Sermaye Piyasası Kurulu

ELEKTRONİK İMZA VE ELEKTRONİK KAYITLARIN MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

Yeterlilik Etüdü

Birsen ACIR
Uzman Hukukçu Yardımcısı

ANKARA
Ekim 2000

YÖNETİCİ ÖZETİ

Internetin dünya çapında giderek artan ve yaygınlaşan kullanımı, daha düşük maliyetli, daha hızlı ve bilgiye dayanan yeni bir ticaret yöntemi olan elektronik ticareti de beraberinde getirmiştir.

Satıcılar ve alıcıların, şeffaf ve tam rekabete yakın bir ortamda bir araya gelmesine imkan tanıyan e-ticaret ile, ticari işlemler daha kolay, daha hızlı ve daha az maliyetle gerçekleştirilebilmektedir. Bu yönüyle elektronik ticaret, uluslararası organizasyonlarca oluşturulmaya çalışılan, daha kolay, uyumlu, ucuz ve hızlı bir uluslararası ticari prosedür için de bir çıkış noktası olarak kabul edilmiş olup, elektronik ticaretin düzenlenmesinde, temel ilkelerde uzlaşma sağlamak ve bu doğrultuda ulusal düzenlemelere yön vermek üzere, bir çok uluslararası örgüt tarafından, elektronik ticaret önündeki hukuki engellerin ortadan kaldırılması ve elektronik ticaretin gelişimi için daha güvenli ve uyumlu bir hukuki ortamın oluşturulmasına yönelik direktif, model kanun, tavsiye ve raporlar hazırlanmıştır.

Ticaretin her alanında yaşanan bu gelişme, menkul kıymet işlemlerinin elektronik ticarete konu olması bağlamında; yatırımcılar, ihraççılar ve diğer sermaye piyasası kurumlarına da pek çok kolaylık ve avantajlar sağlayarak sermaye piyasalarının gelişimine katkıda bulunacaktır.

E-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. Ayrıca internetin mekan farklılığını ortadan kaldıran özelliği sayesinde elektronik sözleşmelerin, yabancılık unsuru içermesi ve dolayısıyla kanunlar ihtilafı kurallarının uygulanması gündeme gelecektir. Çalışmamızın ikinci bölümünde elektronik sözleşmelere ilişkin hukuki sorunlar incelenecektir.

Elekronik 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.

Elektronik ticaretin anahtar unsuru sayılan elektronik imza konusunda da, ülkeler arası yeknesaklığı diğer bir ifadeyle güvenliği sağlama amacıyla, uluslararası

kuruluşlarca hazırlanan direktif, rapor, model kanun ve öneriler bulunmaktadır. Türk mevzuatına ilk kez 4487 sayılı Kanunla Sermaye Piyasası Kanunu'na eklenen 22/(u) hükmü ile giren elektronik imza ve elektronik imzanın kullanımı ile ilgili esasları düzenleme ve denetleme yetkisi Sermaye Piyasası Kurulu'na verilmiştir. Kurulca elektronik imza kullanımı ile ilgili esaslar belirlenirken, yukarıda belirtilen uluslararası uyumu sağlamayı amaçlayan metinlerin dikkate alınması yararlı olacaktır.

Çalışmamızın üçüncü bölümünde elektronik imzanın teknik altyapısı ile sistemin işleyişi ile elektronik imza sahibi (kullanıcı), onay kurumları ve güvenen taraf arasındaki ilişkiler, riskin tahsisi, tarafların sorumlulukları ve elektronik imzalı belgelerin geçerlilik ve delil değerini düzenleyen kuralları belirleyen hukuki altyapı UNCITRAL E-İmza Yeknesak Kuralları esas alınarak incelenecektir.

Medeni usul hukukumuzun delil sisteminde, hukuki işlemlerin ancak kanuni delillerle, özellikle de en önemli kanuni delil olan senetle ispatlanabileceği öngörülmüştür. Bu nedenle HUMK'nun mevcut delil sistemi çerçevesinde elektronik kayıtların hukuki işlemlerin ispatında bir delil olarak kabulü, ancak HUMK md. 287/II hükmü çerçevesinde, taraflar arasında yazılı ve geçerli bir delil sözleşmesi akdedilerek, sözü edilen kayıtların mahkemelerde caiz delil olarak kullanılacağının kararlaştırılması halinde mümkündür. Elektronik kayıtlar ve bu arada elektronik imza, ancak bu şartların karşılanması halinde HUMK md. 367'de belirtilen bir takdiri delil olarak mahkemece değerlendirilebilecektir.

Dördüncü bölümde elektronik kayıtların medeni usul hukukumuzun ispat kuralları karşısındaki durumu ile mevcut delil sisteminin e-ticaretten doğan uyuşmazlıkların çözümünde, ihtiyacı karşılayıp karşılayamayacağı, ispat sorununun senede bağlı delil sisteminde değişiklik yapılmasını gerektirip gerektirmediği tartışılacaktır.

Beşinci ve son bölümde, etüdde bölümler halinde tartışılan konularda ulaşılan sonuçlara yer verilerek, SPKn md. 22/(u) hükmü ile Kurul'a verilen, elektronik imza ve elektronik imzanın kullanım esaslarının belirlenmesini düzenleme görevinin yerine getirilmesine ilişkin somut öneriler getirilecek, ayrıca ele alınan hususlar sermaye piyasası mevzuatı açısından değerlendirilecektir.

Hukukta atıf usullerinde, atıfların metnin bütünlüğünü bozmaması yöntemi benimsendiğinden, 16.10.1998 tarih ve 1998/16 sayılı Genelge'den farklı olarak, atıflar aynı sayfada dipnot olarak verilmiştir.

E-İMZA VE ELEKTRONİK KAYITLARIN MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

İÇİNDEKİLER

KISALTMALAR CETVELİ.....7

GİRİŞ.....8

BİRİNCİ BÖLÜM

İNTERNET VE ELEKTRONIK TİCARET.....9

1.1. INTERNET.....9
1.2. ELEKTRONİK TİCARET.....9
1.2.1.Tanımı.....9
1.2.2.Avantajları.....10
1.2.3. Uluslararası Alanda E-ticareti Geliştirmeye Yönelik Çalışmalar.....10

İKİNCİ BÖLÜM

ELEKTRONİK SÖZLEŞMELER.....11

2.1. KAVRAM VE TANIM.....11
2.2. E-SÖZLEŞMELERİN KURULMASI VE HÜKÜMLERİ.....13
2.2.1 E-Sözleşmelerin Kurulduğu An.....15
2.2.2. E-Sözleşmelerin Hüküm ve Sonuçlarını Doğurmaya Başladığı An.....16
2.3. E-SÖZLEŞMELERİN KATILMA SÖZLEŞMELERİ OLMASI 17
2.4. E-SÖZLEŞMELERE UYGULANACAK HUKUK.....17
2.4.1. Yabancı Unsur İçeren E-Sözleşmeler.....18
2.4.1.1. Taraflarca Belirlenen Hukuk.....18
2.4.1.2. Borç İlişkisinin Ağırlığını Teşkil Eden Edimin İfa Yeri Hukuku..... 18
2.4.1.3. Sözleşme ile En Yakın İrtibatlı Hukuk.....19
2.4.2. Taraflarından Biri Tüketici Olan ve Milletlerarası Özel Hukukun Tüketiciyi Koruma Amacının Bulunduğu E-sözleşmeler.....19
2.4.2.1. Tüketicinin (Fiziki Olarak) Mutad Meskeni Ülkesinde Bulunması.....19
2.4.2.2. Ticari Yönelme.....20
2.4.3. Türkiye'de Yerleşik Yatırımcılara Yönelik, Kurul'un İznine Tabi Sermaye Piyasası Faaliyetlerinin Tespitinde Ticari Yönelme Kriteri……..20

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK İMZA.....22

3.1.KAVRAM VE TANIM.....22
3.2. E-İMZANIN AMACI VE İŞLEVLERİ.....23
3.2.1. E-İmzanın Amacı.....23
3.2.2.Kağıda Dayanan Geleneksel Sistemde Elle Atılan İmzanın İşlevleri.....24
3.2.2.1. İmza Sahibinin Kimliğini Gösterme İşlevi.....24
3.2.2.2. Tarafları İmzaladıkları Sözleşme ile Bağlayıcı Bir Muameleye Giriştikleri Konusunda Uyarma İşlevi.....24
3.2.2.3. İmzalanan Metindeki İradenin, İmzalayanın Gerçek, Nihai ve Kesin İradesi Olduğunu Gösterme (Onaylama) İşlevi.....24
3.2.2.4. İspatta Güvenlik ve Kolaylık Sağlama İşlevi.....24
3.2.3. E-İmzanın İşlevleri.....25
3.2.3.1. İmza Sahibinin Kimliğini Tanımlama İşlevi.....25
3.2.3.1.1. Biyometri Tekniklerinin Kullanıldığı Yöntem ve Araçlar.....25
3.2.3.1.2. Şifreleme Tekniklerinin Kullanıldığı Yöntem ve Araçlar.....25
3.2.3.1.2.1. Dijital İmza.....26
3.2.3.2. Elektronik Bilgi Mesajının İçeriğindeki Bilginin İmzalayan Tarafından Onaylandığını Gösterme İşlevi 27
3.2.3.3. Elektronik Bilgi Mesajının Orjinalliğini ve İmzalandıktan Sonra Değişmediğini Gösterme İşlevi.....27
3.2.3.4. İspat İşlevi.....27
3.2.4. E-İmza ile Elle Atılan İmzanın Karşılaştırılması 28
3.2.4.1.E-İmzanın Elle Atılan İmzaya Denkliği Konusunda Farklı Yaklaşımlar.....28
3.2.4.1.1. Genel Eşitlik.....28
3.2.4.1.2. Sektörel Eşitlik.....28
3.2.4.1.3. Delil Değerinde Eşitlik.....28
3.2.4.1.4. Avrupa Birliğinin Yaklaşımı.....28
3.2.4.1.5. Almanya Örneğinde Kara Avrupası Hukuk Sistemi ve Amerika Örneğinde Anglo Amerikan Hukuk Sistemindeki Yaklaşımlar.....29
3.3. E-İMZANIN TEKNİK ALTYAPISI VE SİSTEMİN İŞLEYİŞİ.....30
3.3.1. Sistemin Kullanıcılarına Sağladığı Bilgi, Güvenlik ve Hizmetler.....31
3.3.2. Sistemin İşleyişi.....32
3.4. E-İMZANIN HUKUKSAL ALTYAPISI 33
3.4.1.Genel Olarak.....33
3.4.2. UNCITRAL E-İmza Yeknesak Kurallar Taslağı.....34
3.4.2.1.Uygulama Alanı (Kapsam).....34
3.4.2.2. Güvenli E-İmza ve İmza Karinesi.....34
3.4.2.3. Orijinallik Karinesi.....35
3.4.2.4. Hukuki Sorumluluk.....35
3.4.2.4.1. İmza (Aracı) Sahibinin Sorumluluğu.....35
3.4.2.4.2. Onay Hizmeti Sağlayıcının (Onay Kurumunun) Sorumluluğu.....37

DÖRDÜNCÜ BÖLÜM

ELEKTRONİK KAYITLARIN MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ.....39

4.1. TÜRK MEDENİ USULÜNDE İSPAT VE DELİL SİSTEMİ.....39
4.2. GEÇERLİK ŞARTI VE İSPAT ŞARTI OLARAK YAZILI ŞEKİL 40
4.3.ELEKTRONİK KAYITLARIN MEVCUT DELİL SİSTEMİMİZDEKİ DEĞERİ.....41
4.3.1. Kapalı Bilgisayar Sistemleri Bakımından.....41
4.3.2. Açık Ağ (Internet) İşlemleri Bakımından.....41
4.3.3. Değerlendirme.....43
4.3.3.1. Özel Hüküm Sebepleri ve Delil Sözleşmesi.....43
4.3.3.2. Yazılı Delil Başlangıcı.....45
4.3.4. Çözüm Seçenekleri.....46
4.3.4.1.Mevcut Delil Sistemi İçinde Çözüm ve/veya İlgili Kanunda Değişiklik Yapılması.....46
4.3.4.2. Delil Sisteminde Değişiklik Yapılması.....47
4.3.4.2.1. Senet Kavramının Genişletilmesi.....47
4.3.4.2.2. E-İmzanın Bir İspat Aracı Olarak Kabulü ve ETKK Hukuk Grubunca Önerilen E-İmza Kanun Tasarısı.....48
4.3.4.3. Karşılaştırmalı Hukukta E-İmzaya Atfedilen Delil Değeri.....49

BEŞİNCİ BÖLÜM

SONUÇ VE SERMAYE PİYASASI MEVZUATI AÇISINDAN DEĞERLENDİRME.....51

KAYNAKÇA.....55

EK 1 : A) UNCITRAL ELEKTRONİK İMZA YEKNESAK KURALLAR TASLAĞI.....59

B) DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES.....70

EK 2 : DİJİTAL İMZA ÖRNEKLERİ

EK 3 : E-İMZA İLE VERİLEN MÜSTERİ EMRİ ÖRNEĞİNDE ELEKTRONİK İMZANIN İSPAT FONKSİYONU VE ELEKTRONİK İMZA İLE UYUŞMAZLIK ÇÖZÜMÜ 80

KISALTMALAR CETVELİ

AAA : Açık Anahtar Altyapısı
AB : Avrupa Birliği
ABD : Amerika Birleşik Devletleri
ARPA : Advanced Research Project Agency
ATM : Automated Teller Machines
BAKred : Bundesaufsichtsamt für das Kreditwesen
BATİDER : Banka ve Ticaret Hukuku Dergisi
BK : Borçlar Kanunu
bkz. : bakınız
Bs. : Bası
CEFACT : Center for Facilitation of Procedures and Practices for Administration, Commerce and Transport
CONSOB : Commissione Nazionale per le Societa e la Borsa
dn. : dipnot
EDI : Electronic Data Interchange
EFTPOS : Electronic Funds Transfer from the Point of Sale
e-imza : elektronik imza
e-sözleşme : elektronik sözleşme
e-ticaret : elektronik ticaret
ETKK : Elektronik Ticaret Koordinasyon Kurulu
HUMK : Hukuk Usulü Muhakemeleri Kanunu
IOSCO : International Organization of Securities Commissions
ISS : Internet Servis Sağlayıcı
md. : madde
MÖHUK : Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun
OECD : Organisation for Economic Co-operation and Development
örn. : örneğin
par. : paragraf
sh. : sayfa
SPKn : Sermaye Piyasası Kanunu
UNCTAD : United Nations Conference in Trade and Development
UNCITRAL : United Nations Commission on International Trade Law
UNECE : Birleşmiş Milletler Avrupa Ekonomik Komisyonu
WHO : World Trade Organisation
vd. : ve devamı
vs. : ve saire
YK : Yeknesak Kurallar
yuk. :yukarıda

ELEKTRONİK İMZA VE ELEKTRONİK KAYITLARIN MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

GİRİŞ

İnternetin dünya çapında giderek artan ve yaygınlaşan kullanımı, daha düşük maliyetli, daha hızlı ve bilgiye dayanan yeni bir ticaret yöntemi olan elektronik ticareti de beraberinde getirmiştir. Ticaretin her alanında yaşanan bu gelişme, menkul kıymet işlemlerinin elektronik ticarete konu olması bağlamında; yatırımcılar, ihraççılar ve diğer sermaye piyasası kurumlarına da pek çok kolaylık ve avantajlar sağlayarak sermaye piyasalarının gelişimine katkıda bulunacaktır.

Sağlıklı bir sermaye piyasasının en önemli koşullarından biri olan güven unsuru, elektronik ticaretin gelişebilmesi ve kullanıcılar tarafından benimsenebilmesinin de ilk şartıdır. Elektronik ticaretin gerçekleştiği ortamda, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu, kurulacak olan teknik ve yasal altyapı ile garanti edilebilmelidir. Bu şartlar ise elektronik imza ile sağlanabilmektedir. Bu nedenle elektronik imza ile ilgili çalışmalarda ileri bir çok ülke, yasal düzenlemelerde önceliği elektronik imza mevzuatı çalışmalarına vermiştir.

Çalışmamızda, e-ticaret, e-sözleşme ve e-imza kavramları, Avrupa Birliği, IOSCO, UNCITRAL tarafından hazırlanan direktif, rapor, model kanun vs. metinlerine ve çeşitli ülkelerde anılan konularda yapılan yasal düzenlemelere de karşılaştırmalı olarak yer verilerek, hukuki açıdan incelenecektir.

Gelişen teknolojinin getirdiği yeni ticari olanaklar ve yeni güvenlik yöntemlerine karşılık, elektronik kayıtların, senetle ispat esasına dayanan Medeni Usul Hukukumuzun mevcut ispat kuralları karşısındaki delil değeri tartışılacak, sorunun delil sistemimizde değişiklik gerektirip gerektirmediği, çeşitli ülkelerin hukuk sistemlerinde e-imzaya tanınan hukuki statü bağlamında değerlendirilecektir.

Sonuç bölümünde ise ulaşılan sonuçlar sermaye piyasası mevzuatı çerçevesinde değerlendirilerek öneriler getirilecektir.

BİRİNCİ BÖLÜM
INTERNET VE ELEKTRONİK TİCARET

1.1. INTERNET

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[1]. Internetin çıkış noktası, 1957 yılında, ABD Savunma Bakanlığı'nca, savaştan önce veya savaş sırasında haberleşme kanallarının kullanılamayacak şekilde tahrip edilmesi halinde dahi, komuta merkezinden balistik füze üslerine gereken emirlerin verilmesini ve savaşın sevk ve idaresini sağlayacak kesintisiz bir haberleşme sistemi yaratılma amacıyla kurulan ARPA[2] (Advanced Research Project Agency)dır. 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 tasarlanmamış, üzerinde her türlü yeni uygulamaların yapılmasına olanak verecek genel ve esnek bir altyapı olarak planlanmıştır.

1.2. ELEKTRONİK TİCARET

1.2.1.Tanımı

Yukarıda, bilgisayarlar vasıtasıyla oluşturulan iletişim ağlarının, kişilerin, birbirleri ile sınırsız amaç ve içerikte ilişki kurmalarını sağladığı ifade edilmişti. İşte kişilerin, bilgisayarlar ile oluşturulan iletişim ağları aracılığıyla birbirleriyle kurdukları *ticari* ilişkiler, elektronik ticaret (kısaca e-ticaret) olarak adlandırılmaktadır. Daha ayrıntılı bir tanımla 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 işlemlerin tümünü ifade etmektedir[3]. Ticari sonuçlar doğuran veya ticari faaliyetleri destekleyecek eğitim, kamuoyunu bilgilendirme, tanıtım, reklam ve benzer amaçlar için elektronik ortamlarda yapılan işlemler de e-ticaret kapsamında sayılmaktadır[4].

---

[1] GÜRAN/AKÜNAL/BAYRAKTAR/YURTCAN/KENDİGELEN/BELLER/SÖZER: Internet ve Hukuk-Ortak Çalışma, Internet Hukuk Forumu, <http://www.superonline.com/hukuk>

[2] ARPA çerçevesinde kurulmuş olan networkün adı ARPANET'di.

[3] Elektronik Ticaret Koordinasyon Kurulu Raporları, Mayıs 1998, sh.1

[4] Bazı uluslararası örgütlerce yapılan e-ticaret tanımları;

WTO:Mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılması;

1.2.2. Avantajları

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 ve daha az maliyetle gerçekleştirilebilmektedir. Böylece kaynakların daha etkin kullanımı ile toplumsal refahın artmasına katkı sağlanacaktır[5].

E-ticaret, yukarıda belirtilen avantajlarıyla OECD, UNCTAD (United Nations Conference in Trade and Development - Birleşmiş Milletler Ticaret ve Kalkınma Konferansı) ve WTO (World Trade Organisation - Dünya Ticaret Örgütü) gibi uluslararası organizasyonlarca oluşturulmaya çalışılan, daha kolay, uyumlu, ucuz ve hızlı bir uluslararası ticari prosedür için çıkış noktasıdır[6].

1.2.3. Uluslararası Alanda E-Ticareti Geliştirmeye Yönelik Çalışmalar

E-ticaretin gelişimi, ulusal alanda gerekli teknik, idari ve hukuki altyapının oluşturulması için önlemler alınmasını, uluslararası alanda ise açık ağ yapısının küresel olma özelliği nedeniyle, ulusal düzenleme ve uygulamaların, uluslararası ilke, standart ve kurallarla uyumlu olmasını gerektirmektedir. Bu amaçla, e-ticaretin düzenlenmesinde, temel ilkelerde uzlaşma sağlamak ve bu doğrultuda ulusal düzenlemelere yön vermek üzere, Avrupa Birliği, UNCITRAL (Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu), OECD, ICC gibi uluslararası örgütlerce elektronik ticaret önündeki hukuki engellerin ortadan kaldırılması ve elektronik ticaretin gelişimi için daha güvenli ve uyumlu bir hukuki ortamın oluşturulmasına yönelik direktif, model kanun, tavsiye ve raporlar hazırlanmış ve hazırlanmakta olup, bu hususlaki çalışmalar sürekli geliştirilmektedir.

OECD: Sayısallaştırılmış yazılı metin, ses ve görüntünün işlenmesi ve iletilmesine dayanan, kişileri ve kurumları ilgilendiren tüm ticari işlemler
(bkz. <http://www.etkk.gov.tr/genel bilgiler.htm> (par.8))

[5] İNCE Murat:Elektronik Ticaret:Gelişme Yolundaki Ülkeler İçin İmkanlar ve Politikalar, Mart 1999, sh.19, <http://ekutup.dpt.gov.tr/ticaret/incem/eticaret.html>.

[6] İNCE, M.: sh.7.

İKİNCİ BÖLÜM
ELEKTRONİK SÖZLEŞMELER

2.1.KAVRAM VE TANIM

Ticaretin hukuk altyapısı ve icra aracı sözleşme kurumudur. Bu bağlamda, e-ticaret de, e-sözleşmeler vasıtasıyla yapılır[7]. Elektronik sözleşme (e-sözleşme) kavramı, Avrupa Parlamentosu ve Konseyi'nin 8.6.2000 tarih ve 2000/31/EC sayılı Elektronik Ticaret Direktifi[8]'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 (conclude) sözleşmelere izin vermesini ve

Özellikle sözleşme usulüne uygulanacak hukuki şartların, e-sözleşmelerin kullanılmasında engel yaratmayacak ve bu sözleşmelerin, 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.

Elektronik sözleşme, doktrinde genellikle EDI (electronic data interchange-elektronik veri değişimi), e-mail (electronic mail - elektronik posta), web sayfası ve usenet kullanılarak yapılan sözleşmeler olarak tanımlanmaktadır[9]. 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[10]. Bununla beraber EDI, zamandan ve işlem maliyetlerinden tasarruf sağladığından ve bilgilerin elektronik ortamda değişimi nedeniyle insan hatalarını ortadan kaldırdığından, e-ticaretin temel araçlarından biri

[7] SÖZER, Bülent: Elektronik Ticaret/Elektronik Sözleşmeler, "TÜSİAV İstanbul Sohbetleri"nde Sunulan Tebliğ (Metni), 21.6.2000, İstanbul, sh.3.
[8] OJ L 178, 17.7.2000
[9] HANCE and BALZ: Business ans and Law on the Internet, 1996 (translated from French by S.D. Balz), 151 ff., 164; SMITH; Internet Law and Regulation, 2nd Edition, London 1999, 208.
[10] GÜRAN/AKÜNAL/BAYRAKTAR/YURTCAN/KENDİGELEN/BELLER/SÖZER: Bölüm II, Par. 3, SÖZER: sh.3, 4.

olarak kabul edilmekte olup, bu konuda çeşitli uluslararası örgütlerce birçok düzenleme yapılmıştır[11].

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[12]. Ancak kanımızca, e-mail ile yapılan sözleşmeler de, ileride görüleceği üzere 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.

E-sözleşmeler yaygın olarak World Wide Web üzerinden websiteleri yoluyla gerçekleştirilmektedir. Web siteleri vasıtasıyla yapılan sözleşmelerde, bir mal veya hizmet arzında bulunmak isteyen (satıcı) taraf, bir server (digital bilgilerin saklandığı bir manyetik ortam) vasıtasıyla, satmak istediği malı veya sunmak istediği hizmeti sergiler, tanıtır. Burada satıcı taraf, işlemin her yönü bakımından "computerised" durumdadır[13]. Satıcının satım iradesi, satıcı yerine server tarafından açıklanır. E-sözleşmelerin bu şekli, EDI'den farklı olarak, açık ağlar üzerinden yapılır. Dolayısıyla, (EDI'den farklı olarak), taraflar arasında, ticari işlemin ve veri değişiminin nasıl yapılacağını düzenleyen, önceden yapılmış bir anlaşma yoktur. Zira e-ticaret, daha önce karşılıklı ticari ilişkiye girmemiş taraflar arasındaki, bir kereye mahsus ticari ilişki olarak düşünülmüş olup, giderek bu yönde gelişmektedir. Diğer bir ifadeyle, e-ticaret, erişim kısıtlaması ve kullanım kontrolü olmayan internet, yani açık ağ üzerinden yapılmaktadır. Ancak bununla beraber e-ticaret alanında yapılan bazı düzenlemelerde[14], tarafların önceden mevcut sözleşmesel kurallar ve prosedür ile bağlandıkları "kapalı" ağ ortamları da e-ticaret kapsamına dahil edilmekte ve e-ticaret için oluşturulan asgari kuralların bu ortamda yapılan sözleşmelere de uygulanacağı öngörülmektedir.

