzada "açık anahtarın" belirli bir kişiye ait olduğunun mutlaka "tamamen güvenilir bir üçüncü kişi (Sertifika Makamı)" tarafından onaylanması gerekir[150].

Simetrik şifreleme yönteminde birbiri ile haberleşen her iki taraf, şifreleme ve deşifre için aynı şifreyi kullanmaktadır. Sadece iki kişi gizli bir bilgiyi paylaşıyorsa, simetrik şifreleme yöntemi herhangi bir sorun yaratmayacaktır. Diğer bir ifade ile, kullanıcı sayısının az olduğu durumlarda bu prensiple yetinmek mümkündür. Ancak kullanıcı sayısı artarsa, özellikle birçok kimseye haberleşmeye katılma imkanı verilirse, hiyerarşik bir alt yapı olmaksızın bunun üstesinden gelinemeyecektir. İşte bu

[150] **Keser Berber**, (Şekil), sh.97.

aşamada onay makamları veya Trustcenter veya Certifikation Authorities olarak adlandırılan kurumlar gündeme gelmektedir [151].

5070 sayılı EİK'nun "Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar" başlıklı ikinci bölümünün "Elektronik Sertifika Hizmet Sağlayıcısı" başlıklı 8. maddesine göre, elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir.

Elektronik Sertifika Hizmet Sağlayıcısı 5070 sayılı Kanunda da belirtildiği üzere kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişiler olabilir[152].

Kanaatimize göre, 5070 sayılı Kanunda mevcut ve önemli diğer bir eksiklik, önüne gelen herkesin sertifika hizmeti sunan kuruluş olarak çalışmasını engelleyecek bir teminat tedbirinin mevcut olmamasıdır. Bu konuda Alman Dijital İmza Kanunu md. 13, faaliyete geçmek için kanunun ve yönetmeliğin aradığı koşulları yerine getiren sertifika hizmet sağlayıcılarının, bunun yanı sıra Dijital İmza Kanununun ve Yönetmeliğin aradığı şartları ihlal etmeleri veya nitelikli elektronik imza veya diğer

---

[151] **Keser Berber**, (Şekil), sh.97; **Hassler, V./Biely, H.:** Digital Signature Management, Internet Research: Electronic Networking Applications and Policy, Volume 9, Number 4, 1999, sh.263; ERSOY, Zeynep: 1999, sh.51.

[152] Örneğin bankalar veya noterler gibi. Ulusal Yargı Ağı Projesinde onay kurumu Adalet Bakanlığıdır. Bkz. **Orta,** sh.167.

teknik güvenlik teçhizatları bakımından ürünlerinin yetersiz olması sebebiyle yol açtıkları zararı tazmin etmek şeklindeki yasal yükümlülüklerini yerine getirebilmek için 250.000 EURO teminat tedbiri göstermeleri gerekmektedir. 5070 sayılı EİK'nda ise, sadece faaliyete geçeceği tarihte dijital imza sertifikası vermek için kanunun aradığı teknik standartları yerine getirmesi yeterli olan, ayrıca akreditasyonları da öngörülmeyen sertifika hizmet sağlayıcılarının, işin daha başında teminat gösterme yükümlülüklerinin olmaması büyük bir eksikliktir.

b. SERTİFİKANIN HAZIRLANMASI

Bir kimsenin dijital imzasının geçerliliği, bu kişinin açık şifresinin bir Trust Center tarafından, dijital bir imza ile tasdik edilmesi suretiyle olur. Bu kapsamda olmak üzere, şifreleri kullanacak olan kişi hakkındaki bilgiler, Trust Center'ın gizli şifresi ile şifrelenecek olan sertifikanın düzenlendiği tarih ve geçerlilik süresi de önem taşımaktadır. Sertifikanın hazırlanması genel olarak şu şekilde gerçekleşir: İmza şifresi sertifikası sahibi olmak isteyen bir kişi, Trust Center'a veya yetkili diğer bir kuruma, kimlik bildiriminde bulunur. Trust Center bunun üzerine, ilgili şahıs tarafından imza için kullanılacak olan bir çift şifre hazırlar, açık şifreyi sertifikalar ve bunu kullanıcının ismi ile birlikte bir " şifre listesinde" yayımlar[153].

Dijital imzalı bir mesajı alan kişi ise, Trust Center'ın şifre listesinden göndericinin açık şifresini bulabilir. Bu şifre ile, dijital imzayı çözer ve yine bu açık şifre yardımıyla metni okunabilir hale getirebilir. Bu açıklamalar bile, bir Trust Center'a

[153] **Keser Berber**, (Şekil), sh.97-98

ne kadar büyük güvenlik ve garanti taleplerinin yöneltildiğini ortaya koymaktadır. Trust Center'ın gizli şifresi hiç bir koşulda kullanıcıdan başka kimseye verilmeyecektir. Hazırlanan her şifrenin, her kullanıcı için ayrı olması; yani her şifre örneğinden sadece bir tane yapılmış olması gerekir[154].

c. SERTİFİKA HİZMET SAĞLAYICININ GÖREVLERİ

Sertifika hizmet sağlayıcının görevi, sertifikayı üretim, dağıtım, yenileme, yeni anahtar üretimi, iptal, geçici iptal gibi bir yaşam döngüsü içerisinde yönetmektir.

Sertifika hizmet sağlayıcılar sıklıkla abonelerin kayıt yetkilerini kendilerinin bir yan kuruluşu olan kayıt tescil kurumlarına devrederler. Bazı durumlarda sertifika hizmet sağlayıcıları kayıt fonksiyonlarını kendileri gerçekleştirirler. Sertifika hizmet sağlayıcılar ayrıca çevrimiçi durumun korunması mekanizmasını ve iptal listeleri yoluyla sertifika durumlarının yansıtılmasından sorumludurlar. Tipik olarak sertifika hizmet sağlayıcısı sayısal sertifikaları ve sertifika iptal listelerini bir dizin halinde yayınlayarak ilgili taraflar için erişilebilir olmasını sağlarlar.

Nitelikli elektronik sertifika için gerekli özellikler AB'nin 1999/93 sayılı Elektronik İmzalar hakkındaki Direktifine uygun olarak 5070 sayılı EİK'nun 9. maddesinde düzenlenmiştir. Buna göre, nitelikli elektronik sertifikada;

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibarenin,

---

[154] **Keser Berber**, (Şekil), sh.98.

b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,

c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,

f) Sertifikanın seri numarasının,

g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,

h) Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgilerinin,

ı)Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin,

j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

bulunması zorunludur.

Elektronik sertifika hizmet sağlayıcısının yükümlülükleri ise 5070 sayılı EİK'nun 9. maddesinde düzenlenmiştir. Buna göre, elektronik sertifika hizmet sağlayıcısı;

a) Hizmetin gerektirdiği nitelikte personel istihdam etmekle,

b) Nitelikli sertifika verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmekle,

c) Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, mesleki veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmi belgelere dayandırarak güvenilir bir biçimde belirlemekle,

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

e) Sertifikanın kullanımına ilişkin özelliklerin ve uyuşmazlıkların çözüm yolları ile ilgili şartların 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,

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

g)Yaptığı hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla,

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

yükümlüdür.

Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz.

V. DİJİTAL İMZA ÇEŞİTLERİ [155]

A. BASİT ELETRONİK İMZA

Basit elektronik imzaya mevcut yasal düzenlemeler çerçevesinde çeşitli sebeplerle ve en önemlisi hukuki işlem güvenliğinin sağlanması bakımından çeşitli şartlar getirilmiştir. Aşağıda basit imza açıklandıktan sonra esasen gelişmiş elektronik imza, güvenli (nitelikli) elektronik imza ve akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilmiş elektronik imza şeklinde yapılan ayırım basit elektronik imza esası üzerinden getirilen ek şartlara göre yapılmış bir ayırımdır.

Bu ayırımın tercih edilmesinin sebebi, gerek Kıta Avrupası'ndaki hukuksal düzenlemelerde, gerekse Türk hukukundaki düzenlemelerde elektronik imzanın çeşidine bakılmaksızın taşıdığı özelliklere göre ayırımlara tabi tutulmuş olmasından kaynaklanmaktadır. Bu tür bir düzenleme tarzı, teknikteki gelişmelerin dikkate alınmasına olanak vermesi bakımından uygun bir tutumdur. Böylece, kanun koyucu, bilimin ve tekniğin, kanunun yapıldığı o günkü durumuyla kendini sınırlamaksızın gelecekteki elektronik imza alanındaki teknolojik gelişmelere de uyarlanabilir bir yol izlemek amacındadır.

Basit elektronik imza ve özellikle basit dijital imza, sadece verinin bütünlüğünün korunduğunu göstermektedir.

---

[155] **Erturgut,** sh.3-5.

Sadece güvenli elektronik imzalar hukuki işlemlerde şekil şartını yerine getirmeye elverişlidir ve yargılamada caiz delil olarak kullanılabilirler. Basit elektronik imzalar bakımından bu sonuca varmak mümkün değildir. Ancak, AB Direktifi md.5'e göre, bir elektronik imzanın,

- sadece elektronik formda olması,
- veya nitelikli bir sertifikaya dayanmaması,
- ya da akredite edilmiş bir sertifika hizmet sağlayıcısı tarafından verilmiş nitelikli bir sertifikaya dayanmaması,
- yahut güvenli bir imza oluşturma aracıyla üretilmemiş olması

gerekçeleriyle hukuki etki doğurmasına veya yargılamada caiz delil olarak kullanılmasına engel olunmaması düzenlenmiştir

Basit elektronik imza başlığı altında bilgisayar ekranına kalemle atılan imza, biyometrik imza, dijital imza ve el yazısıyla imzanın tarayıcıdan geçirilerek elektronik belgelere eklenmesi durumları incelenebilir.

B. GELİŞMİŞ ELEKTRONİK İMZA

Gelişmiş elektronik imza, genel olarak elektronik imza tanımından yola çıkılarak, bu tanıma çeşitli unsurların eklenmesi suretiyle tanımlanmaktadır.

Gelişmiş elektronik imza, verinin bütünlüğünün korunduğunu göstermesi yanında, imzalayanın kimliğinin tespitini de sağlar.

AB Direktifine göre (Art. 2), gelişmiş elektronik imza, sadece imzalayana bağlı olan; imzalayanın kimliğini belirlemeye imkan veren; sadece imzalayanın kontrolü altında tutabileceği araçlarla yaratılan ve verilerde sonradan yapılacak değişikliklerin bilinmesini sağlayan elektronik imza olarak tanımlanmıştır.

Buna karşılık, Türk hukukunda gelişmiş elektronik imza tanımına yer verilmemiştir. Ancak gelişmiş elektronik imzanın unsurları, güvenli elektronik imza tanımındaki unsurlarda yer almaktadır (EİK m.4).

C. GÜVENLİ ELEKTRONİK İMZA

AB Direktifinde, güvenli (nitelikli) elektronik imza tanımı yapılmamış, bunun yerine, üye ülkelerin el yazısı ile imzaya eşdeğer kabul edecekleri ve yargılamada delil olarak kullanılmasını temin edecekleri imzanın unsurları bakımından güvenli elektronik imza kabul edilmiştir. Bunun için gerekli şartlar, gelişmiş elektronik imzanın unsurlarını taşıyan bir elektronik imzanın, nitelikli elektronik sertifikaya dayanması ve güvenli imza oluşturma araçları ile oluşturulmuş olmasıdır. Bu unsurların varlığı halinde üye ülkeler bu imzanın el yazısı ile imzaya eşdeğerliğini ve yargılamada delil olarak kullanılmasını sağlayacaklardır (Art. 5).

Türk hukukunda, "nitelikli elektronik imza" kavramı yerine "güvenli elektronik imza" kavramı tercih edilmiştir. Buna göre güvenli elektronik imzada bulunması gereken özellikler şunlardır:

- Münhasıran imza sahibine bağlı olmalı,
- Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulmuş olmalı,
- Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamalı,
- İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlamalıdır.

AB 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, AB Direktifinde belirtildiği üzere el yazısıyla imzaya eşdeğer sayılacak ve yargılamada caiz delil olarak kullanılacaktır. Hukukumuz açısından bu hususların gerçekleştiği söylenmelidir. Zira EİK'nda, güvenli elektronik imza, el yazısıyla imzaya eşdeğer kabul edilmiş (md.22) ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir (md.23).

D. AKREDİTE EDİLMİŞ SERTİFİKA HİZMET SAĞLAYICISI TARAFINDAN VERİLEN İMZA

Hukukumuzda sertifika hizmet sağlayıcıları bakımından akreditasyon sistemi kabul edilmemiştir. Buna karşılık, AB Direktifinde ihtiyari akreditasyona yer verilmiştir. İhtiyari akreditasyon, bir sertifika hizmet sağlayıcısı işletmesi için özel hak ve yükümlülüklere bağlı olarak izin verilme usulüdür. Sertifika hizmet sağlayıcısı, yetkili makama başvurarak akredite edilmek isteyebilir. Bu durumda EİK'nda yer alan ve EİK'na dayanarak çıkartılmış olan Yönetmelikteki şartları taşıdığını ispat etmelidir. Bu halde yetkili makam, ilgili sertifika hizmet sağlayıcısının akreditasyonunu sağlar. Akredite edilmiş sertifika hizmet sağlayıcısı, yetkili makamdan bir işaret alır ve bu işaretle sertifika hizmet sağlayıcısının nitelikli sertifikaya dayanan nitelikli elektronik imzası için kapsamlı teknik ve yönetsel güvenlik araştırması yapıldığı konusunda bir ispat sağlanır.

Akredite edilmiş sertifika hizmet sağlayıcıları tarafından verilmiş nitelikli sertifikaya dayanan nitelikli elektronik imzaların, hukuki işlemin şekli veya belgelerin ispat gücü bakımından nitelikli elektronik imzalara nazaran bir faklılığı bulunmamaktadır. Çünkü kanunda hukuki işlemler açısından şekil ve elektronik imzalı belgelerin delil olarak kullanılmasına ilişkin düzenlemelerde akredite edilmiş sertifika hizmet sağlayıcılarından bahsedilmemektedir.

VI. DİJİTAL İMZANIN AMACI VE İŞLEVİ

A. DİJİTAL İMZANIN AMACI

E-imzanın amacı, e-ticaretin gelişmesi ve yaygınlaşmasını teminen, elektronik ortamda (ticari) sözleşmesel ilişkiye giren tarafların karşılıklı olarak güvenliklerini sağlamaktır. Elektronik ortamda ticari ilişkiye giren taraflarca duyulan güven ihtiyacı, elektronik olarak gönderilen verinin alıcısının, verinin kaynağını, verinin bütünlüğünü ve doğruluğunu kontrol etmesine olanak sağlayan e-imza ile karşılanmaktadır[156].

E-imzanın amacının ve işlevinin belirlenmesinde ve hatta e-imza düzenlemelerine ilişkin politikaların belirlenmesinde, o hukuk sisteminde elle atılan imzanın işlevinin ne olduğu büyük önem taşımaktadır. Zira birçok ulusal düzenlemelerde, elle atılan imzanın tanımındaki farklar, e-imza düzenlemelerinde ifadesini bulmaktadır. Bu çerçevede, öncelikle kağıda dayanan geleneksel hukuk sisteminde şekle ilişkin düzenlemelerin bir unsuru olan elle atılan imzanın işlevi, daha sonra e-imzanın işlevleri incelenecektir[157].

---

[156] **Acır,** sh.23.

[157] **Acır,** sh.23.

B. KAĞIDA DAYANAN GELENEKSEL SİSTEMDE ELLE ATILAN İMZANIN İŞLEVLERİ

İmza, Türk Hukuk Sisteminde, gerek Borçlar Kanunu'nda (BK md. 14 vd.) düzenlenen geçerlik şartı olan şeklin, gerek Hukuk Usulü Muhakemeleri Kanunu'nda (HUMK. md. 288) düzenlenen ispat şartı olan şeklin önemli bir parçasını teşkil etmektedir.