---

[11] Avrupa Komisyonu 'nun EDI anlaşmaları hakkındaki 19.10.1994 tarihli Tavsiye Kararı; UNCITRAL'in EDI Çalışma Grubu'nca 1993 yılında ilki sunulan çalışma ve raporlar ile EDI'ye İlişkin Temel Hukuki Kavramlar Model Kanun Taslağı çalışmaları; UNECE (CEFACT), 1991 yılından beri yaptığı çalışmalar sonucunda bir model anlaşma hazırlamıştır.

[12] SÖZER; sh. 4.

[13] GÜRAN/AKÜNAL/BAYRAKTAR/YURTCAN/KENDİGELEN/BELLER/SÖZER:Bölüm II, E-Contract, (par. 3).

[14] Report of the UNCITRAL Working Group on Electronic Commerce Thirty-Sixth Session, New York, 14-25 Feb. 2000, General Remarks, <http://www.uncitral.org/english/sessions/wg_ec/index.htm> (par.16).

2.2. E-SÖZLEŞMELERİN KURULMASI VE HÜKÜMLERİ

Elektronik sözleşmelerin kurulması ile, tarafların sözleşmeyi ifa yükümlülüğü doğar. Bu nedenle sözleşmenin kurulduğu ânın tespiti önemlidir. Sözleşmenin uygulanma yükümlülüğünün doğması halinde ise, uygulanacak hukukun ve sözleşmenin yapıldığı yer de dahil olmak üzere, bazı faktörlerin tespiti gerekmektedir.

Elektronik sözleşmeler her ne kadar klasik haberleşme araçları dışında, elektronik iletişim tekniği kullanılarak yapılsa da, sözleşmenin kurulması, Borçlar Kanunu'nun akdin in'ikadına (sözleşmenin kurulması) ilişkin 1. ve 10. madde hükümleri çerçevesinde değerlendirilebilecektir. BK'nun 1. maddesine 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[15].

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.

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 sözleşmeler gibi, satıcı tarafından kesin ve yazılı bilgi verilmesini gerektiren sözleşmelerde önemli problemler doğacaktır.[16]

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,

---

[15] EREN, Fikret: Borçlar Hukuku Genel Hükümler, C.I, 4. Bs., Ankara 1991, sh. 290; TEKİNAY/AKMAN/BURCUOĞLU/ALTOP: Borçlar Hukuku, Genel Hükümler, 6. Bs., İstanbul 1988, sh.99.

[16] ROWE Heather/HAFTKE, Mark: A Practitioner's Guide to The Regulation of The Internet, 1999/2000 Ed., sh.80.; Benzer bir nedenle, AB'nin E-Ticaret Direktifi'nde; Üye Devletlerin, hukuk sistemlerini elektronik araçlarla tamamlanan sözleşmelere izin verecek şekilde düzenlemeleri öngörülmekle beraber, *üye devletlerin, hukuk sistemlerinde, taşınmazlara ilişkin olarak kira dışındaki hakların doğumu ve devrine ilişkin sözleşmeler; mahkemeler, kamu otoriteleri veya kamu otoritesini idare eden uzmanların katılımını gerektiren sözleşmeler ve aile hukuku ve miras hukukuyla ilgili sözleşmelerin elektronik araçlarla yapılmasına (e-sözleşmelere konu edilmesine) izin vermeyebilecekleri* öngörülmüştür.

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. 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, Borçlar Kanunu'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 7/III gereğince, bu web sitesinde icapta bulunulduğu kabul edilebilir[17]. 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. Yabancı yazarlar genellikle web sitesi yoluyla yapılan beyanları icaba davet olarak kabul etmektedirler[18].

Öte yandan, mal veya hizmetin bir web sitesinde satılmak üzere sergilenmesinin icap mı icaba davet mi olduğununun, 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[19].

E-sözleşmenin kurulduğu an ile hüküm ve sonuçlarını doğurduğu anın tespiti de önemlidir ve bunun tespit edilebilmesi için Borçlar Kanunumuzun kabul ettiği teorinin dikkate alınması gereklidir.

---

[17] bkz. aynı görüşte GÜRAN/AKÜNAL/BAYRAKTAR/YURTCAN/KENDİGELEN/BELLER/SÖZER: Bölüm II, E-Contract, Sözleşmenin Kurulması; SÖZER: sh. 5.

[18] ROWE/HAFTKE: sh.81, Örn. İngiliz Hukukunda dükkanda mal teşhiri icap değil, icaba davet olarak kabul edilir. Bu nedenle bir websitesinde mal ve hizmetlerin reklamının ve sergilenmesinin icap mı icaba davet mi olduğu tam olarak belli değilse, icaba davet olarak kabul edilir. Bu noktadan hareketle, alıcının satıcıya cevabı icap olarak kabul edilir. Sözleşmenin kurulabilmesi için alıcı tarafından yapılacak teklifin, satıcının standart şartlarına atfen yapılması gerekmektedir. Alıcı, aksi taktirde satıcının yapılan teklifi kabul etmeyebileceği hususunda bilgilendirilmelidir. Ayrıca bkz. SÖZER: agç, s.5, dn. 19.

[19] 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.

2.2.1. E-sözleşmelerin Kurulduğu An

Sözleşmelerin kurulduğu anı açıklayan bir çok teoriler bulunmaktadır. Bu konuda Türk Borçlar Kanunu'nun kabul ettiği teoriye göre, sözleşmenin kurulduğu anın tespitinde, icabın 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[20]. Borçlar Kanunu, 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 (instantaneous) müzakere yapma imkanının olduğu chat ve internet üzerinden sesli mesajlarla gerçekleştirilen sözleşmeler de hazırlar arası 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.

Bir sözleşmenin kurulmasına yönelik icap ve kabulün yapıldığı taraflar arasında yer ve zaman unsurlarının bulunması halinde hazır olmayanlar arasındaki (gaipler arasındaki) sözleşmelerden bahsedilir. BK. md. 5 uyarınca 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 İnternet Servis Sağlayıcıları (İSS) aracılığıyla iletilmesi ve bu aracıların ise tarafların müstahdemi olmaması sebebiyle tarafların hakimiyet alanı olarak kabul edilemeyeceği görüşü mevcuttur. Bilginin, icapta bulunan tarafından İnternet Servis Sağlayıcının mail serverından alınması anında sözleşmenin kurulacağının kabulü halinde ise, Borçlar Kanunumuzun benimsediği ulaşma teorisinden farklı olan öğrenme teorisinin kabulü söz konusu olur[21]. E-sözleşmelerle ilgili olarak, internetin geleneksel posta servislerinden farklılığından kaynaklanan bu gibi tartışmalar ülkemiz dışında, başka hukuk sistemlerinden de mevcuttur[22].

---

[20] EREN: C.I, sh. 313.
[21] SÖZER: sh. 7.
[22] E-mail vasıtasıyla kurulan sözleşmelerde, internet ortamının değişkenliği, altyapısının geleneksel posta servislerine nazaran güvenilmezliği, tarafların internet bağlantılarının sürekli veya geçici olması gibi sebeplerle, benzer tartışmalar gönderme teorisinin kabul edildiği İngiliz Hukukunda da yapılmaktadır. Bu konuda yaygın kanaat icabın ödemede bulunuluncaya kadar kabul edilmiş sayılmayacağı yönündedir. (bkz. ROWE/HAFTKE: sh. 82, 83).

2.2.2. E-sözleşmelerin Hüküm ve Sonuçlarını Doğurmaya Başladığı An

Hazırlar arasındaki sözleşmeler, hüküm ve sonuçlarını kabul iradesinin açıklandığı, diğer bir ifadeyle akdin kurulduğu anda doğurur. 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 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.

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[23].

Avrupa Birliği'nin 8.6.2000 tarih ve 2000/31/EC sayılı Elektronik Ticaret Direktifi'nin 11. maddesine 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.

[23] Nakleden SÖZER: sh. 8.

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.

2.3. E-SÖZLEŞMELERİN KATILMA SÖZLEŞMELERİ OLMASI

E-sözleşmelerin, satıcı tarafından belirlenen standart şartları içeren katılma sözleşmeleri (iltihaki sözleşmeler) olduğu kabul edilmektedir. Bu tür sözleşmelerde, akdin içeriğinin tamamı ya da belirli bir kısmı daha önce taraflardan biri ya da üçüncü kişi tarafından belirlenmiş olup, taraflar arasında sözleşmenin şartları ile ilgili olarak görüşme imkanı bulunmamaktadır. Bu sebeple sözleşmenin diğer tarafı, sözleşmeyi ya kendisine sunulan şartlarda kabul edecek veya sözleşmeyi yapmaktan vazgeçecektir[24].

E-ticarette de, özelllikle 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[25]. Ayrıca iltihaki 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[26]. Bu sebeple bu sözleşme türünde icaba davet söz konusu değildir[27].

Bu noktada, tüketiciyi koruma düzenlemeleri de gözönünde bulundurularak, tüm standart şartların alıcının dikkatine yeterli olarak sunulması, tüm şartlar açıkça görülebilecek bir şekilde web sitesinde yer almalıdır.

2.4. E-SÖZLEŞMELERE UYGULANACAK HUKUK

Açık ağlar üzerinden gerçekleştirilen e-sözleşmelerin taraflarının genellikle farklı ülkelerde bulunması nedeniyle, bu sözleşmelerin uluslararası sözleşme özelliği taşıması ihtimali çok yüksektir. Bu durumda, e-sözleşmeden doğan hukuki ihtilaflara

---

[24] EREN, F.: C.I, sh. 277.

[25] GÜRAN/AKÜNAL/BAYRAKTAR/YURTCAN/KENDİGELEN/BELLER/SÖZER: Bölüm II, E-Contract, Sözleşmenin Kurulması, İcap-Kabul, son par.

[26] SÖZER; s.6.

[27] Ancak web sitesinde yapılan mal ve hizmet sunuşunun icaba davet olduğunun kabul edildiği İngiliz Hukukunda dahi, satıcı tarafından websitesinde sunulan icaba davette, satıcının, mal ve hizmetler için alıcılar tarafından kabul edilemez şartlarda icapta bulunulmasını istemediği için, icabın yapılabileceği şartları belirleyeceği ve tabi olacağı usulü kontrol edeceği kabul edilmektedir. Her bir icabın birbirinden farklı ve müzakereye açık olması halinde dahi, websitesi sahibinin, icabın sunuluş usulünde birörneklik (yeknesaklık) sağlamak isteyeceği ve bunun ise, web sitesine erişimde standart formların kullanımı ve icapta bulunulan ticari işlemin standart şartlara tabi olması ile mümkün olacağı, diğer bir ifadeyle e-sözleşmelerin standart şartlara dayanan sözleşmeler olduğu kabul edilmektedir. (bkz.ROWE/HAFTKE: sh. 81 vd.).

hangi hukukun uygulanacağı, diğer bir ifadeyle e-sözleşmelerin kanunlar ihtilafı hukuku boyutu gündeme gelecektir[28].

2.4.1. Yabancı Unsur İçeren E-Sözleşmeler

Yabancı unsur içeren sözleşmelere uygulanacak hukuk, Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun'un 24. maddesinde düzenlenmiştir. Maddenin ilk fıkrasında, sözleşmeden doğan borç ilişkilerinin tarafların açıkça seçtikleri hukuka tabi olacağı öngörülmektedir. Taraflar, aralarındaki sözleşmeye uygulanacak hukuku seçmemişlerse, borcun ifa edileceği yerin hukuku, ifa yerinin birden fazla olması halinde borç ilişkisinin ağırlığını teşkil eden edimin ifa yeri hukuku, bu yerin de tespit edilemediği hallerde sözleşmenin en yakın irtibat halinde bulunduğu yer hukuku uygulanır. (MÖHUK md. 24/II)

2.4.1.1.Taraflarca Belirlenen Hukuk

MÖHUK md. 24 hükmünün ilk fıkrasında düzenlenen hukuk seçimi kuralı, özellikle taraflarından biri tüketici olan e-sözleşmelere, gerek sistemin teknik özelliği bakımından e-sözleşmenin genellikle hukuk seçimine imkan veren bir şekilde gerçekleşmemesi, gerek tüketicinin elektronik olarak doldurduğu sipariş formu üzerinde standart bir hukuk seçimi şartı bulunsa dahi, tüketicinin sözleşmeye yönelmiş esas akit iradesinin, hukuk seçimi şartını da kapsamayacağı, dolayısıyla hukuk seçimi şartının varlığı ve hukuki geçerliğinin tartışılır olması nedenleriyle, uygulanamamaktadır[29].

2.4.1.2. Borç İlişkisinin Ağırlığını Teşkil Eden Edimin İfa Yeri Hukuku

Milletlerarası özel hukukta mevcut yaygın görüş uyarınca, satım akitlerinde borç ilişkisinin ağırlığını teşkil eden edim satıcının teslim borcudur. Bu nedenle, e-sözleşmelerde satıcının teslim borcunu ifa etmesi gereken yer hukuku önemlidir. Buna göre konusu maddi mal satımı olan e-sözleşmelerde, tarafların ifa yeri konusundaki ortak iradesinin tüketicinin gösterdiği açık adres olduğu, dolayısıyla tüketicinin mutad meskeninin bulunduğu yer hukukunun uygulanacağı kabul edilmektedir. Sözleşmenin konusu dijital bir mal ise (bilgi, belge, yazılım, ses vs.) akdin ifa edileceği yer konusunda, tarafların ortak ve açık iradesinden muhtemelen bahsedilemeyecek, taraf iradeleri her bir tarafın bulunduğu yere yönelmiş olacaktır. Bu durumda tarafların ortak ve açık iradesinin araştırılmasını öngören yorum kuralını içeren Borçlar Kanunu md. 73/f.II,b.2 hükmünde öngörülen, borcun doğduğu anda borçlunun mukim olduğu yer hukuku, e-sözleşmeler bakımından da karakteristik

[28] GÜNGÖR, Gülin: "Internet Yoluyla Girişilen Elektronik Tüketici Akitleri ve Milletlerarası Özel Hukukta Tüketicinin Korunması", Ankara Universitesi Hukuk Fakültesi Dergisi, C.46 (1997), S.1-4, sh.105 vd.
[29] GÜNGÖR: sh.110, 111.

edim borçlusu olan satıcının teslim borcunun doğduğu anda onun mukim bulunduğu yer hukuku uygulanacaktır. Ancak bu kuralın satıcının alıcıya yönelmediği, alıcının satıcıya yöneldiği hallerle sınırlı olarak uygulanması tüketicinin korunmasına daha uygundur.

2.4.1.3. Sözleşme ile En Yakın İrtibatlı Hukuk

Sözleşmeyle en yakın irtibatlı hukuk, akit ve taraflarla en yakın irtibatlı hukukun araştırılmasını öngörür ve taraflarından biri tüketici olan e-sözleşmeler bakımından, her zaman tüketicinin mutad meskeni sonucunu vermeyebilir. Bu nedenle tüketicinin korunmasına hizmet edecek hukukun tayininde bağımsız bir bağlama kuralı olarak kabul görmemektedir.

2.4.2 Taraflarından Biri Tüketici Olan ve Milletlerarası Özel Hukukun Tüketiciyi Koruma Amacının Bulunduğu E-Sözleşmeler

Son yirmi yıldan beri, koruyucu milletlerarası yetki kuralları ve koruyucu bağlama kuralları öngörülmek suretiyle, milletlerarası özel hukuk kuralları ile tüketicinin korunması sağlanmaktadır. Koruyucu bağlama kurallarında, *tüketicinin mutad meskeninin,* tüketicinin milletlerarası korunmasına hizmet eden bağlama noktası olduğu kabul edilmektedir[30].

2.4.2.1. Tüketicinin (Fiziki Olarak) Mutad Meskeni Ülkesinde Bulunması

Tüketicinin kendi mutad meskeninin bulunduğu ülkede taraf olduğu sözleşmeler (home deal), tüketiciyi koruma amacının bulunduğu sözleşmeler olup, milletlerarası tüketiciyi koruyucu bağlama kuralları, ancak bu sözleşmelere uygulanabilir. Koruyucu bağlama kuralları, akdin kurulmuş sayıldığı yeri değil, tüketicinin fizik varlığı bakımından sözleşmeye giriştiği yeri dikkate almaktadır. Telefon, tele-fax gibi araçlar vasıtasıyla kurulan akitlerde, her iki tarafın fizik olarak bulunduğu ülkede sözleşmeye taraf olduğu kabul edildiği gibi, telefon hatları aracılığıyla internet erişimi sağlanan hallerde de, tüketicinin, fizik olarak mutad meskeninin bulunduğu ülkede sözleşmeye taraf olduğu kabul edilebilir. Bu noktadan hareketle, tüketicinin taraf olduğu e-sözleşmeler bakımından da, tüketici, sanal olarak mutad meskeninin bulunduğu ülkeden ayrılmış, sanal bir ifa yerinde sanal bir ifa elde etmiş olsa da, karşı tarafın tüketiciye veya onun mutad meskeninin bulunduğu ülkeye ticari olarak yönelmiş olması ve tüketicinin de mutad meskeninin bulunduğu ülkede e-sözleşmeye girişmiş, diğer bir ifadeyle akdin kurulması için

[30] Buna göre, tarafların uygulanacak hukuku belirlemeleri halinde (subjektif bağlama metodu), tüketicinin mutad meskeni hukukunun daha iyi koruma sağlaması şartıyla, seçilen hukukun uygulama alanı tüketicinin mutad meskeni hukuku ile sınırlandırılmaktadır. Objektif bağlama metoduna başvurulduğu hallerde ise, sözleşmeye tüketici ile en sıkı irtibatlı hukuk olduğu kabul edilen tüketicinin mutad meskeni hukukunun maddi hukuk kuralları uygulanmaktadır. (GÜNGÖR: sh.103, 104).

kendisinin tamamlaması gereken hukuki safhaları fizik varlığı itibariyle orada (bulunduğu yerde) tamamlamış olması şartıyla, koruyucu bağlama kurallarının sağladığı hukuki himayeden yararlanmasına bir engel yoktur[31].

2.4.2.2. Ticari Yönelme

Tüketici, e-sözleşmeye kendi mutad meskeninin bulunduğu ülkede, sözleşmenin karşı tarafının, e-mail, reklam vs. yollarla, ticari olarak ve bilerek kendisine yönelmesi üzerine taraf olduysa, koruyucu hukuk kurallarının sağladığı hukuki korumadan yararlanabilir. Buna karşılık tüketici, bir yerel ağdan diğerine atlayarak satıcıyı kendisi bulmuş, satıcıya yönelmiş ise, milletlerarası özel hukukun koruma amacının bulunmadığı kabul edilerek, tüketicinin taraf olduğu e-sözleşme, koruyucu bağlama kurallarının değil, akitleri idare eden genel bağlama kurallarının konusu olacaktır.

Ancak önemle ifade etmek gerekir ki, milletlerarası özel hukukun tüketiciyi koruma amaçlı, tüketicinin mutad meskeni hukuku objektif bağlama kuralı, henüz pozitif kural düzeyinde Türk hukukuna kazandırılmamıştır. Bu bakımdan sorun, MÜHUK md. 24 çerçevesinde değerlendirilmelidir[32].

Öte yandan, kanunlar ihtilafı kurallarının, hukuk sistemlerinin parça parça uygulanmasını öngörmesi ve bu nedenle uluslararası ticaretin gelişimini güçleştirdiği yönündeki kanaatlerle, e-ticaret alanında farklı ulusal hukuk sistemlerinin harmonizasyonu amacıyla bir takım girişimlerde bulunulmuş olup, Avrupa Birliği E-Ticaret Direktifi de anılan amaca hizmet eden bir düzenlemedir[33]. Ayrıca 20.5.1997 tarih ve 97/7/EC sayılı AB Direktifi, mesafe satımı şeklinde gerçekleşen maddi mal satımlarının e-posta yoluyla gerçekleştirilmesi halini de dikkate alarak, üye devletlere, yabancı unsurlu tüketici akitlerinde, tüketiciyi koruyucu nitelikteki adı geçen Direktif hükümlerini bertaraf edici hukuk seçimlerini önleyecek hukuki tedbirler alma yükümlülüğü getirmektedir[34].

2.4.3. Türkiye'de Yerleşik Yatırımcılara Yönelik, Kurul'un İznine Tabi Sermaye Piyasası Faaliyetlerinin Tespitinde Ticari Yönelme Kriteri

Milletlerarası özel hukukun tüketiciyi koruma amacının gerçekleştiği ve tüketicinin mutad meskeni hukukunun uygulanacağı sözleşmelerin tayininde esas alınan bir kriter olan *ticari yönelme* kriterinin, yurt dışında yerleşik kuruluşların, internet üzerinden, Türkiye'de yerleşik yatırımcılara yönelik sermaye piyasası faaliyetlerinde bulunmalarına ilişkin esaslarla ilgili olarak, faaliyetin Türkiye'deki yatırımcılara yönelik olup olmadığının tespitinde de kullanılabileceği kanaatindeyiz. Zira Türkiye'deki yatırımcılara yönelmiş bir sermaye piyasası faaliyeti, yatırımcıların

[31] GÜNGÖR: sh.106.
[32] GÜNGÖR: sh. 119.
[33] ROWE/HAFTKE: sh.94 vd.
[34] bkz. GÜNGÖR: sh.111, dn.27.

korunması amacı ile, Türkiye'deki yatırımcıların mutad meskeni hukuku olan Türk sermaye piyasası mevzuatı gereğince Sermaye Piyasası Kurulu'ndan alınacak izne tabi olacaktır.

Bu hususta, Almanya Federal Bankacılık Denetim Kurumu BAKred'in, Internette Yabancı Yatırım Projelerinin Pazarlanması Hakkındaki Rapor'unda da, internetteki menkul kıymet arzları ve alım-satımların etkin bir şekilde denetlenebilmesi amacıyla, yabancı bir kurumsal yatırımcının Federal Bankacılık Denetim Kurumuna önbildirimde bulunmaksızın Almanya'da halka arzda bulunamayacağı öngörülmüştür. BAKred, açıkça ve doğrudan Alman yatırımcılara hitap etmeyen, yabancı dilde yazılmış web sayfalarını Almanya'da halka arz, ilan veya reklam saymamakta, ancak bu sayfalar Almanya'da bulunan adres ve bağlantıları içeriyorsa ya da özellikle Alman yatırımcılara yönelik olduğu başka bir şekilde belirtiliyorsa Almanya'da halka arz saymaktadır. Bu kapsamda Almanya'daki yatırımcılara, bu yatırımcıların talebi olmaksızın gönderilen e-mailler de, Alman yatırımcılara yönelik olmadığı anlaşılsa bile, Almanya'da halka arz sayılmaktadır[35].

İtalya'da ise, CONSOB'un Temmuz 1999'da duyurduğu, *yatırımcı hizmetleri ve finansal araçların internet vasıtasıyla arz ve talebi faaliyetlerine ilişkin metin*de, internet vasıtasıyla yapılan sermaye piyasası faaliyetlerinin hangi durumlarda İtalya'da yapılmış sayılacağı da belirlenmiştir. Buna göre, e-mail vasıtasıyla yapılan arz ve alım –satım faaliyetlerinde e-mailin gönderildiği kişi İtalya'da ikamet ediyorsa veya bu arz ve alım - satım faaliyetini içeren web sitesi İtalya'da ikamet eden kişilere yönelikse sözü edilen faaliyetler İtalya'da yapılmış sayılır. CONSOB bir web sitesinin İtalya'da ikamet eden kişilere yönelik olup olmadığının tespitine ilişkin unsurları, web sitesinin içeriği ve diğer koşulları da dikkate alarak ayrıntılı olarak belirlemiştir[36].

[35] VON ILBERG, P., BENZLER, M.: "Statement Issues on Internet Marketing of Foreign Collective Investment Schemes", World Securities Law Report, 1999, Volume 5, No.1, sh.7,8.
[36] "CONSOB Clarifies Solicitation and Placement Through the Internet", International Financial Law Review, 1999, Volume Xviii, No:7, sh. 55, 56.

ÜÇÜNCÜ BÖLÜM
ELEKTRONİK İMZA

3.1. KAVRAM VE TANIM

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.

E-imza, kimliğini ve mesaj içeriğine onay verildiğini göstermek amacıyla bir kimse tarafından (veya onun namına) mesaja eklenen veya mantıksal olarak mesaja bağlı olan elektronik bilgidir. Başka bir tanımda[37] 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.

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, uluslarası ticaretin gelişimine yönelik olarak paralel düzenlemeler yapılmasını teşvik etmek amacıyla hazırlanan *"Draft Uniform Rules on Electronic Signatures"*[38] (*Elektronik İmza Yeknesak Kurallar Taslağı)'*nın (Ek:1) 2. 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.

Avrupa Birliği'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 December 1999 on a Community framework for electronic signatures"[39] (Elektronik İmzalar için Ortak Altyapıya Dair Avrupa Parlamentosu ve

---

[37] Elektronik Ticaret Hukuk Altyapısı, Etkk, <http://www.igeme.org.tr/tur/etrade/etkk/hukuk/haltyapi.htm> (par.2).

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

[39] 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).

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"[40] (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.

3.2. E-İMZANIN AMACI VE İŞLEVİ

3.2.1. E-İmzanın Amacı

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. Bonn Bakanlık Bildirgesi'nde bir e-imza çeşidi olan digital (sayısal) imzanın, e-ticaretin anahtarı olarak kabul edilmesi gerektiği ifade edilmiştir[41].

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 irdelenecek, daha sonra e-imzanın işlevleri elle atılan imzanın işlevleri ile karşılaştırmalı olarak incelenecektir.

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

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

[41] Proposal for a European Parliament and Council Directive on a Common Framework for Electronic Signatures, Explanatory Memorandum, <http://www.ispo.cec.be/eif/policy/com98297.html>, (par.4).

3.2.2. Kağıda Dayanan Geleneksel Sistemde Elle Atılan İmzanın İşlevleri

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.

3.2.2.1. İmza Sahibinin Kimliğini Gösterme (Kimlik Tespiti) İşlevi

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[42].

3.2.2.2. Tarafları, İmzaladıkları Sözleşme ile Bağlayıcı Bir Muameleye Giriştikleri Konusunda Uyarma İşlevi

İmza sahibi, imzaladığı belgenin içeriği ile bağlanma isteğini ortaya koyar. İmza, aynı zamanda, belgeye (ve içinde yer akan iradeye) son şeklinin verildiğini teyidi ve uyarısı anlamındadır.

3.2.2.3. İmzalanan Metindeki İradenin, İmzalayanın Gerçek, Nihai ve Kesin İradesi Olduğunu Gösterme İşlevi (Onaylama İşlevi)

İmza, bir belgedeki beyan ve yüklenimlerin sağlıklı olduğunu göstermek için o belgenin altına o kişinin (imzalayan), adı için kullandığı, karakteristik biçimde koyduğu yazıdır[43]. İmza ile, imzalayan kimse iradesini kesin olarak açıklamış olur[44].

3.2.2.4. İspatta Güvenlik ve Kolaylık Sağlama İşlevi (İspat İşlevi)

İmzanın el yazısıyla olmasından amaç, imzalayanın, imzayı şahsen ve bizzat atmasıdır[45]. 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

[42] TUNÇOMAĞ, Kenan:Türk Borçlar Hukuku, C.I, Genel Hükümler, İstanbul 1976, sh.222; EREN; sh.326; ALTAŞ: Hüseyin; Şekle Aykırılığın Olumsuz Sonuçlarının Düzeltilmesi, Ankara 1998, sh.74 vd.
[43] YILMAZ, Ejder: Hukuk Sözlüğü, Ankara 1985, sh. 333.
[44] TUNÇOMAĞ, Kenan: sh.222; EREN: C.I, sh.326; ALTAŞ: sh. 64-67.
[45] EREN; C.I, sh.339.

şeklindeki iddiası, HUMK md. 308 ve devamı hükümlerinde düzenlenen usullerle araştırılabilmektedir. Bu husus imzanın ispat işlevine işaret etmektedir.

3.2.3. E-imzanın İşlevleri

E-imzanın işlevlerini, e-imza tanımından çıkartmak mümkündür. Buna göre e-imza aşağıdaki işlevleri yerine getirmektedir:

3.2.3.1. İmza Sahibinin Kimliğini Tanımlama (Kimlik Tespiti) İşlevi

E-imza, elektronik olarak gönderilen bir verinin göndericisinin kimliğini belirlemeye yarar. Elektronik kimlik tespiti yöntem ve araçları çok çeşitlidir. Bunlar kullanılan teknolojiye göre sınıflandırılabilir.

3.2.3.1.1. *Biyometri tekniklerinin kullanıldığı yöntem ve araçlar*

Parmak izi, göz retinası ve ses tanıyıcı biyometrik kimlik belirleme tekniklerini içerir.

3.2.3.1.2. *Şifreleme (cyrptography) tekniklerinin kullanıldığı yöntem ve araçlar*

PIN kodu, password (şifre), dijital (sayısal) imza gibi şifreleme teknikleridir.

Yukarıda belirtilen kimlik belirleme mekanizmaları, genellikle kimlik belirlemenin yüksek düzeyde güvenli olmasını sağlamak amacıyla, birleştirilmekte ve birlikte kullanılmaktadır.

Elektronik ortamda kimlik belirlemeye yarayan bu yöntem ve tekniklerin herbiri e-imzanın kimlik belirleme işlevini yerine getirebilmekle beraber, bunların herbirinin, e-imza için aranan, elle atılan imzanın diğer işlevlerini yerine getirme (kişi ve veri arasında ilişki kurma ve hukuki sonuç doğuran bir iradeyi onaylama ve doğrulama) kapasitesine sahip olduğu söylenemez. Bu nedenle bu tekniklerin herbirini elyazısı imzanın geçerli bir alternatifi olarak kabul edilmemektedir[46]. Örneğin kompüterize edilmiş parmak izi tanıma sistemi, scan edilmiş elyazısı imza veya bir kimsenin adının bir e-mailin sonuna işlenmesi, elyazısı imzanın bütün işlevlerini yerine getiremediklerinden, bu gibi kimlik belirleme tekniklerinin e-imza olarak adlandırılması doğru olmayacaktır.

Ancak bu kimlik belirleme tekniklerinden, dijital imza, göndericinin (imzalayanın) kimliğinin açık ve net biçimde teyidi ile beraber, elektronik belgenin

[46] The Legal Aspects of Digital Signatures, Interdisciplinary Centre for Law and Information Technology (ICRI), <http://www.law.kuleuven.ac.be/icri/projects/report.data/executive.html>

orjinalliğini ve güvenilirliğini temin etmek suretiyle e-imzanın aşağıda açıklanan diğer iki işlevini de yerine getirdiğinden, elle atılan imzanın en güvenilir alternatifi olarak kabul edilir[47]. Bu nedenle Avusturya, Finlandiya, Norveç, İsveç, Hollanda, Arjantin ve İtalya gibi birçok devlet ile OECD ve AB gibi uluslararası kuruluşlarca, dijital imzanın hukuki altyapısının gerekliliği kesin olarak tanınmış olup; Almanya, Kanada, ABD, Japonya, Malezya ve Rusya gibi ülkelerde ise spesifik dijital imza düzenlemeleri[48] yapılmış veya düzenleme çalışmaları devam etmektedir.

3.2.3.1.2.1. *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.

Avrupa'da e-imza alanında ilk yasal düzenleme yapan ülkelerden biri olan Almanya'nın Dijital İmza Kanunu[49]'nun 2/1 hükmünde dijital imza şu şekilde tanımlanmıştır: Dijital imza, dijital (sayısal) veri üzerinde, bir özel imza anahtarı (private signature key) ile yaratılan bir mühür anlamına gelir. Bu mühür, ilgili açık anahtarların kullanımı ile, bir onaylayıcının (certifier[50]) veya bu kanunda belirtilen Kurum'un (Authority) imza anahtar sertifikası[51]na eklenmek suretiyle, imza anahtarının sahibinin ve verinin doğruluğunun anlaşılmasını sağlar.

Burada bir e-imza türü olarak dijital imzanın tanımına yer verilmiş olup, birçok devletin e-imza düzenlemesinde esas alınan yaygın ve gelişmiş bir e-imza türü olduğundan, dijital imzaya ilişkin ayrıntılı bilgiler, sistemin işleyişi ile teknik ve yasal altyapı, ilgili bölümlerde yeri geldikçe incelenecektir.

Öte yandan e-imzaya ilişkin bazı uluslararası düzenlemelerde[52], 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

---

[47] The EDI Law Review, Legal Aspects of Paperless Communication, Volume 7/2000, sh.7; The Legal Aspects of Digital Signatures, Digital Signature as Most Effective Alternative, <http://www.law.kuleuven.ac.be/icri/projects/report.data/executive.html>

[48] Örn. Almanya'da 13.6.1997 tarihinde kabul edilerek, 1.8.1997 tarihinde yürürlüğe giren Signaturgesetz (Dijital İmza Kanunu), ABD'nin Missouri eyaletinde Temmuz 1998 'de kabul edilen Digital Signature Act, yine ABD'nin UTAH eyaletinde 1995 yılında kabul edilen Utah Digital Signature Code vs. (Utah Digital Signature Code için bkz. <http://www.jmls.edu/cyber/statutes/udsa.html>)

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

[50] Aynı hükmün 2. bendinde "Certifier", gerçek kişilerin dayandığı açık imza anahtarlarını onaylayan gerçek veya tüzel kişi olup, bu Kanun'un 4. paragrafı uyarınca bir lisans sahibi olarak tanımlanmıştır.

[51] Aynı hükmün 3. bendinde, "Certificate", bir açık imza anahtarının bir gerçek kişiye bağlanmasına ilişkin dijital onay olarak tanımlanmıştır.

[52] 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.

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 (Technology Neutrality) 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 yapılmış bulunan düzenlemelerin, zaman içinde gelişen e-imza teknolojilerinden yararlanamaması tehlikesi karşısında, mevcut düzenlemelerin sık sık güncellenmesi ihtiyacı bertaraf edilmeye çalışılmaktadır.

3.2.3.2. Elektronik Bilgi Mesajının İçeriğindeki Bilginin İmzalayan Tarafından Onaylandığını Gösterme İşlevi

E-imza, eklendiği veri mesajının içeriğinin mesajı gönderen tarafından onaylandığını gösterir. Bu sayede, hukuki sonuç doğuran bir irade beyanını içeren bir veri mesajının içeriğindeki beyan, beyanın sahibi olan imzalayan tarafından kabul edilmektedir. E-imzanın bu işlevinin, elyazısı imzanın, imza sahibinin, imzaladığı belgenin içeriği ile bağlanma isteğini gösterdiğine dair onaylama işlevini karşıladığı söylenebilir.

3.2.3.3. Elektronik Bilgi Mesajının Orijinalliğini ve İmzalandıktan Sonra Değişmediğini Gösterme İşlevi

Elektronik imzanın veri mesajının imzalandığı zamandaki orjinal haliyle gönderilene ulaşıp ulaşmadığını gösterme işlevi "hash function" olarak adlandırılmaktadır. E-imzanın bu işlevi, gönderilen bir mesajın içeriğinin, imzalandığı zamandaki orijinal haliyle gönderilene ulaştığını belirtmektedir. Bu işlev, veri mesajının içeriğinin imzalayan tarafından onaylanması işleviyle yakından ilgilidir. Çünkü imzalandığı zamandaki orijinal haliyle gönderilene ulaşmayan bir mesajın içeriğinin de, imzalayan tarafından onaylanma sonucunu vermesi mümkün olmayacaktır.

3.2.3.4. İspat İşlevi

E-imza ile imzalanarak yapılan sözleşmeler veya diğer hukuki işlemlerde, e-imzanın, yukarıdaki işlevleri yerine getirdiği kabul edilir. Başka bir deyişle, e-imzanın, e-imza ile imzalanan bir bilgi mesajının, e-imzanın sahibi tarafından imzalandığı, imzalayanın mesajın içeriğindeki bilgiyi onayladığı ve mesajın içeriğinin orijinal haline uygun olduğu ispat eder.

3.2.4. E-İmza ile Elle Atılan İmzanın Karşılaştırılması

Kağıda dayanan geleneksel hukuk sisteminde şekle ilişkin geçerlilik ve ispat koşulunun önemli bir parçası olan elle atılan imzanın kimlik belirleme, uyarma, onaylama ve ispatta güvenlik ve kolaylık sağlama işlevleri, e-imza ile büyük ölçüde karşılanabilmekle beraber, e-imzanın elle atılan imza ile hukuki denkliği konusunda farklı yaklaşımlar bulunmaktadır.

3.2.4.1. E-imzanın Elle Atılan İmzaya Denkliği Hususunda Farklı Yaklaşımlar[53]

3.2.4.1.1. Genel Eşitlik (General Equivalence)

Kanunun, bir kağıt belge veya elle atılan imza koşulunu gerektirdiği durumlarda, bu koşul her zaman için elektronik araçlarla da yerine getirilebilir. İtalya'da 15.3.1997 tarih ve 59 sayılı Kanun ile dijital imzanın elle atılan imza yerine kullanılabileceği öngörülerek bu yaklaşım benimsenmiştir. Bu Kanun'un 15. maddesinde elektronik araçların kullanımı hukuken geçerli sayılmaktadır. UNCITRAL E-İmza Taslak Kurallarının 6. maddesinde de, kanunun imzayı koşulunu gerektirdiği yerde, taslağın 2. maddesinde tanımlanan "güvenli e-imza"nın kullanılması halinde, aranan imza koşulunun yerine getirildiğinin kabul edildiği öngörülerek genel eşitlik benimsenmiştir.

3.2.4.1.2. Sektörel Eşitlik (Sectoral Equivalence)

Belirli alanlarda, elektronik belgeleme ve imzanın kullanımını kabul eden belirli usullerin düzenlendiği spesifik kurallar öngörülebilir. İsveç'te, e-imza ve elektronik belgeleme, gümrüğe ilişkin düzenlemelerde kabul edilmektedir.

3.2.4.1.3. Delil Değerinde Eşitlik (Equivalence in Evidence)

Medeni, idari, cezai veya diğer yargılama usullerinde yer alan ispat hukukuna ilişkin genel kurallarda, elektronik belgeler ve imzaların mahkemelerde kullanılabileceği ve kabul göreceği öngörülebilir. Belçika Medeni Kanunu'nda e-imza ile ilgili olarak bu yönde düzenlemeler yapılmıştır.

3.2.4.1.4. Avrupa Birliği'nin Yaklaşımı

30 Kasım 1999 tarihinde Telekomünikasyon Bakanlar Komitesi'ce kabul edilen Elektronik İmzalar için Ortak Altyapıya Dair Avrupa Parlamentosu ve Konseyi Direktifi'nin e-imzanın elle atılan imza karşısındaki statüsü, anılan Taslak Direktif'in

[53] The Legal Aspects of Digital Signatures, Regulatory Intervention by European Member States <http://www.law.kuleuven.ac.be/icri/projects/report.data/executive.html> (par.2).

20. paragrafında düzenlenmiştir. Anılan Paragraf gereğince, elle atılan imza için aranan koşulları yerine getiren gelişmiş e-imzalar (advanced e-signatures[54]), elle atılan imzaya hukuken eşit kabul edilebilir.

Direktifin "E-İmzaların Hukuki Etkileri" başlığını taşıyan 5. maddesinde ise bu doğrultuda, üye devletlerce, nitelikli bir sertifikaya dayanan ve güvenli imzalama aracıyla yaratılan gelişmiş e-imzaların, elektronik formdaki bir veriyle ilgili olarak, elle atılan imzada kağıda dayanan veriye ilişkin olarak aranan koşullarla aynı koşulları karşılaması halinde elle atılan imzanın hukuki sonuçlarını doğurmasını sağlamaya ve bu imzaların, hukuk usulünde delil olarak kabul edilir olmasının teminine yönelik düzenlemeler yapılması gerektiği öngörülmektedir.

Bu çerçevede AB'nin konuya yaklaşımının, e-imzaların, elle atılan imzalarda aranan koşulları gerçekleştirmesi şartıyla, elle atılan imza yerine kullanılması, diğer bir ifadeyle elle atılan imzaya eşdeğer sayılması şeklinde olduğu söylenebilir.

3.2.4.1.5. Almanya Örneğinde Kara Avrupası Hukuk Sistemi ve Amerika Örneğinde Anglo Amerikan Hukuk Sistemindeki Yaklaşımlar

Öte yandan e-imza (dijital imza), bilginin bütünlüğü ve doğruluğu konusunda yüksek ölçüde güvenli delil teşkil edebilecek yeterlikte görülmesi nedeniyle, Almanya'da elle atılan imza koşuluna elektronik ortamda denklik sağlayacak bir alternatif olarak ilgi odağı oluşturmuştur. Bununla beraber 1.8.1997 tarihinde kabul edilen Alman Dijital İmza Kanunu ve Dijital İmza Kararnamesi'nde (Digital Signature Ordinance), dijital imzanın, elle atılan imza ve diğer e-imza türleri ile hukuki denkliği hususu, bu konudaki düzenlemelerin henüz yeni olduğu ve bu düzenlemeler bir süre uygulanarak deneyim elde eldilmesi gerektiği gerekçesiyle irdelenmemiştir. Anılan Kanun'da dijital imzanın kimlik tespitinde (ve bunun ispatlanmasında) kullanılmasına yönelik olarak, dijital imzaların güvenli sayılabilmeleri için aranan genel koşullar ve bütün e-imza türlerinin güvenli kabul edilebilmesini sağlayacak ihtiyari teknik standartlar düzenlemiştir[55]. Öte yandan taraflarca, mahkemeye gidildiğinde, diğer dijital imza standartlarına kanundaki standart ile eşit değer verilmesi konusunda anlaşma yapılmasına bir engel yoktur.

Anglo-Amerikan hukuk sisteminde (Common Law) imza ile ilgili yaklaşım şu şekildedir. İmza tarafın iradesini yansıtıyorsa ve maddi bir şey üzerinde kayıtlı ise, hukuken geçerli imza olarak kabul edilir. Elle atılan imzanın yukarıda belirtilen

[54] Anılan paragrafta gelişmiş e-imzalar (advanced e-signatures), nitelikli bir sertifikaya (a qualified certificate) dayanan ve güvenli imzalama araçları (secure-signature-creation device) ile yaratılan e-imzalar olarak ifade edilmiştir.

[55] KUNER, Christopher/MIEDBRODT, Anja:: Written Signature Requirements and Electronic Authentication:A Comparative Perspective, Written Signatures in The Civil Law (Germany), <http://www.kuner.com/data/sig/signature_perspective.html> (par.8).

işlevleri, Türk hukuk sisteminin de dahil olduğu Kara Avrupası hukuk sisteminde söz konusu olduğu halde, Common Law hukuk sistemine yabancıdır. ABD hukuku, belirli asgari koşullar mevcutsa (örn. elektronik ortam dahil olmak üzere *maddi bir ortamın kullanımı*) taraf iradesine, imza prosedürünün güvenliğinden daha çok önem verir. Bu bağlamda, ABD'nin federal ve federe devlet yasaları, e-imzaların kağıda dayanan imzalarla (elle atılan imza vs.) eşit statüde sayılması gerektiğini kabul eder. Oysa Kara Avrupası sisteminde maddi belge üzerindeki taraf iradesi yeterli görülmemekte, damga, daktilo veya faksla imza elle atılan imza sayılmamaktadır. Elle imzalanan bir belge, imzalanan iradenin imzalayanın kendi iradesi olduğu varsayılarak güvenilir delil teşkil ettiği halde, elle imzalanmayan elektronik bir belge ise güvenilir delil olarak kabul edilmemektedir. Elektronik belgeler sanal delil veya bilirkişi incelemesine göre mahkemece takdir edilen delil sayılmaktadır.

Diğer taraftan elektronik onaylamaya ilişkin politikalarla ilgili olarak da her iki hukuk sistemi arasında imzanın tanımından kaynaklanan farklı yaklaşımlar mevcuttur. Common Law sistemi hukukçuları, yazılı imza kurallarını büyük bir kısmının kaldırılması ve ancak çok sınırlı bir kaç durumda korunması gereken şekil şartı olarak kabul ederken, Kara Avrupası sistemi hukukçuları, yazılı imza kurallarını güçlü bir kamusal role sahip güvenlik koşulları olarak görmektedirler. Bu nedenle Almanya, elektronik onaylamada yüksek düzeyli güvenlik teknolojileri ile kimlik ispatını esas almaktayken, ABD'de kimlikle ilgili olarak daha düşük seviyeli teknolojiler yeterli görülmektedir.

3.3. E-İMZA TEKNİK ALTYAPISI VE SİSTEMİN İŞLEYİŞİ

Yukarıda kimlik belirleme teknolojilerine değinilirken ifade edildiği üzere, e-imzanın kimlik belirleme işlevini yerine getirmede, şifreleme veya biyometri tekniklerine dayanan çeşitli teknolojilerin kullanılabildiği, ancak e-imzada aranan, veri ile kaynağı arasındaki ilişkiyi sağlama işlevinin, her kimlik belirleme tekniği ile sağlanamadığı ifade edilmişti. Bu bağlamda, e-imzanın elle atılan imzaya alternatif olabilmesini sağlayan işlevlerini yerine getirebilecek en elverişli teknik, açık (çift) anahtarlı kriptografi ya da asimetrik kriptografi; en etkin e-imza ise, bu tekniğin kullanıldığı dijital (sayısal) imzadır. Dijital imza, asimetrik kriptografinin kullanılması suretiyle, elektronik mesajların doğruluğunu onaylayan ve bu mesajların içeriğinin bütünlüğünü garanti eden açık anahtarlı kriptografi sistemleri ile yapılan teknolojik uygulamaların adıdır. Dijital imzanın, fail-stop dijital imza, blind imza, undeniable (inkar edilemez) dijital imza gibi pek çok türleri vardır[56]. (EK:2) Dijital imza, elektronik belgeleri elektronik olarak imzalama teknolojisinin özel bir türüdür.

[56] AALBERTS/VAN DER HOF:Digital Signature Blindness, Analysis of Legislative Approaches to Electronic Authentication, <http://cwis.kub.nl/~frw/people/hof/Ds-art2.htm>

Elle atılan imzanın en güvenilir alternatifi olarak kabul edilen dijital imza, e-imzaya ilişkin pek çok ulusal ve uluslararası düzenlemede, kurulacak teknik altyapıda esas alınmış olan bir e-imza türüdür. Bu sebeple sistemin işleyişi, dijital imza, diğer bir ifadeyle açık anahtarlı kriptografi tekniği esas alınarak açıklanacaktır[57].

3.3.1. Sistemin Kullanıcılarına Sağladığı Bilgi, Güvenlik ve Hizmetler:

* ***Göndericinin Doğrulunu Kanıtlama***	Mesajı **Kim** Gönderdi?
* ***Veri Bütünlüğü***	Mesajın içeriğinde **ne** vardı?
* ***İnkar Edilmezlik***	a) Mesajın **gönderildiğinin** b) Mesajın **içeriğinin gerçeğe aykırı olarak inkar edilmesini engelleme**
* ***Zaman Damgası (Pulu)***	Mesaj **ne zaman** gönderildi?
* ***Gizlilik***	**Özel Bilgi**

Bazı açık anahtarlı kriptografik algoritmalar, dijital imzaları sağlama kapasitesine ek olarak, gizlilik hizmeti de sağlar. Ancak burada, dijital imza sağlamaya yönelik asimetrik kriptografi tarafından sağlanan, sadece göndericinin doğruluğunu kanıtlama, veri bütünlüğünü, mesajın gönderildiğini ve içeriğini onaylamaya dair güvenlik hizmetleri esas alınacaktır. Açık anahtar altyapısı (AAA) tek başına mesajın gönderildiği zamana ilişkin zaman damgası güvenlik hizmetini sağlama yeterliliğine sahip değildir. Ancak Onay Kurumu tarafından güvenli bir zaman damgası hizmeti sağlanıyorsa, diğer üç (KİM, NE ve İNKAR EDİLEMEZLİK'e ilişkin) güvenlik hizmeti daha güvenilir hale gelir.

İNKAR EDİLEMEZLİK, KİM ve NE hususlarındaki güvenlik hizmetleri ile aynı konuya ilişkin olmakla beraber, ancak farklı bir bakımdan e-ticaretin hukuksal kuralları bakımından büyük öneme sahiptir. KİM ve NE güvenlik hizmetleri hususunda, gönderici ve alıcı, mesajı bozmak isteyen bir sahteci veya dolandırıcıya karşı, mesajın bütünlüğü ve doğruluğunun teyidini desteklemekte olduklarından, aynı taraftadırlar. İNKAR EDİLEMEZLİK ise, göndericinin ve alıcının bir hukuki uyuşmazlığın farklı taraflarında olduğu noktasından hareket eder[58].

---

[57] Bu açıklamada, Amerikan Barosu Bilim ve Teknoloji Bölümü Bilgi Güvenliği Komitesi'nce, Ağustos 1996 yılında 70'den fazla teknolojist ile dünyanın her yerinden avukatların 4 yıllık işbirliği neticesinde yayınladığı Digital Signature Guidelines'da (Digital İmza Kılavuzu) tanımlanan açık imza altyapısı esas alınmaktadır. Kılavuz, ticaret hukukunun hukuki prensipleri ile asimetrik kriptosistemin güçlü teknolojik kapasitelerini birleştiren bir açık imza altyapısı sistemi tanımlamaktadır.

[58] MERRILL, C.:Proof of WHO, WHAT and WHEN in Electronic Commerce, Delivering Security Services A Merger od Technological and Legal Viewpoints, <http://abanet.org/scitech/ammerr.html>

3.3.2. Sistemin İşleyişi

Açık anahtar kriptografisi, birbirinden farklı, ama matematiksel olarak birbiriyle ilişkili iki anahtardan oluşan bir anahtar çifti kullanır. Anahtarların biri, şifrelemede/bilgiyi dönüştürmede kullanılırken, diğer anahtar deşifre etmede/orjinal şekline dönüştürmede kullanılır.

Anahtarlardan biri, gizli anahtar (private key) olarak adlandırılır. Sahibi tarafından gizli tutulur ve kimse ile paylaşılmaz. Diğer anahtar, açık anahtar (public key) olarak adlandırılır. Bu anahtara on-line olarak herkes tarafından ulaşılabilir. Açık anahtarın bilgisinden, hesaplama yoluyla, gizli anahtarın bilgisine ulaşmak olanaksızdır. Bu düzenleme, INKAR EDİLEMEZLİK'i güçlü bir şekilde desteklemektedir. Zira gizli anahtarın açığa çıkmasının tek nedeni, sadece gizli anahtarın bilgisine sahip olan veya açık anahtarı elinde tutma iznine sahip olan (yetkili) kişi olmalıdır.

Kriptografik yazılımı kullanarak, bir mesajı (bu, kağıda dayanan kayıt olmayıp bilgisayar tabanlı kayıttır) imzalayan, mutlaka, göndericinin gizli anahtarını ve mesajı dijital imzaya dönüştürürken tek yönlü "hash" işlevini[59] kullanacaktır.

Dijital imzayı alan ve ona güvenme durumunda olan tarafa, güvenen taraf (relying party) denir.

Güvenen taraf, dijital imzanın, açık anahtara uyan gizli anahtar ile yaratıldığını doğrulamak için göndericinin açık anahtarını kullanır. Mesaj, imzalandığı sırada tek yönlü "hash" ile dönüştürüldüğünden, doğrulama, mesajın dijital olarak imzalandığı zamandan itibaren değiştirilmediğini de belirtir.