1. İMZA SAHİBİNİN KİMLİĞİNİ GÖSTERME (KİMLİK TESPİTİ) İŞLEVİ

Hukuki bir fiil olan iradenin ifadesi, imzalayanın hukuki durumunda bir değişiklik meydana getirilmesi amaçlanır. Sözü edilen fiilin (iradenin) varlığının ve failin (kimliğinin) onayı prosedürüne kimlik tespiti denir. Bu prosedür, kağıda dayanan sistemde imza ile gerçekleştirilir. Zira bir kimsenin kendi karakteristik yazısı ile adını bir belgenin altına koyması, o kimsenin bu suretle imzaladığı belgenin içeriğini kabul ettiğini gösterir. İmza, kişinin kimliğini tespit etmeye yarayan bir işarettir[158].

---

[158] **Tunçomağ, K.:** Türk Borçlar Hukuku, C.I, Genel Hükümler, İstanbul 1976, sh.222; **Eren,** (1991), sh.326; **Altaş, H.:** Şekle Aykırılığın Olumsuz Sonuçlarının Düzeltilmesi, Ankara 1998, sh.74 vd.; **Keser Berber,** (Şekil), sh.127; **Keser Berber,** (İmza), sh.517.

2. TARAFLARI İMZALADIKLARI SÖZLEŞME İLE BAĞLAYICI BİR MUAMELEYE GİRİŞTİKLERİ KONUSUNDA UYARMA İŞLEVİ

İmza sahibi, imzaladığı belgenin içeriği ile bağlanma isteğini ortaya koyar. İmza, aynı zamanda, belgeye (ve içinde yer alan iradeye) son şeklinin verildiğini teyidi ve uyarısı anlamındadır[159]. İmza sayesinde beyanda bulunan kişi, imzalanan beyanın hukuki bağlayıcılığını ve sonuçlarını hesaba katmak zorundadır. Böylece kişiler, hukuki işlemler bakımından aceleci davranmaktan, düşüncesizce hareket etmekten korunmuş olacaklardır[160].

3. İMZALANAN METİNDEKİ İRADENİN, İMZALAYANIN GERÇEK, NİHAİ VE KESİN İRADESİ OLDUĞUNU GÖSTERME İŞLEVİ (ONAYLAMA İŞLEVİ)

İmza, bir belgedeki beyan ve yüklenimlerin sağlıklı olduğunu göstermek için o belgenin altına o kişinin (imzalayan), adı için kullandığı, olağan biçimde koyduğu yazıdır[161]. İmza ile, imzalayan kimse iradesini kesin olarak açıklamış olur[162].

---

[159] **Acır,** sh.24.

[160] **Keser Berber,** (Şekil), sh.127-128

[161] **Yılmaz, E.:** Hukuk Sözlüğü, Genişletilmiş Beşinci Bası, Ankara 1996, sh. 384.

[162] **Tunçomağ,** sh.222; **Eren,** (1991), sh.326; **Altaş,** sh. 64-67; **Keser Berber,** (Şekil), sh.127.

4. İSPATTA GÜVENLİK VE KOLAYLIK SAĞLAMA İŞLEVİ (İSPAT İŞLEVİ)

İmzanın el yazısıyla olmasından amaç, imzalayanın, imzayı şahsen ve bizzat atmasıdır[163]. Zira senet ve tek tarafa borç yükleyen sözleşmeler bakımından borç altına giren tarafın, iki tarafa borç yükleyen sözleşmeler bakımından sözleşmenin her iki tarafının, sözleşmede veya senette bulunan imzanın kendisine ait olmadığı şeklindeki iddiası, HUMK md. 308 ve devamı hükümlerinde düzenlenen usullerle araştırılabilmektedir. Bu husus imzanın ispat işlevine işaret etmektedir[164].

C. DİJİTAL İMZANIN İŞLEVLERİ

1. SONUÇLANDIRMA İŞLEVİ (METNİN TAMAMLANMASI)

Öncelikle elektronik ortamda hazırlanan metnin tümünün gizli imza anahtarı ile imzalanacak olan bir hash değerinin oluşturulması gerektiği için, dijital imzalama süreci belgenin tümüne ilişkindir. Bu şekilde hazırlanan belgeye ilişkin olan imza, ancak metnin hazırlanmasından sonra oluşturulabilecektir. İmzalanan metin ve imza arasındaki bu mantıki bağlantı, sonuçlandırma işlevini yerine getirmektedir[165].

---

[163] **Eren,** (1991), sh. 339.

[164] **Acır,** sh.24-25.

[165] **Keser Berber,** (Şekil), sh.128; **Şenocak,** sh.126.

2. KİMLİĞİ TESPİT ETME İŞLEVİ

Elektronik şekil, belgeyi düzenleyen kişinin belgeye ismini eklemesini öngörmektedir. Ancak beyan sahibinin kimliğinin tespit edilmesi doğrudan doğruya, doğal ve taklit edilemez el yazısı ile atılan bir imza vasıtasıyla yapılamayacaktır. Dijital imzada kimlik tespit etme işlevi, belirli makamlar (onay makamları) tarafından belirli bir gerçek kişiye bir defa olmak üzere koordine edilen imza anahtarlarının, yine bu makamlar tarafından kontrol edilmesi ile yerine getirilmektedir. Bu koordinasyon bir imza anahtarı sertifikası ile yapılmaktadır. Anahtar sahibinin açık anahtarını bilen alıcı, herkes tarafından ulaşılabilen imza anahtarı sertifikasının kontrolü sayesinde, tanzim eden kişinin kimliği hakkında bilgi sahibi olabilecektir. İmza sertifikasının üçüncü kişilerin eline geçmesi ve şifrenin çözülmesi ihtimali, biyometrik kökenli kimlik belirleyicilerin kullanılması ve diğer teknik önlemlerin alınmasıyla ortadan kalkacaktır[166].

3. GERÇEKLİK İŞLEVİ

Metin ve imza arasındaki matematiksel-mantıki bağlantı nedeniyle, beyan ve imzalama arasında da sıkı bir bağlantı ortaya çıkmaktadır. Bu suretle beyanın içerik olarak imzalayan tarafından hazırlandığı ve sonradan değiştirilmediği garanti edilmiş olacaktır. İşte metnin imzalayan tarafından görüldüğü ve kabul edildiği, dolayısıyla

[166] **Keser Berber,** (Şekil), sh.128; **Şenocak,** sh.126.

imzanın beyan sahibine ait olduğu, dijital imzanın gerçeklik işlevi olarak ifade edilir[167].

4. UYARI İŞLEVİ

Doktrinde dijital imzanın uyarı işlevini yerine getirmediği iddia edilmekteyse de[168], bizim de katıldığımız görüşe göre, geçerli bir dijital imza kullanımı için geçen zaman ve imzalama prosedürü dikkate alındığında, dijital imzanın uyarı işlevini yerine getirdiğini söylemek mümkündür[169].

Dijital imzalama prosedürüne bakıldığında, imza atacak olan kişinin öncelikle ilgili metni bilgisayarda hazırlaması gerekmektedir. Daha sonra chip kartını kart okuyucuya takması ve PIN kodunu girmesi veya yazılım programının kullanılması gündeme gelir. Sadece bu prosedür bile, işin ne kadar bağlayıcı olduğu konusunda imza atacak olan kişinin dikkatini çekmektedir[170].

Bundan başka, 5070 sayılı EİK'nun "Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri" başlıklı 10. maddesi, elektronik sertifika hizmet sağlayıcısının, güvenli elektronik imzanın elle atılan imza ile eşdeğer olduğu hakkında sertifika

---

[167] **Keser Berber,** (Şekil), sh.128; **Şenocak,** sh.126.

[168] **Şenocak,** sh.127, dp.92.

[169] **Keser Berber,** (Şekil), sh.131; **Altınışık,** sh. 93.

[170] **Keser Berber,** (Şekil), sh.131; **Altınışık,** sh. 93.

talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirme yani uyarma ile yükümlü tutmuştur.

5. DEVAMLILIK (KALICILIK İŞLEVİ)

Elektronik olarak imzalanan bir belge de, kaydedilmek suretiyle, bu elektronik metnin istenildiği zaman okunabilmesini ve kontrol edilebilmesini mümkün kılmaktadır[171].

6. İSPAT İŞLEVİ

Yasanın aradığı özellikleri taşıyan bir dijital imza, bu imza ile imzalanan elektronik belgeye önemli bir delil değeri vermektedir.

DTM, ETKK tarafından hazırlanan "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanun Tasarısı Taslağı"nın 39. maddesinde, elektronik imzayla imzalanmış belgelerin delil değeri şu şekilde düzenlenmek istenmiştir:

Kanunda aksine bir hüküm bulunmadığı takdirde;

a) Elektronik belge, HUMK m.292 f.II kapsamında yazılı delil başlangıcı,

b) Nitelikli sertifikaya dayanan elektronik belge adi senet,

---

[171] **Keser Berber,** (Şekil), sh.128; **Şenocak,** sh.128.

c) Nitelikli sertifikaya dayanan ve nitelikli zaman damgası bulunan elektronik belge, tarihi açısından, HUMK. md. 299 f.II kapsamında üçüncü kişileri bağlayan adi senet hükmündedir.

5070 sayılı EİK ise, güvenli e-imzanın hukuki sonucu ve uygulama alanını, bir yandan doğrudan. md.5 ile öte yandan ise md.20 ve md.21'de yapılan değişikliklerle BK md. 14 ve HUMK md. 295/A maddeleriyle düzenlemeye yönelmiştir. Dijital imzalı belgelerin Türk İspat Hukuku bakımından delil değeri dördüncü bölümde incelenecektir.

VII. DİJİTAL İMZALI BELGELERDE ŞEKİL SORUNU

A. SÖZLEŞMELERİN ŞEKLİ

1. ŞEKİL KAVRAMI

İrade beyanları değişik şekillerde dışa yansır. Bu yansıma, yazılı, sözlü veya davranışla olabilir. İrade beyanlarının hukuki bir anlam ifade edebilmesi için mutlaka belli bir kalıpla dış dünyaya açıklanması gerekir. Bu anlamda olmak üzere, her irade beyanının bir kalıbı vardır. İşte, iradeyi açıklamak için kullanılan bu kalıba veya vasıtaya şekil denir[172].

[172] **Oğuzman/Öz,** sh. 115; **Altaş,** sh.60 vd.; **Tuğ, A.:** Türk Özel Hukukunda Şekil, Konya, 1994, sh. 3; **Eren,** (1998), sh.243.

Hukuk sistemleri için iradenin açıklanmasında belirli bir şekle uyma zorunluluğu; tarafların sözleşmenin kapsamını kolaylıkla tayin etmeleri, tarafları dikkatli harekete sevk etme ve nihayet hukuki ilişkinin ispatı yönlerinden önem taşımakta ve tarafların nasıl bir hukuki yükümlülük altına girdiklerini hesaba katmaları bakımından yararlı olmaktadır. Ancak bir hukuk düzenindeki bütün hukuki işlemlerin şekle bağlı olması (özellikle geçerlilik şartına), hukuk hayatında büyük güçlükler yaratacaktır. Sözleşmedeki önemsiz şekil noksanları sebebiyle işlemin hükümsüz olması çeşitli sakıncalar ortaya çıkaracak ve kötü niyetli kimselerin şekil noksanına bağlı geçersizlikten haksız ölçülerde yararlanmalarına sebep olacaktır. Modern hukuk sistemleri, bu ve benzeri sakıncalar sebebiyle kural olarak "şekil serbestisi" ilkesini, istisnai olarak da belli hukuki işlemler için şekil zorunluluğunu kabul etmişlerdir[173]

Ancak hukuk düzenlerinin iradenin açıklanmasında belli bir şekle uyma zorunluluğu ilkesine bağladıkları hukuki sonuçlar da her zaman aynı değildir. Bazen hukuki işlemin geçerli olması için belli bir şekle uyulması gerekmektedir. Bu şekle uyulmadıkça sözleşme geçerli olmayacaktır. Burada artık şekil, o hukuki işlem bakımından bir "geçerlilik (sıhhat) şartı"dır. Buna karşılık bazen bir sözleşmenin geçerli olarak meydana gelmesi için herhangi bir şekle uyulması zorunluluğu yoktur. Fakat, sözleşmeden herhangi bir uyuşmazlık doğarsa, işlemin ispat edilebilmesi ancak belli bir şekilde yapılmış olması şartına bağlıdır. Bu durumda ise şekil bir "ispat şartı"dır ve medeni usul hukuku kuralıdır[174].

---

[173] **Reisoğlu, S.:** Borçlar Hukuku Genel Hükümler, 14. Bs., İstanbul, 2000, sh.60-61.

[174] **Keser Berber,** (Şekil), sh.55-56.

2. GEÇERLİLİK ŞARTI OLARAK ŞEKİL

BK md.11 f. I, Türk Sözleşmeler Hukuku bakımından kural olarak "şekil serbestisi" ilkesini benimsemiştir[175]. Bu hükme göre, "Sözleşmenin sıhhati, kanunda açıklık olmadıkça hiçbir şekle bağlı değildir".

O halde kanunun açıkça bir şekli öngörmediği hallerde, taraflar iradelerini sözlü olarak açıklayabilirler ve sözleşme karşılıklı ve birbirine uygun irade beyanlarının varlığı halinde geçerli olarak meydana gelir[176].

Ancak kanun, bir sözleşmenin belirli bir şekilde yapılacağını öngörmüşse, kanunun emrettiği şekil kural olarak "sıhhat şartı" dır. BK md. 11/f. 2'ye göre, "Kanunun emrettiği şeklin kapsam ve etkisi hakkında başkaca hüküm yoksa, sözleşme bu şekle uyulmadıkça geçerli olmaz".

Bu hükme göre; aksine bir hüküm mevcut değilse, kanunun emrettiği şekilde yapılmayan sözleşmeler geçersizdir.

Kanunun şekil zorunluluğuna ilişkin kuralları emredici nitelikte olduğu için, taraflar aralarında yapacakları anlaşma ile bu kuralları bertaraf edemeyeceklerdir. Sözleşmenin şekil noksanlığı nedeniyle geçerli olmadığını hakim re'sen dikkate

---

[175] **Kılıçoğlu,** sh.73.

[176] **Keser Berber,** (Şekil), sh. 56.

alabileceği gibi, taraflar da yasal şekle uyulmadığı için sözleşmenin geçerli olmadığını ileri sürmek hakkına sahiptir[177].

3. YAZILI ŞEKİL

Kanun, bazı sözleşmelerin geçerli olmasını yazılı şekilde yapılmış olmasına bağlamış ve BK md. 12 vd. hükümlerinde yazılı şekli düzenlemiştir. Örneğin; BK'ya göre, alacağın temliki (BK.md. 163), bağışlama vaadi (gayrımenkuller dışındaki) (BK. md. 238), kefalet sözleşmesi (BK. md. 484) gibi sözleşmelerin yazılı şekilde yapılması gerekir[178].

Yazılı şekle bağlı sözleşmelerde, sözleşmenin metni el yazısı ile, daktilo veya bilgisayar ile yazılmış olabilir. Metnin sözleşmenin bütün esaslı noktalarını kapsaması gerekir.

Yazılı şekle bağlı sözleşmelerde, borç altına giren tarafın veya tarafların metni imzalaması gerekir (BK. md. 13/f.1). İmzalanan metnin karşı tarafa verilmesi veya gönderilmesi, yani karşı tarafa ulaştırılması gerekir. Ulaşması gereken bir yazılı beyan ancak karşı tarafa ulaştıktan sonra hükümlerini doğurur.

İmza, borç altına giren kimsenin el yazısı ile atılmalıdır (BK. md. 14/f. 1). İmzada isim ve soyadının belirli bir şekilde atılmasına gerek yoktur. İmzanın borç altına

---

[177] **Reisoğlu,** sh. 62-64; **Keser Berber**, (Şekil), sh.56-57.

[178] **Kılıçoğlu,** sh.75.

giren tarafın metni benimsediğini gösterir ve imza sahibini tespite imkan verir bir nitelik taşıması yeterlidir. Bir alet aracılığı ile atılan imza (örneğin mühür ile) BK md. 14/f.2 gereğince, ancak örf ve adetçe kabul edilen hallerde ve özellikle çok sayıda kıymetli evrakın imzalanmasında geçerli sayılır.

İmza, bütün metnin benimsendiğini (kabul edildiğini) gösterir şekilde metnin altına atılmalıdır. Metnin üstüne veya yanına atılmış imzalar yetersizdir. Metinde yapılan ilave ve çıkıntılar ayrıca imza edilmelidir. Metin birden çok sayfadan oluşuyorsa, her sayfanın imzalanması, olası anlaşmazlıkları önleme bakımından yararlıdır.

4. RESMİ ŞEKİL

Türk Hukukunda bazı sözleşmelerin geçerliliği resmi şekilde yapılmış olmalarına bağlanmıştır. Buradaki resmi şekilden maksat, işlemin yetkili bir makam veya şahıs (noter, tapu memuru, sulh hakimi gibi) önünde, kanunların öngördüğü usul ve koşullara uygun olarak yapılmasıdır. Örneğin; gayrımenkul alım satımı, gayrımenkul satış vaadi, vefa ve iştira sözleşmelerinin resmi şekilde yapılması gerekir. Kanun koyucu, resmi şekli emrettiği bazı hallerde yetkili makamı da göstermiştir. Bu konuda özel bir hüküm yoksa, noterler kanunlarda resmi şekilde yapılması öngörülüp de görevlisi gösterilmemiş olan bütün sözleşmeleri düzenlemeye yetkilidir (Noterlik Kanunu md. 60). Resmi şekle bağlanmış bir sözleşmeye ilişkin değişikliklerin de resmi şekilde yapılması gerekir[179].

---

[179] **Keser Berber**, (Şekil), sh.59; **Kılıçoğlu,** sh.75.

B. DİJİTAL İMZANIN EL YAZISI İLE İMZANIN YERİNİ TUTMAMASI

5070 sayılı EİK md.3'te, elektronik imza, "Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"(md.3/b); aynı maddede imza sahibi, "Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi" (m.3/c), imza 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"(m.3/d), imza oluşturma aracı, "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı"(md.3/e) şeklinde tanımlanmıştır.

5070 sayılı EİK md.5/1, elektronik imzanın el ile atılan imza ile aynı hukuksal sonuçları doğurduğunu ifade etmiştir.

Bu Kanunun kapsamına ancak adi yazılı geçerlilik şekline bağlı olan hukuksal işlemler girebilir. Adi yazılı şeklin kanundan ya da anlaşmadan kaynaklanması önem taşımaz. Örneğin, alacağın temliki BK. md. 163 gereğince kanun tarafından adi yazılı şekle bağlanmış bir sözleşmedir. Kira sözleşmesi ise yazılı geçerlilik koşuluna bağlanmamıştır. Ancak taraflar kira sözleşmesinin yazılı şekilde yapılmasını kararlaştırmışlarsa, sözleşme yazılı şekilde yapılmadıkça geçerli olmayacaktır[180].

[180] **Kılıçoğlu,** sh.83.

5070 sayılı EİK resmi yazılı geçerlilik koşuluna bağlanmış hukuksal işlemler için uygulama alanı bulamaz. Nitekim, Kanunun 5. maddesinin 2. fıkrasında, "Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez." hükmüyle bunu ortaya koymuştur. Maddede "kanunların resmi şekle" bağlı tuttuğu ifadesi kullanılmasına rağmen, bu ifadeyi sadece kanunla resmi şekle bağlanmış sözleşmelerle sınırlı tutmamak, tarafların anlaşma ile resmi yazılı geçerlilik koşuluna bağladığı sözleşmelerin de buraya girdiğini kabul etmek gerekir. Örneğin, finansal kiralama sözleşmesi, 3226 sayılı Kanun md. 8 ile noterde resmi yazılı yapılması koşuluna bağlanmıştır. Bu sözleşmenin elektronik imza yoluyla kurulması olanaklı değildir. Buna karşılık bir işhanının kiralanması sözleşmesi Kanunda herhangi bir yazılı geçerlilik koşuluna bağlı olmadığı halde, taraflar bu sözleşmenin noterde resmi şekilde yapılması konusunda anlaşmış iseler, elektronik imza yoluyla kurulamaz[181].

EİK sadece resmi yazılı geçerlilik koşuluna bağlı sözleşmelerin değil, "teminat sözleşmeleri"nin de elektronik imza yoluyla kurulamayacağını kabul etmiştir. Bu hüküm taşınır rehni bakımından önem taşımaktadır. Zira taşınmaz rehni TMK, md.856 gereğince kanunen resmi şekle bağlı bir sözleşme olduğundan zaten bu Kanun kapsamına girmez. Taşınır rehni ile ilgili TMK. md.939 hükmü bir şekil koşulu öngörmediği halde, 5070 sayılı EİK'nun bu hükmü karşısında, buna ilişkin bir sözleşme elektronik imza yoluyla kurulamayacaktır[182].

---

[181] **Kılıçoğlu,** sh.83.

[182] **Kılıçoğlu,** sh.83.

5070 sayılı EİK 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? Kanunun md. 5/f.2 hükmünün lafzından çıkan sonuç bu işlemlerde elektronik imzanın mutlak olarak kullanılamayacağıdır. Oysa ABD'deki Eyaletlerarası veya Dış Ticarette Elektronik Kayıtların ve İmzaların Kullanılmasını Kolaylaştıracak Kanun Bölüm 103'de, dijital imzanın şimdilik kullanılamayacağı alanlar belirlenmiş; fakat 103c hükmünde ise Ticaret Bakanının üç yıllık süre içinde, bu yasaklamanın tüketicilerin korunması için gerekli olmaya devam edip etmediğini kontrol edeceği kabul edilerek, söz konusu yasaklamanın mutlak olmadığının altı çizilmiştir. Dolayısıyla ABD'de kanun koyucu bugünkü teknolojik olanaklar karşısında dijital imzanın kullanılamayacağı alanları tespit etmiş; ancak söz konusu işlemler bakımından 5070 sayılı EİK'nun aksine mutlak bir yasaklama getirmemiş, bilakis dijital imzanın bu gibi işlemler için 3 yıl kullanılamayacağını, ancak üç yıl sonra durum ve teknolojik koşullar yeniden değerlendirilerek ona göre hareket edileceğini hükme bağlamıştır.

§8. HUKUKİ SORUMLULUK

1. SERTİFİKA HİZMET SAĞLAYICILARININ- ONAY KURUMLARININ SORUMLULUĞU

A. GENEL OLARAK

Onay kurumları hakkında yapılması gereken en önemli şey, bu kurumların sorumluluklarının sınırının tespit edilmesi ve bu kurumların hizmetlerindeki aksaklıkların riskini kimin taşıyacağıdır. Örneğin, sahte bir kimlik belgesine dayanılarak sertifika alınmış olabilir ve üçüncü bir kişi bu sertifikaya güvenerek sözleşme yapmış ve edimini yerine getirmiş olabilir. Sertifikaya güvenen kişinin, adına haberi olmaksızın imza anahtarı hazırlanan ve sertifika düzenlenen kişiye (görünüşte imza sahibine) zararını tazmin ettirmesi mümkün değildir. Bu sahte sertifikayı düzenlettiren kişinin tespit de edilememesi halinde, sertifikaya güvenen üçüncü kişi zarara kendisi mi katlanacaktır? Yine, sertifikanın yanlış yere iptal edilmesinden veya imza anahtarı sahibinin bu hususta bildirimine rağmen iptal edilmemesinden doğan zararı kim taşıyacaktır[183]? Bu noktada sertifika hizmetleri sağlayıcısının sorumluluğu önem kazanmaktadır.

---

[183] Örnekler için bkz. Botschhaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, Art. 16, Nr.2.1.7.1. **(Şenocak, Z.:** Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından İncelenmesi, AÜHFD, C.50, S.2, 2001, sh.133'ten naklen)

UNCITRAL E-Ticaret Çalışma Grubu tarafından oluşturulan E-İmza Yeknesak Kurallar Taslağının (Draft Uniform Rules on Electronic Signatures) 10. maddesinde, AB'nin 1999/93 sayılı Elektronik İmzalar hakkındaki Direktifinin 6. maddesinin 1. fıkrasında onay hizmetleri sağlayanların sorumluluklarının düzenlenmiş olduğunu görmekteyiz.

B. KARŞILAŞTIRMALI HUKUKTA SERTİFİKA HİZMET SAĞLAYICILARININ SORUMLULUĞUNA ATFEDİLEN DEĞER

1. UNCITRAL E-İMZA YEKNESAK KURALLAR TASLAĞI (DRAFT UNİFORM RULES ON ELECTRONIC SIGNATURES)

UNCITRAL E-Ticaret Çalışma Grubu tarafından oluşturulan E-İmza Yeknesak Kurallar Taslağının (Draft Uniform Rules on Electronic Signatures) 10. maddesine göre, onay kurumları, beyanlarına uygun davranma, sertifikaların geçerlik süresi ve içeriğine ilişkin olarak doğru ve tam beyanda bulunma hususunda makul bir dikkat göstermelidir. Buna ek olarak, bu kurumlar, imzaya güvenen tarafça; onay hizmetleri sağlayıcının kimliği, sertifikada tanımlanan kimsenin, ilgili zamanda, sertifikanın dayandığı imza aracını elinde tuttuğu, imza aracı sahibini tanımlamakta kullanılan yöntem, imza aracını kullanılmasında mevcut olabilecek amaç ve miktar sınırlamaları, imza aracının geçerli olup olamadığı veya tehlike altında bulunup bulunmadığı hususlarının doğruluğunu araştırılmasında imkan verecek araçlar temin etmekle yükümlüdürler. Bu yükümlülüklerini yerine getirmede başarısız olan (ihmali bulunan) sertifika hizmet sağlayıcı kurumlar sorumlu tutulurlar. Maddede, zararın

tespitinde, sertifikayı elde etme bedeli, sertifikaya bağlanan bilginin özelliği, sertifikanın kullanma amacına yönelik olarak herhangi bir sınırlama olup olmadığı, varsa miktarı ve sertifika hizmet sağlayıcıların sorumluluk alanını veya miktarını sınırlandıran bir kaydın olup olmadığı vs. hususların da dikkate alınması gerektiği öngörülmüştür.

Sertifika hizmet sağlayıcıları, imza aracı sahipleri için, imza aracının tehlikeye düşmüş olduğunu bildirmeye ve zamanında iptal hizmeti işlemini sağlamaya yarayan araçlar temin etme ve hizmetlerini yerine getirirken, güvenilir sistemler, usuller ve personelden yararlanmakla yükümlüdürler. Maddede anılan kurumlarda kullanılan sistem, usul ve personelin güvenilirliğinin tespitinde gözönünde tutulacak hususlar belirlenmiştir.

2. 1999/93 SAYILI VE 13 ARALIK 1999 TARİHLİ ELEKTRONİK İMZANIN MÜŞTEREK ÇERÇEVE ŞARTLARININ BELİRLENMESİ HAKKINDA AVRUPA BİRLİĞİ YÖNERGESİ

AB'nin 1999/93 sayılı Elektronik İmzalar hakkındaki Direktifinin 6. maddesine göre, onay kurumunun verdiği hizmetlere ve garanti ettiği bilgilere iyi niyetle güvenen üçüncü kişilerin uğradıkları zararlardan onay kurumları sorumludurlar.

a. Dijital sertifikadaki ayrıntıların ve bilgilerin sertifikanın verilme tarihinde doğru olması,

b. Sertifikanın veriliş tarihinde, imzacının imza doğrulama verisine karşılık gelen imza atma verisine sahip olması,
c. Onay kurumunun her ikisini de ürettiği durumlarda, imza atma verisiyle imza doğrulama verisinin birbirlerini tamamlayıcı olarak kullanılma garantisi

ile ilgili olarak onay kurumları ihmalkar davrandığını ispatlayamazsa, doğan zarardan sorumludur. Burada ispat yükünün ters çevrilmiş olduğu görülmektedir. Zaman kaşesindeki tarihin doğru olmamasından dolayı doğan zararlardan da onay kurumları sorumludur. Ancak üçüncü taraf (kişi) verinin doğru olmadığını biliyor veya bilmesi gerekiyorsa tazminat ödemesi gerekmez[184].

3. 16 MAYIS 2001 TARİHLİ ALMAN ELEKTRONİK İMZA KANUNU

Kanun'un 11. paragrafında sertifika hizmet sağlayıcılarının nitelikli bir sertifikaya, nitelikli bir zaman kaşesine ya da sertifika listesi hizmetleriyle vermiş olduğu bilgilere güvenen üçüncü kişilere karşı sorumluluğu düzenlenmiştir. Sertifika hizmet sağlayıcıları söz konusu sorumluluktan kusursuzluklarını ispat ederek kurtulabilirler (§ 11/fk.2). AB Elektronik İmza Yönergesi bu konuda bir uyarlama zorunluluğu öngörmediği halde, sertifika hizmet sağlayıcılarının, bu Kanun ve Tüzük'e göre yükümlü oldukları ödevlerin yerine getirilmesinde kullandıkları yardımcı kişilerin davranışlarından dolayı sorumluluktan kurtuluş kanıtı getirme imkanı tanınmamıştır. Ancak bu düzenleme, sadece belirli şahıslara münhasırdır (§ 11/fk.4). Bu kişiler, sertifika hizmet sağlayıcılarının, § 4 fk.5'e göre ödevlerini devrettiği kişiler ile § 23

[184] **Altınışık,** sh.88-89.

fk.1 Nr.2'ye göre kefil olduğu sertifikaları düzenleyen AB'ne üye olmayan üçüncü bir ülkede yerleşik sertifika hizmet sağlayıcılarıdır. Diğer yardımcı kişiler için ise, sertifika hizmet sağlayıcıları, BGB § 831 çerçevesinde, "yardımcı kişilerin seçiminde, denetlenmesinde ve gerekli araçları temin etmede gerekli özeni gösterdiğini veya böyle bir özeni göstermiş olsaydı bile zararın ortaya çıkacağını" ispatla sorumluluktan kurtulabilmektedir[185].

EİK'nda sertifika hizmet sağlayıcısının, imza anahtarı sahibine karşı aralarındaki sözleşmeden doğan sorumluluğu bilinçli olarak düzenlenmemiştir. Bunların, bizzat ya da yardımcı kişilerin davranışları dolayısıyla Kanun ve Tüzük'ten doğan yükümlülüklerini ihlal etmesi halinde doğabilecek akdi sorumluluğuna, Alman Medeni Kanunu'nun genel hükümleri (BGB § 276, § 278) uygulanacaktır[186].

Buna göre; onay makamı, şifre sahibine karşı; BGB md. 278'e göre, çalışanlarının ve diğer ifa yardımcılarının kusurlarından ve onay sözleşmesinin pozitif ihlalinden doğan zararlardan, kurtuluş beyyinesi ileri sürme hakkı olmadan sorumludur (kusursuz sorumluluk). Şifre sahibi ise sadece yükümlülüğün ihlal edildiğini ve bunun da sonuç olarak zarara sebebiyet verdiğini ispat edecektir. Onay makamı, üçüncü kişilere karşı, sadece kendi çalışanlarından birinin kasten yaptığı işlemlerden dolayı, maddi zarar ödemekle sorumludur (BGB md. 831; md. 826; md. 823/f.2). Ancak burada dikkat edilecek olursa, çalışanların ihmale dayanan davranışlarının

[185] **Şenocak,** sh.113-114.

[186] **Şenocak,** sh. 114.

veya üçüncü kişinin eylemlerinin, şifre sahibinden başka bir şahsa verebileceği maddi zararlar konusunda bir hüküm boşluğu söz konusudur[187] .

4. ELEKTRONİK İMZA ALANINDA SERTİFİKA HİZMETLERİNE İLİŞKİN İSVİÇRE FEDERAL KANUNU

İsviçre'de elektronik imzayla ilgili ilk kanuni düzenleme 12 Nisan 2000 tarihinde çıkarılan ve 1 Mayıs 2000 tarihinde yürürlüğe giren Elektronik Sertifika Hizmetleri Hakkında Tüzüktür. Tüzük, dijital imzayı esas alarak sertifika hizmet sağlayıcılarının faaliyetlerini düzenlemektedir. 19 Aralık 2003 tarihinde Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin Federal Kanun kabul edilmiştir. Kanun esas itibariyle Sertifika Hizmetleri Hakkında Tüzüğü ile aynı muhtevaya sahiptir. Kanun'da Tüzük'ten farklı olarak, imza anahtarı sahibinin ve sertifika hizmet sağlayıcılarının sorumluluğuna ilişkin hükümler yer almaktadır. Kanun 1 Ocak 2005 tarihinde yürürlüğe girmiştir[188].