Mesajın gizliliği, dijital imza amacı için gerekli olmamakla beraber, gizliliğe ilişkin güvenlik hizmeti istendiği taktirde, alıcının, uygun gizli anahtarı kullanarak mesajı deşifre etmesinden sonra, göndericinin, gizliliği amacıyla alıcının açık anahtarını kullanarak mesajı şifrelemesini sağlamak için, bazı açık anahtar algoritmaları ters çevrilebilir.

Doğrulama usulü, mesajın imzalanmasında, güvenen tarafça ulaşılabilen açık anahtara uyan gizli anahtarın kullanıldığını belirtir. Ancak mesajla hukuken bağlı olanı bırakır ve mesajı gerçekte kimin imzaladığını söylemez.

Bağlantılar zincirini tamamlamada önemli olan, göndericinin (imzalayanın) kimliğini, göndericinin açık anahtarına bağlamaktır. Bu nedenle güvenen tarafın,

[59] Hash işlevi, standart boyutta bir hash değeri veya hash sonucu yaratan bir algoritma olup, mesaj değişmiş ise hash işlevi farklı bir hash sonucu üretecektir. Bu nedenle hash işlevi, mesajın imzalandığı andan itibaren değiştirilmemesini sağlar.

göndericinin dijital imzasını doğrulamada kullanılan açık anahtarın, gerçekte imzalayanın açık anahtarı olduğuna, imzalayanın açık anahtarını kullanan üçüncü kişinin (sahtekar veya dolandırıcının) açık anahtarı olmadığına inanmasını sağlayacak bir sebep olmalıdır.

İmzalayanın kimliğini, onun açık anahtarına bağlama işi ise bir Onay Kurumu (Certification Authority) tarafından yapılır. Onay kurumu, abone statüsünde bulunan imzalayan (gönderici) adına sertifika çıkaran, güvenilir üçüncü taraftır. Onay kurumu, bir sertifikasyon uygulama statüsü yayımlar. Bu statü, onay kurumunun uygulamalarını, prosedürünü, onay kurumu, abone ve güvenen taraf arasındaki hukuksal hak ve sorumlulukların tahsisine ilişkin kuralları düzenler.

Sertifikasyon uygulaması gereğince, onay kurumu, başvuru, onaylama, (sertifika) ihraç ve kabul prosedürü yürütür. Onay kurumuna veya onun temsilcisine göre belirli kimlik tanımlama prosedürleri doğrultusunda, onay kurumu, imzalayan A kişisi için yapılmış olan sertifika başvurusunun, gerçekten o kişi (A) tarafından yapılmış olduğunu onaylar. Onay kurumu, daha sonra sertifikayı, taklit edilmesini önlemek için, (onay kurumunun) doğrulanabilir dijital imzasıyla dijital olarak onaylar. Sertifika, onay kurumu tarafından açıkça veya örtülü olarak bir kez kabul edildiyse, on-line olarak yayımlanır, kabul edilmediyse, sertifika sahibi tarafından ve/veya müstakbel güvenen taraflarca erişilebilecek başka bir şekilde yayımlanır.

3.4. E-İMZANIN HUKUKSAL ALTYAPISI

3.4.1. Genel Olarak

E-imzanın, e-ticaretin gelişip yaygınlaşmasını teminen kullanıcıların karşılıklı güvenlerini sağlaması, sistemin taraflarının (kullanıcı-onay kurumu-üçüncü kişi) hak ve sorumlulukları ile riskin tahsisini, e-imza ile imzalanan sözleşme ve kayıtların hukuki geçerliliğini ve ispat değerini düzenleyen, yukarıda belirtilen teknik altyapıya uygun bir hukuki altyapının kurulmasına bağlıdır.

Diğer yandan e-ticaretin, açık ağlar üzerinden yapılan uluslararası bir ticaret olduğu dikkate alınarak, kurulacak hukuksal altyapının, bu hususstaki dünya düzenlemeleriyle uyumlu olması (harmonizasyonu) da önemlidir. Daha açık bir ifadeyle, farklı ülkelerde, farklı düzenlemelere tabi olan onay kurumlarınca çıkarılan sertifikaların ve onaylanan e-imzaların ülke dışında geçerli olup olmayacağı ve geçerliliğin tabi olduğu kuralların, diğer ülke düzenlemeleriyle işbirliği içinde ve/veya UNCITRAL, OECD, AB gibi uluslararası kuruluşlarca e-ticaret ve e-imza konusunda hazırlanan ve ulusal düzenlemelerin harmonizasyonunu amaçlayan standartlar getiren Yeknesak Kurallar, Rehber ve Direktifler dikkate alınarak belirlenmesi

gerekmektedir. E-ticaretten beklenen faydaya ancak bu şekilde ulaşılabileceği yaygın kanaattir.

Bu çerçevede UNCITRAL E-Ticaret Çalışma Grubunun 14-25 Şubat 2000 tarihleri arasında New York'da yapılan 36. toplantısında ulaşılan Draft Uniform Rules on Electronic Signatures[60] (E-İmza Yeknesak Kurallar Taslağı)'nın, sorumluluk ve e-imzaların hukuki etkisine ilişkin hükümleri incelenecektir.

3.4.2. UNCITRAL E-İmza Yeknesak Kurallar Taslağı

3.4.2.1. Uygulama Alanı (Kapsam)

Yeknesak Kurallar (YK) Taslağı'nın kapsama ilişkin ilk maddesi, Yeknesak Kurallar'ın ticari faaliyetlerde e-imza kullanımına uygulanacağını ve tüketicinin korunması amaçlı hukuk kurallarına aykırı olamayacağını öngörmektedir.

Maddede yer alan "Ticari" ibaresinin, sözleşmesel olan veya olmayan, ticaretin doğasını ilgilendiren tüm sorunlarını içerecek geniş bir yoruma açık şekilde düzenlenmesi önerilmektedir. Mal ve hizmet alış verişi veya temini; dağıtım anlaşması; ticari temsilcilik veya acentalık; faktoring; leasing; inşaat işi; danışmanlık; mühendislik; lisanslama; yatırım; finans; banka; sigorta; patent veya ruhsat anlaşması; iş ortaklığı (joint venture); ve diğer endüstriyel ve ticari işbirlikleri; hava, deniz, kara ve demiryoluyla mal veya yolcu taşıma gibi. Ancak bunlarla sınırlı olmamak üzere herhangi bir ticari muamele ticaretin doğasını ilgilendirmektedir.

3.4.2.2. Güvenli E-İmza ve İmza Karinesi

Taslağın 2. maddesinde, YK'da yer alan e-imza, güvenli e-imza, sertifika, veri mesajı, imza sahibi ve bilgi onaylayıcı terimlerinin tanımı yapılmıştır. Bu noktada özellikle önem taşıyan güvenli e-imzanın üzerinde durulmasının faydalı olacağı kanaatindeyiz.

Güvenli e-imza, kullanıldığı imzalama aracına münhasır olması nedeniyle *teklik*[61], eklendiği veri mesajına münhasıran imza sahibi tarafından konulduğu anlamında *kimlik tespiti*, e-imzayı kullananın gerçekten veri mesajını imzaladığı ve imzalanan veri mesajının bütünlüğünün onaylandığı ve imzalandıktan sonra değişmediği anlamında *güvenilirlik ve bağlantı* özelliklerine sahip olan tüm e-imzalara atfen kullanılan bir terimdir. Güvenli imzanın önemi, farklı kimlik belirleme tekniklerine dayansa da yukarıda belirtilen özelliklere (standartlara) sahip tüm e-imzaların, e-imza olarak kabul edilebileceği ve imza karinesinden

[60] Sözü edilen Taslak'ın Türkçe'ye çevrilmiş metni, çalışmamızın 1 nolu ekinde yer almaktadır.

[61] E-imzaların birbirinden farklı olması anlamına gelir. Parmak izi, retina taraması gibi biyometrik tekniklerin ya da asimetrik kriptografi gibi çift anahtar kullanımına ilişkin yöntemlerin kullanımıyla bu şart yerine getirilmektedir.

yararlanabileceğine ilişkin düzenlemelere esas teşkil etmesindedir. Zira Taslağın 6. maddesinin 3. bendinde imza karinesinden yararlandırılacak güvenilir e-imzaların standartları güvenli e-imza tanımındaki özelliklere uygun şekilde belirlenerek, Kanunun bir kimsenin imzasının varlığını aradığı (şart koştuğu) yerde, güvenli bir elektronik imzanın kullanılması halinde, aranan imza koşulunun, karineten o e-imza ile yerine getirilmiş sayılacağı belirtilmiştir.

Benzer bir düzenleme AB E-İmza Direktifinin 2. maddesinde Advanced E-Signature[62]" (Gelişmiş E-İmza) olarak adlandırılarak, yukarıda belirtilen özelliklerle bire bir paralel standartlara bağlanmıştır. Yine UNCITRAL düzenlemesine benzer şekilde Direktif'in "İmzaların Hukuki Etkileri" başlıklı 5. maddesinde, gelişmiş e-imzaların elle atılan imzanın hukuki sonuçlarını doğurması ve hukuk usulünde delil olarak kabul edilmesinin tüm üye devletlerce teminine ilişkin düzenlemeler yapılması yükümlülüğü öngörülmüştür[63].

3.4.2.3. Orijinallik Karinesi

YK Taslağının 7. maddesinde, e-imza ile imzalanarak gönderilen bir mesajın, imzalandığı zamanki orijinal halini ve bütünlüğünü koruduğu, gönderildikten sonra değişmediğinin karineten kabul edileceği öngörülmektedir.

3.4.2.4. Hukuki Sorumluluk

3.4.2.4.1. İmza (Aracı) Sahibinin Sorumluluğu

YK 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,

---

[62] Anılan Direktif'in 2. maddesinde yer alan hüküm şu şekildedir:
"Gelişmiş elektronik imza", "Advanced electronic signature" aşağıdaki koşulları karşılayan bir elektronik imzadır.
(a) Münhasıran imza sahibine bağlanan,
(b) İmza sahibini tanımlayabilen
(c) İmza sahibinin münhasır (yegane) kontrolü altında muhafaza edilen araçlarla yaratılan,
(d) Veride sonradan meydana gelen değişiklikleri gösterecek şekilde veriye eklenen

[63] Anılan Direktifin 5. maddesi şu şekildedir:
Madde 5:
E-İmzaların Hukuki Sonuçları (Etkileri)
1. Üye devletler, güvenli imza yaratma aracı ile yaratılan ve nitelikli sertifikaya dayanan *gelişmiş elektronik imzaların*: elektronik formdaki bir veriyle ilgili olarak, elle atılan imzada kağıda dayanan veriye ilişkin olarak aranan koşullarla aynı koşulları karşılaması halinde elle atılan imzanın hukuki sonuçlarını doğurmasını sağlamaya ve bu imzaların, hukuk usulünde delil olarak kabul edilir olmasının teminine yönetlik olarak,
(a) elektronik formdaki bir verinin, elle atılan imzada kağıda dayanan veriye ilişkin olarak aranan koşullarla aynı koşulları karşılaması halinde, elle atılan imzanın hukuki sonuçlarını doğurmasını,
(b) hukuk usulünde delil olarak kabul edilebilir olmasını
(sağlamalıdırlar) güvence altına almalıdırlar. (.....)

imza aracının izinsiz ve yetkisiz olarak kullanımından kaçınması[64] ve bu hususta makul bir dikkat göstermesi gerektiği öngörülmektedir. Bu yükümlülük 1998 tarihli Illinois Elektronik Ticaret Güvenliği Kanunu ve Singapur Elektronik İşlemler Kanunu'nda da düzenlenmiştir.[65].

Ayrıca imza aracının (gizliliğinin) tehlikeye düştüğü ve tehlikeye girmesine yol açacak şartların gerçekleştiği durumlarda, imza aracı sahibine bildirim yükümlülüğü getirilmiştir. İmza sahibinin bildirim yükümlülüğü, çeşitli ülkelerin e-imza mevzuatlarında düzenlenmiştir[66].

---

[64] **Illinois Electronic Commerce Security Act 1998 (1997 Illinois House Bill 3180; 5 Ill. Comp. Stat. 175, enacted August 1998)** <http://www.legis.state.il.us/legisnet/legisnet90/hbgroups/hb/900HB3180LV.html>

Section10-125: İmza araçlarının yaratılması ve kontrolü

Aksi başka bir uygulanabilir hukuk tarafından kararlaştırılmadıkça, (....) hükmü uyarınca yaratılan güvenilir güvenlik prosedürü ile meydana getirilen bir e-imzanın yaratılması, geçerliliği veya güvenilirliği (söz konusu olması durumunda) imza sahibinin imza aracını kontrolü veya gizliliğine dayanır.

(1) İmza aracını yaratan veya somutlaştıran kimse bunu güvenilir bir usulde yapmalıdır.

(2) İmza sahibi ve imza aracına hukuki olarak erişim hakkına sahip olan diğer kimseler, imza aracını kontrol altında tutma ve gizliliğini sürdürme hususlarında makul bir özen göstermeli ve onu (imza aracını), bu araç tarafından yaratılan imzaya güvenin makul (uygun) olduğu dönem boyunca izinsiz erişimlerden, ifşadan veya kullanımdan korumalıdır.

(3) İmza sahibi veya imza aracına hukuki olarak erişim hakkına sahip olan diğer kimselerin bir imza aracının kontrolü veya gizliliğinin tehlike altında olduğunu bilmesi veya bilmesini gerektiren bir nedenin olması durumunda, bu kimsenin, bu tehlike durumunun sonucunda zarar görebilecekleri öngörülebilen herkese(kimselere) derhal bildirim hususunda veya tehlike altına girmeye ve ondan sonra yaratılan imzanın doğruluğunun kabul edilmemesine ilişkin ilanın yayımlanmasına yönelik olarak uygun bir ilan mekanizmasının kullanılabilir olması halinde derhal ilan hususunda makul bir çaba göstermelidir.

[65] **Illinois Electronic Commerce Security Act**

Madde 20: Abonenin Sorumlulukları

Section 20-101:Bir Kimlik Elde Etme

Bir kimse tarafından, abone olarak kendi adına sertifika edinme amacıyla, bilerek bir onay kurumuna yapılan bütün esaslı (esasa etkili) beyanlar, abonenin bildiğine ve güvendiğine göre doğru ve tam olmalıdır.

Section 20-105 Bir Sertifikanın Kabulü

(...)

(b) Bir sertifikanın kabulü, sertifikada adı geçen abonenin, sertifikada yer alan makul bir bilgiye iyiniyetle ve işlem süresince güvenen bir kimseye;

(1) Abonenin, sertifikada belirtilen açık anahtara tekabül eden (uyan) özel anahtarı yasal olarak elinde tuttuğunu,

(2) Abone tarafından onay kurumuna yapılan ve sertifikada belirtilen bilgiye ilişkin bütün esaslı beyanların doğru olduğunu,

(3) Sertifikada yer alan tüm bilgilerin abonenin bilgisi dahilinde doğru olduğunu

ifade eder.

Singapure Electronic Transactions Act 1998, Act No 25 of 1998 (<http:/www.cca.gov.sg/eta/part1.html>)

Bölüm IX.Abonelerin Sorumlulukları

Sertifika Edinme

37. Abone tarafından, onay kurumuna bir sertifika edinme amacıyla yapılan ve abone tarafından bilinen ve sertifikada temsil edilen bütün esaslı beyanlar, onay kurumu tarafından teyit edilip edilmediği dikkate alınmaksızın, doğru ve abonenin bildiğine ve güvendiğine göre tam olmalıdır.

[66] **Illinois Electronic Commerce Security Act**

Madde 20. Abonelerin Sorumlulukları

Section 20-110 Sertifikanın İptali

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[67]. Maddenin 2. paragrafında, bu sorumluluğa bağlanan hukuki sonuçlar, anılan hususta yasal düzenleme yapacak ülkede uygulanan kurallara bırakılmıştır.

3.4.2.4.2.Onay Hizmetleri Sağlayıcının (Onay Kurumunun) Sorumluluğu

YK Taslağının 10. maddesinde onay hizmetleri sağlayanların sorumlulukları düzenlenmiştir. Buna göre onay kurumları, beyanlarına uygun davranma, sertifikaların geçerlik süresi ve içeriğine ilişkin olarak doğru ve tam beyanda bulunma hususunda makul bir dikkat göstermelidir.

Aksi, başka bir uygulanacak hukuk kuralı tarafından öngörülmedikçe, geçerli bir sertifikada belirtilen açık anahtara ait (uygun) gizli anahtarın kaybolması, çalınması veya yetkisiz bir kişi tarafından erişilebilir olması veya sertifikanın geçerlilik döneminde başka tehlikelerin söz konusu olması durumunda, *(bu)* tehlikeyi öğrenen bir abone, ihraççı onay kurumundan sertifikanın iptalini ve abonenin önceden sertifikayı yetkilendirdiğini ilan ettiği tüm dükkanlarda iptalin ilanını derhal talep etmelidir. (veya iptalin ilanını gerektiren başka makul durumlarda)

Sec. 20-125 İmza Araçlarının Yaratılması ve Kontrolü

Aksi başka bir uygulanacak hukuk kuralı tarafından öngörülmedikçe, güvenli güvenlik usulü ile (....) gereğince meydana getirilen bir elektronik imzanın yaratılması, geçerliliği veya güvenilirliği, imzalayanın imza aracını kontrolü veya gizliliğine tabidir:

(1) İmza aracını oluşturan veya yaratan kimse bunu güvenilir usulde yapmalıdır.

(2) İmzalayan ve imza aracına yasal olarak erişim imkanına sahip diğer kimseler, imza aracını kontrol altında tutma ve gizliliğini koruma hususunda makul bir özen göstermeli ve böyle bir araç tarafından yaratılan imzaya güvenilen dönem boyunca onu yetkisiz (izinsiz) erişimlerden, ifşadan (açığa vurulmasından) veya kullanımlardan korumalıdır.

(3) İmzalayanın veya imza aracına yasal olarak erişim imkanına sahip kimselerin bu imza aracının kontrolünün veya gizliliğinin tehlike altına girmiş olduğunu bilmeleri veya bunu bilmelerine sebep olacak bir gerekçenin olması durumunda; bu kimse, söz konusu tehlikeye girmenin sonucu olarak zarara uğraması öngörülebilen tüm kişilere derhal bildirme hususunda makul bir çaba göstermelidir veya tehlikenin ve bundan sonra yaratılan imzaların doğruluğunun kabul edilmediğinin bildiriminin ilanı için uygun ilan mekanizmaları kullanılır (...),

Singapure Electronic Transactions Act

Başlangıçta Erteleme ve İptal

Bir sertifika kabul etmiş bir abone, sertifikadaki açık anahtara tekabül eden özel anahtarın tehlikeye düşmesi durumunda, mümkün olan en kısa süre içinde ihraççı onay kurumundan sertifikanın ertelenmesini veya iptalini talep eder.

[67] **Singapure Electronic Transactions Act**

Bölüm IX. Abonenin Sorumlulukları

Özel Anahtarın Kontrolü

39. (1) sertifikada tanımlanan bir abone, bir onay kurumu tarafından çıkarılan bir sertifikayı kabul etmekle, bu sertifikada ifade edilen açık anahtara tekabül eden gizli anahtarı kontrol altında tutma ve abonenin dijital imzasını atmaya yetkili olmayan bir kimseye açıklamama hususunda makul bir özen gösterme sorumluluğunu üstlenir

(2) Bu sorumluluk, sertifikanın geçerlik süresi boyunca ve sertifikanın askıda bulunduğu süre boyunca devam etmelidir.

Yine anılan kurumlar, imzaya güvenen tarafca; onay hizmetleri sağlayıcının kimliği, sertifikada tanımlanan kimsenin, ilgili zamanda, sertifikanın dayandığı imza aracını elinde tuttuğu, imza aracı sahibini tanımlamakta kullanılan yöntem, imza aracının kullanılmasında mevcut olabilecek amaç ve miktar sınırlamaları, imza aracının geçerli olup olmadığı veya tehlike altında bulunup bulunmadığı hususlarının doğruluğunu araştırılmasına imkan verecek araçlar temin etmekle yükümlüdürler. Bu yükümlülüklerini yerine getirmede başarısız olan (ihmali bulunan) onay hizmetleri 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 onay hizmetleri sağlayıcıların sorumluluk alanını veya miktarını sınırlandıran bir kaydın olup olmadığı vs. hususların da dikkate alınması gerektiği öngörülmüştür.

Onay hizmetleri sağlayıcılar, 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.

Ayrıca bir sertifikada yer alması gereken bilgiler de, güvenen tarafca doğruluğunun araştırılmasına imkan verilecek hususlarla paralel olarak düzenlenmiştir.

Bu konu, AB E-İmza Direktifinin "Güvenilir sertifika çıkaran onay hizmeti sağlayıcıların (kurumlarının) koşulları" başlıklı II nolu EK'inde yukarıdaki düzenlemeye benzer şekilde düzenlenmiştir.

DÖRDÜNCÜ BÖLÜM

ELEKTRONİK KAYITLARIN MEDENİ USUL HUKUKUNUN İSPAT KURALLARI YÖNÜNDEN DEĞERLENDİRİLMESİ

4.1. TÜRK MEDENİ USULÜNDE İSPAT VE DELİL SİSTEMİ

İspat, bir iddianın veya vakıanın doğruluğu konusunda hakimi ikna etmeye yönelik bir faaliyettir[68]. Tarafların öne sürdükleri ispat araçları ise delil olarak adlandırılır[69].

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[70] üzerindeki hukuki 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[71]. Senetle ispat zorunluluğu olarak da adlandırılan bu kural, hukuki işlemlerin ve hukuki sonuç doğurmaya yönelmiş irade beyanlarının[72], 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[73].

---

[68] ÜSTÜNDAĞ, S.:;Medeni Yargılama Hukuku, C. I-II, Genişletilmiş 6. Bs. İstanbul 1997, sh.613; KONURALP, Haluk:Medeni Usul Hukukunda İspat Kurallarının Zorlanan Sınırları, Ankara 1999, sh.9.

[69] UMAR, B./YILMAZ, E:İspat Yükü, İstanbul 1980, Genişletilmiş 2. Bs., sh.2.

[70] HUMK'nun 288 ve 290. maddelerindeki parasal sınır, 26.2.1985 tarih ve 3156 sayılı Kanunla 1086 sayılı HUMK'na eklenen Ek Madde 2 gereğince 1.1.1990 tarihinden itibaren yimi bin liraya, 20.6.1996 tarih ve 4146 sayılı Kanunun 1. maddesiyle 10 milyon liraya yükseltilmiştir. Anılan geçici maddede, sözü edilen parasal sınırın (on milyon lira) 1.1.2000 tarihinden itibaren dört katı olarak uygulanacağı öngörüldüğünden, senetle ispat ve senede karşı senetle ispat zorunluluğuna tabi hukuki işlemlerin ve iddiaların tabi olduğu sınır, çalışmamız tarihi itibariyle 40 milyon TL'dir.

[71] KURU/ARSLAN/YILMAZ:Medeni Usul Hukuku, Ankara 1992, sh.348; ÜSTÜNDAĞ: sh.650

[72] ÜSTÜNDAĞ: sh.650.

[73] KURU, Baki:Hukuk Muhakemeleri Usulü, C.II, Ankara 1980, sh.1426, 1427.

4.2. 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[74]. Kanunun (veya taraflar iradelerinin), bir işlemin geçerli olması için mutlaka öngörülen şekle uyulmasını gerektirdiği durumlarda, geçerlik şartı olan şekilden bahsedilirken; 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, Borçlar Kanunumuzun md. 11/I hükmü ile, kanunda açıkça düzenlenen haller dışında[75], 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[76].

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

Bu çerçevede çalışmamızda, ağırlıklı olarak, elektronik ortamda gerçekleştirilen, e-imzanın kullanıldığı sözleşmeler ile elektronik (ortamdaki) kayıtların, medeni usul hukukunun ispat kuralları karşısındaki durumu ele alınacak, elektronik ortamda yapılan hukuki işlemlerin, geçerlik şartı olan şekle uygunluğuna yeri geldikçe değinilecektir.

---

[74] KURU/ARSLAN/YILMAZ: sh. 348; ÜSTÜNDAĞ: sh. 649 vd.
[75] 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.
[76] ALTAŞ, H.: sh.72.

4.3. ELEKTRONİK KAYITLARIN MEVCUT DELİL SİSTEMİMİZDEKİ DEĞERİ

4.3.1. Kapalı Bilgisayar Sistemleri Bakımından

Bankacılık alanında 1970'lerden itibaren elektronik sistemlere geçilmesi ile, müşteri tarafından herhangi bir belge doldurulmaksızın plastik bir kart kullanarak harekete geçirilen elektronik sistemler aracılığıyla bankacılık işlemleri gerçekleştirilmektedir[77]. Bu sistemler, otomatik vezne makinaları (ATM), satış noktasından otomatik fon transferi (EFTPOS), ev ve ofis bankacılığı adı altında bankacılık faaliyetleri göstermektedir.

Bankalar, acentesi oldukları aracı kurumların sermaye piyasası faaliyetlerinde de bu elektronik sistemler vasıtasıyla, yatırımcılara, menkul kıymet alım satımı, yatırım fonu katılma belgeleri alım satımı ve benzer nitelikte işlemleri gerçekleştirme imkanı sağlamaktadırlar.

Benzer şekilde Sermaye Piyasası Kanunu'na 15.12.1999 tarih ve 4487 sayılı Kanun ile eklenen 10/A maddesi uyarınca, sermaye piyasası araçları ve bunlara ilişkin kişisel hakların, Merkezi Kayıt Kuruluşu adlı, özel hukuk tüzel kişiliğini haiz bir kuruluş tarafından bilgisayar ortamında kayden izleneceği, kaydedilen hakların senede bağlanmayacağı öngörülmüştür. Kapalı bir bilgisayar sistemi içinde tutulacak olan kayıtlar, sermaye piyasası araçları üzerindeki hak sahipliğine ilişkin bir uyuşmazlık halinde, gerçek hak sahipliğini öğrenmek üzere kendisine başvurulacak, "doğrudan doğruya" bir delil olacaktır. Zira Merkezi Kayıt Kuruluşunun kayıtlarında hak sahibi görünen kişi bakımından bu kayıt, o kişinin hak sahipliği iddiasını doğrulayan bir delildir. Bu kayıttan printer aracılığıyla alınan çıktı ise "dolaylı" bir delildir[78]. Bu kayıt ve kayıttan alınan çıktının mevcut delil sistemimiz içindeki yeri ve delil değeri aşağıda incelenmiştir.

4.3.2. Açık Ağ (Internet) İşlemleri Bakımından

Elektronik ortamda gerçekleştirilen, örneğin bir web sitesinde sunulan mal ve hizmetlerin alım satımına ilişkin bir elektronik sözleşme ile ilgili olarak, gerek sözleşmenin kurulması aşamasında, alıcının, bilgisayar ekranında bulunan bir butona tıklamak suretiyle satın alma iradesini bildirmesi[79], satıcının, satım iradesini, digital bilgilerin saklandığı bir manyetik ortam olan kendi “server[80]”ı vasıtasıyla

---

[77] ARKAN, Sabih: Bankacılıkta Kullanılan Yeni Elektronik Sistemlerle İlgili Hukuki Sorunlar, Ankara 1991, sh.2.

[78] KONURALP: sh.73

[79] Bu beyanın icap mı kabul mü olduğu hususundaki farklı görüşler için bkz. yuk. sh.6 vd.

[80] Server, belli kapasitesi olan ve diğer bilgisayarlara hizmet sağlayan bir bilgisayar veya bir programdır. Server aynı zamanda da digital bilgilerin saklandığı (depo edildiği) bir manyetik ortamdır. Adından da anlaşılacağı gibi, server başka bilgisayara veya manyetik ortama hizmet / destek sağlama

açıklaması ve sözleşmenin kurulduğunun bilgisayar ekranında beliren bir teyit mesajı ile alıcıya bildirilmesi; gerek sözleşmenin ifası aşamasında, alıcının, mal veya hizmetin bedelini kredi kartı, elektronik para veya diğer elektronik ödeme araçlarıyla ödemesi sırasında, imza unsurunu taşıyan yazılı bir belge düzenlenmemektedir[81]. Bu işlemlerle ilgili olarak, alıcının elinde olan ve yazılı belge sayılabilecek tek şey, yukarıdaki işlemlerin yapıldığı sırada, bilgisayar ekranında, bu işlemlerin yapıldığına dair beliren görüntü veya teyit mesajlarından printer aracılığıyla alınan çıktılardır.

Öte yandan taraflara (alıcının adı, kredi kartı numarası vs. bilgiler) ve yapılan alım satım işlemine ilişkin bilgilerin satıcı tarafından belirlenen bir serverda[82] veya satıcının hostunda[83] saklanması halinde, - ki elektronik ticarete ilişkin düzenlemelerle, satıcıya, elektronik ortamda yapılan e-sözleşmelerden doğabilecek uyuşmazlıklarda başvurulabilecek bir delil vasıtası olarak, sözleşmeye ilişkin bilgilerin kaydının tutularak, elektronik ortamda saklanmasını temin etme yükümlülüğü getirilebilir[84] - sözleşmenin yapılıp yapılmadığı ve şartlarına ilişkin bilgiler, kayıtların tutulduğu bilgisayar (server) kaydına doğrudan ulaşım ile öğrenilebilir. Banka işlemleriyle ilgili olarak kapalı bilgisayar sistemlerinde tutulan kayıtlar gibi, e-sözleşmelerde de bilgisayar ortamında sözleşmelere ilişkin kayıtların

---

fonksiyonunu ifa eder. (GÜRAN/ AKÜNAL/ BAYRAKTAR/ YURTCAN/ KENDİGELEN/ BELLER/ SÖZER: Bölüm I, <http://www.superonline.com/hukuk/> (par.3).

[81] Kredi kartı kullanılmak suretiyle yapılan mail order alışverişlerinde iki yöntem uygulanmakta olup, bir yöntemde, mal alımına ilişkin sipariş formuna, kredi kartı numarası yazılmak ve kart hamilince (alıcı tarafca) imzalanmak suretiyle satıcı üye işyerine posta ile veya faks yoluyla gönderilir. Burada sipariş formu gerekli belgeleri içeriyorsa, imzalı olduğu için senet sayılmaktadır. Yine kredi kartı kullanılarak yapılan ve genellikle telefonla ve ***internet ortamında*** gerçekleştirilen ikinci tür mail order alış veriş yönteminde ise, harcama belgesinin kart hamili tarafından imzalanması zorunluluğu bulunmamaktadır. Kart hamili, harcama bedelini kredi kartı ile ödemek istediğini satıcıya (üye işyerine) beyan ederek kredi kartı numarası verir ve satıcı, kart hamilinin imzasını taşımayan harcama belgesi düzenlenerek bedeli tahsil eder. Bu nedenle bu tür alışverişlere imzasız alış veriş de denilmektedir.İmzasız alış verişlerde kart hamili olan alıcının harcama tutarına itiraz etmesi durumunda satıcı tarafından düzenlenen belge imza unsurunu taşımadığından alıcıya karşı delil olarak ileri sürülemez. (bkz. KONURALP: sh.71, 72).

[82] Web sitesinin, ISS'nin serverında, site sahibinin serverında veya üçüncü şahsın serverinde tutulması mümkündür. Web sitesinin ISS'nin serverında tutulması halinde, İSS şirketin birinci yükümlülüğü Web sitesi sahibinin istediği surette gereken bilgilerin saklanması ve kullanılmaya hazır halde tutulmasıdır. Bu yükümlülüğün içeriği oldukça çeşitlidir: Bilgilerin gerektiği gibi saklanması, bu amaçla serverde - olası gelişmeleri de öngörerek- yeteri kadar kapasite (alan) tahsis edilmesi, zamanında güncelleştirilmesi (up-dating), bozulmaması ve müdahalelere ve tasalluta karşı korunması, sözleşme hükümlerine uygun olarak teşhiri, siteye yapılan "ziyaretlerin", site ile ilgili olarak alınan mesajların, belli ölçüler ve zaman dilimleri içinde site malikine intikal ettirilmesi anlamında raporlama yükümlülüğüdür. Bu üçüncü kategori yükümlülüğün içeriğinin tesbiti ve sınırlarının çizilmesi oldukça zordur; bu bakımdan ayrıntılarının taraflar arasında yapılacak sözleşmede belirtilmesi yararlı olacaktır. (GÜRAN/ AKÜNAL/ BAYRAKTAR/ YURTCAN/ KENDİGELEN/BELLER/SÖZER:I Bölüm I, <http://www.superonline.com/hukuk/> (par.II,4,c).

[83] Host, bilgilerin saklandığı ve İnternet'e bağlı bulunan bilgisayardır. (GÜRAN/AKÜNAL/BAYRAKTAR/ YURTCAN/KENDİGELEN/BELLER/SÖZER:Bölüm I, <http://www.superonline.com/hukuk/> (par.4).

[84] Nitekim AB'nin 8.6.2000 tarih ve 2000/31/EC sayılı E-Ticaret Direktifi'nin "Temin Edilecek Bilgi" başlıklı 10. maddesinin 1./(b) bendinde, tüketicilerin taraf olduğu sözleşmelerde aksi kararlaştırılamayacak şekilde, servis sağlayıcıların, sipariş vermeden once müstakbel alıcıya sunmaları gereken bilgiler arasında, *tamamlanan sözleşmenin hizmet sağlayıcı tarafından dosyalanıp dosyalanmayacağı ve bu bilginin erişilebilir olup olmadığına* ilişkin bilgi de bulunmaktadır.

tutulması halinde, saklanan bilgilerin bulunduğu bilgisayardan (terminal monitöründen) incelenen kayıtlarda, sözleşmenin (harcamanın) yapıldığına ve şartlarına dair bilgi varsa, bu kayıt, o sözleşmenin (harcamanın) yapıldığını gösteren bir delildir. Bu kayıttan printer aracılığıyla alınan alınan çıktı ise dolaylı bir delildir[85]. Bu çıktı, istenildiğinde bilgisayardan yeni kopyalar alınabilecek bir kayıt olduğundan, orijinal değildir. Oysa HUMK'nda kesin delil olarak tanımlanan senet, "tek" olması nedeniyle "orijinal" bir delildir. Ancak burada senede "orijinal"lik ve kesin delil olma özelliği veren, imzadır[86]. Bilindiği üzere, bilgisayar kayıtları ve bu kayıtlardan alınan çıktılar ise imzalı değildir.

4.3.3. Değerlendirme

4.3.3.1. Özel Hüküm Sebepleri ve Delil Sözleşmesi

Bilgisayar ortamında saklanan kayıtlar ve bu kayıtlardan printer aracılığıyla alınan çıktılar, borç altına girenin (iki tarafa borç yükleyen sözleşmelerde her iki tarafın) imzasını taşımadığından, senet sayılmamaktadır. Bu nedenle bu bilgisayar kayıtları ve bunlardan elde edilen çıktılar, ancak belirli hususların ispatında başvurulabilecek olan ve HUMK md. 376'da *"Hususi Esbabı Hüküm"* (Özel Hüküm Sebepleri) başlığı altında düzenlenen, kanunda öngörülmeyen delillerden sayılırlar. Anılan hüküm, senetle ispatı gerekmeyen davalarda, re'sen veya talep üzerine HUMK'nda gösterilmemiş olan delillerin de dinlenmesi ve incelenmesine mahkemece karar verilebileceğini öngörmektedir[87]. Kanun, özel hüküm sebeplerinin senetsiz ispatı caiz olan davalar bakımından söz konusu olabileceğini ifade ederek, özel hüküm sebeplerinin takdiri delillerden olduğunu ifade etmek istemiştir[88]. Özel hüküm sebepleri serbest ispat araçlarından olup, kural olarak dava şartlarının ispatı ile resen araştırılması gereken konularda ikame edilebilirler.

Özel hüküm sebeplerinin, hukuki işlemlerin ispatında kullanılmaları ve mahkemece dinlenebilmeleri, ancak HUMK md. 287/II'de düzenlenen delil sözleşmesi ile mümkün olur[89].

Delil sözleşmesi, senetle ispat zorunluluğu ile senede karşı senetle ispat zorunluluğunun istisnasıdır[90]. Belirli bir hususun (vakıanın veya hukuki işlemin), belirli bir delille ya da diğer deliller yanında o delille de ispat edileceğine ilişkin olarak

---

[85] KONURALP: sh.73; Ayrıca, AB'nin E-Ticaret Direktifi'nin 10/3 hükmünde, servis sağlayıcıların sözleşme şartları ve genel şartları, *saklanmaya ve kopyalanmaya elverişli şekilde* alıcının erişimine açık şekilde temin etmeleri, tüketicilerin taraf olduğu sözleşmelerde aksi kararlaştırılamayacak şekilde, zorunlu tutulmuştur.
[86] KONURALP; sh.73:
[87] ÜSTÜNDAĞ: sh.613, 614; KURU/ARSLAN/YILMAZ: sh.408.
[88] KURU/ARSLAN/YILMAZ: sh.408.
[89] KONURALP: sh.73.
[90] KURU/ARSLAN/YILMAZ: sh.409.

yapılan sözleşmedir[91]. Delil sözleşmesi ile senetle ispatı gereken bir hukuki işlemin başka bir delille ispatlanabileceği kararlaştırılabilir. Delil sözleşmesi HUMK md. 287/II uyarınca yazılı şekle tabi bir sözleşmedir.

Delil sözleşmesi, aralarında önceden yazılı bir sözleşme yapma imkanı olan bankalar ve aracı kurumlar ile müşterilerine, gerek bankacılık sistemleri, gerek sermaye piyasası işlemleri dolayısıyla, kullanılan *kapalı elektronik sistemler*de, elektronik kayıtların delil olarak ikame edilebilmesi imkanını sağlayarak, ispat sorunlarına çözüm getirebilecek bir hukuki araç olarak kabul edilebilir. Bunun için, önceden, ya aracı kurum (veya acente banka) ile yatırımcı arasında ayrı bir delil sözleşmesi yapılması ya da aracı kuruluşların yatırımcılarla akdettikleri genel işlem şartları niteliğindeki çerçeve sözleşmelerine, bilgisayarlar sistemleri vasıtasıyla gerçekleştirilen işlemlerden doğan uyuşmazlıkların çözümünde, bu işlemlere ilişkin elektronik kayıtların mahkemede caiz delil olarak kullanılabileceğine dair bir kayıt konulması gerekmektedir.

Bununla beraber, bir çok bankanın ve aracı kurumun, müşterileriyle akdettikleri delil sözleşmelerinde olduğu gibi, aracı kuruluşun kayıtlarının kesin delil olacağına dair kayıtlar, HUMK md. 240 hükmü ile hakime tanınan delilleri takdir yetkisini ortadan kaldırıcı nitelikte olduğu[92], müşterinin bu delilleri peşinen kabul ettiği ve her türlü itiraz haklarını kullanmaktan feragat ettiğine dair kayıtlar, dava ve savunma imkanını esaslı ölçüde zedeleyen, objektif iyi niyet kurallarına aykırı olduğu gerekçesiyle hakim tarafından geçersiz sayılabileceğinden[93], elektronik kayıtların davada delil olarak ileri sürülebilmesi, HUMK md. 288 vd. hükümleri karşısında mümkün olamayacaktır[94]. Bu nedenle bilgisayar ortamında gerçekleştirilen işlemlere ilişkin elektronik kayıtların mahkemede delil olarak dinlenebilmesi, aracı kuruluş ve yatırımcı arasında yapılan delil sözleşmesinin veya çerçeve sözleşmesindeki buna ilişkin kaydın geçersizlikle sonuçlanmayacak şekilde düzenlenmesine bağlıdır.

Delil sözleşmesinin, *açık ağ ortamında (internet üzerinden)* gerçekleştirilen sözleşmelerde ve diğer hukuki işlemlerde, bilgisayar ortamında tutulan kayıtların delil olarak kullanılabilmesini ve bu delillerin mahkemece dinlenebilmesini sağlayıp sağlayamayacağı ise, e-ticaretin yukarıda değinilen özellikleri karşısında şüphelidir. Zira delil sözleşmesinin, HUMK md. 287/II hükmü uyarınca yazılı şekle tabi bir sözleşme olduğu, açık ağ (internet) ortamında gerçekleştirilen e-sözleşmelerin ve diğer hukuki işlemlerin ise, önceden birbirini tanımayan ve dolayısıyla önceden

[91] KURU/ARSLAN/YILMAZ: sh.409
[92] KONURALP: sh. 75.
[93] KONURALP: sh.64; BATTAL, Ahmet:"Bankacılık Sözleşmelerinde İspat Usulü ve Delil Sözleşmeleri", BATİDER, 1997, C.XIX, Sa.2, s.135, 136; ATAMER, Yeşim; Sözleşme Özgürlüğünün Sınırlandırılması Sorunu Çerçevesinde Genel İşlem Şartlarının Değerlendirilmesi, Ağustos 1999, sh.285.
[94] KONURALP: sh.74.

(yazılı) bir sözleşme yapma imkanları söz konusu olmayan kimseler arasında akdedildiği dikkate alındığında, delil sözleşmesinin e-ticarete ilişkin ispat problemlerinin çözülmesinde pek de elverişli olmadığı anlaşılmaktadır.

4.3.3.2. Yazılı Delil Başlangıcı

Bilgisayar kayıtlarının veya kayıtlardan printer vasıtasıyla alınan çıktıların, senetle ispat kuralının istisnaları arasında sayılan ve HUMK md. 292'de yer alan mukaddimei beyyine (yazılı delil başlangıcı) sayılıp sayılmayacağı da tartışılabilir.

Bir iddianın senetle ispatı gereken durumlarda, senet mevcut değilse, bu iddiaya komşu olan vakıaları somutlaştıran belgelere mukaddimei beyyine (yazılı delil başlangıcı) denir[95]. Bu suretle, senetle ispat edilmesi gereken hususlarda bir yazılı delil başlangıcı varsa, hakimde yeterli bir kanaat oluşuncaya kadar tanık veya diğer takdiri delillere başvurulabilmesi mümkün olabilmektedir[96]. Ancak Konuralp, HUMK'nun 292. maddesinin kaleme alınış biçiminin, yazılı delil başlangıcının özel niteliği bulunan bir takdiri delil olduğu ve koşulları varsa başlı başına bir takdiri delil oluşturacağı görüşündedir[97].

HUMK'nun 292. maddesi uyarınca, yazılı delil başlangıcından bahsedilebilmesi için şu üç şartın birlikte gerçekleşmesi gerekmektedir. Bunlar, (a) yazılı bir belgenin bulunması, (b) bu belgenin aleyhine ileri sürülen tarafca verilmiş olması ve (c) bu yazılı belge varlığı iddia edilen hukuki işlemi tam olarak ispata yetmemekle beraber o hukuki işlemin vukuuna delalet etmesidir[98].

Kanunda yazılı delil başlangıcı için öngörülen bu koşullar incelendiğinde, elektronik kayıtların, yazılı bir belgenin varlığı koşulu bulunmadığından yazılı delil sayılamayacağı sonucuna varılmaktadır[99]. Bilgisayar kayıtlarından alınan çıktılar ise yazılı delil başlangıcı sayılabilme bağlamında, yazılılık koşulunu yerine getirebilmekle beraber, ikinci koşul olan, aleyhine ileri sürülen tarafça verilmiş olma koşulunun gerçekleşme ihtimali, kapalı bilgisayar sistemlerinde kaydın çıktısının müşteriye verilmesi veya gönderilmesi durumu söz konusu olmadığı taktirde, son derece azdır. Bunun dışında anılan koşul, ancak aleyhine delil ileri sürülen tarafın, belgenin kendisine ait olduğunu ikrar etmesi veya yazı karşılaştırması yoluyla

---

[95] ÜSTÜNDAĞ: sh.676; KONURALP: sh.38 vd.
[96] KONURALP: 41
[97] KONURALP: sh.76, dn. 55.
[98] KURU/ARSLAN/YILMAZ: sh.372; ÜSTÜNDAĞ: 676 vd.; KONURALP: sh.39.
[99] Ancak Yargıtay 15. H.D.'nin 30.6.1975 tarihli bir kararında, alacağın tespiti davasında, davalının tediye hakkındaki ödeme ikrarını içeren teyp bandı delili bulunduğuna göre, banttaki sesler dinlenerek davacıya ait bulunup bulunmadığı, gerçekten ödeme hakkında uyuşmazlığa çözüm getiren ve davacıyı bağlayan bir beyanın yer alıp almadığının araştırılması gerektiği yönünde hüküm verilmiş olup, bu karar KURU ve KONURALP tarafından, HUMK md. 288'de yer alan senetle ispat kuralına aykırı olduğu gerekçesiyle eleştirilmektedir. (YILDIRIM: Medeni Usul Hukukunda Delillerin Değerlendirilmesi, İstanbul 1990, sh.216).

belgenin borçludan sadır olduğunun anlaşılması halinde söz konusu olur[100]. Bir bilgisayar çıktısından yazı karşılaştırılması yapılması ise mümkün değildir.

Bu çerçevede, bilgisayar kayıtlarının, yazılı delil başlangıcının kanundaki tanımında belirtilen unsurları içermemesi; bu kayıtlardan alınan çıktıların ise borçlu tarafından verilmesi veya ikrar edilmesi gibi durumlar dışında yazılı delil başlangıcı sayılamaması nedeniyle, hukuki bir işlemin yazılı delil başlangıcı sayılamayacağı sonucuna varılmıştır[101].

4.3.4. Çözüm Seçenekleri

4.3.4.1. Mevcut Delil Sistemi İçinde Çözüm ve/veya İlgili Kanunda Değişiklik Yapılması

Görüldüğü üzere HUMK'nun, hukuki işlemlerin kanuni delille (senetle) ispat edilmesi zorunluluğunu öngören delil ve ispat sistemi karşısında, internet ortamında gerçekleştirilen e-sözleşmeler ve diğer hukuki işlemlere ilişkin bilgisayar kayıtları ve bu kayıtlardan printer vasıtasıyla alınan çıktıların, taraflar arasında yapılmış geçerli bir delil sözleşmesi olmaksızın, uyuşmazlıkların çözümünde mahkemece dinlenebilecek bir delil olma niteliği taşıdığını söylemek zordur.

Bununla beraber, doktrinde, özellikle elektronik bankacılık işlemleri bağlamında, banka tarafından çeşitli kaynaklardan toplanmış bilgilerin yazılı delil başlangıcı sayılıp, sonucun hakimin takdirine bırakılması şeklinde çözüm önerisi getiren yazarlar da bulunmaktadır[102].

Gelişmekte olan teknoloji ve buna paralel olarak e-ticaretin gelişimine ayak uydurabilmek, bilgisayar ve açık ağ bağlantısı teknolojileri kullanılmak suretiyle gerçekleştirilen hukuki işlemlerle ilgili uyuşmazlıkların, bu teknolojilerin kağıda dayanmayan tabiatı dikkate alınarak, kağıda dayanan mevcut delil ve ispat sistemi içinde çözümlenmesi, kısa vadede, Sermaye Piyasası Kanunu'nda olduğu gibi[103] ilgili konuda kanuni değişiklik yoluna gidilmek suretiyle o kanuna ilişkin alanla sınırlı olarak, kısmen giderilebilecektir[104].

---

[100] ÜSTÜNDAĞ: sh. 678.
[101] Bkz. Aynı görüşte Baki KURU: Elektronik Bankacılık ve Hukuk, sh. 134. (Nakleden: KONURALP: sh. 76, dn. 54).
[102] Aynı görüşte Şeref ÜNAL: Bankacılık Sektörü ve Bilgisayar Verilerinin Delil Olma Niteliği, Elektronik Bankacılık ve Hukuk, (Nakleden: KONURALP: sh.76, dn.53).
[103] 2499 sayılı Sermaye Piyasası Kanunu'nun 22. maddesinde 4487 sayılı Kanunla yapılan değişiklikle eklenen ve yeniden düzenlenen (d), (s) ve ispat açısından, soruna sermaye piyasası faaliyetleri kapsamında genel bir çözüm getirebilecek e-imza kullanım esaslarına ilişkin düzenlemelerin yapılmasında Kurul'a düzenleme yapma yetkisi veren (u) bendi hükümleri.
[104] KONURALP: sh.84.

Sermaye Piyasası Kanunu'ndaki bu hükümle, bir e-imza altyapısı oluşturulduktan sonra, aracı kuruluşların internet üzerinden sermaye piyasası faaliyetlerinde bulunmaları söz konusu olabilecek, ancak bu işlemlerden doğan uyuşmazlıkların çözümünde e-imzanın sağladığı kimlik tespiti ve ispat yükünü belirleyen karinelerin birer ispat kuralı olarak geçerli olabilmesi, HUMK'daki delil sisteminde gerekli değişiklik yapılıncaya veya e-imzanın mahkemelerde delil olarak kabul edileceğini öngören bir yasal düzenleme yapılıncaya kadar, aracı kuruluşların yatırımcı ile yazılı bir delil sözleşmesi imzalayarak, e-imzanın, uyuşmazlık çıktığında caiz delil olarak ikame edilebileceğinin kabul edilmesi halinde mümkün olabilecektir. Bunun dışında e-imza, gerekli teknik ve sermaye piyasası mevzuatında yapılacak düzenlemeler şekilde gerçekleştirilecek hukuki altyapının sağlanması ile, HUMK'daki delil sisteminde değişiklik yapılmadan önce de Borsa uyuşmazlıklarının çözümünde bir ispat vasıtası olarak kullanılabilecektir.

4.3.4.2. Delil Sisteminde Değişiklik Yapılması

Soruna e-ticarete konu diğer mal ve hizmetlerle ilgili hukuki işlemlerden doğan ispat sorunlarının giderilmesi amacıyla uzun vadeli bir çözüm getirilmesi, ancak senet merkezli bir ispat hukuk sisteminden uzaklaşmak[105] ve hatta elektronik ortamın doğasına uygun ve elle atılan imzanın işlevlerini yerine getirmeye elverişli teknolojilere dayanan elektronik imza yöntemlerinin kullanılabilmesine imkan sağlayacak teknik ve hukuki altyapıyı oluşturmak gerekmektedir.

4.3.4.2.1. Senet Kavramının Genişletilmesi

Kara Avrupası hukuk sisteminde kanuni ispat kuralından delillerin serbestçe değerlendirilmesi ilkesine giden bir gelişim söz konusudur[106]. Örneğin 1980'lerde, Medeni Kanunlarının, HUMK'muzun md. 293 ve 294 hükümlerine tekabül eden hükümlerinde, EDI (elektronik veri aktarımı) sistemlerinde senet elde edilmesinin fiilen imkansızlığına dayanılarak, EDI'den doğan uyuşmazlıklarda da senetle ispat zorunluluğu aranmayacağı şeklindeki yoruma elverişli değişiklikler yaparak çözüm arayan ülkeler olduğu gibi, senet kavramını çok geniş bir içerikle yeninden düzenleyen ülkeler de bulunmaktadır[107].

Benzer şekilde, Avrupa Konseyi'nin "Yazılı Delilin Koşullarına ve Belge Röprodüksiyonları ile Bilgisayar Kayıtlarının Kabul Edilebilirliği Hakkında R (81)20 sayılı Tavsiye Kararı" ile, bir yandan doğru ve orijinallerine uygun olan mikrofilm

[105] KONURALP: sh.84.
[106] YILDIRIM, M.K.: sh.211.
[107] Böylece, bir irade beyanının teknik bazı cihazlarla ortaya konabildiği taşıyıcı da kapsayan "modern anlamda senet" kavramı geliştirilerek, bununla kağıda dayanan klasik anlamdaki senede bağlanan hukuki sonuçlara ulaşmak mümkün kılınmıştır. (ÖZTAN, Fırat: Kıymetli Evrak Hukuku, 2. Bs., sh.17; KONURALP: sh.76-78).

röprodüksiyonları ile bilgisayar kayıtlarının davalarda delil olarak kabul edilmesi yani caiz delil sayılması esası önerilirken, diğer yandan üye devletlere, bu röprodüksiyonların ve bilgisayar kayıtlarının, aksi ispat olununcaya kadar doğru kabul edilmesine ilişkin düzenlemeler yapılması tavsiye edilmektedir[108]. Tavsiye Kararı, Türkiye gibi, belirli meblağı bir meblağı aşan hukuki işlemlerin ispatı için yazılı delil zorunluluğunu öngören devletlerde bu zorunluluğun kaldırılması veya senetle ispat zorunluluğu sınırının yükseltilmesini önermiştir.

4.3.4.2.2. E-İmzanın Bir İspat Aracı Olarak Kabulü ve ETKK Hukuk Grubunca Önerilen E-İmza Kanun Tasarısı

Ülkelerin delil sistemlerinde köklü değişiklikleri gerektirmeyen, senede dayalı mevcut sistemi koruyan değişiklikler, internet üzerinden gerçekleştirilen e-ticarete ilişkin ispat sorunlarını çözümlemekte yetersiz kaldığından, sözü edilen ülkelerde ve AB'de e-imza kullanımına yönelik yasal düzenleme ve öneriler hazırlanmaktadır[109].

Kaldı ki tarihsel açıdan bakıldığında, senede birinci derecede önem verilmesinin, temsililik ve güvenilirliğin uyuşmazlığa daha yakın delillerde daha fazla olmasından kaynaklandığı[110] dikkate alındığında, e-imzanın yukarıda incelenen işlevleri ve sağladığı güvenlik sayesinde, elle atılan imzaya etkin bir alternatif oluşturabilmesinin mümkün olduğu, dolayısıyla ispat kurallarını temelindeki amaçlarda bir değişiklik olmayacağı düşünülmektedir.

Zira **ülkemizde** *Başbakanlık Dış Ticaret Müsteşarlığı* bünyesinde, e-ticarete ilişkin temel kavramların ülkemiz hukuk sistemine dahil edilmesi amacıyla oluşturulan *Elektronik Ticaret Koordinasyon Kurulu (ETKK) Hukuk Grubu*'nca AB, UNCITRAL ve ABD tarafından hazırlanan e-imza düzenlemeleri de incelenerek yapılan çalışmalar sonucunda, e-imzaların gerektirdiği teknik (güvenlikle ilgili standartların kullanımı, bunların kullanım süresi vs.) ve idari (onay kurumları vs.) gereklilikleri düzenleyen ***"Elektronik İmzanın Teknik ve İdari Yönleri Hakkında"*** **bir *"Kanun Tasarısı"*** hazırlanarak, bu Tasarıda, sistemin işleyişinin hukuken belirlenmesi gerektiği sonucuna varılmıştır.

1 Temmuz 2000 tarihi itibariyle ulaşılan sonuçlar arasında, e-imzanın delil değeri konusunda, geçerlilik şartına tabi olmayan sözleşmeler bakımından, "*Elektronik İmzanın Teknik ve İdari Yönlerine İlişkin Kanun Tasarısı"*na, ***"bu tasarı kapsamına giren elektronik imzalarla hazırlanan belgelerin mahkemelerce delil olarak kabul*** **edileceği**"ni öngören bir hükmün de ilave edilmesi de bulunmaktadır.

---

[108] KONURALP: sh. 78, 79.
[109] Eylül 1999'da Fransız Hükumeti, elektronik imzalarla ilgili bir yasa tasarısı kabul etti .Tasarı, e-imzaya elle atılan imza ile aynı statünün verilmesini öngörmektedir. (Digital Signature Law Survey, France <http://cwis.kub.nl/frw/people/hof/DS-lawsu.htm>).
[110] KONURALP: sh.10.

E-imzanın, hukuki işlemlerin ispatlanmasında, elle atılan imzaya eşdeğer bir alternatif olarak kabul edilmesi halinde, kurulacak hukuki altyapıya model teşkil etmek amacıyla oluşturulan kurallarla, ispat hususunda UNCITRAL E-İmza Yeknesak Kuralları'ndaki imza karinesi ve orijinallik karinesi gibi çeşitli karineler öngörülmekte, taraflara sistemin özelliğinden doğan bir takım bilgileri gizleme ve bir takım durumları derhal bildirim yükümlülükleri yüklenmekte ve bu yükümlülüklerin yerine getirilmemesi halinde doğacak sorumluluğun kuralları belirlenmektedir.

Çalışmamızın 3 nolu ekinde, bir yatırımcının, e-imza ile imzaladığı bir e-mail ile menkul kıymet alım-satımı talimatı vermesi halinde, çıkabilecek uyuşmazlıklar ve bu uyuşmazlıkların çözümlenmesinde e-imzanın sağladığı ispat fonksiyonunu ortaya koyan varsayımsal bir örnek olaya yer verilmiştir. (EK:3)

4.3.4.3. Karşılaştırmalı Hukukta E-İmzaya Atfedilen Delil Değeri

AB'nin 2000/31/EC sayılı E-Ticaret Direktifi'nin 9. maddesinde, Üye Devletlerin hukuk sistemlerinde, sözleşme usulüne uygulanacak hukuki şartların, e-sözleşmelerin kullanılmasında engel yaratmayacak ve bu sözleşmelerin, elektronik araçlarla yapılmış olmaları nedeniyle hukuki etkinlik ve geçerlilikten yoksunlukla sonuçlanmayacak şekilde düzenleme yapılması gerektiği öngörülmüştür.

1999/93/EC sayılı E-İmza Direktifi'nin başlangıç kısmının (recital) 20. paragrafında, belirli şartlara sahip, gelişmiş (advanced) e-imzaların, hukuki olarak elle atılan imzaya eşit kabul edilebilir olması, 21. paragrafında, tüm üye devletlerce, elektronik onaylama (e-imza) yöntemlerinin hukuk usulünde delil olarak kabul edilmesinin sağlanması ve bunun (delil olarak kabul edilebilmenin) objektif kıstaslara bağlanması gerektiği öngörülmüştür. Bununla beraber E-ticaret Direktifinde, Üye Devletlerin, taşınmazlara, miras ve aile hukukuna ilişkin vs. sözleşmelerin elektronik araçlarla yapılmasına izin vermeyebileceği de ifade edilmiştir.

Benzer şekilde **UNCITRAL**, E-İmza Taslak Kuralları'nın 6. maddesinde, kanunun imza koşulunu aradığı yerde, bu koşulun güvenli bir e-imza yöntemi ile karşılanabileceğine dair imza karinesi, 7. maddesinde, bilginin, bir e-imza kullanılarak bağlandığı veri mesajının, orjinal şeklinde olduğu (orjinal şeklinin bozulmadığı) ifade edilerek orjinallik karinesi getirilmiş ve 8. maddede bu iki karinenin şartlarının kanun koyan devletçe uluslararası standartlara uygun olarak tespit edileceği öngörülmüştür.

Öte yandan, bünyesinde senetle ispat zorunluluğuna ilişkin hükümler taşımayan ve delil serbestisi ilkesinin geçerli olduğu **ABD**'de de, *kanunda zorunlu tutulan yazılı olma ve imzalanma koşullarıyla ilgili olarak, elektronik kayıtların ve*

elektronik imzaların hukuki statüsünün açıklığa kavuşturulması amacıyla (SEC. 101-(e)) E-İmza Kanunu çıkarılmıştır.

Anılan Kanun'un "Genel Geçerlilik Kuralı" başlıklı SEC.101 hükmünün (a) bendinde, eyaletler arası veya yabancı ticaretle ilgili olarak girişilen bir sözleşme, anlaşma veya kaydın hukuki etkisinin, geçerliliğinin veya uygulanabilirliğinin, bu hususta herhangi bir kanun, düzenleme veya hukuk kuralı olsa da,

(1) bu sözleşme, anlaşma ve kayıt, elektronik bir kayıt (şeklinde) ise, yazılı olmadığı gerekçesiyle;

(2) bu sözleşme, anlaşma veya kayıt, e-imza ile imzalanmış ise, imzalı olmadığı veya imza ile onaylanmadığı gerekçesiyle,

inkar edilmemesi (yok sayılmaması) gerektiği öngörülmüştür.

Ancak E-Ticaret Direktifi'nde olduğu gibi, E-Sign Kanunu'nun SEC.103 hükmünde, e-imza ve elektronik kayıtlarının geçerliliğinin reddedilememesi kuralının, vasiyetname, boşanma ve aile hukukuna ilişkin hususlarla, yargılama usulü sırasında yürütülen mahkeme emirleri ve bildirimlerine, resmi mahkeme yazışmalarına (dava dilekçesi vs.) ve bazı hususlara ilişkin bildirimlere uygulanmayacağı düzenlenmiştir.

E-imzanın en yaygın türü olan digital imza konusunda dünyada ilk düzenleme yapan devletlerden olup, Türk Hukuk sistemi gibi Kara Avrupası sistemine (civil law) tabi olan **Almanya'**da, 1997 yılında Alman Dijital İmza Kanunu çıkarılmış olmakla beraber, yazılı şekle tabi işlemlerde aranan, *elle atılan imza koşulu* ve *imzanın maddi (elle tutulur) bir ortamda somutlaşması* koşulları yerine getirilmemiş sayıldığından, elektronik belge, güvenli delillerden kabul edilmemekte, bu tür deliller "sanal delil" olarak adlandırılarak, "bilirkişi incelemesi"ne bağlı olarak mahkemenin takdirine göre değerlendirilebilmektedir.

İtalya'da, geçerli bir e-imza, elle atılan imza ile eşit delil değerine sahiptir.

BEŞİNCİ BÖLÜM

SONUÇ
VE
SERMAYE PİYASASI MEVZUATI AÇISINDAN DEĞERLENDİRME

Internetin dünya çapında giderek artan ve yaygınlaşan kullanımı, daha düşük maliyetli, daha hızlı ve bilgiye dayanan yeni bir ticaret yöntemi olan elektronik ticareti de beraberinde getirmiştir. Ticaretin her alanında yaşanan bu gelişme, menkul kıymet işlemlerinin elektronik ticarete konu olması bağlamında, yatırımcılar, ihraççılar ve diğer sermaye piyasası kurumlarına da pek çok kolaylık ve avantajlar sağlayarak sermaye piyasalarının gelişimine katkıda bulunacaktır. Zira, IOSCO'nun "Securities Activity on The Internet" adlı Raporu'nda, internetin sermaye piyasalarında kullanılmasının, bilginin daha çok sayıda kişiye hızlı ve düşük maliyetle dağıtılmasını, yatırımcıların menkul kıymet ihraçları ve finansal hizmetlere ilişkin bilgilere daha kolay ulaşarak bu bilgileri daha iyi analiz etmesini ve daha geniş bir ürün yelpazesine ulaşılmasını sağlayacağı, bu faydaların ise, sermaye piyasası düzenlemelerinin temel amaçlarına da hizmet edeceği ifade edilmiştir.

Türk sermaye piyasası bakımından da, internetin Türk sermaye piyasasının gelişimine ve dünya sermaye piyasaları ile entegrasyonuna önemli yararları olacağı dikkate alınarak, 2499 sayılı Sermaye Piyasası Kanunu'nun 22. maddesine, 15.12.1999 tarih ve 4487 sayılı Kanunla yapılan değişiklikle eklenen ve yeniden düzenlenen (d), (s) ve (u) bendi hükümleri ile, bağımsız denetim, yatırım danışmanlığı, ihraç ve halka arz da dahil olmak üzere sermaye piyasası faaliyetlerinin elektronik ortamda yapılması ve e-imza kullanım esaslarının Kurul'ca düzenlenmesi ve denetlenmesi öngörülmüştür.

SPKn'ndaki söz konusu değişiklikle, özellikle e-imza kavramı ilk kez Türk mevzuatına girmiştir. E-imza, internet üzerinden gerçekleştirilen tüm ticari faaliyetlerin güvenli bir şekilde gerçekleştirilebilmesini sağlayabilecek anahtar bir unsurdur. Zira e-imza, elle atılan imzanın kullanıldığı her yerde kullanılabilecek bir işlevi yerine getirmek üzere oluşturulmuş bulunan ve hem teknik hem hukuki boyutu olan bir kavramdır.

ÖNERİ: E-imzanın internet üzerinden gerçekleştirilen sermaye piyasası işlemlerinde kullanılabilmesi için, SPKn'nun 22. maddesinde yapılan yasal düzenlemenin, gerekli teknik ve hukuksal altyapıyı kuran diğer düzenlemeler aracılığıyla hayata geçirilmesi zorunludur. Bu düzenlemelerle, e-imza, sertifika gibi kavramların tanımlanması; güvenilir üçüncü taraf veya diğer adıyla onay kurumu/kurumları oluşturulması ve onay prosedürünün belirlenmesi; sistemin tarafları (imza sahibi -güvenilir üçüncü kuruluş – güvenen taraf) arasındaki ilişkiler, tarafların sorumlulukları ve riskin tahsisi ile en önemlisi e-imza ile imzalanan sözleşme ve kayıtların (mesajların) hukuki statüsü, kurallara bağlanmalıdır.

ÖNERİ: E-imzanın hukuki işlem ve sözleşmelerde, geçerli bir kimlik belirleme aracı ve bir güvenlik unsuru olarak kullanılabilmesi için kurulması gereken teknik ve hukuki altyapının belirlenmesinde, bu konuda Avrupa Birliği ve UNCITRAL gibi uluslarüstü ve uluslararası kuruluşlarca hazırlanan direktif ve model kurallar dikkate alınmalı, bu hususta diğer ülkelerle işbirliği yapılmalıdır. Böylece, uluslararası yeknesak e-imza kurallarına uygun olarak kurulan e-imza sistemimiz çerçevesinde çıkarılan sertifikalar ve yaratılan e-imzaların, uluslararası alanda da geçerliliği sağlanacaktır.

ÖNERİ: Oluşturulacak teknik altyapının dayanağı olarak seçilecek elektronik kimlik belirleme mekanizması, elektronik bilginin kaynağını, bütünlüğünü ve doğruluğunu onaylamaya elverişli olmalıdır. Örneğin açık anahtar altyapısına dayanan dijital imza, elle atılan imzaya en etkin alternatif olarak kabul edilmekteyken, scan edilmiş elle atılan imza veya parmak izi tanıma sistemleri, kişi ile mesaj arasında ilişki kurmaya elverişli olmadığından, hukuki işlemlerin doğrulanmasında güvenilir bir e-imza olarak kullanılamamaktadırlar.

ÖNERİ: E-imza altyapısı, bir başkasının adı ile bir anahtar çifti (açık anahtar ve gizli anahtar) yaratılması ve bu şekilde başkasının adı ile bir elektronik mesajın imzalanması tehlikesine karşı, hangi açık anahtarın hangi kişiye ait olduğunu gösteren sertifikalar (elektronik kimlik belgeleri) ihraç ederek, kişinin açık anahtarını kimliğine bağlayan tarafsız ve güvenilir üçüncü kuruluşların (onay kurumu –sertifika hizmeti sağlayıcı) varlığını gerektirmektedir. Kurulumuzca, onay kurumlarının oluşturulması aşamasında, bu kurumların tabi olacakları statü belirlenirken aşağıdaki hususların göz önünde tutulması yararlı olacaktır.

Onay kurumlarının statüsü hususunda farklı uygulamalar vardır. Kimi ülkelerde, onay kurumlarının, bir şirketin kuruluşuna ilişkin genel koşulları haiz olmaları yeterli görülürken, bazı ülkelerde bu kurumlar zorunlu veya ihtiyari lisanslamaya tabi tutulmaktadır. Ancak uluslarüstü ve uluslararası düzenleyici kuruluşlar, onay kurumlarının sayısında, gerekçesiz olarak kısıtlamaya gidilmesinin ve ayrım yapılmasının, kuruluş özgürlüğünü zayıflatacağını ifade etmektedir. Bazı ülkelerde ise onay kurumlarının faaliyetleri sadece devlet tarafından yerine getirilmekte ve sertifikaların çıkarılmasından, tek başına devlet sorumlu olmaktadır. Ancak sertifika hizmetlerinin yalnız devlet tarafından yerine getirilmesinin, devlet onay kuruluşlarını dokunulmaz kılacağı ve bu durumun, güvenilen hizmetlere duyulan güveni zayıflatacağı belirtilmektedir. IOSCO'nun "Internet Üzerinden Menkul Kıymet İşlemlerine İlişkin Raporu"nda da, internet kullanımı ile ilgili olarak özel sektörün lider konumunda olması gerektiği ve bu konumun, yeni uygulamaların geliştirilmesi ile hizmetlerin genişletilmesi için elverişli olduğu ifade edilmiştir.

HUMK'da, değeri 40 milyon TL'nin üzerinde olan hukuki işlemlerin ancak kanuni delillerle (bunlardan en önemlisi senettir) ispatlanabileceği öngörülmekte olup, elektronik kayıtlar ve bu kayıtlardan printer vasıtasıyla alınan çıktılar ise,

senette bulunması gereken imza unsurunun eksikliği nedeniyle senet sayılmamaktadır. Ayrıca bu kayıtlardan alınan çıktılar, söz konusu çıktının, aleyhine delil teşkil ettiği kişi tarafından verilmiş olması veya o kişi tarafından ikrar edilmesi durumları dışında yazılı delil başlangıcı da sayılmamaktadır.

ÖNERİ: Söz konusu bilgisayar kayıtları ve bunlardan printer vasıtasıyla alınan çıktıların mahkemede delil olarak dinlenebilmesi, HUMK'nun senetle ispat zorunluluğunu öngören mevcut delil sistemi karşısında, ancak işlemin tarafları arasında yazılı bir delil sözleşmesi imzalanması halinde mümkün olabilecektir. Bu nedenle HUMK'nda ve ETKK Hukuk Grubunca hazırlanması önerilen E-imza Kanunu'nda, elektronik kayıtlara, hukuki işlemlerin ispatında delil değeri veren bir hüküm öngörülünceye kadar, sermaye piyasası işlemleri ile ilgili e-imza kullanımı ve bu işlemlerden doğan uyuşmazlıkların adli merciler önünde çözümünde elektronik kayıtların delil olarak dinlenebilmesi, ancak e-imza ile imzalanacak hukuki işlemin tarafları arasında, e-imzanın ve bilgisayar kayıtlarının mahkemede caiz delil olarak olacağına dair yazılı bir delil sözleşmesi yapılması ile mümkün olabilecektir. Bu nedenle Kurulumuzca, e-imza kullanım esaslarının, e-imzaya delil değeri veren söz konusu yasal düzenlemelerden önce belirlenmesi halinde, e-imzanın kullanılacağı hukuki işlemin tarafları arasında, e-imzaya ilişkin elektronik kayıtların ve e-imza ile imzalanan belgelerin, mahkemede caiz delil olabileceğine dair yazılı bir delil sözleşmesi yapılması sağlanmalıdır.

ÖNERİ: Ancak bilgisayar kayıtlarının mahkemede caiz delil olarak kabulünü içeren delil sözleşmelerinin, aracı kuruluşlar ve yatırımcılar arasında imzalanan sözleşmelerde yaygın olarak rastlanan, yatırımcı aleyhine aracı kuruluş lehine olağan üstü haklar sağlayan ve yatırımcının dava ve savunma haklarını zedeleyici kayıtlar içermesi durumunda, delil sözleşmesi hakim tarafından geçersiz sayılabilecek ve dolayısıyla, bilgisayar kayıtlarının veya e-imzanın mahkemece delil olarak dinlenmesi hukuken mümkün olamayacaktır. Bu nedenle, Kurulumuzun, özellikle aracı kuruluşlar ve yatırımcılar arasında imzalanan ve e-imzanın ve bilgisayar kayıtlarının mahkemede caiz delil olacağına dair delil sözleşmelerinin, geçersizlikle sonuçlanmasına yol açacak hükümler ve kayıtlar içermemesini temin etmesi gerekmektedir.

Bununla beraber, e-ticarete ilişkin temel kavramların ülkemiz hukuk sistemine dahil edilmesi amacıyla *Başbakanlık Dış Ticaret Müsteşarlığı* bünyesinde oluşturulan *Elektronik Ticaret Koordinasyon Kurulu (ETKK) Hukuk Grubu*'nca yapılan çalışmalar sonucunda, e-imzaların gerektirdiği teknik (güvenlikle ilgili standartların kullanımı, bunların kullanım süresi vs.) ve idari (onay kurumları vs.) gereklilikleri düzenleyen ***"Elektronik İmzanın Teknik ve İdari Yönleri Hakkında"*** bir ***"Kanun Tasarısı"*** hazırlanarak, sistemin işleyişinin hukuken belirlenmesi gerektiği sonucuna varılmış olup, bu Tasarıya, geçerlilik şartına tabi olmayan sözleşmeler bakımından, *tasarı kapsamına giren elektronik imzalarla hazırlanan*

belgelerin mahkemelerce delil olarak kabulünü öngören bir hükmün de ilave edilmesi gerektiği sonucuna varılmıştır.

Bu çerçevede yukarıda belirtilen E-İmza Kanun Tasarısı kanunlaştığında, SPKn'nun 22/(u) maddesi gereğince kullanım esasları belirlenen e-imza ve e-imza ile imzalı mesaj ve belgeler, geçerlik şartına tabi olmayan hukuki işlemlerle ilgili uyuşmazlıkların çözümünde mahkemelerde delil olarak kullanılabilecektir.

Böylece, halka açık şirketler ve Borsa şirketleri, kamuyu aydınlatıcı belgeler ve diğer belgelerini internet vasıtasıyla e-imza ile imzalamak suretiyle internet üzerinden sunabilecek, e-imzanın sağladığı kimlik belirleme işlevi ile bilgi ve belgenin kaynağını, bilgiyi/belgeyi imzalayanın bilginin/belgenin içeriğini onayladığını ve bilginin/belgenin imzalandıktan sonra değişmediğini (orijinalliğini) gösterme işlevleri sayesinde de bilginin/belgenin doğruluğu güvenli bir şekilde ortaya konulacaktır.

Yatırımcılar tarafından internet ortamında alım-satım emirleri e-imza ile imzalanarak verilebilecektir. Bu emirlerden doğan uyuşmazlıklar, e-imzanın, gönderilen emri gönderenin kimliğini, gönderilen emrin içeriğini ve orijinalliğini onaylayacağından, telefonla verilen emirlerden doğan uyuşmazlıklardan daha emin bir şekilde çözümlenebilecektir.

ÖNERİ: Ancak IOSCO Raporu'nda da belirtildiği üzere, e-imza kullanımı halinde de, aracı kuruluşların belge ve kayıt düzenine ilişkin yükümlülükleri devam etmeli, gerek bilgisayar ortamında gerek kağıt üzerinde tutulan kayıtların, kalıcı, değiştirilemez ve Kurul'ca istenildiğinde ulaşılabilir şekilde saklanması gerekmektedir. Ayrıca, aracı kuruluşların, internet üzerinden iletişim yapabilecek mesleki yeterlilikteki yeterli sayıda personel ile yeterli güvenilirlik ve kapasitedeki teknik donanıma sahip olmalıdır.

E-imza, genel kurul toplantılarında oy kullanımını, hem yatırımcı hem de şirketler bakımından güvenli ve kolay bir şekilde sağlayacaktır.

ÖNERİ: Milletlerarası özel hukukun tüketiciyi koruma amacının gerçekleştiği, tüketicinin mutad meskeni hukukunun uygulanacağı sözleşmelerin tayininde esas alınan bir kriter olan *ticari yönelme* kriterinin, yurt dışında yerleşik kuruluşların, internet üzerinden, Türkiye'de yerleşik yatırımcılara yönelik sermaye piyasası faaliyetlerinde bulunmalarına ilişkin esaslarla ilgili olarak, faaliyetin Türkiye'deki yatırımcılara yönelik olup olmadığının tespitinde kullanılabileceği kanaatindeyiz. Zira Türkiye'deki yatırımcılara yönelmiş bir sermaye piyasası faaliyeti, yatırımcıların korunması amacı ile, Türkiye'deki yatırımcıların mutad meskeni hukuku olan Türk sermaye piyasası mevzuatı gereğince Sermaye Piyasası Kurulu'ndan alınacak izne tabi olacaktır.

KAYNAKÇA

I. BASILI ESERLER

ALTAŞ Hüseyin
1998 Şekle Aykırılığın Olumsuz Sonuçlarının Düzeltilmesi, Ankara

ARKAN Sabih
1991 Bankacılıkta Kullanılan Yeni Elektronik Sistemlerle İlgili Hukuki Sorunlar, Ankara

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

BATTAL Ahmet
1997 "Bankacılık Sözleşmelerinde İspat Usulü ve Delil Sözleşmeleri", BATİDER, C.XIX, Sa.2, sh.125-140, Ankara

Studio Legale Beltramo
1999 "CONSOB Clarifies Solicitation and Placement Through the Internet", International Financial Law Review, Volume Xviii, No:7, sh. 55, 56.

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

ESCH Rob E. v., PRINS Corien
2000 The EDI Law Review, Legal Aspects of Paperless Communication, Volume 7, No.1, Netherlands

GÜNGÖR Gülin
2000 "Internet yoluyla Girişilen Elektronik Tüketici Akitleri ve Milletlerarası Özel Hukukta Tüketicinin Korunması", Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 46, S.1-4, Ankara, sh. 101-120

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

VON ILBERG, Phılıp, BENZLER, Mark
1999 "Statement Issues on Internet Marketing of Foreign Collective Investment Schemes", World Securities Law Report, Volume 5, No.1, sh.7,8.

KONURALP Haluk
1999 Medeni Usul Hukukunda İspat Kurallarının Zorlanan Sınırları, Ankara

KURU Baki
1980 Hukuk Muhakemeleri Usulü, C.II, 4. Bs, Ankara

KURU/ARSLAN/YILMAZ
1992 Medeni Usul Hukuku, Ders Kitabı, Genişletilmiş 4. Bs., Ankara

ROWE Heather, HAFTKE Mark
2000 The Practitioner's Guide to The Regulation of The Internet, Surrey ENGLAND

ÖZTAN Fırat
1997 Kıymetli Evrak Hukuku, 2. Bası, Ankara

SMITH
1999 Internet Law and Regulation, 2nd Edition, London

TEKİNAY/AKMAN/BURCUOĞLU/ALTOP
1988 Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 6. Baskı, İstanbul

TUNÇOMAĞ Kenan
1976 Türk Borçlar Hukuku, C.I, Genel Hükümler, 6. Bası, İstanbul

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

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

YILDIRIM Mehmet Kamil
1990 Medeni Usul Hukukunda Delillerin Değerlendirilmesi, İstanbul

YILMAZ Ejder
1985 Hukuk Sözlüğü, 3. Baskı, Ankara

II. INTERNET'TEN ELDE EDÝLEN KAYNAKLAR

1. KANUN, DİREKTİF ve DİĞER DÜZENLEYİCİ METİNLER

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>

Electronic Signatures In Global and National Commerce Act, List of Enacted Statutes and Regulations, McBride Baker&Coles, <http://www.mbc.com/ecommerce/legis/congress.html>

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

Illinois Electronic Commerce Security Act, <http://www.legis.state.il.us/legisnet/legisnet90/hbgroups/hb/900HB3180LV.html>

Singapur Electronic Transactions Act 1998 <http:/www.cca.gov.sg/eta/part1.html>

Utah Digital Signature Code, <http://www.jmls.edu/cyber/statutes/udsa.html>

Washington Electronic Authentication Act, Washington Code ch. 19.34 <http://www.mbc.com/ecommerce/summary.asp?states=Washington&PubID=20001029212328 >

2. RAPOR ve MAKALELER

AALBERTS B.P., VAN DER HOF Simone, Digital Signature Blindness, <http://cwis.kub.nl/ frw/people/hof/DS-art.htm>

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

GÜRAN/AKÜNAL/BAYRAKTAR/YURTCAN/KENDİGELEN/BELLER/SÖZER Internet ve Hukuk, Internet Hukuk Forumu, <http://www.superonline.com/hukuk/>

İNCE Murat:Elektronik Ticaret:Gelişme Yolundaki Ülkeler İçin İmkanlar ve Politikalar, Mart 1999, < http://ekutup.dpt.gov.tr/ticaret/incem/eticaret.html>

KUNER, Christopher, MIEDBRODT, Anja: Written Signature Requirements and Electronic Authentication:A Comparative Perspective, <http://www.kuner.com/data/sig/signature_perspective.html>

MERRILL Charles, Proof of WHO, WHAT and WHEN in Electronic Commerce, <http://www.abanet.org/scitech/ammerr.html>

The Legal Aspects of Digital Signatures, ICRI (Interdisciplinary Centre for Law&Information Technology), <http://www.law.kuleuven.ac.be/icri/projects/report.data/executive.htm>

VAN DER HOF Simone, Digital Signature Law Survey, <http://cwis.kub.nl/frw/people/hof/DS-lawsu.htm>

III. KONFERANS ve SEMİNERLER

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

SÖZER Bülent
"Elektronik Ticaret/Elektronik Sözleşmeler", TÜSİAV İstanbul Sohbetlerinde Sunulan Tebliğ (Metni), 21.6.2000, İstanbul

EK 1. A) UNCITRAL ELEKTRONİK İMZA YEKNESAK KURALLAR TASLAĞI

I. GENEL YORUM

II. ELEKTRONİK İMZA KURALLARI TASLAĞI

Madde 1. Uygulama Alanı (Kapsam)

Madde 2. Tanımlar

Madde 3. Tarafsız Teknoloji - İmzalara Eşit Muamele

Madde 4. Yorumlama

Madde 5. Tarafların Özerkliği - Sözleşme Özgürlüğü

Madde 6. İmza Şartlarına Uyum - İmza Karinesi

Madde 7. Orjinallik Karinesi

Madde 8. 6. ve 7. Maddelerin Yerine Getirilmesi

Madde 9. İmza Aracı Sahibinin Sorumlulukları

Madde 10. Onay Hizmetleri Sağlayıcının Sorumlulukları

Madde 11. E-İmzaya Güven

Madde 12. Sertifikaya (Kimliğe) Güven

Madde 13. Yabancı Sertifikaların ve E-İmzaların Tanınması

GENEL YORUM

Yeknesak kuralların amacı, e-imzanın uluslararası ticari muamelelerde giderek artan kullanımını kolaylaştırmaktır. Bir çok ülkede pek çok düzenleyici kural hazırlanmakta ve uygulanmakta olup, bununla beraber, bu taslak kurallar ile, dijital imza veya tanınabilecek diğer e-imzaların yasal etkileri gözönüne alınarak belirlenen bir takım standartların oluşturulması ve bu suretle e-ticarete uygulanacak yasal kuralların uyumsuzluğunun önlenmesi amaçlanmaktadır.

Yeknesak kurallar ticari işlemlerin özel hukuk yönüne odaklandığından, e-imzanın kullanımından doğabilecek tüm sorunları çözme çabasında değildir.

Model Kanun esasına dayanarak, Yeknesak Kuralların özellikle yansıtmayı amaçladığı şey, tarafsız araç ilkesi, kağıda dayanan geleneksel kavram ve uygulamaların işlevsel denkliği yaklaşımında önyargılı davranılmaması ve geniş bir taraf özerkliğidir. Bu kurallar ile, hem önceden

sözleşme olmaksızın tarafların elektronik ortamda iletişimde bulundukları "açık" ortamda, hem de tarafların önceden mevcut, sözleşmesel kurallar ve prosedür ile bağlandıkları "kapalı" ortamda geçerli olacak asgari standartların kullanılması amaçlanmaktadır.

ELEKTRONİK İMZA YEKNESAK KURALLAR TASLAĞI

Madde 1. Uygulama Alanı (Kapsam)

Bu kurallar, ticari[111] faaliyetlerle ilgili olarak e-imza kullanımına uygulanır. Bu kurallar tüketiciyi koruma amacına yönelik hukuk kurallarına aykırı olamaz.

Madde 2. Tanımlar

a) Elektronik İmza: Elektronik formdaki bir bilgiye eklenmiş olan veya mantıksal olarak o bilgi mesajı ile bağlantısı kurulabilen, bilgi mesajıyla ilgili kişinin (imza sahibinin) kimliğini tanımlamaya ve bilgi mesajının içeriğinde yer alan bilginin imza sahibince onaylandığını göstermeye yarayan bir yöntemdir.

b) Güvenli elektronik imza:(Enhanced electronic signature)

Güvenli imza, bir imzadır ki, bu imzanın (güvenlik usulünün) (yönteminin) kullanımı aracılığıyla aşağıdaki hususlar (kanıtlanabilir) ortaya konulabilir:

i) kullanıldığı imza aracına münhasır olduğu,

ii) eklendiği veri mesajına, imza sahibi tarafından, imza sahibinin münhasır kontrolü altındaki bir araç kullanılmak suretiyle eklendiği,

iii) eklendiği veri mesajının bütünlüğünü temin eden bir usule ilişkin olduğu

c) Kimlik belgesi - Sertifika (Certificate): Anahtar çiftine (imza aracına) sahip olan bir gerçek veya tüzel kişinin kimliğinin doğruluğunu araştırma anlamındaki bir veri mesajı veya onaylayıcı (certifier) tarafından çıkarılan diğer kayıt anlamına gelir.

[111] E-imza çalışma grubuna göre, "Ticari" ibaresi, sözleşmesel olan veya olmayan, ticaretin doğasını ilgilendiren tüm sorunlarını içerecek geniş bir yoruma açık olarak düzenlenmelidir. Mal ve hizmet alış verişi veya temini; dağıtım anlaşması; ticari temsilcilik veya acentalık; faktoring; leasing; inşaat işi; danışmanlık; mühendislik; licencing; yatırım; finans; banka; sigorta; patent veya ruhsat anlaşması; iş ortaklığı (joint venture); ve diğer endüstriyel ve ticari işbirlikleri; hava, deniz, kara ve demiryoluyla mal veya yolcu taşıma gibi ancak bunlarla sınırlı olmamak üzere herhangi bir ticari muamele, ticaretin doğasını ilgilendirmektedir.

d) Veri Mesajı (Data Message) Elektronik veri değişimi (EDI), elektronik posta, telgraf, telex veya telecopy gibi (ancak bunlarla sınırlı olmamak üzere) elektronik, görsel veya benzer araçlar ile üretilen (oluşturulan), gönderilen, alınan veya saklanan bilgidir.

e) İmza sahibi (Signature Holder) (Araç sahibi, anahtar sahibi, abone, imza aracı sahibi, imzalayan); bir veri mesajına, onun tarafından veya onun adına güvenli imza konulabilen veya eklenebilen bir kimsedir.

f) Bilgi onaylayıcı (information certifier) (Güvenli) elektronik imzanın kullanımını desteklemede kullanılan (bilgi onaylama, kimlik belirleme) hizmetleri sağlama ve onaylama işini gören bir kişi veya varlıktır.

Madde 3:Teknolojik Tarafsızlık (İmzalara Eşit Muamele)

(Technology Neutrality- Equal Treatment of Signatures)

Bu Kurallar'ın hiçbir hükmü, (Kurallar'ın 6(1) hükmünde belirtilen koşulları sağlayan)(uygun bir anlaşmayı da içeren bütün koşulların ışığında, veri mesajının oluşturulması veya ilişkilendirilmesi amacına uygun olduğu kadar güvenilir de olan) herhangi bir elektronik imza yöntemini dışlamak, kısıtlamak veya hukuki sonuçtan yoksun bırakmak amacıyla uygulanmamalıdır.

Madde 4. Yorum

(1) Bu Kurallar'ın yorumlanmasında, Kurallar'ın uluslararası orijinlerine ve uygulanmasında, yeknesaklığı geliştirme amacı ve iyiniyetin yerine getirilmesine (observance of good faith) itibar edilmesi zorunludur.

(2) Bu Kurallarla düzenlenen ve açıkça çözüme bağlanmamış olan konulara ilişkin sorular, bu (Yeknesak) Kuralların dayandığı genel ilkelere uygun olarak çözülür.

Madde 5. (Anlaşma ile değiştirilebilme) (Taraf Özerkliği) (Sözleşme Özgürlüğü)

Bu Kurallar'da veya kanun koyucu Devletin hukukunda aksi kararlaştırılmadıkça, bu Kuralların etkileri, anlaşma ile azaltılabilir veya değiştirilebilir.

Madde 6:(İmza Koşullarına Aykırılık) (İmza karinesi)

(1) Kanunun bir kimsenin imzasının varlığını aradığı (şart koştuğu) yerde, bir veri mesajının oluşturulması veya ilişkilendirilmesi amacı için uygun olduğu kadar güvenilir de olan bir elektronik imza kullanılırsa, ilgili anlaşma da dahil olmak üzere, bütün koşullar gözönünde bulundurularak, bu koşul o veri mesajına atfen karşılanır.

(2) 1. Paragraf, o zamanki koşulların bir senet gerektirip gerektirmediği ya da kanunun sadece imzanın yokluğuna bağladığı sonuçları sağlayıp sağlamadığına göre uygulanır.

Maddenin (2). bendinden sonraki hükümleri iki farklı şekilde düzenlenebilir.

Varyant A

(3) Aşağıdakileri sağlayan bir elektronik imzanın, 1. Paragrafta belirtilen koşulları yerine getirme amacı için güvenilir olduğu varsayılır:

(a) e-imzanın atılmasında (yaratılmasında) kullanılan veri, kullanıldığı konuda, imza aracı sahibine (imza sahibine) münhasırdır.

(b) imza aracını elinde tutan (imza sahibi), (ilgili zamanda) imza aracı üzerindeki kontrole münhasıran sahiptir.

(c) e-imza, bilgiye (veri mesajına veya o mesajın parçasına), bilginin bütünlüğünü garanti eden usulde bağlıdır

(d) İmza aracını elinde tutan, veri mesajının kullanıldığı araç konusunda nesnel (tarafsız) olarak tanımlanır.

Varyant B

(3) Aksi yönde kanıt bulunmadıkça, e-imzanın kullanımının,

(a) e-imzanın 1. Paragrafta öngörülen güvenilirlik standartlarını karşıladığı,

(b) yetkili imza sahibinin kimliğini,

(c) yetkili imza sahibinin, e-imzaya ilişkin bilgiyi onayladığı

hususlarını ispatladığı varsayılır.

(4) 3. Paragraftaki varsayım sadece,

(a) e-imzaya güvenme niyetinde olan bir kimsenin, yetkili imza sahibine, e-imzaya (3. Paragrafta sayılan hususların kanıtı olarak) (yetkili imza sahibinin elle atılan imzasına eşit olduğu) hususlarında güvendiğini bildirmesi,

(b) yetkili imza sahibinin, alt paragraf (a)'da belirtilen, (3. Paragrafta sayılan hususların kanıtı olarak) (yetkili imza sahibinin elle atılan imzasına eşit olduğu) hususlarda e-imzaya güvenilmemesini gerektiren nedenlerden dolayı, bildirimde bulunan kişiye derhal bildirimde bulunmayı ihmal etmesi,

hallerinde uygulanır.

Madde 7: Orjinallik Karinesi

(1) Bir veri mesajının,

(a) bilginin, ilk oluşturulduğu zamandaki son şeklinin bütünlüğünü güvenilir şekilde sağlayan bir veri mesajı olarak veya başka bir şekilde: ve

(b) bilginin sunulmasının gerektiği yerde, sunulduğu kişiye gösterilebilecek durumda olan,

ve 6. maddede belirtilen bir yöntem (bir e-imza) kullanılarak bağlandığı veri mesajının, orjinal şeklinde olduğu (orjinal şeklinin bozulmadığı) varsayılır.

Bu madde hükümleri aşağıdaki durumlarda uygulanmaz (.....)

Madde 8: 6. ve 7. Maddelerin Yerine Getirilmesi

(1) Kanun koyucu devlet tarafından belirlenen bir otorite veya organ, 6. ve 7. madde hükümlerinin koşullarını karşılayan yöntemleri belirleyebilir.

(2) (1). Paragraf gereğince yapılan belirleme, tanınmış olan uluslararası standartlara uygun olmalıdır.

Madde 9:İmza Aracı Sahibinin Sorumlulukları

(1) Bir imza aracı sahibi (imzalayan):

(a) İmza aracının yetkisiz (izinsiz) kullanımından kaçınma hususunda makul bir dikkat göstermelidir.

(b) Aşağıdaki durumlarda aşırı gecikme olmaksızın ilgili kişilere bildirimde bulunmalıdır.

(i) imza aracı sahibinin (imza sahibinin), imza aracının tehlike altına girdiğini bildiği veya

(ii) imza aracı sahibince, imza aracının tehlike altına girmesine yol açabilecek esaslı risklere neden olduğu bilinen şartlar,

(c) (İmza aracını destekleme amacıyla bir kimlik belgesinin (sertifikanın) kullanıldığı yerde) (İmza aracının sertifika kullanımını gerektirdiği yerde) sertifikada yer alan veya sertifikanın geçerlilik döneminde imza aracı sahibi tarafından yapılan bütün maddi beyanların doğruluğunu ve bütünlüğü sağlamak için makul bir dikkat göstermelidir.

(2) Bir imza aracı sahibi, 1. Paragrafın gereklerini yerine getirmediği taktirde sorumlu olmalıdır[112].

Madde 10:Onay (Sertifika) Hizmetleri Sağlayıcıların Sorumluluğu

(1) Bir onay hizmetleri sağlayıcı,

(a) uygulamaları uyarınca yaptığı beyanlara uygun davranmalıdır.

(b) onay kurumları tarafından, sertifikanın geçerlik süresine veya sertifikanın içeriğine ilişkin yapılan bütün maddi beyanların doğruluğunu ve bütünlüğünü sağlamak için makul bir dikkat göstermelidir.

(c) güvenen bir tarafın aşağıdaki hususların doğruluğunu araştırabilmesine izin veren, makul olarak erişilebilir araçlar temin etmelidir.

i) onay hizmetleri sağlayıcının kimliğini,

ii) sertifikada tanımlanan kimsenin ilgili zamanda, sertifikada dayanılan imza aracını elinde tuttuğunu,

[112] 2. Paragraf, imza aracı sahibinin 1. Paragrafta belirtilen koşulları yerine getirmemesi halinde sorumlu tutulması gerektiği ilkesini getiriyor ve bu sorumluluğa bağlanan hukuki sonuçları Yeknesak Kurallarında dışında, bu hususu kanunlaştıran herbir ülkede uygulanabilir kurallara bırakıyor.

iii) imza aracını (sahibini) elinde tutanı tanımlamakta kullanılan metodu (yöntemi),

iv) imza aracının kullanılabilmesine ilişkin amaç veya miktar sınırlamalarını ve

v) imza aracının geçerli olup olmadığını ve tehlike altında bulunmadığını,

(d) İmza aracı sahipleri için, imza aracının tehlikeye düşmüş olduğunu bildirecek ve zamanında iptal hizmeti işlemini sağlayacak vasıtalar temin etmelidir.

(e) Hizmetlerini yerine getirirken, güvenilir sistemler, prosedürler (usuller) ve insan kaynaklarından yararlanmalıdır.

(2) Sistemler, usuller ve insan kaynaklarının 1. paragrafın (e) alt paragrafı amacına yönelik olarak güvenilir olup olmadığının ve ölçütünün tespitinde aşağıdaki unsurlar dikkate alınmalıdır:

(a) yasal yetki sınırları içindeki varlıkların (alacakların) mevcudiyeti de dahil olmak üzere finansal ve beşeri kaynaklar;

(b) donanım ve yazılım sistemlerinin güvenilirliği;

(c) sertifika işlem usulleri, sertifika başvuruları ve kayıtların muhafazası (saklanması);

(d) sertifikalarda tanımlanan imzalayanlar (sertifikanın sujesi) ve potansiyel (müstakbel) güvenen taraflar bakımından bilginin edinilebilirliği (kullanılabilirliği),

(e) bağımsız bir kuruluşca yapılan düzenli, kapsamlı ve sistemli inceleme,

(f) yukarıda belirtilenlerin varlığı veya bunlara uygunluk hususunda Devlet, görevli bir güvenilir kuruluş veya onay hizmetleri sağlayıcı tarafından yapılan bir bildirimin (ilanın) varlığı,

(g) Kanun yapan devlet mahkemelerinin yargı yetkilerinin dikkate alınması,

(h) Onay hizmeti sağlayıcının davranışlarına uygulanacak hukuk ile kanun yapan hukuk arasındaki farklılığın derecesi

(3) Bir sertifika;

(a) onay hizmeti sağlayıcının kimliğini,

(b) sertifikada tanımlanan kimsenin, ilgili zamanda sertifikanın dayandığı imza aracını elinde tuttuğunu,

(c) imza aracının sertifikanın çıkarıldığı tarihte veya bu tarihten önce geçerli olduğunu,

(d) sertifikanın kullanılabileceği miktar (değer) için veya amaç için bir takım sınırlamaları,

(e) onay hizmeti sağlayıcının herhangi bir kimseye karşı kabul ettiği sorumluluğun ölçütü veya kapsamı üzerindeki sınırlamaları

belirtmelidir.

4. Bir onay hizmetleri sağlayıcı (1). paragrafın gereklerini yerine getirmedeki ihmalinden sorumlu olmalıdır.

Varyant A:

5. Zararın tespitinde aşağıdaki etkenler dikkate alınmalıdır:

(a) Sertifikayı elde etme bedeli,

(b) Sertifikaya bağlanan bilginin özelliği,

(c) Sertifikanın kullanma amacına yönelik olarak herhangi bir sınırlama olup olmadığı, varsa miktarı,

(d) Onay hizmetleri sağlayıcıların sorumluluk alanını veya miktarını sınırlandıran bir kaydın olup olmadığı,

(e) güvenen taraf ile herhangi bir fon, aidat işlemi

Varyant B:

Onay hizmetleri sağlayıcının sorumluluğu, bu kurumun, 1. paragrafın gereklerini yerine getirmedeki ihmalinin meydana geldiği zamandaki olaylar veya muhtemel sonuçlarını bildiği veya bilmesi gereken meseleler dikkate alınarak, önceden gördüğü veya görmesi gereken zararlardan fazla olamaz.

Madde 11. Elektronik İmzalara Güven

(1) Bir kimse, bir elektronik imzaya, öyle davranması makul olmayan bir derecede güvenme hakkına sahip değildir.

(2) Güvenin makul olup olmadığının tespitinde, uygun olduğu taktirde,

(a) elektronik imzayı teşvikin amaçlandığı temel işlemin doğası;

(b) Güvenen tarafın e-imzanın güvenilirliğini tespit etmek için uygun tedbirleri alıp almadığı (girişimde bulunup bulunmadığı),

(c) Güvenen tarafın, e-imzanın bir sertifika ile desteklenip desteklenmediğini araştırmak için gereken girişimlerde bulunup bulunmadığı,

(d) Güvenen tarafın, e-imza aracının tehlikeye girmiş olduğunu veya iptal edilmiş olduğunu bilip bilmediği veya bilmesi gerekip gerekmediği,

(e) Bir anlaşma veya güvenen tarafın, abone ile parçası olduğu muamele veya uygulanabilecek herhangi bir ticari örf adet,

(f) diğer ilgili etkenler

dikkate alınmalıdır

Madde 12. Sertifikalara Güven

(1) Bir kimse, bir sertifikada yer alan bilgiye, öyle davranması makul olmayan bir derecede güvenme hakkına sahip değildir.

(2) Bir sertifikadaki bilgiye güvenmiş olan bir kimsenin güveninin makul olup olmadığının tespitinde, uygun olduğu taktirde,

(a) Sertifika üzerinde yer alan kısıtlamalar,

(b) Güvenen tarafın, sertifikanın güvenilirliğini belirlemek için, ilgili yerdeki sertifika iptali veya askıya alınma listesine başvuruyu da içeren, (tedbirler alıp almadığı) girişimlerde bulunup bulunmadığı,

(c) herhangi bir anlaşma veya güvenen tarafın sahip olduğu veya ilgili zamanda sahip olmuş bulunduğu onay hizmetleri sağlayıcı veya abone ile ya da uygulanabilir ticari örf ve adet

(d) diğer ilgili etkenler

dikkate alınmalıdır.

Variant A:

Paragraf (1)'e ilişkin etkenlere ilişkin şartlar altında, elektronik imzaya güven makul değilse, güvenen taraf imzanın geçerli olmaması riskini üstlenir.

Variant B:

Paragraf (1)'e ilişkin etkenlere ilişkin şartlar altında, elektronik imzaya güven makul değilse, güvenen taraf, imza aracı sahibine veya onay hizmeti sağlayıcıya karşı bir talepte bulunma hakkına sahip olmamalıdır.

Madde 13: Yabancı Sertifikaların ve Elektronik İmzaların Tanınması

(1) Bir sertifikanın (veya e-imzanın) hukuki olarak yürürlükte olup olmadığının veya ölçüsünün tespitinde, sertifikanın (veya e-imzanın) çıkarıldığı yer ve ihraççının ticari işinin yeri dikkate alınmamalıdır.

(2) Yabancı onay hizmetleri sağlayıcıların işlemleri, kanun koyucu devletin hukuku uyarınca onay hizmetleri sağlayıcılarda aranan koşullarla en azından denk bir güvenilirlik derecesi sağlıyorsa, yabancı bir onay hizmeti sağlayıcı (onay kurumu) tarafından çıkarılan sertifikalar, kanun koyucu devletin hukuku gereğince işletilen onay hizmeti sağlayıcılar tarafından çıkarılan sertifikalara hukuken eşit olarak tanınır. Bu tanıma, Devletin yayımladığı bir karar gereğince veya ilgili devletin taraf olduğu iki taraflı veya çok taraflı anlaşma ile yapılabilir.

(3) Diğer devletin hukuku, kanun koyucu devletin hukuku gereğince böyle imzalar için aranan koşullara eşit düzeyde asgari güvenilirlik koşulları gerektiriyorsa, elektronik imzalara ilişkin diğer devlet hukukuna uygun elektronik imzalar, yasa koyucu devletin hukuku gereğince çıkarılan imzalara hukuken denk olarak tanınır. Bu tanıma, Devletin yayımladığı bir karar gereğince veya ilgili devletin taraf olduğu iki taraflı veya çok taraflı anlaşma ile yapılabilir.

(4) Denkliğin tespitinde, uygun olduğu taktirde, (10. maddenin 2. paragrafındaki etkenler) aşağıdaki etkenler dikkate alınmalıdır:

(a) yasal yetki sınırları içindeki varlıkların (alacakların) mevcudiyeti de dahil olmak üzere finansal ve beşeri kaynaklar;

(b) donanım ve yazılım sistemlerinin güvenilirliği;

(c) sertifika işlem usulleri, sertifika başvuruları ve kayıtların muhafazası (saklanması);

(d) sertifikalarda tanımlanan imzalayanlar (sertifikanın sujesi) ve potansiyel (müstakbel) güvenen taraflar bakımından bilginin edinilebilirliği (kullanılabilirliği),

(e) bağımsız bir kuruluşca yapılan düzenli, kapsamlı ve sistemli inceleme,

(f) Yukarıda belirtilenlerin varlığı veya bunlara uygunluk hususunda Devlet, görevli bir güvenilir kuruluş veya onay hizmetleri sağlayıcı tarafından yapılan bir bildirimin (ilanın) varlığı,

(g) Kanun yapan devlet mahkemelerinin yargı yetkilerinin dikkate alınması,

(h) Onay hizmeti sağlayıcının işlemlerine uygulanacak hukuk ile kanun yapan Devletin hukuku arasındaki farklılığın derecesi

(5) 2. ve 3. paragraflara rağmen, ticari veya diğer işlemlerin tarafları, özel bir onay hizmetleri sağlayıcıyı, onay hizmetleri sağlayıcıların sınıfını veya sertifikaların sınıfını, onlara eklenen imzalar ve mesajlar ile ilgili olarak kullanılması gerektiğini açıkça belirleyebilirler.

(6) 2. ve 3. paragraflara rağmen, tarafların, kendi aralarında, belli tip e-imzalar ve sertifikaların kullanımında anlaşmaları halinde, (bu anlaşma sınır ötesi tanıma amacı için yeterli olarak tanınmalıdır), bir e-imzanın veya sertifikanın hukuken yürürlükte olup olmadığının veya bunun ölçüsünün tespitinde, o imzanın veya sertifikanın kullanıldığı işlemin tarafları arasındaki anlaşma dikkate alınmalıdır.

EK:1-B

Annex I. DRAFT UNIFORM RULES ON ELECTRONIC SIGNATURES

Article 1. Sphere of application

These Rules apply where electronic signatures are used in the context* of commercial** activities and do not override any rule of law intended for the protection of consumers.

* The Commission suggests the following text for States that might wish to extend the applicability of these Rules:

"These Rules apply where electronic signatures are used, except in the following
situations: [...]."

** The term "commercial" should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not.
Relationships of a commercial nature include, but are not limited to, the following transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement; commercial representation or agency; factoring; leasing; construction of works; consulting; engineering; licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of these Rules:

(a) "Electronic signature" means [data in electronic form in, affixed to, or logically
associated with, a data message, and] [any method in relation to a data message] that may be used to identify the signature device holder in relation to the data message and indicate the signature device holder's approval of the information contained in the data message;

[(b) "Enhanced electronic signature" means an electronic signature in respect of which it can be shown, through the use of a [security procedure] [method], that the signature:

(i) is unique to the signature device holder [for the purpose for][within the context in] which it is used;

(ii) was created and affixed to the data message by the signature device holder or using a means under the sole control of the signature device holder [and not by any other person];

[(iii) was created and is linked to the data message to which it relates in a manner which provides reliable assurance as to the integrity of the message";]].

(c) "Certificate" means a data message or other record which is issued by an information certifier and which purports to ascertain the identity of a person or entity who holds a particular [key pair] [signature device];

(d) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

(e) "Signature holder" [device holder] [key holder] [subscriber] [signature device holder] [signer] [signatory] means a person by whom, or on whose behalf, an enhanced electronic signature can be created and affixed to a data message;

(f) "Information certifier" means a person or entity which, in the course of its business, engages in [providing identification services] [certifying information] which [are][is] used to support the use of [enhanced] electronic signatures.

Article 3. [Technology neutrality] [Equal treatment of signatures]

None of the provisions of these Rules shall be applied so as to exclude, restrict, or deprive of legal effect any method [of electronic signature] [that satisfies the requirements referred to in article 6(1) of these Rules] [which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement] [or otherwise meets the requirements of applicable law].

Article 4. Interpretation

(1) In the interpretation of these Uniform Rules, regard is to be had to their international origin and to the need to promote uniformity in their application and the observance of good faith.

(2) Questions concerning matters governed by these Uniform Rules which are not expressly settled in them are to be settled in conformity with the general principles on which these Uniform Rules are based.

Article 5. [Variation by agreement] [Party autonomy] [Freedom of contract]

These Rules may be derogated from or [their effect may be] varied by agreement, unless otherwise provided in these Rules or in the law of the enacting State.

Article 6. [Compliance with requirements for signature] [Presumption of signing]

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if [a method] [an electronic signature] is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement..

(2) Paragraph (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

Variant A

(3) It is presumed that [a method] [an electronic signature] is reliable for the purpose of satisfying the requirement referred to in paragraph (1) if that method ensures that:

(a) the data used for the creation of an electronic signature are unique to the holder of the signature [creation] device within the context in which they are used;

(b) the holder of the signature [creation] device [has] [had at the relevant time] sole control of that device;

(c) the electronic signature is linked to the [information] [the data message or the part of that message] to which it relates [in a manner which guarantees the integrity of that information];

(d) the holder of the signature [creation] device is objectively identified within the context [in which the device is used][of the data message].

Variant B

(3) In the absence of proof to the contrary, the use of an electronic signature is presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (1);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the information to which the electronic signature relates.

(4) The presumption in paragraph (3) applies only if:

(bbb) the person who intends to rely on the electronic signature notifies the alleged signer that the electronic signature is being relied upon [as equivalent to the hand-written signature of the alleged signer][as proof of the elements listed in paragraph (3)]; and

(ccc) the alleged signer fails to notify promptly the person who issues a notification under subparagraph (a) of the reasons for which the electronic signature should not be relied upon [as equivalent to the hand-written signature of the alleged signer][as proof of the elements listed in paragraph (3)].

Variant C

(3) In the absence of proof to the contrary, the use of an electronic signature is presumed to prove:

(a) that the electronic signature meets the standard of reliability set out in paragraph (1);

(b) the identity of the alleged signer; and

(c) that the alleged signer approved the information to which the electronic signature relates.

[(4)][(5)] The provisions of this article do not apply to the following: [...].

[Article 7. Presumption of original

(1) A data message is presumed to be in its original form where, in relation to that data message, [a method] [an electronic signature] [within article 6] is used which:

(a) provides a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented;

(2) The provisions of this article do not apply to the following: [...].]

Article 8. Satisfaction of articles 6 and 7

Variant A

(1) *[The organ or authority specified by the enacting State as competent]* may determine which methods satisfy the requirements of articles 6 and 7.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

Variant B

(1) One or more methods of electronic signature may be determined as satisfying the requirements of articles 6 and 7.

(2) Any determination made under paragraph (1) shall be consistent with recognized international standards.

Article 9. Responsibilities of the signature device holder

(1) Each signature device holder shall:

(a) Exercise reasonable care to avoid unauthorized use of its signature device;

(b) Notify appropriate persons without undue delay if:

(i) the signature device holder knows that the signature device has been compromised; or

(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised;

(c) [Where a certificate is used to support the signature device,] [Where the signature device involves the use of a certificate,] exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder which are relevant to [the life-cycle of the] certificate, or which are to be included in the certificate.

(2) A signature device holder shall be liable for its failure to satisfy the requirements of paragraph (1).

Article 10. Responsibilities of a supplier of certification services

(1) A supplier of certification services shall:

(a) act in accordance with the representations it makes with respect to its practices;

(b) exercise due diligence to ensure the accuracy and completeness of all material representations made by the supplier of certification services that are relevant to the life-cycle of the certificate or which are included in the certificate;

(c) provide reasonably accessible means which enable a relying party to ascertain:

(i) the identity of the supplier of certification services;

(ii) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;

(iii) the method used to identify the signature device holder;

(iv) any limitations on the purposes or value for which the signature device may be used; and

(v) whether the signature device is valid and has not been compromised;

(d) Provide a means for signature device holders to give notice that a signature device has been compromised and ensure the operation of a timely revocation service;

(e) Utilize trustworthy systems, procedures and human resources in performing its services.

(5) In determining whether and the extent to which any systems, procedures and human resources are trustworthy for the purposes of subparagraph (e) of paragraph (1), regard shall be had to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the supplier of certification services regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and

(h) the degree of discrepancy between the law applicable to the conduct of the supplier of certification services and the law of the enacting State.

(3) A certificate shall state:

(a) the identity of the supplier of certification services;

(b) that the person who is identified in the certificate holds, at the relevant time, the signature device referred to in the certificate;

(c) that the signature device was effective at or before the date when the certificate was issued;

(d) any limitations on the purposes or value for which the certificate may be used; and

(e) any limitation on the scope or extent of liability which the supplier of certification services accepts to any person.

Variant X

(4) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

(5) Liability of the supplier of certification services may not exceed the loss which the supplier of certification services foresaw or ought to have foreseen at the time of its failure in the light of facts or matters which the supplier of certification services knew or ought to have known to be possible consequences of the supplier of certification services' failure to [fulfil the obligations [duties] in][satisfy the requirements of] paragraph (1).

Variant Y

(4) A supplier of certification services shall be liable for its failure to satisfy the requirements of paragraph (1).

(5) In assessing the loss, regard shall be had to the following factors:

(a) the cost of obtaining the certificate;

(b) the nature of the information being certified;

(c) the existence and extent of any limitation on the purpose for which the certificate may be used;

(d) the existence of any statement limiting the scope or extent of the liability of the supplier of certification services; and

(e) any contributory conduct by the relying party.

Variant Z

(4) If damage has been caused as a result of the certificate being incorrect or defective, a supplier of certification services shall be liable for damage suffered by either:

(a) a party who has contracted with the supplier of certification services for the provision of a certificate; or

(b) any person who reasonably relies on a certificate issued by the supplier of certification services.

(5) A supplier of certification services shall not be liable under paragraph (2):

(a) if, and to the extent, it included in the certificate a statement limiting the scope or extent of its liability to any relevant person; or

(b) if it proves that it [was not negligent][took all reasonable measures to prevent the damage].

Article 11. Reliance on electronic signatures

(1) A person is not entitled to rely on an electronic signature to the extent that it is not reasonable to do so.

(6) [In determining whether reliance is not reasonable,] [In determining whether it was reasonable for a person to have relied on the electronic signature,] regard shall be had, if appropriate, to:

(a) the nature of the underlying transaction that the electronic signature was intended to support;

(b) whether the relying party has taken appropriate steps to determine the reliability of the electronic signature;

(c) whether the relying party took steps to ascertain whether the electronic signature was supported by a certificate;

(d) whether the relying party knew or ought to have known that the electronic signature device had been compromised or revoked;

(e) any agreement or course of dealing which the relying party has with the subscriber, or any trade usage which may be applicable;

(f) any other relevant factor.

Article 12. Reliance on certificates

(1) A person is not entitled to rely on the information in a certificate to the extent that it is not reasonable to do so.

(2) In determining whether reliance is not reasonable,] [In determining whether it was reasonable for a person to have relied on the information in a certificate,] regard shall be had, if appropriate, to:

(a) any restrictions placed upon the certificate;

(b) whether the relying party has taken appropriate steps to determine the reliability of the certificate, including reference to a certificate revocation or suspension list where relevant;

(c) any agreement or course of dealing which the relying party has or had at the relevant time with the supplier of certification services or subscriber or any trade usage which may be applicable;

(d) any other relevant factors.

Variant A

(3) If reliance on the electronic signature is not reasonable in the circumstances having regard to the factors in paragraph (1), a relying party assumes the risk that the signature is not a valid signature.

Variant B

(3) If reliance on the signature is not reasonable in the circumstances having regard to the factors in paragraph (1), a relying party shall have no claim against the signature device holder or the supplier of certification services.

Article 13. Recognition of foreign certificates and electronic signatures

[(1) In determining whether, or the extent to which, a certificate [or an electronic signature] is legally effective, no regard shall be had to the place where the certificate [or the electronic signature] was issued, nor to the State in which the issuer had its place of business.]

(2) Certificates issued by a foreign supplier of certification services are recognized as legally equivalent to certificates issued by suppliers of certification services operating under ... *[the law of the enacting State]* if the practices of the foreign suppliers of certification services provide a level of reliability at least equivalent to that required of suppliers of certification services under ... *[the law of the enacting State*]. [Such recognition may be made through a published determination of the State or through bilateral or multilateral agreement between or among the States concerned.]

(3) Signatures complying with the laws of another State relating to electronic signatures are recognized as legally equivalent to signatures under ... *[the law of the enacting State]* if the laws of the other State require a level of reliability at least equivalent to that required for such signatures under ... *[the law of the enacting State*]. [Such recognition may be made by a published

determination of the State or through bilateral or multilateral agreement with other States.]

(4) In determining equivalence, regard shall be had, if appropriate, [to the factors in paragraph (2) of article 10] [to the following factors:

(a) financial and human resources, including existence of assets within the jurisdiction;

(b) trustworthiness of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to the [signers][subjects] identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the State, an accreditation body or the certification authority regarding compliance with or existence of the foregoing;

(g) susceptibility to the jurisdiction of courts of the enacting State; and.

(5) Notwithstanding paragraphs (2) and (3), parties to commercial and other transactions may specify that a particular supplier of certification services, class of suppliers of certification services or class of certificates must be used in connection with messages or signatures submitted to them.

(6) Where, notwithstanding paragraphs (2) and (3), parties agree, as between themselves, to the use of certain types of electronic signatures and certificates,[that agreement shall be recognized as sufficient for the purpose of cross-border recognition]. [In determining whether, or the extent to which, an electronic signature or certificate is legally effective, regard shall be had to any agreement between the parties to the transaction in which that signature or certificate is used.]

EK 3 : E-İMZA İLE VERİLEN MÜŞTERİ EMRİ ÖRNEĞİNDE E-İMZANIN İSPAT FONKSİYONU VE E-İMZA İLE UYUŞMAZLIK ÇÖZÜMÜ[113]

VARSAYIMSAL ÖRNEK[114]

Yatırımcı A'nın bir aracı kurumda aktif bir menkul kıymet alım satım hesabı vardır. A, aracı kurum temsilcisi B'ye, hesabındaki menkul kıymetlerin alım veya satımına ilişkin talimat vermek için sık sık internet e-mailini kullanmaktadır.

Aracı Kurum temsilcisi B, aşağıdaki belgeyi, kendisine ait kişisel bilgisayarının hard diskinden printer vasıtasıyla (çıktı) almıştır.

to: B @ abc.com

from:A @) xyz.com

Date:27 Şubat 1997 10:00

*" Hesabıma hemen Netscape A.Ş.'nin 100 adet hissesini geçerli piyasa fiyatından **AL** lütfen"*

27 Şubat Perşembe günü A'nın hesabına 100 adet Netscape hissesi alıyor. 28 Şubat günü Netscape'in piyasa fiyatı düşüyor ve bu durum söz konusu işlemde esaslı bir düşüş yaratıyor. A, 100 adet Netscape alım işleminin yazılı ekstresini aldığında aşağıdaki iddialardan birini öne sürebilir.

1. E-mail mesajı göndermedim.

2. E-mail mesajı gönderdim ancak "100 adet Netscape hissesi **SAT**" dedim.

---

[113] Bu başlık altındaki açıklamalarda, Amerikan Barosu Bilim ve Teknoloji Bölümü Bilgi Güvenliği Komitesi'nce, Ağustos 1996 yılında 70'den fazla teknolojist ile dünyanın her yerinden avukatların 4 yıllık işbirliği neticesinde yayınladığı Digital Signature Guidelines'da (Digital İmza Kılavuzu) tanımlanan açık imza altyapısı esas alınmaktadır. Kılavuz, ticaret hukukunun hukuki prensipleri ile asimetrik kriptosistemin güçlü teknolojik kapasitelerini birleştiren bir açık imza altyapısı sistemi tanımlamaktadır.

[114] MERRILL, C.;Proof of WHO, WHAT and WHEN in Electronic Commerce, Delivering Security Services A Merger od Technological and Legal Viewpoints, <http://abanet.org/scitech/ammerr.html>

3. E-mail mesajı gönderdim ancak 28 Şubattan önce değil, fiyat düştükten sonra gönderdim.

Problem ve açık ağ üzerinden e-ticaret için esas zorluk, atomlar yerine bitlerin oluşturduğu dijital bir ortamda, kağıda ve insan ilişkilerine dayanan ortamdaki ihtilafların çözümü için geleneksel olarak uygun olabilen ipuçlarından yoksun olmaktır.

Burada uyuşmazlığı çözen otoritenin (hakim, hakem vs.) karşı karşıya kalacağı üç muhtemel teori vardır:

I. A yalan söylüyor, B doğru söylüyor.

A mesajı gönderdi ve B mesajda herhangi bir tahrifat yapmadı. A, hisse senedi alma niyetindeydi, ancak piyasa düştükten sonra zarardan kaçınmak için verdiği talimatı inkar etti. Ya da "sat" demek istediği halde "al" mesajı gönderdi. Veya 27 Şubat'ta mesajı gönderdiği halde, 28 Şubatta fiyatlar düştükten sonra mesajı gönderdiğini iddia ediyor.

II. B yalan söylüyor, A doğru söylüyor. ,

B mesajı tahrif etti ve tahrif edilmiş halinin çıktısını aldı.

A, hiç mesaj göndermedi.

B, hisseleri kendi hesabına veya başka bir müşterisi hesabına aldı ve piyasa düşükten sonra zararı A'ya yüklemeye çalıştı.

Ya da A, "al" mesajı gönderdiği halde, B bunu "sat" anladı.

Veya A, 28 Şubatta mesajı gönderdi ve B, bilgisayarının 27 Şubat olarak göstermesini sağladı.

III. Hem A, hem de B doğru söylüyor.

A, mesaj göndermedi ancak B, 27 Şubat'ta bilinmeyen bir kimseden (bir sahteciden) mesaj aldı. Bu kimse A'nın mesajındaki "al" ifadesini "sat"a çevirdi.

A veya B'nin ifadelerinin göreli değerine göre, uygun ve tanıdık hukuki sistemdeki usulle, karar verilebilir. Hukuk bilimi bakımından en zor olasılık, her tarafın da doğru söylediği ve her iki tarafın da mağdur olduğu son durumdur.

Bu sorunlar, e-imza ile imzalanmamış, dolayısıyla bunun getirdiği garantilerden yoksun bir e-mail ile verilen bir yatırımcı emrinden doğabilecek sorunlardır. E-mailin dijital imza ile imzalanması durumunda durum nasıl olurdu.

Yukarıdaki varsayımsal örnek, Amerikan Barosu'nca hazırlanan Dijital İmza Kılavuzu (ABA Digital Signatures Guidelines) ile bu Kılavuza benzer hükümler içeren Utah[115] ve Washington[116] eyaletlerindeki e-imza düzenlemelerine göre değerlendirilmiştir.

DİJİTAL İMZA KILAVUZU UYARINCA KARAR VERME

1. ADIM: Mesajda bir dijital imza varsa, bu imza aşağıdaki hususları belirleyebilir:

a) E-imza kullanılarak şifrelenerek veya diğer bir ifadeyle dönüştürülerek gönderilen mesajın, dönüşümünün (şifrelemesinin), imzalayanın açık anahtarına tekabül eden gizli anahtarla yapılıp yapılmadığı,

b) Başlangıçtaki mesajın, dönüşüm yapıldığından beri (e-imza ile imzalandıktan sonra) değiştirilip değiştirilmediği

Mesajda dijital imza varsa Dijital İmza Kılavuzu uygulanır ve 2. adıma geçilir. Bu ihtiyari bir sistemdir. Bunun anlamı, dijital imzanın kullanımı, kullanıcılar için ihtiyaridir. Kullanıcı mesajı dijital olarak imzalamadıysa, Kılavuz uygulanmaz, mevcut hukuk uygulanır.

2. ADIM: Güvenen tarafa dijital imzalı bir mesaj geldiyse, bu kişi uygun bir açık anahtara da sahipse, kripto yazılımı, güvenen tarafın, **dijital imzanın, açık anahtara tekabül eden gizli anahtarı kullanan kimse tarafından atılıp atılmadığını** belirlemesine imkan verir. Sonuç, dijital imzayı o açık anahtarı bağlamaktadır, ancak o mesajı kimin imzaladığı hala bilinmemektedir.

3. ADIM: Güvenilir üçüncü taraf, (onay kurumu) tarafından çıkarılmış bir dijital sertifikaya sahip miyiz?

Sertifika, diğer bilgilerle beraber, aboneyi diğerlerinden ayıran adını ve açık anahtarını da içerir. Sertifika, genellikle 1 yıllık işlem süresi boyunca abonenin kimliğini, onun açık anahtarına bağlar.

4. ADIM: Dijital imzayı ve mesaj bütünlüğünü teyit etme

Dijital imzanın geçerli bir sertifikanın işlem periyodu (dönemi) sırasında yaratılmasını gerekir. Buna göre, e-imza, işlem periyodun başlangıcından önce veya geçerlilik süresinin dolmasından veya sertifikanın iptal edildiği tarihten sonra yaratılmış olmamalıdır. Bu şart yerine getirildiyse dijital imza doğrulanır. (teyit edilir)

İlk üç adımın birarada bulunması ile dijial imza yatırımcı A'ya bağlanmış olur.

---

[115] UTAH Digital Signature Code, (<http://www.jmls.edu/cyber/statutes/udsa.html>)
[116] Washington Electronic Authentication Act (http://www.search.leg.wa.gov/wslrcw/RCW)

5. ADIM: Karineler

Bu noktada analizler, uyuşmazlık çözüm prosedürünün uygulanması bağlamında, hukuki bir boyut kazanır.

Bir dijital imzayı içeren bir uyuşmazlığın çözümünde, **aksi ispat edilebilen bir karine** olarak,

1. Geçerli bir sertifikada açık anahtar ile doğrulanan bir dijital imza, o sertifikada yer alan abonenin imzasıdır.

2. Teyit edilen bir dijital imza, ilgili mesajın orjinal halinden farklı değildir (değişmemiştir).

Kağıda dayanan geleneksel hukuk gereğince, imzalı bir belgeye güvenen bir kimsenin, belgenin ilgili kişi tarafından imzalanmış olduğunu ispat külfeti vardır. Ancak, asimetrik kriptosistem teknolojisinin güçlü güvenlik yeteneğinin sonucu olarak, Digital İmza Kılavuzu, dijital imzanın tam olarak teyit edildiği yerde bu karineyi ters çevirir.

Örnek olayda, e-mail mesajı dijital olarak imzalandıysa, ve A'nın geçerli sertifikasına atfen önceki 4. adıma göre teyit edildiyse, A, e-mail mesajının kendisi tarafından imzalandığı ve imzalandığı andan itibaren değişmemiş olduğu karinesini çürütmekte başarılı olmadıkça B'ye karşı sorumlu olur.

A'nın karineyi çürütme ve sorumluluktan kurtulma konusunda 2 önemli yolu vardır:

6. ADIM: a) A'nın mesajı imzaladığı karinesini çürütebileceği ilk ve en ciddi yol, onay kurumunun açık anahtarı içeren sertifikanın abonesi olarak A'yı tanımlamada (kimlik tespitinde) yanlışlık yaptığına dair ispat yükünü taşımasıdır. A'nın ulaşabileceği gerçek bir teori de, bir sahtekarın A'nın adına sertifika başvurusunda bulunarak A'nın kimliğini kullanmasıdır. A, bunu ispatlayabildiği taktirde, güvenen tarafın yanlış sertifikaya güvenmek suretiyle uğradığı zararın, onay kurumunun hatasından kaynaklandığı gerekçesiyle, onay kurumunca tazmin edilmesi talebinde bulunur.

7. ADIM: b) A'nın mesajı kendisinin imzaladığı karinesini çürütebilmesi için 2. yol, A'nın gizli anahtarı mesajda kullanılmış olsa bile, bu anahtarın yetkisiz olarak kullanıldığı hususunun ispatlanmasıdır.

A, gizli anahtarı üzerindeki kontrolünü kaybetmiş olduğunu, gizli anahtarın deşifre olduğunu veya izni olmaksızın elinden çıkmış olduğunu ve bu mesajı imzalamakta kullanıldığını ispat yükü altındadır.

8. ADIM: A'nın, gizli anahtarını deşifre olmaktan koruma yükümlülüğü vardır. 7. adıma göre A, gizli anahtarının, bir başkası tarafından mesajı imzalamakta kullanıldığını ispatlayabildiyse, A'nın kendisine ait gizli anahtarı korumakta kusurlu olup olmadığı araştırılacaktır. A, gizli anahtarını deşifre olmaktan koruma hususunda kusurluysa, her iki tarafın da kusursuz olduğu durumda olduğu gibi, zararını gizli anahtarının yetkisiz kullanıcısından tazmin talebinde bulunabilir.

Kılavuz da A'nın kendi özen yükümlülüğünü ispat külfetinin olup olmadığı ve B'nin Anın ihmalini ispat yükümlülüğü olup olmadığı hususunda açıklık yoktur. Bu kural iki taraftan birine daha fazla serbesti bırakma dileğindeki devlet veya yargı gücü tarafından belirlenecek yaklaşımlarla sağlanacaktır.

Özen standardının, dijital imza yazılımının yerleştirildiği smart kartlara veya deşifrasyonu korumayı sağlayan aşağıdaki üç donanıma bağlanması olasıdır.

a) maddi emare şartı

b) gizli PIN şartı

c) fiziki varlığın biyometrik ispatı kanıtı

9. ADIM: A, gizli anahtarının deşifre olduğunu fark ettiğinde, güvenen taraflara karşı sorumluluğunu, en azından sertifikayı iptal etmek suretiyle kaldırabilir. Böylece sertifika, iptal edilen sertifikalar listesine girer ve sertifikanın işlem dönemi o tarihten sonra dijital imza yaratılıp teyit edilmez.

10. ADIM: A, bazı nedenlerle güvenen tarafı zamanında uyarmaya yarayan, sertifikayı iptal yükümlülüğünü yerine getirmekte başarısız olursa, (iptal etmezse) ve B'nin sertifikaya güvenmemesini gerektiren bazı şartlar gerçekleşmişse, bu defa B'nin mesaja güvenmeden önce, neden telefon vs. yollarla A'yı arayarak mesajı teyit etmediği konusu gündeme gelecektir.