Kanuna göre, sertifika hizmet sağlayıcıları bu Kanun ya da (bu Kanun'a dayanılarak çıkarılacak) tüzüğün öngördüğü yükümlülüklerin yerine getirilmemesi dolaysıyla, sertifikaya güvenen üçüncü kişilerin ya da imza anahtarı sahibinin uğramış olduğu zararları tazminle yükümlüdür[189].

---

[187] **Keser Berber,** (Şekil), sh. 105.

[188] **Şenocak,** sh. 116-117; **Erturgut, M.:** Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Ankara, 2004, (Delil), sh. 162-163.

[189] **Şenocak,** sh. 119.

Kanunun 16. maddesinin 2. fıkrasına göre, sertifika hizmet sağlayıcıları, bu Kanun ve Tüzükten doğan yükümlülüklerin yerine getirildiğini ispat ederek sorumluluktan kurtulabilirler. Öte yandan, sertifika hizmet sağlayıcıları, kendilerinin ya da yardımcı kişilerin davranışlarından dolayı 16. maddenin 3. fıkrası gereğince bu Kanun'dan doğan sorumluluklarını ortadan kaldıran anlaşmalar yapamazlar. Dolayısıyla, bu türden kayıtlar batıldır[190].

5. TÜRK HUKUKU AÇISINDAN SERTİFİKA HİZMET SAĞLAYICILARININ SORUMLULUĞU

DTM, ETKK'nın hazırlamış olduğu taslağın 18. maddesinde, iyiniyetli üçüncü kişilerin sertifikanın içeriğine ve zaman damgasına güvenmeleri sonucu uğradıkları zararlardan onay kurumlarının (nitelikli sertifika hizmet sağlayıcısı) sorumlu olacağı düzenlenmiştir. Aynı düzenlemeyle, onay kurumları, zararın doğmaması için gereken bütün dikkat ve özeni gösterdiğini veya bütün dikkat ve özeni göstermiş olsaydı bile zararın doğmasına engel olamayacağını ya da üçüncü kişinin sertifikadaki ve zaman damgasındaki bilgilerin doğru olmadığını bildiğini veya bilmesi gerektiğini ispat ederek sorumluluktan kurtulabilirler[191].

Onay kurumlarının sorumluluğu konusunda önemli sorunlardan birisi, elektronik sertifika sağlayıcılarının bilgi edinme sınırları ve edindiği bilgileri gizleme yükümlülükleridir. Kanun koyucu bu hususu 5070 sayılı EİK'nun 12. maddesinde

---

[190] **Şenocak,** sh. 119-120.

[191] **Altınışık,** sh. 89.

hükme bağlamıştır. Bu hükme göre, elektronik sertifika hizmet sağlayıcısı; elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler dışında bilgi talep edemeyecek ve bu bilgileri kişinin rızası dışında elde edemeyecek; temin ettiği sertifikayı başkalarının elde etmemesi için gerekli önlemleri alacak; sertifika talep eden kişinin yazılı rızası olmadan başkalarının bu bilgileri elde etmesini engelleyecek; sertifika sahibinin onayı olmadan başkalarına iletemeyecek ve başka amaçlarla kullanamayacaktır[192].

5070 sayılı Kanun elektronik imza nedeniyle elde edilen verilerin korunmasını amaçlamıştır. Bu hükümlere aykırı davranış halinde, elektronik imza sertifika sahibinin, kişilik hakkının korunmasıyla ilgili TMK. m.24 vd. hükümlerinde öngörülmüş olan hukuksal koruma yollarına başvurması mümkün olduğu gibi, uğradığı maddi ve BK. m.49 gereğince uğradığı manevi zararının tazmin edilmesi hakkı da doğacaktır[193].

EİK'nun 13. maddesinin birinci fıkrasına göre, elektronik sertifika hizmet sağlayıcısının, elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tabi tutulmuştur. Bu durumda, genel kural niteliğindeki BK'nun borcun ifa edilmemesi halinde borçlunun sorumluluğunu düzenleyen 96 vd. maddelerinin ve yardımcı şahısların fiilleri dolayısıyla 100. maddesinin uygulanması gerekmektedir. Buna göre buradaki sorumluluk kusur sorumluluğudur. Ancak kanun burada ispat yükü ters

---

[192] **Kılıçoğlu, A. M.:** Borçlar Hukuku Genel Hükümler, Genişletilmiş 4. Bası, Ankara, 2004, sh.83.

[193] **Kılıçoğlu,** sh.84.

çevrilmiş bir kusur sorumluluğu düzenlemiştir. 5070 sayılı Kanunun 13. maddesinin 2. fıkrasına göre, elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlali suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz[194].

5070 sayılı Kanunun 13. maddesinin 3. fıkrasına göre, elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlalinin istihdam ettiği kişilerin davranışına dayanması halinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, BK'nun 55. maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz.

Kanun koyucu, zararın elektronik sertifika hizmet sağlayıcısının istihdam ettiği kişilerin davranışına dayanması halinde, BK'nun genel düzenlemesinden ayrılmak suretiyle BK'nun 55. maddesinde öngörülen türden bir kurtuluş kanıtının ileri sürülmesini engellemiştir. Böylelikle teknik anlamda sıradan kullanıcılardan daha fazla bilgi ve organizasyon gücüne sahip elektronik sertifika hizmet sağlayıcıları ile kullanıcıları arasında denge sağlanarak sertifika hizmet sağlayıcılarının personel seçiminde daha dikkatli olmaları amaçlanmıştır[195]. Buna göre bu hizmeti sağlayanlar çalıştırdıkları kişilerin bu zarara sebebiyet vermemeleri için gerekli dikkat ve özeni

---

[194] **Kılıçoğlu,** sh.84.

[195] Bkz. 5070 sayılı Elektronik İmza Kanununun Madde Gerekçeleri, http://www.basbakanlik.gov.tr./tasarilar/Tasari9.htm.

gösterdiklerini veya bu dikkat ve özeni gösterseydi dahi zararın kaçınılmaz olduğunu kanıtlayarak sorumluluktan kurtulamayacaktır[196].

Ayrıca, 5070 sayılı Kanunun 13. maddesinin 4. fıkrasında düzenlenen "Nitelikli elektronik sertifikanın içerdiği kullanım ve maddi 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." şeklindeki hüküm ile kanun koyucu bir adım daha ileri giderek, elektronik sertifika hizmet sağlayıcılarının yapacakları sözleşmelerde sorumluluğu ortadan kaldıran veya sınırlayan şartları yani sorumsuzluk kayıt ve anlaşmalarını da geçersiz saymıştır. Böylece bu düzenleme ile bu alanda BK m.99 f.II ve m.100 f. II hükmüne dayanan sorumsuzluk anlaşmalarının yapılamayacağı kabul edilmiştir[197].

II. DİJİTAL İMZA SAHİBİNİN SORUMLULUĞU ve DİJİTAL İMZA ARACININ YETKİSİZ KULLANIMI SORUNU

A. GENEL OLARAK

Dijital imzanın doğurduğu sorunlardan biri de, dijital imza aracının yetkisiz kullanılmasıdır. Biyometrik yöntemlerle emniyet altına alınmamış bir imza aracının üçüncü kişilerin eline geçmesi ihtimal dahilindedir. İmzanın, başkasına ait imza

---

[196] **Kılıçoğlu,** sh.84.

[197] **Kılıçoğlu,** sh.84.

aracının kullanılarak atılması durumunda, fiilen imzayı atan ile imza anahtarının sahibi farklı kişilerdir. Şüphesiz imza anahtarının sahibi, böyle bir işleme sonradan icazet verdiği takdirde bu hukuki işlem kendisini bağlar. Buna karşılık, gizli anahtarın sahibi kendisi adına kurulan bu hukuki işleme icazet vermediği takdirde, bir yetkisiz temsil durumu söz konusu olur. Bu noktada, imza aracının üçüncü kişiler tarafından rıza dışı kullanımından doğan risklerin, imza anahtarının sahibi ile hukuki işlem yapan muhatap arasında nasıl paylaştırılacağı sorunu ortaya çıkar[198]. Burada ortaya çıkan risklerden biri, imza aracının rıza dışı kullanıldığının ispatlanamaması riskidir.

B. KARŞILAŞTIRMALI HUKUKTA DİJİTAL İMZA SAHİBİNİN SORUMLULUĞUNA ATFEDİLEN DEĞER

1. ELEKTRONİK İMZA ALANINDA SERTİFİKA HİZMETLERİNE İLİŞKİN İSVİÇRE FEDERAL KANUNU

Elektronik imzanın yetkisiz kullanımından doğan risklerin imza anahtarı sahibi ve sertifikaya güvenen üçüncü kişiler arasında dağılımı hususu İsviçre Borçlar Kanunu'na eklenmesi teklif edilen 59a maddesinde düzenlenmektedir. 19 Aralık 2003 tarihinde kabul edilen ve 1 Ocak 2005 tarihinde yürürlüğe giren Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin Federal Kanunu'na göre, imza aracının yetkisiz kullanımından doğan riski, esas itibariyle nitelikli sertifikaya güvenen kişi (muhatap) taşımaktadır. Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin

[198] **Şenocak,** sh. 131.

Federal Kanun'un 17. maddesinin 1. fıkrası, gizli anahtarının rıza dışında kullanıldığını iddia eden kişinin bu hususu ispatla yükümlü olduğunu hükme bağlamış, daha sonra bu hükmün imza anahtarı sahibi için ağır sonuçlar doğurması sebebiyle, söz konusu düzenlemeden vazgeçilmiştir[199]. Ön tasarının 17. maddesinin 2. fıkrasına göre, özel anahtarın rızası dışında kullanıldığını iddia eden kişi, bunu ispatlamakla yükümlüydü. Burada ispat yükü ters çevrilmiş olup, sertifikaya güvenerek hukuki işlem yapan üçüncü kişi, imza aracının bizzat imza anahtarı sahibi tarafından kullanıldığını değil, aksine imza sahibi aracının rızası dışında bir başkası tarafından kullanıldığını ispat etmek zorundaydı. İmza sahibi bu hususu ispat edemediği takdirde, yetkisiz üçüncü kişinin sertifikaya güvenen kişi ile kendi adına yapmış olduğu hukuki işlemin sonuçlarına katlanmak zorundaydı; yani, bu durumda hukuki işlemi kendisi yapmış ya da bu konuda bir temsilci atamış gibi hüküm ve sonuç doğacaktı. Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin Federal Kanun'da ise, elektronik olarak imzalanan beyanın imza anahtarı sahibinden neşet ettiğini kabul sonucu doğuracak böyle bir düzenlemeden, bu düzenlemenin imza anahtarı sahibini çok büyük bir risk altına soktuğu düşüncesiyle kaçınılmıştır[200]. Bununla beraber, teklif edilen 59a maddesine göre, kusuru bulunduğu takdirde imza anahtarı sahibi, üçüncü kişilerin, Sertifika Hizmetleri Kanun anlamında "tanınmış bir sertifika hizmet sağlayıcısının" geçerli bir nitelikli sertifikasına güvenmeleri dolayısıyla uğramış olduğu zararları tazminle yükümlüdür[201]. İsviçre Borçlar

---

[199] **Şenocak,** sh. 118.

[200] **Botschhaft,** Art.59 a, Nr.2.2.2.3.(**Şenocak,** sh. 118, dp.60'dan naklen.)

[201] **Botschhaft,** Art.59 a, Nr.2.2.2.3. Ön Tasarı'ya göre, imza anahtarı sahibi, imza aracının üçüncü kişiler tarafından rızası dışında kullanıldığını ispatlaması durumunda

Kanunu'na eklenmesi teklif edilen 59a maddesinin 2. fıkrasına göre, imza anahtarı sahibi, imza anahtarının gizli tutulması için hal ve şartların gerektirdiği tedbirleri almış olduğunu ya da temyiz kudretinin eksikliği nedeniyle sorumlu tutulamayacağını ispatlayarak sorumluluktan kurtulabilir. Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin Federal Kanun'un gerekçesinde, elektronik imza kullanımında olumsuz bir etki yaratacağı düşüncesiyle imza anahtarı sahibinin sorumluluğunun bir sebep sorumluluğu şeklinde düzenlenmediği ifade edilmektedir[202].

Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin Federal Kanunu'nun 59a maddesinin 3. fıkrası, imza anahtarı sahibinin, imza anahtarını teslim ettiği kişilerin davranışlarından da sorumlu olduğunu öngörmektedir. Bu nedenle imza anahtarı sahibi, kendisinin değil üçüncü bir kişinin imza anahtarının gizli tutulmasında dikkatsiz davrandığını ileri sürerek sorumluluktan kurtulamaz. Son fıkraya göre,

---

yapılan hukuki işlemle bağlı tutulmakla beraber, Elektronik İmza Alanında Sertifika Hizmetlerine ilişkin Federal Kanun'la getirilen OR 59a maddesindeki düzenlemede olduğu gibi, sertifikaya güvenen üçüncü kişinin, tanınmış bir sertifika hizmet sağlayıcısının geçerli bir sertifikasına güvenmekten dolayı uğradığı zararı tazminle yükümlüydü. (mad.17/Fk.2) Söz konusu sorumluluk da, bir kusur sorumluluğu şeklinde düzenlenmişti (**Şenocak,** sh. 118, dp.61'dan naklen.).

[202] **Botschhaft,** Art.59 a, Nr.2.2.2.3. Söz konusu hükmün, sadece, "tanınmış bir sertifika hizmet sağlayıcısının", "nitelikli sertifikasına" güvenen üçüncü kişilerin zararından dolayı sorumluluğu düzenlediğine dikkat çekmek gerekir(**Şenocak,** sh. 119 dp.62'dan naklen.).

imza anahtarının gizli tutulması için gerekli tedbirleri, çıkaracağı bir tüzükle Federal Konsey belirler[203].

2. UNCITRAL E-İMZA YEKNESAK KURALLAR TASLAĞI (DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES)

UNCITRAL E-Ticaret Çalışma Grubu tarafından oluşturulan E-İmza Yeknesak Kurallar Taslağının 9. maddesinde e-imza kullanıcılarının sorumlulukları düzenlenmiştir. Maddede e-imza kullanarak bir mesajı imzalayan kullanıcılar, imza aracı sahibi olarak ifade edilmiştir. Maddede, imza aracı (anahtar çifti) sahibinin, imza aracının izinsiz ve yetkisiz olarak kullanımından kaçınması ve bu hususta makul bir dikkat göstermesi gerektiği öngörülmektedir. Diğer yandan imza aracı sahibine, imza aracının sertifika kullanımını gerektirdiği yerde, sertifikada yer alan veya sertifikanın geçerlilik döneminde yaptığı bütün beyanlarının doğru ve tam olması ve bu hususta makul bir dikkat gösterme yükümlülüğü yüklenmiştir. İmza aracı sahibi, bu yükümlülüklerini yerine getirmediği taktirde sorumlu olur[204].

---

[203] **Şenocak,** sh. 119.

[204] **Acır,** sh.35-37.

3. ŞEKİL HÜKÜMLERİNİN UYARLANMASI HAKKINDAKİ ALMAN KANUNU İLE ALMAN MEDENİ USUL KANUNU'NA EKLENEN İLK GÖRÜNÜŞ İSPATI YOLUYLA İSPAT KOLAYLIĞI (§292a ZPO)

Dijital imzanın, imza sahibinin dışında üçüncü kişilerce kullanılarak yapılan işlemlerde, imza sahibi, yapılan işleme icazet verirse bu işlemle bağlıdır. İmza sahibinin işleme icazet vermediği durumlarda ise yetkisiz temsil durumuyla karşılaşırız. Bu gibi durumlarda imza aracının rıza dışı kullanıldığının ispat edilmesi bir sorun teşkil eder[205]. Alman Medeni Usul Kanunu ZPO'ya eklenen bir hükümle (§292a), ilk görünüş ispatı prensiplerine göre, sertifikaya güvene kişiye ispat kolaylığı getirilmiştir. Bu düzenlemeye göre, §292a ZPO hükmü şöyledir[206]:

"Nitelikli Elektronik İmzada İlk Görünüş İspatı

İmza Kanunu'na göre kontrol edilmesi sonucu elektronik şekilde bulunan bir irade açıklamasının gerçekliği konusundaki ilk görünüş, imza anahtarı sahibinin rızasıyla verildiği hususunda sadece ciddi şüphelerle gerekçelendirilebilirse sarsılabilir."

Bu hüküm, sadece elektronik imzalanan metnin gerçekliğini değil, aynı zamanda imzanın gerçekliğini de amaçlamaktadır. Böylece el yazısıyla imzada, senedin maddi

---

[205] **Şenocak,** sh.131.

[206] İlk görünüş ispatı yoluyla ispat kolaylığı hakkında ayrıntılı bir çalışma için bkz. **Erturgut,** (Delil), sh.155-159.

gücüne ilişkin kurala yaklaşır bir düzenleme getirilmiştir[207]. İlk görünüş ispatıyla düzenlemenin amacı, alıcı bakımından, güvenli elektronik imzalı bir belgenin gerçekliğinin ispatını, usul hukukundaki senet deliline yaklaşır bir şekilde kolaylaştırmaktır[208].

İlk görünüş ispatı, açıklamanın bütünlüğü, açıklama yapan kişinin kimliğinin belirlenmesi ve irade açıklamasının yetkili kişi tarafından yapıldığını konularını kapsamaktadır.

İlk görünüş ispatı kuralına göre, irade beyanının doğru olduğu yönündeki ilk görünüş, ancak ciddi vakıalar gösterilmek suretiyle bertaraf edilebilir[209]. İmza kullanan kişi bu durumda, iki gerekçeye dayanabilir:

İlk olarak, elektronik açıklamadaki yetkisizlik durumudur. İmza kullanan kişi imza işlemi için gerekli olan çip kartın PIN koduyla çalındığını veya kaybolduğunu, böylece kartının üçüncü kişi tarafından kullanıldığını ileri sürebilir. Bu durumda, imza anahtarı sahibinin PIN kodunu gizli tutma ve kartın kaybolması veya herhangi bir kötüye kullanım ihtimali durumunda gerekli koruma tedbirlerini alması yükümlülüğü olduğu söylenmelidir. Bu anlamda, kartın çalınması veya kaybolması

---

[207] **Oertal, K.:** Elektronische Form und notarielle Aufgaben im elektronischen Rectsverkehr, MMR 7/2001, sh.420 (Nakleden **Erturgut,** (Delil), sh. 156.).

[208] **Becker, A.:** Elektronische Dokumente als Beweismittel im Zivilprozess, Bockum, Univ.Diss., 2003, sh. 69 (Nakleden **Erturgut,** (Delil), sh. 156).

[209] **Şenocak,** sh.131, **Oertal,** sh. 420 (Nakleden **Erturgut,** (Delil), sh. 157).

halinde hemen bloke edilmesi için başvurması gerekir. Elektronik imza usulünün avantajlarından yararlanmak isteyen taraf, kendi hakimiyet alanında gerçekleşebilecek kötüye kullanımlara karşı gerekli tedbirleri almak zorundadır[210].

İkinci olarak, imza kullanan kişi, imza usulünde kullanılan imza bileşenlerinin güvenli olmadığını veya işletim sisteminden kaynaklanan bir sebeple imzalamak istediği veriyi göremediğini iddia edebilir. Bu iddianın sebebi, elektronik belgenin ekranda yanlış veya eksik temsilidir[211].

Elektronik imzalı belgenin alıcısı, elektronik imza sahibiyle sertifika hizmet sağlayıcısı arasındaki sözleşmeye yabancı bir kişi olduğu için sertifika hizmet sağlayıcıya başvurarak güvenli elektronik imzadan beklenen koşulların sağlanıp sağlanmadığı konusunda bilgi alamaz[212].

4. TÜRK HUKUKU AÇISINDAN DİJİTAL İMZA SAHİBİNİN SORUMLULUĞU

DTM, ETKK'nın hazırlamış olduğu taslağın 18. maddesinin 2. fıkrasında da, "İmza sahibinin imza verisini kaybetmesi veya çaldırması ve bu durumu derhal sertifika

---

[210] **Erturgut,** (Delil), sh. 159.

[211] **Erturgut,** (Delil), sh. 159.

[212] **Rossnagel, A.:** Die Sicherheitsvermutung des Signaturgesetzes, NJV 1998, sh.3318, (Nakleden **Erturgut,** (Delil), sh. 155).

hizmet sağlayıcısına bildirmemesi veya imza verisini üçüncü kişilerle paylaşması durumunda sorumluluk imza sahibine aittir." hükmü ile bu sorumluluk benimsenmiştir.

5070 sayılı EİK'nda imza aracının yetkisiz kullanımı halinde imza aracı sahibinin sorumluluğunu düzenleyen bir hüküm getirilmemiştir. Bu nedenle Türk Hukukunda şu an itibariyle imza aracının yetkisiz (rıza dışı) kullanımı halinde, risklerin paylaşımı hususunda değişik görüşler ortaya çıkabilir. Her şeyden önce, mevcut kanun hükümlerinin herhangi bir zorlama olmaksızın olduğu gibi uygulanması gerektiği, yani, imza aracının yetkisiz kullanılması halinde, sertifikaya güvenen muhatabın BK md.39 uyarınca yetkisiz temsilciye başvurabileceği görüşü ileri sürülebilir. Ancak, yetkisiz temsilcinin kimliğinin belirlenemediği durumlarda zararın tazmini mümkün olamayacağından, bu görüş yeterli değildir[213]. Doktrinde ileri sürülen bir başka görüş[214], BK md.33/2'nin kıyasen uygulanarak, imza anahtarı sahibinin yapılan işlemle bağlı olması gerektiğini savunur. Anılan hüküm, temsil yetkisinin derecesinin üçüncü kişilere bildirilmesi halinde, bu bildirime itibar olunacağını düzenlemektedir. Bu hükmün, sadece temsil yetkisinin derecesi hakkında değil, temsil yetkisinin verilmesinde de uygulama alanı bulacağı kabul edilmektedir[215]. Gerçi imza aracının rıza dışında kullanımında (özellikle imza

---

[213] **Şenocak,** sh.131.

[214] **Rosenthal, D.:** Digitale Signaturen: von Missverstandnissen nd gesetzlichen Tüchen. Jusletter, 29 Januar 2001, 3 vd. < www.jusletter.ch> (Nakleden **Şenocak,** sh.132).

[215] **Eren,** (1998), sh.406

aracının çalınması durumunda), imza anahtarı sahibi, temsil yetkisinin herhangi bir kişiye verildiği hususunda bir bildirimde bulunmamaktadır. Sertifikaya güvenen muhatap, karşısında (internetin öbür ucunda) gerçekten kim olduğunu dahi bilmemektedir; ancak o, gizli anahtar sahibinin almış olduğu sertifikaya güvenerek, sertifikada ismi kayıtlı açık anahtar (dolayısıyla gizli anahtar) sahibi ile işlem yaptığını düşünmektedir. Burada BK md.33/2'nin kıyasen uygulanabilirliği için, imza anahtarı sahibinin, kendisi için kanunen tanınmış bir sertifika düzenlettirmekle, hukuki işlemlere katılma ve kendisini bağlayıcı irade beyanlarında bulunma konusunda bir görünüş yarattığı, dolayısıyla bu görünüşe güvenen iyiniyetli üçüncü kişilerin korunması gerektiğinden hareket etmek gerekir ki, doktrinde Şenocak, pozitif bir düzenleme olmadan bu görüşün kabulünü, mevcut hükümlerin aşırı şekilde zorlanması olarak görmektedir[216].

Son olarak, imza aracının yetkisiz kullanımı hallerine BK md.36/2 hükmünün kıyasen suretiyle uygulanması suretiyle Elektronik İmza Alanında Sertifika Hizmetlerine İlişkin İsviçre Federal Kanunu'nun benimsediği görüş tarzı, bir görüş olarak ileri sürülebilir. BK md.36/2, temsil yetkisini içeren belgeyi geri almakta ihmali bulunan temsil olunan veya haleflerinin, iyi niyetli üçüncü kişilerin sözleşmenin geçerli olmamasından doğan menfi zararlarını tazmin etmesini düzenlemektedir. Söz konusu sorumluluk bir kusur sorumluluğu olup, bu hükmün uygulanması, muhafazasındaki kusur nedeniyle üçüncü kişilerin eline geçen imza aracının yetkisiz kullanılması halinde, imza anahtarı sahibinin, sertifikaya güvenen

[216] **Şenocak,** sh.132.

iyiniyetli muhatabın bu suretle uğramış olduğu menfi zarardan sorumlu tutulması sonucunu doğuracaktır[217].

[217] **Şenocak,** sh.133.

DÖRDÜNCÜ BÖLÜM

DİJİTAL İMZALI ELEKTRONİK BELGELERİN TÜRK MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

§9. TÜRK MEDENİ USULÜNDE İSPAT VE DELİL SİSTEMİ

İspat, bir iddianın veya vakıanın doğruluğu konusunda hakimi ikna etmeye yönelik bir faaliyettir[218]. Tarafların öne sürdükleri ispat araçları ise delil olarak adlandırılır[219].

Türk Medeni Usul Hukukunda deliller, kesin (kanuni) deliller ve takdiri deliller olmak üzere iki türlüdür. Kesin deliller, ikrar (HUMK md. 236), kesin hüküm (HUMK md. 237), senet (HUMK md. 287 vd.) ve yemin (HUMK md.377 vd.); takdiri deliller ise, tanık (HUMK md.245), bilirkişi (HUMK md.275 vd.), keşif (md. 363 vd.) ve özel hüküm sebepleri (HUMK md.367)dir.

Kesin deliller, hakimi bağlayıcı nitelikte deliller olup, bu delillerin en önemli özelliklerinden biri, HUMK md. 288'de belirtilen meblağın[220] üzerindeki hukuki

---

[218] **Üstündağ, S.:** Medeni Yargılama Hukuku, C. I-II, Genişletilmiş 6. Bası, İstanbul 1997, sh.613; **Konuralp, H.:** Medeni Usul Hukukunda İspat Kurallarının Zorlanan Sınırları, Ankara 1999, (İspat), sh.9.

[219] **Umar, B./Yılmaz, E.:** İspat Yükü, İstanbul 1980, Genişletilmiş 2. Bası, sh.2.

[220] 146 sayılı Kanun ile HUMK'a eklenen Ek md. 3.

işlemlerin ve senede karşı iddiaların (HUMK md. 290) kural olarak yalnız kesin delillerle ispat edilebilmesidir (HUMK md. 287, c.1). Kesin deliller arasında en önemlisi ise senettir. Zira hukuki işlemler, kural olarak yalnız senetle ispat edilebilir[221]. Senetle ispat zorunluluğu olarak da adlandırılan bu kural, hukuki işlemlerin ve hukuki sonuç doğurmaya yönelmiş irade beyanlarının[222], HUMK'nun 289, 292, 293 ve 294. maddelerinde düzenlenen istisnalar dışında, ancak senetle ispat edilebileceğini, tanıkla veya diğer takdiri delillerle ispat edilemeyeceğini ifade etmektedir.

Senet, yazılı bir belgede açıklanan bir irade beyanı olup, aleyhine delil teşkil edeceği kişinin, borçlunun imzasını, mühürünü veya elle yapılmış bir işaretini taşıyan bir belgedir[223].

I. GEÇERLİK ŞARTI VE İSPAT ŞARTI OLARAK YAZILI ŞEKİL

Senetle ispat zorunluluğu, ispat şartı olarak öngörülen yazılı şekle ilişkin olup, BK md. 11'de düzenlenen geçerlik şartı olan yazılı şekilden farklıdır[224]. Kanunun (veya taraflar iradelerinin), bir işlemin geçerli olması için mutlaka öngörülen şekle uyulmasını gerektirdiği durumlarda, geçerlik şartı olan şekilden bahsedilirken;

---

[221] **Kuru, B./Arslan, R./Yılmaz, E.:** Medeni Usul Hukuku, Ankara 1992, sh.348.

[222] **Üstündağ,** sh.650.

[223] **Kuru, B.:** Hukuk Muhakemeleri Usulü, Altıncı Baskı, C.II, Ankara 2001, sh. 2073, 2074.

[224] **Kuru/Arslan/Yılmaz,** sh. 348; **Üstündağ,** sh. 649 vd.

kanunla veya taraf iradeleriyle, sözleşmenin, ancak kararlaştırılan şekilde ispatlanabileceğinin öngörülmesi durumunda ispat şartı olan şekilden bahsedilir. Buna göre geçerlik şartına uyulmaksızın yapılan şekle tabi hukuki işlem geçersiz olacak, ispat şartına uyulmadan yapılan bir hukuki işlem ise öngörüldüğü şekilden başka bir şekilde ispat edilemeyecektir. Kağıda dayalı geleneksel hukuk sistemimizde, BK'nun md. 11/I hükmü ile, kanunda açıkça düzenlenen haller dışında[225], hukuki işlem iradesinin belirli bir şekle tabi olmadığı, sözlü, yazılı veya diğer şekil türlerinden herhangi birisiyle beyan edilebileceği öngörülerek, kural olarak şekil serbestisi ilkesi kabul edilmiştir.

Ancak HUMK md. 288 ve 290 hükümlerinde düzenlenen, belirli meblağın üzerindeki işlemleri senetle ispat ve senede karşı senetle ispat koşulu, şekil serbestisi ilkesini neredeyse ortadan kaldırmıştır. Zira ispat edilemeyen bir hakkın varlığı da tartışmalı hale gelecektir[226].

Bu nedenle e-ticarete konu e-sözleşmelerin, geçerlik şartı olan şekle uygunluğu da önemli olmakla beraber, geçerlik şartı olan şekle tabi sözleşmelerin hukukumuz ve mevcut hukuk sistemleri açısından oldukça dar bir alanı kapsadığı ve e-ticarete konu olan e-sözleşmelerin kural olarak şekil serbestisine tabi ve genellikle tüketici sözleşmeleri olduğu dikkate alındığında, e-ticaretin taraflarınca aranan hukuki

---

[225] Örneğin BK md. 213/I uyarınca, taşınmaz mala ilişkin satım sözleşmesinin geçerliliği resmi şekle tabi, BK md. 163/I uyarınca alacağın temlikinin geçerliliği yazılı şekle tabidir.

[226] **Altaş,** sh.72.

güvenliğin, elektronik ortamda yapılan sözleşmelerden doğan uyuşmazlıkların ispatı ve elektronik kayıtların delil değeri noktasında yoğunlaştığı görülmektedir.

II. ELEKTRONİK KAYITLARIN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

5070 sayılı EİK güvenli e-imzanın unsurlarını düzenlemiş ancak güvenli e-imza dışında kalan e-imzanın hukuki niteliğini düzenlememiştir. Bu bilinçli olarak bırakılmış bir tür boşluktur. Çünkü AB'nin 1999/93 sayılı Direktifin 5. maddesinin 2. bendine göre, üye devletler her tür e-imzanın delil olarak kullanılabilmesine olanak sağlamayı üstlenmişlerdir. Başka bir deyişle güvenli olmayan e-imza da onun kadar bağlayıcı olmasa da bir ölçüde caiz delil sayılma özelliği tanınmak istenmiştir. Bu durumda güvenli olmayan e-imza (diğer bir ifadeyle güvenli e-imzalar dışında kalan e-imzalar) hiç değilse bir tür takdiri delil olarak dikkate alınabilecektir. Buna göre:

1. Güvenli e-imza ile imzalanmış belgeler EİK md. 5, BK md. 14, HUMK md.295/A hükümleri nedeniyle kesin delil olma sonucu doğuracak;

2. Güvenli e-imza dışında kalan e-imzalar bakımındansa kanunda bir düzenleme olmadığı için HUMK md. 367'ye müracaat edilecek ve bu hüküm doğrudan uygulanacaktır. Ancak md. 367'nin uygulanabilmesi için şu ihtimallerden birinin gerçekleşmesi gerekir:

a) Güvenli e-imza dışında kalan e-imzalara ilişkin bir delil sözleşmesi olacak,

b) Karşı taraf güvenli e-imza dışında kalan e-imzaların delil olarak kullanılmasına muvafakat edecek,

c) Senetsiz ispatı caiz olan durumlardan biri söz konusu olacaktır.

Yukarıdaki açıklamalar doğrultusunda HUMK'un 292. maddesini geniş yorumlamak amacı aşar. Kıyas yoluyla uygulamak yeterlidir. Güvenli e-imza dışında kalan e-imzalar md. 367'den dolayı caiz delil haline geleceğinden ayrıca düzenleme yapılmasına gerek yoktur. Zaten güvenli e-imza dışında kalan e-imzalar bugün md. 287 ve md. 367 nedeniyle uygulamada kullanılmaktadır. EİK bu konuya ilişkin yeni bir düzenleme getirmemiştir. Güvenli e-imza dışında kalan e-imzalar açıklanan gerekçeler sonucunda takdiri delil olarak nitelendirilmelidir[227].

Kanun, genel gerekçesinde de belirtildiği gibi, elektronik belgeyi değil; elektronik imzayı düzenlemiştir. Güvenli e-imzaya m. 5/f.1'deki hüküm ile elle atılan imza ile aynı hukuki sonuç bağlanmıştır.

Bu noktada cevaplanması gereken soru, elle atılan imzanın hukuki değerinin ne olduğudur. Uyuşmazlık çıkması halinde mahkeme öncelikle imza sahibine imzanın kendisine ait olup olmadığını sorar. Zira, imzanın hukuki çerçevesi asıl imzanın inkar edilmesine göre çizilmiştir. Aynı durum e-imza bakımından da söz konusu olacaktır. Yani, mahkeme imza sahibine öncelikle e-imzanın kendisine ait olup olmadığını soracaktır. İmza sahibi imzasını inkar ettiği takdirde imza incelemesi yapılacaktır[228].

---

[227] **Konuralp,** (İspat), sh.3-4; **Erturgut,** sh.8-9.

[228] **Konuralp,** (İspat), sh.5;

E-imzaya tanınan bu hukuki değer sadece medeni usul hukuku bakımından geçerlidir. Bu nedenle, EİK'nda, sadece, güvenli e-imzanın elle atılan imza ile aynı hukuki sonucu doğuracağının belirtilmesi yetmeyeceği için HUMK'a md. 295/A eklenmiştir. Ceza yargılaması bakımından ise farklı esaslar dikkate alınacaktır. Kanunla HUMK'a eklenen 295/A maddesi, dolaylı bir biçimde elektronik senedi düzenlemiştir. Elektronik senet tanımı maddeye konulmamıştır. Çünkü, bu kavram uygulamada ortaya çıkacaktır. Zira, HUMK'da kağıda dayalı senet kavramının da tanımı yapılmamıştır. Ancak, yine de genel kabul gören bir senet tanımı kanundan çıkarılabilmektedir. Buna göre, benzer bir biçimde e-senet kavramı da tanımlanabilir: Elektronik senet, bir kimsenin kendi güvenli e-imzası ile meydana getirdiği ve aleyhine delil olarak kullanılma amacı taşıyan ve bilgisayar ortamında varlığını sürdürebilen elektronik verilerdir. Bu verilerin bir kayıt ortamına aktarılmasıyla e-belge oluşur. Yani sanal ortamdaki bilgi veridir. Elektronik veriler HD, disket veya CD üzerine alınırsa veya yazıcıdan çıktı alınırsa; yani veri saklanabilir hale geldiyse, belge veya elektronik belge halini alır. Dönüşüm gerçekleştirecek bir araç yardımı olmaksızın bilgiye ulaşılabiliyorsa, bu bir belgedir. Bir araç vasıtasıyla bilgiye ulaşılabiliyorsa buna elektronik belge denilir. Örneğin, veri kağıt üzerinden mikrofilme alındığında mikrofilm belge olarak kabul edilmelidir. Ancak veri bilgisayar ortamında diskete kaydedilirse disketteki kaydı elektronik belge olarak kabul etmek gerekir. Kanunda elektronik senetlerin delil olma niteliği ve değeri bakımından senet kavramı kullanılmayıp "senet hükmündedir" ibaresi kullanılmıştır. Çünkü, veri o anda senet halinde değil de elektronik belge halinde de olabilir[229].

[229] **Konuralp,** (İspat), sh.5.

Bu başlık altında kambiyo senetlerinin elektronik olarak düzenlenmesinin mümkün olup olmadığı değerlendirilebilir. TTK'nın 668. maddesine göre, poliçe üzerindeki beyanların el yazısı ile olması şarttır. El yazısıyla imza yerine mihaniki (kendiliğinden olan, mühür, baskı gibi) herhangi bir araçla veya el ile yapılan yahut tasdik edilmiş olan bir işaret ya da resmi bir şahadetname (resmi makamın verdiği belge) kullanılarak poliçenin imzalanması mümkün değildir. Bu durumda Ticaret Kanunundaki hüküm değişmediği sürece, kambiyo senetlerinin elektronik yolla imzalanması mümkün gözükmemektedir. Poliçeler hakkında düzenleme içeren imzalar hakkındaki bu hüküm bonolar için de geçerlidir (TTK md.690). Aynı şekilde çekler bakımından da, poliçedeki el yazısıyla imzaya ilişkin hükümler uygulanacaktır (TTK md.730, 19)[230].

5070 sayılı EİK "Çeşitli Hükümler" kenar başlıklı 22 inci ve 23 üncü maddelerinde, bu Kanun dolayısıyla değiştirilmesi gereken kanunları ve değiştirilmesi veya yeni ilave edilmesi gereken hükümleri tespit etmiştir. Ancak, söz konusu değişikliklerin yapılması gereken yer bu kanun değil, bilakis ilgili kanunlardır. EİK dolayısıyla BK, HUMK gibi kanunlarda yapılacak değişikliklerle bu yeni düzenlemelere yer verilmesi daha isabetli olacaktır. Çünkü; hem EİK dolayısıyla değişmesi gereken kanunların sayısı 22 ve 23. maddelerde tespit edilenden daha fazladır, hem de söz konusu kanunlara yeni ilave edilmesi gereken veya değiştirilmesi gereken hükümlerin sayısı tespit edilenden daha fazladır.

---

[230] **Erturgut,** sh.5.

5070 sayılı EİK'nun 22. maddesi ile, BK md. 14/f.1 hükmüne şöyle bir cümle eklenmesi kararlaştırılmıştır: "Güvenli elektronik imza kağıt üzerindeki imza ile aynı ispat gücünü haizdir". Kanaatimize göre bu hüküm BK'nu değil, HUMK'nu ilgilendirmektedir. Bir belgenin ispat hukuku açısından değerinin ne olacağı sorunu Medeni Usul Hukuku sorunudur. O yüzden bu cümledeki hükmün bir Borçlar Hukuku hükmü olarak "güvenli elektronik imza, hukuki ilişkilerde aynen el yazısı ile atılan imza gibi hukuki sonuç doğurur" şeklinde değiştirilmesi gerekmektedir. Bunun dışında kanun koyucunun, "Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur." şeklindeki md. 5/f.1 hükmü karşısında, ayrıca md. 22 hükmüne yer vermesinin de bir anlamı yoktur. Çünkü; Borçlar Hukuku bakımından dijital imza ile el yazısı ile atılan imzanın aynı hukuki sonuç doğuracağı zaten md. 5/f.1'de tespit edilmiştir. O nedenle yapılması gereken md. 22 hükmü yerine BK'nda yapılacak bir değişiklikle bu ibareyi Kanuna sokmaktır.

Öte yandan, 5070 sayılı EİK md. 23 hükmü ile kanun koyucu, md. 22'de koyduğu kurala ilişkin olarak, bu defa HUMK'nda 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." ilkesini benimsemiştir. Dijital imzalı elektronik belgelerin senet ve dolayısıyla Medeni Usul Kanunu anlamında kesin delil sayılacağı konusundaki bu ilke kanun koyucunun teknolojiye olan güveninin tam olduğunu göstermektedir. Şifreleme teknolojisine hakim olan "birileri bir şeyleri şifreliyorsa, birileri de bunu deşifre ediyordur" şeklindeki slogandan pek etkilenmeyen Türk Kanun Koyucusu, dijital imzaya bu denli güvenerek onunla imzalanan belgeleri delil olarak kabul etmekte biraz erken ve

hatalı davranmıştır. Gerçekten dijital imzalı belgelerin delil değerini tespit ederken, bu konuda kurallar koyarken değişen teknoloji karşısında kolay uyumlaştırma yapılabilecek hükümlere yer vermek zorunluluğu unutulmamalıdır. Bugün dijital imzalı belgeler senet sayılır şeklindeki bir hukuk kuralı, teknolojinin yarın bize sunacağı yeni çözümler karşısında kanun koyucuyu çıkmaza sokabilir. O yüzden dijital imzalı belgelerin kesin delil niteliğinde sayılması, oldukça iddialı bir yaklaşımdır. Bu konuda çok aceleci davranılmamalı, bilgisayar ve internet işlemlerinin her zaman bir risk taşıdığı hususunun göz önünde bulundurulmalı ve ona göre hareket edilmelidir.

5070 sayılı Kanun md. 23' de ayrıca, "Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkar ederse, bu Kanunun (HUMK) 308. maddesi kıyas yoluyla uygulanır." şeklinde bir hüküm yer almaktadır. HUMK md. 308 vd. hükümleri ise, adi senette yer alan imzanın borçlu tarafından inkar edilmesi halinde, mahkemenin yapacağı imza inceleme prosedürüne ilişkindir. Bu hükümler incelendiğinde, hakimin imza incelemesi yaparken imzayı inkar eden tarafa kendi önünde yazı yazdıracağı veya imza attıracağı (istiktap edeceği), o borçlu tarafından imzalandığı muhakkak olan diğer belgelerle (uygulamaya elverişli belgeler), adi senet altındaki imzasını karşılaştıracağı, bunlardan kanaat edinemiyorsa bilirkişiye müracaat edebileceği şeklinde bir yol çizilmektedir. HUMK md. 308 vd. hükümlerinin bu niteliği itibariyle, elektronik bir belgede yer alan dijital imzanın inkarı halinde aynen uygulanabilmesi mümkün değildir. 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 kanaatimize göre 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 olacaktır. 5070 sayılı EİK'nda HUMK md. 308 vd. hükümlerine doğrudan atıf yapmak yerine, dijital imzanın inkarı halinde hakimin bilirkişiye, yani dijital imza sertifikası veren kuruma müracaat etmesi gerektiğini belirlemek yeterli olacaktır.

SONUÇ

Günümüzde geleneksel ve alışılmış iletişim yöntemlerinden elektronik iletişim yöntemine doğru hızlı bir değişim ve gelişim yaşanmaktadır. Bilgi ve iletişim teknolojilerinin bu değişimi ve hızlı gelişimi, ekonomik faaliyet alanlarında ve sosyal yaşamda yeni olanaklar yaratmaktadır

Bilgisayar ve internetin sosyal ve ekonomik yaşama girmesi, bu alandaki gelişim ve değişimi hızlandırmıştır. Özellikle elektronik imzanın çeşitli alanlarda kullanılır olması sonucu bazı düzenlemelerin yapılması ihtiyacı ortaya çıkmıştır. Internet kullanımının bir parçasını oluşturan elektronik imzanın kullanımının sağlanması için uluslararası düzeyde bu konuda çalışmalar başlatılmış ve sürdürülmektedir. 13 Aralık 1999 tarihli Avrupa Parlamentosu ve Konseyi Elektronik İmza Direktifi ile Birleşmiş Milletlerin 14 Haziran 1996 tarihli Elektronik Ticarete İlişkin Model Kanunu bu kapsamda sayılabilir. Diğer yandan çeşitli ülkelerin mevzuatında elektronik imzaya ilişkin yasal düzenleme yapıldığı bir kısmında ise çalışmaların devam ettiği görülmektedir. Örneğin, Fransa'da 13 Mart 2000 tarihli ve 2000-230 sayılı Kanunla elektronik imza Medeni Kanunun 1316-4 üncü maddesinde yer almış olup, bu maddenin uygulanması amacıyla 30 Mart 2001 tarihli ve 2001-272 sayılı Kararname ile elektronik imza hakkında bir düzenleme yapılarak yürürlüğe konulmuştur. Avusturya'da ise l Ocak 2000 tarihinde yürürlüğe giren Elektronik İmza Kanunu ile bu konuda düzenlenme yapılmıştır. Bundan başka Amerika Birleşik Devletlerinde federal bir kanun olarak "Küresel ve Ulusal Ticarette Elektronik İmzalar Kanunu" yürürlüğe girmiştir. Öte yandan, birçok Avrupa ülkesinde konuya ilişkin mevzuat

hazırlanmış ya da hazırlanan tasarılar ilgili ülkelerin hukuki yapılarına göre yürütme veya yasama organları gündeminde bulunmaktadır.

Ülkemiz de elektronik ticaretin son on yılda büyük bir hızla gelişme göstermesi ve daha da artan bir hızla gelişmeye devam etmesi, elektronik ticaret hacminin her yıl katlanarak büyümesi, artık internette olmanın bir tercih ya da teknolojiye ayak uydurmanın bir avantajı olmaktan çıkıp, bir zorunluluk haline gelmesi, kısaca, teknolojinin baş döndürücü bir hızla geliştiği ve sınırların kalktığı küresel bir dünyada elektronik ticaretin mutlak hükümranlığını ilan etmek üzere olmasına daha fazla kayıtsız kalamamış ve 5070 sayılı EİK, 15.01.2004 tarihinde uzun bir çalışma maratonunun ardından kabul edilmiştir. 23.01.2004 tarihine RG'de yayınlanan Kanun, yayımı tarihinden itibaren 6 ay sonra 23.07.2004 tarihinde yürürlüğe girmiştir.

5070 sayılı EİK hazırlanırken elektronik ticaretin bütünü ile düzenlenmesi hedef alınmamış; elektronik ticaret ve kamu alanında yürütülecek "e-devlet" olarak adlandırılan projenin alt yapısının asli unsuru olan elektronik imza düzenlenmiştir. Hem Kanunun adı olarak, hem de temel kavram olarak elektronik imza kavramı benimsenmiştir. Böylece, bir yandan kapsayıcı bir üst kavram kullanılarak sayısal imza veya biyometrik tanımlama yöntemlerinin kullanımına olanak sağlanmış, öte yandan Amerika Birleşik Devletleri ve Fransa gibi ülkelerin kanunlarında ve Avrupa Birliği düzenlemelerinde kullanılan başlık ve temel kavramlarla uyum sağlanmıştır.

Elektronik ticaretin gelişmesi ve elektronik imzanın kullanıcılar tarafından benimsenmesi için açık ağ sistemine güven duyulmasının sağlanması gerekir. Bu güvenin sağlanabilmesi, taraflar arasında karşılıklı olarak iletilen bilgilerin gizliliğinin ve bütünlüğünün korunması, tarafların kimliklerinin doğruluğunun güvence altına alınmasına ilişkin hukuki düzenlemelerin yapılması ile mümkün olabilecektir. Hukuki ve ticari işlemlerde zaman, yer ve iş gücü tasarrufu sağlaması bakımından, kullanıcıların gelecekte elektronik imzayı tercih edecekleri daha şimdiden görülmektedir. Bu amaçla, e-ticaretin gerçekleştiği ortamda, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu, kurulacak teknik ve hukuki bir altyapı ile garanti edilebilmesi ihtiyacı duyulmaktadır. İşte e-imza, bu ihtiyacın karşılanması amacıyla kullanılan bir teknolojidir.

Hukuk bu konuda yasa koyma işinin altyapısını kuracak bilimlerden olması yönüyle, çok büyük bir sorumluluk altındadır. Elektronik ticaretin güvenli bir ortama kavuşabilmesi için tavsiye edilen elektronik imzaların kullanılması yönteminin hukuksal yönlerine ilişkin değerlendirmelere ihtiyaç duyulduğu açıktır. Bilişim teknolojileri hukuka ihtiyaç duymaktadır, hukuk da bilişim teknolojilerini irdelemek zorundadır.

Elektronik ticaret üzerinde gereksiz sınırlamalar getirecek düzenlemelerden kaçınılması gereğinin yanında, hukuksal düzenlemelerin, eğer doğru yapılabilirse, elektronik ticareti sınırlamaktan daha çok geliştirmeye, törpülemekten çok cesaretlendirmeye hizmet edeceği muhakkaktır. Elektronik ticaretin daha iyi gelişebilmesi için her şeyden önce geleneksel ticaret ve elektronik ticaret arasında

ayırım yapılmaması, kanunların bu anlamıyla teknolojik tarafsız (technology neutral) olması gerekir.

Elektronik imzalar, işlemlerinin güvenlik ve güvenilirliğine katkı sağlayarak, elektronik ticaretin gelişiminde önemli bir rol oynayacaktır. Bilişim teknolojilerinin meyvelerinin toplanabilmesi için her kesimden gayretler sürmektedir. Araştırmacılar yüzde yüze yakın güvende elektronik imza teknolojileri oluşturmaya çalışırken, yasa koyucular da elektronik imzaları el yazısı imzalar gibi geçerli kılabilmek için çalışmalar yapmaktadırlar.

Hukuk, doğru politikalar ve doğru zamanlama ile oluşturularak, değişimle birlikte hareket edebildiği takdirde, ekonomik refahın ve elektronik ortamın güvenliğinin sağlanmasında istikrarı sağlayıcı etki yapacaktır.

Türkiye gibi toplumlarda "dijital imza", yalnız elektronik ticaret ve özel hukuku değil, "e-devlet"e geçiş ve bilgi-okuryazarlığını teşvik açısından kamu hukukunu da ilgilendiren bir konudur. Bu bir bakıma devletin ve bireylerinin kimliklerini elektronik ortama taşıyıp, birbirleriyle yeni bir düzlemde iletişim kurması olacağı için, önemli bir dönüşümün ve bilgi toplumunun anahtarı demektir.

ÖZET

Tezimizin konusu "Elektronik İmza"dır. Tezimizde dört bölüm ve bir giriş kısmı bulunmaktadır.

Tezimizin birinci bölümünde, elektronik ticaretin özünü teşkil eden internet ve elektronik ticaret kavramlarının gelişimi ve avantajları giriş mahiyetinde kısaca değerlendirilmiştir. Özellikle bilgisayarların birbirine bağlanması ile ortaya çıkan bir açık ağ (Web) sistemi olan internet; başlangıcındaki askeri ve akademik amacının dışında, küresel düzeyde her alanı kapsayan ve ticari yönü de gittikçe artan bir özellik arzetmektedir. Internetin dünya çapında giderek artan ve yaygınlaşan bu kullanımı, daha düşük maliyetli, daha hızlı ve bilgiye dayanan yeni bir ticaret yöntemi olan elektronik ticareti de beraberinde getirmiştir.

Elektronik ticaret son on yılda büyük bir hızla gelişmiştir ve daha da artan bir hızla gelişmeye devam etmektedir. Elektronik ticaret hacmi her yıl katlanarak büyümektedir. Artık internette olmak bir tercih ya da teknolojiye ayak uydurmanın bir avantajı olmaktan çıkmış, bir zorunluluk haline gelmiştir. Kısaca, teknolojinin baş döndürücü bir hızla geliştiği ve sınırların kalktığı küresel bir dünyada elektronik ticaret mutlak hükümranlığını ilan etmek üzeredir.

Elektronik ticaret, dar anlamda Internet üzerinden yapılan ticareti ifade etmektedir. Geniş anlamda ise, açık ve kapalı ağlar üzerinden, fiziki temas kurmaksızın, telekomünikasyon araçları kullanılarak yapılan ticari faaliyeti ifade eder. Genel

anlamdaki elektronik ticaretin başlıca altı aracı vardır: Telefon, televizyon, faks, elektronik ödeme ve para transfer sistemleri, elektronik veri alışverişi ve Internettir. Elektronik ticaret başlıca dört kategoride gerçekleşmektedir. Bunlar; işletmeden işletmeye, işletmeden tüketiciye, işletme ile devlet ve devlet ile tüketici arasındadır.

Çalışmamızın ikinci bölümünde elektronik sözleşme kavramı incelenmiştir. Elektronik ticaretin hukuki temeli ve icra aracı, elektronik sözleşmelerdir. Elektronik sözleşmeler, internet üzerinden gerçekleştirilmesi nedeniyle, kendine özgü bazı özellikler arz etse de, kuruluşuna ve hükümlerine, uygun düştüğü ölçüde borçlar hukukunda düzenlenen geleneksel sözleşmelere uygulanan hükümler uygulanabilecektir.

Türk Hukukunda elektronik satım sözleşmesi, kurulması ve tarafların hak ve yükümlülükleri bakından, BK ve TKHK'nun ilgili hükümlerine tabi olmalı, ancak bu hükümler uygulanırken, elektronik ticaretin kendine özgü özellikleri dikkate alınmalıdır.

Elektronik satım sözleşmesi "mesafeli sözleşme" kavramından da bağımsız olarak ele alınmalıdır. Mesafeli sözleşme, bir tüketici sözleşmesi olarak çeşitli konularda olmak üzere mesafeli yöntemlerle kurulan sözleşmeleri ifade eder. Elektronik satım sözleşmesinin kurulmasında kullanılan iletişim araç ve yöntemleri de mesafelidir. Bununla birlikte, bir elektronik satım sözleşmesi ancak tüketiciler ile işletmeler arasında gerçekleşen elektronik ticarette, diğer bir ifadeyle, tüketici konumunda olan

bir alıcı ile kurulduğu takdirde mesafeli sözleşme niteliği kazanır. Buna karşılık, işletmeler arası elektronik ticarette kurulan elektronik satım sözleşmeleri mesafeli iletişim araç ve yöntemleri ile kurulmalarına rağmen, mesafeli sözleşme niteliğine sahip olamayacaklardır.

Çalışmamızın üçüncü bölümünde çalışmamızın ana konusunu teşkil eden elektronik imzanın teknik altyapısı, dijital imza kavramı, sistemin işleyişi ve özellikleri, elektronik imza sahibi (kullanıcı), onay kurumları ve güvenen taraf arasındaki ilişkiler, tarafların sorumlulukları ve elektronik imzalı belgelerin geçerlilik ve delil değerini düzenleyen kuralları belirleyen hukuki altyapı Türk hukuku ve yabancı hukuklar bakımından, UNCITRAL E-İmza Yeknesak Kuralları ve 5070 sayılı EİK ve AB Direktifleri hükümleri çerçevesinde araştırılmıştır.

E-ticaretin gelişebilmesi ve kullanıcılar tarafından benimsenebilmesinin ilk şartı, açık ağ sistemine güven duyulmasının sağlanmasıdır. Bu amaçla, e-ticaretin gerçekleştiği ortamda, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu, kurulacak teknik ve hukuki bir altyapı ile garanti edilebilmesi ihtiyacı duyulmaktadır. İşte e-imza, bu ihtiyacın karşılanması amacıyla kullanılan bir teknolojidir.

Elektronik imzanın, kişilerin biyometrik özelliklerine dayalı (ses, göz retinası taraması, parmak izi taraması gibi) biyometrik yöntemler, kredi kartlarında kullanılan PIN kodları, elle atılmış imzanın tarayıcıdan geçirilerek elektronik ortama aktarılmış hali, bilgisayar ekranında bu amaçla yapılmış bir kalemle atılan imza tekniği veya

çift anahtarlı kriptografiyle oluşturulan dijital (sayısal) imzayı da içeren bir üst kavram olarak karşımıza çıktığı görülmektedir.

Elektronik imza tanımlarında herhangi bir teknolojiye üstünlük tanınmadan, sadece ondan beklenen fonksiyonlar dikkate alınarak tanım yapılması "teknolojik tarafsızlık" kavramıyla açıklanabilir. Böylece elektronik imza alanında gerçekleşen değişikliklerin kanun değişikliğine gerek kalmaksızın uygulanabilmesi sağlanmış olmaktadır. Kanuni düzenlemeler, bu anlamda teknolojinin gerisinde kalmamış ve her değişikliğe uygulanabilir bir duruma getirilmiştir. Elektronik imza, şimdiye kadar imzalamada kullanılan ve ileride kullanılabilecek tüm yöntemleri kapsar bir şekilde hukuki düzenlemeye kavuşmuştur.

İradeyi açıklamak için kullanılan kalıba şekil denir. Şekil konusunda elektronik sözleşmelerde de Türk Borçlar Hukukundaki genel kural olan şekil serbestisi geçerlidir. Ancak, Kanunun aradığı hallerde resmi ve yazılı şekil şartının yerine getirilmesi gerekmektedir. Sözleşmeler kurulurken yazılı şekil aranmasa da ispat aşamasında elektronik imzaların imzalanması gerekmektedir.

İmza konusunda elektronik imza, dijital imzayı ve diğer biyometrik tabanlı imzaları kapsayan bir üst kavramdır. Dijital imzalar için onay kurumlarının varlığı gerekmektedir. Onay kurumları, kişiler adına, açık ve gizli anahtar adı verilen bir çift şifre üretir, saklar ve yönetimini yapar. Özel anahtar/gizli anahtar (imza oluşturma verisi) kişiye özgüdür ve özenle saklanması gerekir. Açık anahtar (imza doğrulama verisi) ise kamunun erişimine açık olarak onay kurumlarınca yayımlanır. Kişi bir

elektronik belgeyi imzalamak istediği zaman, ilk önce matematiksel bir algoritma kullanarak mesajın özetini çıkarır. Buna hash değeri denir. Sonra bunu onay kurumunun verdiği özel anahtarıyla şifreleyecektir. Daha sonra şifreli hash değerini alıcının genel anahtarıyla şifreleyip mesajı gönderecektir. Mesajı alan kendi özel anahtarıyla mesajı deşifre eder. Sonra aynı algoritmayla mesajın özetini (hash değeri) çıkarır. Mesajı alan göndericinin genel anahtarını kullanarak gönderenin bulduğu hash değeriyle kendi bulduğu değeri karşılaştırır. Sonuçlar aynıysa, mesaj değişikliğe uğramamış demektir.

Çalışmamızın dördüncü bölümünde, elektronik imzalı belgelerin ispat hukuku yönünden değerlendirilmesi yapılmıştır.

Kanun koyucu 5070 sayılı EİK ile güvenli e-imza ile imzalanmış belgelere kesin delil niteliği vermiştir. Güvenli e-imza dışında kalan e-imzalar bakımından ise kanunda bir düzenleme olmadığı için HUMK md. 367'ye müracaat edilecek ve bu hüküm doğrudan uygulanacaktır. Ancak md. 367'nin uygulanabilmesi için şu ihtimallerden birinin gerçekleşmesi gerekir: Güvenli e-imza dışında kalan e-imzalara ilişkin bir delil sözleşmesi olması, karşı tarafın güvenli e-imza dışında kalan e-imzaların delil olarak kullanılmasına muvafakat etmesi veya senetsiz ispatı caiz olan durumlardan birinin söz konusu olması gerekmektedir. Güvenli e-imza dışında kalan e-imzalar açıklanan gerekçeler sonucunda takdiri delil olarak nitelendirilmelidir.

SUMMARY

The subject of my thesis is "electronic signature". In my thesis, there are four sections and an introduction part. In the introduction part, I have given some information about my thesis and its content.

In this thesis, the subject of electronic signature was examined with regard to Electronic Signature Law Numbered 5070, the principles of Turkish Code of Obligations, United Nations Commission on International Trade Law Draft Uniform Rules on Electronic Signatures, Directive 2000/31/EC of The European Parliament and of The Council of 8 June 2000 on Electronic Commerce, Directive 1999/93/EC of The European Parliament and of The Council of 13 December 1999 on a Community Framework for Electronic Signatures and other codes of foreign countries which accepted the Electronic Signature Codes.

Technological and market trends, history that cover Internet, electronic commerce, electronic contracts, electronic signature concept, basics of digital signatures, international initiatives and studies that have been executed in our country and in the world were investigated in detail in my thesis.

The main subject of my thesis is electronic signature but to addition this, I have examined Internet, electronic commerce and electronic contracts briefly as far as possible in the content of my thesis.

The name of the first part of my thesis is "Internet and Electronic Commerce". In this part, I investigated Internet from the point of view of its technical meaning, history and background and its advantages. I also examined electronic commerce in the first part. Fistly I have defined electronic commerce and I gave some definitions made by international institutions. Telephone, fax, TV, electronic fund transfer, electronic data intrchange and Internet are the tools of electronic commerce. Electronic commerce takes place in four categories which are business to business, business to consumer, consumer to administration and business to administration. Then I have mentioned the advantages of electronic commerce and I also examined development of electronic commerce and international initiatives and studies that have been executed in our country about electronic commerce.

The second part of my thesis is about electronic contracts. Electronic contracts can be defined as contracts that are concluded by using electronic communication means through Internet. The types and formation methods of electronic contracts are also examined briefly.

In the third part of my thesis I have examined electronic signature that is the main subject of my thesis. An electronic signature means data which affixed to or logically associated, with a data message, used to identify the signature holder and indicate his/her approval of the information contained in the data.

A digital signature is a sub category of the electronic signatures and it can be defined as a message digest created by processing the message contents using a special

algorithm encrypted using the sender's private key. There are two keys in the digital signature which are public key and private key. Private key is used to encrypt the message and public key is used to decrypt it. These keys are produced, stored and administrated by the certification authorities that may be a public or a private enterprise.

In this part, I have investigated the electronic signature concept, basics of digital signatures within the scope of Electronic Signature Law Numbered 5070, international initiatives and studies that have been executed in our country and in the world, the definitation, the kinds of electronic signature, the methods of encryption, certification authorities, the holder of the dijital signature, the scope of legal responsibilities of the certification authorities' and the holder's of the digital signature, the aim and function of the digital signature, the comparison between dijital signature-electronic signature and dijital signature-hand signature and the technical infrastructure of digital signature.

In the last part of my thesis, I have investigated dijital signatures from the point of view of value of proof. There is a freedom of form regarding with the conclusion of the contracs in Turkish Law, as a rule. But when it comes to the proof, there are mandatory rules requiring writing and hand signature. Numbered 5070 Electronic Signature Law made digital signature possible by Article 5, 22 and 23. According to Article 5 of Numbered 5070 Electronic Signature Law, the secure electronic signature has same legal results like hand signature. But legal transactions which

Laws subject to legal way or a private procedure and guarantee contracts cannot be conclude by the secure electronic signature.

Article 22 of Numbered 5070 Electronic Signature Law added a sentence to Turkish Code of Obligations Article 14 sub paragraph II. According to this, the secure electronic signature has same value of proof like hand signature.

And Article 23 of Numbered 5070 Electronic Signature Law added Article 295/A to Turkish Procedure Law. Accordig to this, electronic datas concluded by the secure electronic signature suitable for its procedure are consired as proissory note. And these datas are respected as definite evidence.

KAYNAKÇA

ACIR, Birsen : Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, Sermaye Piyasası Kurulu Yeterlik Etüdü, Ankara,2000.

AHİ, Gökhan M. : Hukuki Bakımdan Dijital İmza (Sayısal İmza), gokhan@hukukcu.com.

AKİPEK ÖCAL, Şebnem : Elektronik Ticarette Sözleşme, Bilişim Teknolojileri ve Hukuk Semineri, http://tubitak.gov.tr/anasayfadan/toplanti/sebnemakipek.htm.

AKKAYA, Mustafa : Elektronik Ticaretin Vergilendirilmesi, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001.

ALTAŞ, Hüseyin : Şekle Aykırılığın Olumsuz Sonuçlarının Düzeltilmesi, Ankara,1998,

ALTINIŞIK, Ulvi : Elektronik Sözleşmeler, Ankara, 2003.

ARIKAN, Saadet : Elektronik Ticaret, Hukuk ve Noterler", Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001.

ASLAN, Yılmaz : Tüketici Hukuku (En Son Değişiklikler ve Yargıtay Kararları Işığında), 2004.

ATAMER,Yeşim : Sözleşme Özgürlüğünün Sınırlandırılması Çerçevesinde Genel İşlem Şartlarının Denetlenmesi, İstanbul, 1999.

AYDEMİR, İbrahim : Elektronik Ticaret Alanındaki Rekabet Sorunları, Rekabet Kurumu Uzmanlık Tezi, Ankara.

BECKER, Arnd : Elektronische Dokumente als Beweismittel im Zivilprozess, Bockum, Univ.Diss., 2003, sh. 69 (Nakleden Erturgut, Mine (Delil)).

BİLGİLİ, Fatih : Özel Hukukta Elektronik İmza ve Elektronik Ticaret, Prof.Dr. Ömer Teoman'a 55. Yaş Günü Armağanı, C.II, Beta Yayınları, İstanbul, 2002.

BOZBEL, Savaş : Internet Üzerinden Yapılan Hukuki İşlemler, YD, C.27, Ocak-Nisan 2001.

BOZBEL, Savaş : Türk Hukukunda Mesafeli Sözleşmeler, AÜEHFD, 2003, C. VII, S.3-4.

BOZKURT, Veysel : Elektronik Ticaretin Ekonomik ve Toplumsal Boyutu, Elektronik Ticaret.

BRYANT, Stephan : The Story of the Internet, Londan,2000.

CANPOLAT, Önder : E-Ticaret ve Türkiye'deki Gelişmeler, Sanayi ve Ticaret Bakanlığı Hukuk Müşavirliği, Ankara, Mart 2001.

ÇAMURDAN, Çiğdem : Elektronik İmza Kanunu Üzerine Bir Değerlendirme,TBD,s.1,http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm.

ÇANGA, Tarık Mete : Elektronik İmza Ve Elektronik İmza Yasa Çalışmaları, www.etkk.gov.tr/hukuk.htm .

DELTA, George B./MATSUURA, Jeffery H.: Law of the Internet, Newyork, 2000.

EKŞİ, Nuray : Elektronik İmzalara İlişkin Uncitral Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme, Yasa Hukuk Dergisi, S.3, Mart, 2001.

EREN, Fikret : Borçlar Hukuku Genel Hükümler, C.I, 4. Bs., Ankara,1991,

EREN, Fikret : Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş 6.Bası, C.I, İstanbul, 1998.

ERSOY, Zeynep : Elektronik Ticaret ve Ticaret Noktaları, İGEME, Ekim 1999.

ERTAŞ, Sacit : Elektronik Ticaret: Tanımı, Gelişimi, Avantajları, Güvenliği, Elektronik Ticaret.

ERTURGUT, Mine : Elektronik İmza Kanunu Bakımından e-Belge ve e-İmza (Hukuki Açıdan Tanıtım ve Değerlendirme), Bankacılık Açısından Elektronik İmza Konferansı, (Konferans) 04.03.2004, İstanbul, www.tbb.org.tr/eklenenler/eklenenler-ocak04.htm.

ERTURGUT, Mine : Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Ankara, 2004, (Delil).

ESENER, Turhan : Turkish Business Law, Law of Obligations-Contracts and Torts, C.I, İstanbul, 2000, (Çeviren: YARSUVAT, Ömür).

FALCIOĞLU, Mete Özgür : Karşılaştırmalı Hukuk ve Türk Hukukunda Elektronik Satım Sözleşmesi ve Kuruluşu, Ankara, 2004.

FORD, Matthew D. : Identitiy Authentication and E-Commerce, http://www.law.worwick.ac.uk/jilt/98-3/ford.html>

GEZDER, Ümit : Mukayeseli Hukuk Açısından İnternette Aktedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, 2004.

GONZENBACH, Rainer : "Pacta sunt servanda" oder neues Licht auf alten Grundsatz- Notizen zu einem Konsumentenschutzproblem, ZSR, 1987 I, (Nakleden GEZDER, Ümit).

GÜRAN, Sait/AKÜNAL, Teoman/BAYRAKTAR, Köksal/ ve diğerleri: Internet ve Hukuk, Superonline Workshop Çalışması.

HANCE and BALZ : Business ans and Law on the Internet, 1996 (translated from French by S.D.Balz), 151 ff.,

HASSLER, Vesna/BIELY, Helmut: Digital Signature Management, Internet Research: Electronic Networking Applications and Policy, Volume 9, Number 4, 1999.

HONSELL, Heinrich/ PIETRUSZAK, Thomas: Der Vernehmlassungsentwurf zu einem Bundesgesetz über den elektronischen Geschaftsverkehr, AJP, 7/2001, (Nakleden GEZDER, Ümit).

İNCE, Murat : Elektronik Ticaret: Gelişme Yolundaki Ülkeler İçin İmkanlar ve Politikalar, Devlet Planlama Teşkilatı Raporu,1999.

KEELER, Len : Cyber Marketing,USA,1995.

KESER BERBER, Leyla : Şekil ve Dijital İmza, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001 (Şekil).

KESER BERBER, Leyla : İmzalıyorum O Halde Varım Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Belgelerin Hukuki Değeri, TBDD, S.2000/2 (İmza).

KESER BERBER, Leyla : Elektronik İmza Kanunu Hükümlerinin Değerlendirilmesi, http://turk.internet.com/haber/yazigoster.php3?yaziid=6212

KILIÇOĞLU, Ahmet M. : Borçlar Hukuku Genel Hükümler, Genişletilmiş 4. Bası, Ankara, 2004.

KIRCA, Çiğdem : Internette Sözleşme Kurulması, Banka ve Ticaret Dergisi (BATİDER) C.XX.

KIRÇOVA, İbrahim/ÖZTÜRK, Pınar: Internette Ticaret ve Hukuki Sorunlar, İstanbul, 2000.

KIDD/DAUGTREY : Adapting Contract Law to Accomodate Electronic Contracts: Overview and Suggestions, rutgers Computer&Tech.L.J., 2000/26.

KONURALP, Haluk : Medeni Usul Hukukunda İspat Kurallarının Zorlanan Sınırları, Ankara,1999(İspat).

KONURALP, Haluk : Genel Hatlarıyla Elektronik İmza Kanunu, Bankacılık Açısından Elektronik İmza Konferansı, 04.03.2004, İstanbul, www.tbb.org.tr/eklenenler/eklenenler-ocak04.htm.

KURU, Baki : Hukuk Muhakemeleri Usulü, Altıncı Baskı, C.II, Ankara 2001.

KURU, Baki/ARSLAN, Ramazan/YILMAZ, Ejder: Medeni Usul Hukuku, Ders Kitabı, Ankara 1992.

NOMER, N. Füsun : Internet Alan Adının (Domain Name) Hukuki Niteliği Ve Marka Ve Ticaret Unvanı Gibi Ayırt Edici Ad Ve İşaretler İle Arasında Benzerlik Bulunması Sebebiyle Doğabilecek Hukuki Sorunlar, Prof.Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı, C.1, Beta Yayınları, İstanbul, 2001.

OERTAL, Klaus : Elektronische Form und notarielle Aufgaben im elektronischen Rectsverkehr, MMR 7/2001, sh.420 (Nakleden ERTURGUT, Mine (Delil)).

OĞUZMAN, Kemal/ÖZ, M. Turgut: Borçlar Hukuku Genel Hükümler, İstanbul, 2000.

ORCAN, Serkan : T.C. Ulaştırma Bakanlığı TUENA Internet ÇalışmaBelgesi,Ocak 1998<http: <http://www.tuena.tub.gov.tr/rapor/cbelgeleri.html.

ORTA, Mesut : Ulusal Yargı Ağı Projesinde Elektronik İmza, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001.

ÖZDEMİR KOCASAKAL, Hatice: Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, İstanbul, 2003.

ÖZEL, Çağlar : Mukayeseli Hukuk Işığında Tüketiciyi Koruyan Geri Alma Hakkı, Ankara,1998.

ÖZGÜ, Mehmet Emin : İnternette Hukuki Güvenlik Ve Dijital İmza.

ÖZSUNAY, Ergun : Elektronik Sözleşmeler, AB'de, Bazı Üye Devletlerde ve Türkiye'de Elektronik Ticaretin Hukuksal Sorunları-Elektronik Sözleşmeler Seminerinde sunulan tebliğ, 12.5.2000, İstanbul Ticaret Odası AB Şubesi, İstanbul.

PEKCANITEZ, Hakan : Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, Uluslararası Internet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002.

PROSISE, Jeff(1996) : Dijital Signatures: How They Work?, http://www.zdnet.com./ccmag/issues/107/pcm.htm>.

REİSOĞLU, Safa : Borçlar Hukuku Genel Hükümler, 14. Bs., İstanbul, 2000.

REED, Chris (2000) : What is a signature?, http://www.elj.warwick.ac.uk/jilt/00-37reed.httm>.

ROSENTHAL, D. : Digitale Signaturen: von Missverstandnissen nd gesetzlichen Tüchen.Jusletter,29 Januar 2001,3vd.< www.jusletter.ch>, (Nakleden ŞENOCAK, Zarife).

ROSSNAGEL, Alexander :Die Sicherheitsvermutung des Signaturgesetzes, NJV 1998, sh.3318, (Nakleden ERTURGUT, Mine, (Delil))

ROTH, Birgit/ SCHULZE, Götz: Verbraucherschutz im Electronic Commerce-Schutz- mechanismen un grenzüberschreitende Geschaefte nach dem Referentenent-wurf eines Fernabsatzgesetzes, RIW, 1999, (Nakleden GEZDER, Ümit).

ROWE Heather/HAFTKE, Mark : A Practitioner's Guide to The Regulation of The Internet, 1999/2000 Ed.

SEVİMLİ, Ahmet : Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası, Prof.Dr. Hayri Domaniç'e 80.Yaş Günü Armağanı, C.II, İstanbul, 2001.

SÖZER, Bülent : Elektronik Sözleşmeler, Beta Yayınları, İstanbul, 2002 (Sözleşme).

SÖZER, Bülent : Elektronik Ticaret/Elektronik Sözleşmeler, TÜSİAV İstanbul Sohbetlerinde Sunulan Tebliğ, İstanbul, (Tebliğ).

STONE, Peter : The Treatment of Electronic Contracts and Torts in Private International Law under European Community Legislation, Information&Communication Technology Law, 2002/11 S.2.

ŞENOCAK, Zarife : Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından İncelenmesi, AÜHFD, C.50, S.2, 2001.

TEKİNAY, Selahattin Sulhi/AKMAN, Sermet/BURCUOĞLU, Haluk/ALTOP, Atilla : Borçlar Hukuku, Genel Hükümler, 6. Bası, İstanbul 1988.

TUNÇOMAĞ, Kenan : Türk Borçlar Hukuku, C.I, Genel Hükümler, İstanbul, 1976.

TUĞ, Adnan : Türk Özel Hukukunda Şekil, Konya, 1994, sh. 3 .

UMAR, Bilge/ YILMAZ, Ejder : İspat Yükü, Genişletilmiş 2. Bs., İstanbul, 1980.

ÜSTÜNDAĞ, Saim : Medeni Yargılama Hukuku, C. I-II, Genişletilmiş 6. Bası, İstanbul 1997.

WINN/HAUBOLD : Electronic Promises: Contract Law Reformand E-Commerce In A Comparative Perspective, E.L., Rev., 2000/27, S.5.

YILMAZ, Ejder : Hukuk Sözlüğü, Genişletilmiş Beşinci Bası, Ankara 1996, sh. 384.

ZAMMIT, Joseph P./GALANT, Felice B.: Electronic Sözleşme, (Çeviren: ÇELİKTAŞ, İlyas), İBD, 1999, C.73,

ZANGER, Lary M. : Electronic Contracts: Some of the Basics, http://www.mbc.com/ecommrce/Itecpubs.asp.

ZEVKLİLER, Aydın : Tüketicinin Korunması Hakkında Kanun, Ankara, 2001

MUHTELİF

Directive 2000/31/EC of The European Parliament and of The Council of 8 June 2000 on Electronic Commerce (Official Journal L 178, 17.7.2000)

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, (Official Journal L 13, 19.01.2000), <http://www.ispo.cec.be/eif/policy/policy.html>

Draft Uniform Rules on Electronic Signatures, Recent Documents of UNCITRAL and its Working Groups, Working Group on Electronic Commerce, http://www.uncitral.org/english/sessions/wg_ec/index.htm

Digital Signature Law (Signaturgesetz) Translated from German by Christopher KUNER) <http://www.kuner.com/data/reg/multimd3.htm> (par.3).

Internet Society, A Brief History of Internet, http://www.isoc.org, s.1.

Elektronik Ticaret Koordinasyon Kurulu Raporları, http://www.igeme.org.tr

Elektronik Ticaret Koordinasyon Kurulu Raporları, Dış Ticaret Müsteşarlığı, Mayıs 1998, Ankara, http://www.foreigntrade.gov.tr.

www.etkk.gov.tr/hukuk.htm: Elektronik Ticaret Koordinasyon Kurulu Raporları, Hukuk Çalışma Gurubu Raporu.

Tübitak Bilten (Bilgi Teknolojileri Elektronik Araştırma Enstitüsü), Türkiye İçin Elektronik Ticarete Geçiş Durum Değerlendirmesi ve Pilot Uygulama Projesi Raporu, 2000.

UNCITRAL Model Law on Electronic Commerce With Guide to Enactment, <http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

T.C. Ulaştırma Bakanlığı, TUENA, Türkiye Ulusal Enformasyon Altyapısı Sonuçlar Özeti,1998,<http://www.tubitak.gov.tr/rapor/pdf/sonuc-ozet>.

Elektronik İmza Kanununun Genel Gerekçesi için bkz. <http://www.basbakanlik.gov.tr/tasarilar/Tasari-9.htm

ElektronikTicaretHukukAltyapısı,Etkk,<http://www.igeme.org.tr/tur/etrade/etkk/huk uk/h altyapi.htm> (par.2).

Recent Documents of UNCITRAL and its Working Groups, Working Group on Electronic Commerce, <http://www.uncitral.org/english/sessions/wg_ec/index.htm>

List of Enacted Statutes and Regulations, McBride Baker&Coles <http://www.mbc.com/ecommerce/legis/congress.html>

"Kamu Hukuku ve Bilişim İletişim Teknolojileri", Avniye Tansuğ-Özgür Uçkan, TBS Hukuk Çalışma Grubu Arşivi http://www.bilisimsurasi.org.tr (Hukuk Çalışma Grubu Dosyaları)

ZİYARET EDİLEN INTERNET ADRESLERİ

http://www.tbb.org.tr/turkce/gruplar/E-ticaret/EBD.

http://www.europa.eu.int/.

http://www.europa.eu.int/comm/internal_market.de/media/sign/composde.htm.

<http: <http://www.tuena.tub.gov.tr/rapor/cbelgeleri.html.

<http://www.wto.org/english/news-e/pr96-e.htm >.

http://www.oecd.org.

<http://www.europa.eu.int./ISPO/ecommerce/answers/introduction> .

<http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>.

http://www.etkk.gov.tr.

http://tubitak.gov.tr/anasayfadan/toplanti/sebnemakipek.htm.

<http://ekutup.dpt.gov.tr/ticaret/incem/eticaret.html>.

http://www.hurriyetim.com.tr

http://www.foreigntrade.gov.tr

http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm.

http://www.e-ticaret.gov.tr

http://www.mbc.com/ecommrce/Itecpubs.asp

www.tbb.org.tr/eklenenler/eklenenler-ocak04.htm,

<http://www.basbakanlik.gov.tr/tasarilar/Tasari-9.htm

<http://www.igeme.org.tr/tur/etrade/etkk/hukuk/h altyapi.htm> (par.2).

http://www.etkk.gov.tr/hukuk.htm>

<http://www.uncitral.org/english/sessions/wg_ec/index.htm>

<http://www.ispo.cec.be/eif/policy/policy.html>.

<http://www.mbc.com/ecommerce/legis/congress.html>

www.tk.gov.tr

http://www.law.worwick.ac.uk/jilt/98-3/ford.html>

http://www.elj.warwick.ac.uk/jilt/00-37reed.httm>.

http://www.etkk.gov.tr/ETKKsozluk.htm>.

<http://www.kuner.com/data/reg/multimd3.htm> (par.3).

http://www.zdnet.com./ccmag/issues/107/pcm.htm>

www.etkk.gov.tr/hukuk.htm:

http://www.bilisimsurasi.org.tr

http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm.