MARMARA ÜNİVERSİTESİ

BANKACILIK VE SİGORTACILIK ENSTİTÜSÜ

SİGORTACILIK ANA BİLİM DALI

ELEKTRONİK SİGORTACILIKTA E-İMZA

HAZIRLAYAN: ZEHRA CAHİDE ÇİTLİ

ÖĞRETİM ÜYESİ: YRD. DOÇ. DR. AYTEN ÇETİN

İstanbul 2012

T.C.
MARMARA ÜNİVERSİTESİ
Bankacılık ve Sigortacılık Enstitüsü

Aşağıda belirtilen lisansüstü tez, Lisansüstü Öğretim Yönetmeliği hükümlerinde belirtilen esaslar çerçevesinde jüri önünde savunulmuş ve jüri tarafından başarılı bulunmuştur.

TEZ BAŞLIĞI : Elektronik Sigortacılıkta E-İmza

TÜRÜ :Yüksek Lisans

TEZİ HAZIRLAYAN : Zehra Cahide ÇİTLİ

ANABİLİM DALI : Sigortacılık

SAVUNMA TARİHİ : 24.02.2012

JÜRİ ÜYELERİ :

GÖREVİ	**ADI SOYADI**	**İmza**
Danışman	Yrd.Doç.Dr.Ayten ÇETİN	
Üye	Prof.Dr.Aslı YÜKSEL MERMOD	
Üye	Yrd.Doç.Dr.Fatma PAMUKÇU	

Marmara Üniversitesi Göztepe Kampusu Bankacılık ve Sigortacılık Enstitüsü 34722 Kadıköy / İSTANBUL
0 (216) 347 69 51 (Faks)
0 (216) 418 20 88
bse@marmara.edu.tr
http://bse.marmara.edu.tr
Ayrıntılı bilgi için: İ.SOYADI Unvan

İÇİNDEKİLER

GİRİŞ

Enformasyon ve iletişim teknolojileri kapitalist sanayi toplumlarını karakterize eden sosyal ilişkilerde ve temel ekonomik yapılarda yaşanan büyük dönüşümü tetikleyen temel etken olarak görülmektedir. Kapitalist birikim sürecinin 1970'ler sonrası girdiği darboğazla başlayan yeniden yapılanma döneminde enformasyon ve iletişim teknolojileri çokuluslu sermayenin küresel ölçekte yayılmasının önündeki engelleri aşmasına yardım edecek altyapıyı oluşturmaktadır. Enformasyonun hızında ve miktarında yarattıkları artışla iletişim maliyetlerinde önemli bir düşüşe olanak veren bu teknolojiler, çokuluslu firmaların belirlediği bu dönemde uluslararası ticaretin dünya çapında genişleyebilmesinde kilit noktaya oturmuşlardır.

Enformasyon ve iletişim teknolojilerini kullanarak genişleyen yeni birikim süreci hükümetlerin ve uluslararası kuruluşların politikalarıyla da mümkün kılınmıştır. İkinci Dünya Savaşı sonrası uluslararası ticaret rejimi içerisine alınmamış olan hizmetler sektörü yeni birikim rejimine dahil edilmiştir. Hizmetler sektörünün uluslararası ticaret rejimi içerisine alınması ise bilgisayar temelli iletişim ağlarının önemini arttırmıştır. Diğer yandan ulusal ve küresel enformasyon altyapısı eylem planları hazırlanmış; kurulacak enformasyon şebekelerinin birleştirilerek geleceğin enformasyon toplumlarının omurgasını oluşturacağı görüşü egemenlik kazanmıştır. Açık elektronik iletişim ağları üzerinden yapılan her türlü işlem ve özellikle de kapitalist sermayenin akışı ise kritik anlamda bilgi güvenliğine bağlıdır. Sayısal ağlar üzerinde gerçekleşen elektronik ticaretin gelişebilmesi ve kullanıcılar tarafından benimsenmesi bu ağlar üzerinde yapılan işlemlerde hukuki açıdan güvenliğin sağlanması ihtiyacını doğurmuştur. Taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu sağlayacak teknik ve hukuki altyapıların kurulmasına yönelik yasal düzenlemeler tüm dünyada hayata geçirilmeye başlanmıştır.

A. Çalışmanın Amacı

Çalışmamızın amacı bilgi güvenliği uygulamalarının hukuki ve teknik altyapısının dünyada ve Türkiye'de inşa sürecinin hangi aşamada olduğunu belli etmek ve bu inşa sürecinde belirleyici olan faktörleri ortaya koymaktır.

B. Çalışma Yöntemi ve Sınırlılıkları

Çalışmamızın şekli, ayrıntılı "literatür taraması" olarak belirlenmiştir. Çalışmamız, 3 ana bölümde oluşmaktadır. İlk bölümde, elektronik imzaya ilişkin tanımlar verilmiş, ikinci bölümde elektronik sigorta ile genel tanımlar belirtilmiş, üçüncü bölümde ise elektronik sigorta ve elektronik imza ilişkisi kanunlar, yönetmelikler ve pratikteki uygulamalar ile incelenmiştir.

BİRİNCİ BÖLÜM

ELEKTRONİK İMZA'NIN TEMEL ÖZELLİKLERİ

1.1. ELEKTRONİK İMZA

Internet üzerinde yapılan işlemlerde, özellikle elektronik ticaret uygulamalarında, en çok ihtiyaç duyulan şeylerin başında güvenlik gelmektedir. Zaman içinde elektronik ortamda el yazısı ile imza yerine geçebilecek kadar güvenilir bir mekanizma kullanılmak üzere düzenleme arayışlarına gidilmiştir. Böylece internet üzerinden yollanan bilgilerin güvenilirliğinin sağlanması, bilgilerin, güvenli ve değişmeden, aynı zaman hukuki koruma sağlayıcı nitelik kazanarak yerine ulaşması gibi amaçlarla teknik çalışmalara başlanmıştır. "Elektronik imza altyapısı, elektronik belgenin şifrelenmesini mümkün kılmakta, değiştirilmesini önlemekte ve ayrıca birden çok kişi ile mesajın şifrelendiği anahtar kelimeyi öğrenmelerine gerek kalmadan, elektronik yoldan haberleşmeyi kolaylaştırmaktır."[1] Gerçekten de elektronik imza elektronik ortamda ihtiyaç duyulan, özellikle elektronik ticaret için zorunluluk arz eden güvenli bir ortam ihtiyacını karşılamayı amaçlamaktadır. "Elektronik imzanın birçok çeşitleri bulunmakta olup bunlardan sayısal imza, düşük maliyeti nedeniyle dünyada en çok kullanılandır".[2]

Dünya çapında e-ticaretin hızla geliştiğini ve online yaşamın hayatın vazgeçilmez bir parçası olduğunu söyleyebiliriz. Fakat bunların önündeki en büyük engel "güvenlik"tir. İşte bu noktada e-imza ortaya çıkmaktadır. Dijital kimlik ve verilerin güvenliği, şirketlerdeki ve kurumlardaki işleyişi önemli oranda etkilemektedir. Tüm araştırma raporları hack olaylarının ve internet zayıflıklarının alarm verecek durumda arttığını göstermektedir. 2006'lı yıllara kadar birçok kredi kartı bilgileri veya internet bankacılığı bilgilerinin hackerlerin eline geçtiği birçok araştırmacı kurum tarafından raporlanmıştır. İşte e-ticaret ve dijital kimliklere olan saldırılar, bu tür bilgilerin korunmasına özel bir ihtiyaç yaratıyor. Bu sorunların sitelerin (e-ticaret, internet bankacılığı gibi) muhatap oldukları kişiyi tanımlamamasından kaynaklandığını göstermektedir. Bu sorunlar gidermek içinde dünya çapında dijital imzalar devreye girmiş durumdadır.

---

[1] Leyla Keser Berber, Şekil ve Dijital İmza, Elektronikteki Gelişmeler ve Hukuk, Ankara, 2001, s. 503-556.

[2] Mehmet Emin Özgül, Internette Hukuki Güvenlik ve Dijital İmza, http://www.*inet-tr.org.tr/inetconf8/bildiri/141.doc erişim tarihi 02.03.2011*

E-ticaretin gelişebilmesi ve kullanıcılar tarafından benimsenebilmesinin "ilk şartı, açık ağ sistemine güven duyulmasının sağlanmasıdır."[3]

1.1.1 Tanımı Ve Kapsamı

Elektronik imzanın neyi ifade ettiği konusunda çeşitli tanımlar bulunmaktadır. Bir tanıma göre "elektronik imza kişinin el yazısı ile attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştirmeye yarayan matematiksel formüllere veya şifreleme programlarına verilen isimdir."[4] Diğer bir tanımla ise elektronik imza, "kişilerin biyometrik özelliklerine dayalı (ses, göz retina taraması, parmak izi taraması gibi) biyometrik yöntemler, kredi kartlarında kullanılan PIN kodları, elle atılmış imzanın tarayıcıdan geçirilerek elektronik ortama aktarılmış hali, bilgisayar ekranında bu amaçla yapılmış bir kalemle atılan imza tekniği ve çift anahtarlı kriptografiyle oluşturulan dijital (sayısal) imzayı da içeren bir üst kavramdır."[5]

Yine başka bir tanıma göre elektronik (dijital) imza, "klasik imzaya tanınan işlevleri de kapsayan bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır."[6]

Başka bir tanıma göre elektronik imza, "klasik imzaya tanınan işlevleri de kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır."[7]

Elektronik imzanın bir diğer tanımı, "bir bilginin üçünü kişilerin erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimliklerini doğrulanarak iletildiğini elektronik

---

[3] Haluk Konuralp, Genel Hatlarıyla Elektronik İmza Kanunu, Bankacılık Açısından Elektronik İmza Konferansı, 04.04.2004 İstanbul. www.tbb.org.tr/eklenenler/eklenenler-ocak2004.htm erişim tarihi: 10.08.2011

[4] Leyle Keser Berber, Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi, http://hukukcu.com/modules/smartsection/item.php?itemid=39&keywords=site, erişim tarihi: 24.05.2010

[5] Mine Erturgut, Elektronik İmza Kanunu, e-Belge ve e-İmza (Hukuki Açıdan Tanıtım Ve Değerlendirme) Bankacılar Dergisi Sayı 48, 2003, s.66

[6] Semra Arıkan, Dünya'da ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım Ek 3, Ankara 1999, s.151

[7] Saadet Arıkan, Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım, Ankara, 1999, s. 151

veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir settir."[8] şeklinde belirtilmiştir.

Birleşmiş Milletler Uluslar arası Ticaret Yasası Komisyonu tarafından hazırlanan Elektronik İmzalar İçin Yeknesak Kurallar Taslağı'nda, e-imza, "veri mesajını imzalayanı ve imzalayanın mesajın içeriğindeki bilgiyi kabulünü belirlemek için kullanılabilen, bir veri mesajına ekli veya mantıken onunla ilişkilendirilmiş elektronik şekildeki veri"[9] şeklinde tanımlanmaktadır.

Elektronik imza, A.B.D Küresel ve Ulusal Ticarette Elektronik İmza Yasası'nda (Electronic Signatures in Global and National Commerce Act) bir sözleşmeye doğrudan eklenmiş yada mantıksal bağlantı kurulabilen ve kaydı imzalamak niyetini güden kişi tarafından oluşturulmuş veya kullanılmış, her türlü elektronik ses, sembol yada kayıt"[10] şeklinde tanımlanmıştır.

Alman Elektronik İmza Kanunu'nda da Avrupa Birliği Direktifi ile hemen hemen aynı unsurları içeren bir tanım yapılmıştır. Buna göre, gelişmiş bir elektronik imza tanımında 4 unsur bir araya gelmelidir:

a) Sadece imza anahtarı sahibi adına özgülenmiş.

b) İmza anahtarı sahibini tanımaya imkan veren.

c) İmza anahtarı sahibinin kendi kontrolü altında bulunan araçlarla yaratılan

d) İmzanın bağlantılı olduğu verilerin sonraki değişikliklerini tespite imkan vermektedir.

Elektronik imza, elektronik ortamda bilginin orijinalliği bozulmadan tarafların kimliğini de belirleyerek karşı tarafa aktarılmasını garanti eden harf ve sembollerden oluşmuş bir settir. Elektronik imza olmadan elektronik ticaretin gelişmesi ve güvenirliliğinin sağlanması mümkün değildir. Elektronik imza, biyometrik imza ve dijital imza olarak ikiye ayrılır. Biyometrik imza, kullanıcının parmak izi veya retina gibi kişiye has özellikler

[8] Elektronik Ticaret Koordinasyon Kurulu Raporları, Hukuk Çalışma Grubu Raporu, s.8
[9] Digital Signature Report, www.un.org.at/uncitral/english/workinggroups/wg_ec/wp-88e.pdf erişim tarihi: 11 Mart 2011)
[10] Marianne Menna, From Jamestown to the Silicon Valley Pioneering A Lawless Frontier: The Electronic Signatures in Global and National Commerce Act, http://www.vjolt.net/vol6/issue2/v6i2-a12-Menna.html erişim tarihi: 9 Ocak 2011

kullanılarak oluşturulan imzadır. Dünyadaki eğilim daha çok dijital imzadan yanadır. Dijital imza ise açık ve gizli anahtarla gönderilen iletiye vurulan bir mühürdür. Dijital imza göndericiden kimliğini tespite yarar ve gönderilen iletinin açık ve net biçimde hem teyidini gem de orijinalliğinin bozulmamasını sağlar.[11]

Elektronik imza, elle atılan imzaya eşdeğer nitelikte kullanılabildiği için, elektronik ortamda her türlü resmi işlemin, kağıt ortamına göre daha hızlı, güvenilir ve maliyet etkin biçimde yürütülmesini sağlar. Bu bağlamda elektronik imza, kamu kuruluşlarıyla yapılan işlemlerde, bankacılık ve sigortacılık işlemlerinde, e-devlet, e-iş ve e-ticaret uygulamalarında, elektronik haberleşme ve sözleşmelerde, Kanun kapsamındaki hukuki işlemlerde kullanılabilir.

1.1.2 Şekli

Dijital imza, elektronik belgeyi şifreleyerek onun değiştirilmesini önlemekte ve ayrıca birden fazla kişinin şifreyi oluşturan anahtarı öğrenmeden elektronik yoldan haberleşmesini sağlamaktadır. Teknik olarak dijital imza, anahtar dediğimiz bu çift şifreden oluşmaktadır. Bu anahtarların birisi elektronik olarak haberleşen taraflardan göndericide, diğeri ise alıcıda bulunur. Bu anahtarlardan göndericide bulunan gizli anahtarla dijital imza oluşturulur. Açık anahtar isimli verilen diğeri ise, alıcıya bildirir ve sadece dijital imzanın doğrulanmasında kullanılır. Sistemin güvenilir bir şekilde işlemesi, her iki anahtarın uzunluğuna ve gizli anahtarın gönderici tarafından güvenli bir şekilde saklanmasına bağlıdır.[12]

Dijital imza birtakım teknik altyapılara ihtiyaç duymaktadır. Kullanıcının bir bilgisayarı ve kendine ait bir bilgisayar programı (software) mevcut olmalıdır. Ayrıca "kullanıcının bunlar yoluyla elde edeceği bir şifresinin de bulunması gerekmektedir."[13]

[11] Mustafa Topaloğlu, Bilişim Hukuku, Karahan Kitabevi, İstanbul 2006, s.119
[12] Mustafa Topaloğlu, ag.e, s.120
[13] Leyla Keser Berber, İmzalıyorum O Halde Varım, TBBD Sayı:2000/2 s. 514

1.2. ELEKTRONİK İMZA UYGULAMASINDA KULLANILAN BELGELER

Elektronik belge dediğimizde, en basit ifadeyle elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler kastedilmektedir. Bu anlamda internet üzerinden yapılan hukuki işlemler, e-mail yoluyla gönderilen irade beyanları, çeşitli veri taşıyıcılarına kaydedilmiş ve irade açıklaması içeren elektronik veriler aklımıza gelmektedir. Elektronik belge veya elektronik kayıt gibi terimler, elektronik ortamda yaratılan bir bilgiyi ifade etmek üzere kullanılmaktadır.[14]

Belgenin sözlük anlamı, "bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika, doküman"dır.[15] Belge, günümüze kadar, günlük hayatta kullanıldığı şekliyle hemen her zaman, kağıt üzerinde cisim bulmuş olma unsuruyla bağdaştırılmıştır. Çünkü bu şekliyle kağıt üzerindeki belgelerin istenildiği anda ibraz edilmesi ve her an gözle algılanabilir şekilde bulunması özelliklerinin getirdiği avantaj, kağıtta tecessüm etmiş belgelerin şimdiye kadar tercih edilmesini ve yaygın kullanımını sağlamıştır. Belgelerin herhangi bir yardımcı araç olmaksızın görülebilmesi her zaman algılanabilir olduğu anlamındadır. Belge, medeni usul hukukundaki senet kavramından geniş bir anlama sahiptir. Her senet bir belgedir, fakat her belge medeni usul hukuku anlamında senet özelliklerini taşımaz. Elektronik belgelerle ilgili teknik tanım olmadığı gibi bir hukuki tanım da henüz bulunmamaktadır. Elektronik belge terimi, kağıda dayalı belgeler karşısında bir sınırlamayı ifade eder ve bununla açıklamanın bulunduğu veri taşıyıcısının nitelemesi anlatılır. Sayfa üzerinde, işaretler ve harflerden oluşan bir yığın taşıyan kağıt belgeler gibi, elektronik belgeler de çoğunlukla o zamanki işletme sistemi anlamında, bir ya da daha fazla veriler formunda, kodlanmış ve/veya kodlanmamış bilgi yığını (bilgiler yığını) içerir. Kağıt belgelerin aksine, elektronik belgelerde en önemli sorun, belgenin içeriğinin sonradan değiştirilip değiştirilmediğinin tespitinin mümkün olmamasıdır. Bu durum, elektronik belgelerin yargılamada ispat aracı olarak kullanılmasına da engel olmaktadır. Özel hukuk alanında hukuki işlemlerin yapılmasında kural olarak şekil serbestisi ilkesi geçerlidir.

[14] Billur Yaltı, E-İmza ve E-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-I, Vergi Sorunları Dergisi, Nisan 2001, s.151
[15] http://www.tdk.org.tr/tdksozluk/sozara.htm, 19.2.2004.

Elektronik belgelerle üç şekilde karşılaşılır:[16]

Bilgisayarın belleğinde veya veri taşıyıcısında kayıtlı veriler: (Bilgisayarın Ana Belleğinde Kayıtlı veya Disket, CD Gibi Taşıyıcılarda Kayıtlı Veriler) Dış bellek birimleri, verilerin kalıcı olarak saklandığı yerdir. Bunlar, sabit diskler (hard disk), disketler, CD ler ve teyplerdir.

-Bilgisayar Ekranında Görülen Veriler (İnternet Aracılığıyla Görülen Veriler): Kişinin e-mail adresinde saklı bulunan elektronik belgeler veya bir internetteki web sitesinde yayınlanan veriler örnektir.

-Bilgisayar Çıktısı ve Bilgisayar Faks: Bilgisayar çıktısı, elektronik ortamda bulunan bir verinin yazıcı (yardımcı araç) vasıtasıyla kağıtta vücut bulmuş halidir. Böylece, elektronik ortamdaki veri, elektrik mevcut olduğu sürece gözle görülebilir olan durumundan, elle tutulabilir ve her zaman görülebilir bir duruma geçmiş olmaktadır. Bilgisayar çıktısı için yazıcıya ihtiyaç bulunmaktadır. Bilgisayara bağlı yazıcı sayesinde, bilgisayar ekranında görülebilen herhangi bir veri, kağıt yüzeye aktarılmış olmaktadır.

1.2.1. Sözleşmeler

Elektronik sözleşmeler, elektronik iletişim araçları kullanılarak yapılan sözleşmeler olarak tanımlanmaktadır. "Elektronik iletişim araçlarıyla yapılan işlemleri, bu kapsamda elektronik sözleşme olarak saymak gerekmektedir."[17]

Elektronik sözleşmenin birçok tanımı yapılmıştır. Bu tanımlardan bir kaçı şöyledir.

- İnternet üzerinden ve bilgisayar desteğiyle telekomünikasyon teknolojisi kullanılarak mal üretilmesi ve hizmet sunulması ve satış bedellerinin tahsil edilmesidir.

-Bilgisayar ve iletişim ağları aracılığıyla elektronik yoldan girişilen hukuki işlemlerdir.
-İnternet üzerinden ve internet araçları kullanılarak yapılan sözleşmelerdir.

-Elektronik araçlarla yapılmış olan ve/ veya elektronik araçlarla tamamlanan sözleşmelerdir.

[16] Hakan Pekcanıtez, Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri, Uluslararası İnternet Hukuku Sempozyumu, İzmir 21-22 Mayıs 2001, s.409.
[17] Mustafa Topaloğlu, Bilişim Hukuku, Karahan Kitabevi, Adana 2005, s.46

Elektronik Sözleşmeler, tanıtım ve teklif internet üzerinden verilse de geleneksel metotla tanzim edilen poliçelere ıslak imza atıldığı için herhangi bir yasal sorun bulunmamaktadır. "İnternet üzerinden akdedilen elektronik sözleşmelerde de Borçlar Kanunu'nun öngördüğü akit serbestîsi prensibi uygulanabilmektedir."[18]

"Ancak, bir anahtarı kullanarak diğerine ulaşmak mümkün değildir."[19]

1.2.2. Sertifikalar

Elektronik Sertifika, yani elektronik kimlik sahibinin kişisel bilgilerini ve bu kişisel bilgilere ait açık anahtar bilgisini taşıyan ve taşıdığı açık anahtar bilgisinin, belirtilen kişi veya kuruma ait olduğunu garanti eden belgedir. Sertifika çift (açık) anahtarlı kriptografi teknolojisine dayanır ve kamuya açıktır, yani sertifikalar gizli tutulması gereken dosyalar değillerdir. Elektronik kimlik belgesi kişilere ait olabildiği gibi kurumların ve web sunucuların da elektronik kimlik belgeleri olabilir. Bir elektronik kimlik belgesinde bulunması gereken bilgiler aşağıdaki gibidir:

"-Sahibinin kamuya açık anahtarı

-Sahibinin adı, soyadı, çalıştığı kurum gibi kimlik bilgileri

-Elektronik kimlik belgesinin geçerlilik süresi

-Seri numarası

-Elektronik kimlik belgesini veren Sertifika Hizmet Sağlayıcı bilgileri

-Sertifikanın kullanım alanlarını belirleyen bilgiler."[20]

Elektronik sertifika günlük hayatta kullanılan ehliyet, pasaport gibi kimlik kartlarını elektronik ortamdaki karşılığıdır denilebilir. "Elektronik sertifikalar sertifika otoriteleri tarafından düzenlenir."[21] "Elektronik sertifika, kullanıcı adıyla onun açık anahtarını içeren ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik

[18] Selda Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, Pusula Yayıncılık, İstanbul 2002, s.68
[19] Ulvi Altınışık, Elektronik Sözleşmeler, Seçkin Yayınevi, İstanbul 2003, s. 82.
[20] 5510 Sayılı Elektronik İmza Kanunu, Kabul Tarihi: 15.1.2004 http://www.tbmm.gov.tr/kanunlar/k5070.html erişim tarihi: 01.04.2011
[21] Özgür Deniz Erzincan, E-imza Deneyimi, Telekom Dünyası Dergisi, Temmuz 2004, s.32

belgedir."[22] Diğer bir deyişle elektronik sertifika imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı ifade eder. Elektronik sertifika, kişilerin veya kuruluşların bilgilerinin elektronik ortamda güvenli bir şekilde iletilmesini sağlamaktadır. Elektronik sertifika imza sahibinin imza doğrulama verisini yani açık anahtarını ve kimlik bilgilerini birbirine bağlayan elektronik kayıt olarak da tanımlanabilir. Bu tanım Avrupa Birliği Direktifindeki ve mevzuatlardaki sertifika tanımlarına uygundur. Elektronik sertifikalar, imzalama-doğrulama işlemi sırasında imzalayanın kimliğinin güvenilir üçüncü kişi (sertifika hizmet sağlayıcısı) tarafından teyit edilmesi amacıyla kullanırlar.[23]

Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir. Elektronik sertifika hizmet sağlayıcısı, Kuruma yapacağı bildirimden iki ay sonra faaliyete geçer.

Elektronik sertifika hizmet sağlayıcısı yapacağı bildirimde;

a) Güvenli ürün ve sistemleri kullanmak,

b) Hizmeti güvenilir bir biçimde yürütmek,

c) Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak,

ile ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.[24]

Elektronik sertifika hizmet sağlayıcıları; hizmetin gerektirdiği nitelikte personel istihdam etmek ve nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle yükümlüdür. Türkiye'de Sertifika Sağlayıcılığı Konusundaki ilk işletme uygulaması, elektronik imzanın Türkçe elektronik belgelere entegrasyonunun

[22] Ömer Ergün, 5070 sayılı Elektronik İmza Kanunu ve Dijital İmza, Türkiye Noterler Birliği Hukuk Dergisi, Sayı:122, 15 Mayıs 2004, s.64

[23] Telekomünikasyon Kurumu, E-İmza Ulusal Koordinasyon Kurulu (UKK) Bilgi Güvenliği ve Standartlar Çalışma Grubu İlerleme Raporu, http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuV1.2.pdf. s.12 erişim tarihi 18 Aralık 2010

[24] 5510 Sayılı Elektronik İmza Kanunu, Kabul Tarihi: 15.1.2004 http://www.tbmm.gov.tr/kanunlar/k5070.html erişim tarihi: 01.04.2011

sağlandığı "Kamuyu Aydınlatma Platformu'nda olmuştur." [25] Türkiye'de şu anda bu hizmetin sağlandığı kurumlardan birisi, Turktrust ismiyle hizmet veren şirkettir.[26]

Yine günümüzde kullanılan e-imza yazılımları üreten kurumlar da şu şekildedir:

ESYA: TÜBİTAK bünyesindeki UEKAE Tarafından geliştirilmiştir.

Zeugma: Yine Türkiye'de TÜBİTAK'ın bir alt yazılım kurumu olarak çalışan BİLTEN tarafından geliştirilen bir yazılımdır.

VeriSign: Amerika'da geliştirilmiş ve dünyanın saygın şirketleri tarafından kullanılan, AAA (Açık Anahtar Altyapısı) destekli bir yazılımdır.

IBM Trust Authority: IBM tarafında geliştirilen bir yazılımdır.

RSA Keon: Amerika'da RSA Security firması tarafından geliştirilmiş bir yazılımdır.

Entrust/PKI: Amerika'da Entrust firması tarafından geliştirilmiş bir yazılımdır.

Baltimore UniCERT: Amerika'da Baltimore Technology firması tarafından geliştirilmiş bir yazılımdır.

1.3. ELEKTRONİK İMZANIN TEKNİK ALTYAPISI

E-imza uygulamalarının bir standarda bağlı olması, Dünya da ülkemizde, gerek e-imza uygulamalarının entegrasyonu gerekse ortak güvenlik seviyesinin oluşturulması açısından oldukça önemlidir. Çünkü, e-imza uygulamalarının yürütüldüğü ortak alanlar üzerinde, standartlaşamama durumunun oluşturacağı uyumsuzluk, teknik ve hukuki açıdan da uyumsuzluğa neden olacaktır. Türkiye'de kabul edilen güvenli e-imza oluşturma standartları, Avrupa Birliği Direktifi'ne dayanarak hazırlanmıştır. Elektronik İmza

[25] TBD, Kamu BİB, Kamu Bilişim Platformu, E-İmzanın Toplumsal Boyutu, Mayıs 2005, Antalya.
[26] http://www.turktrust.com.tr/

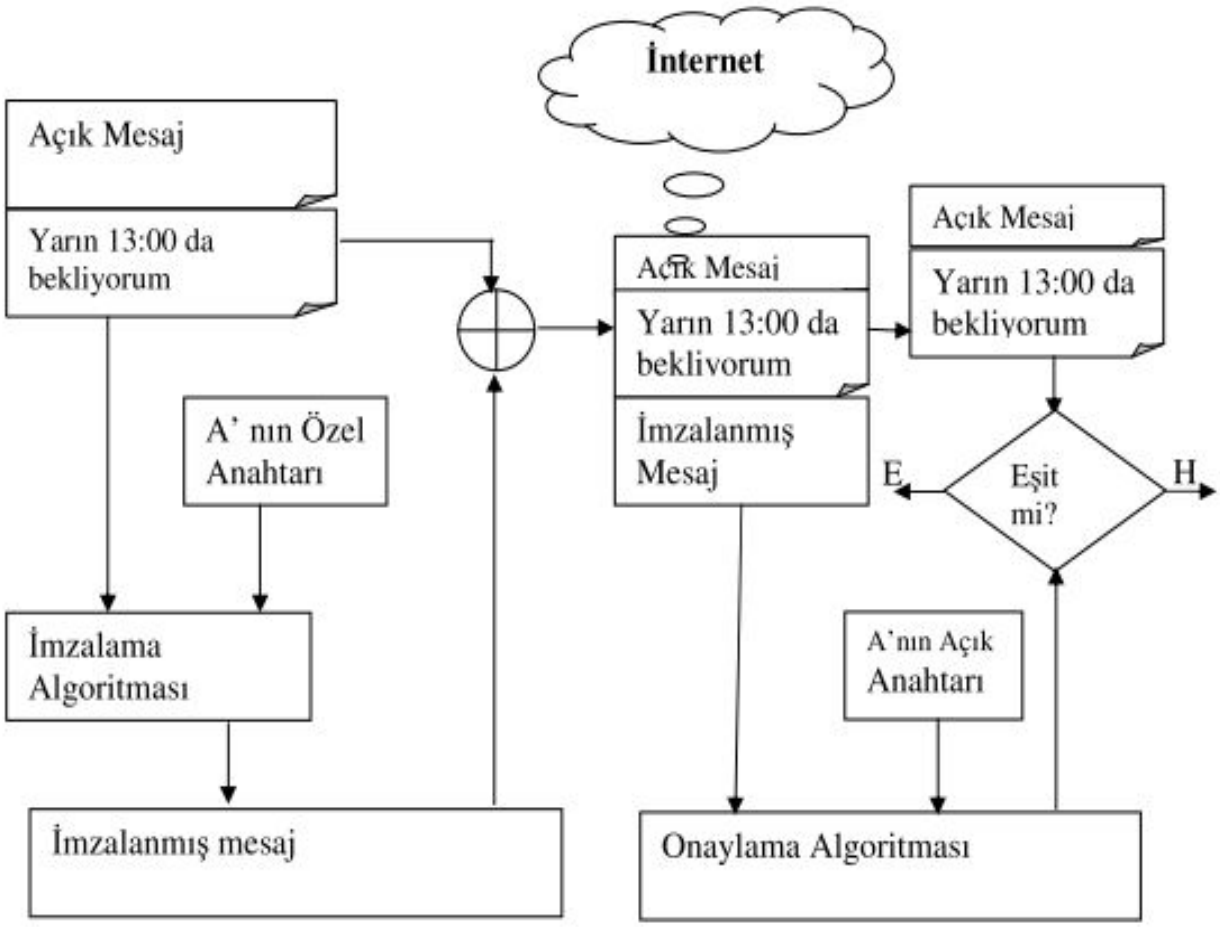
Kanunu'nda "Güvenli Elektronik İmza" olarak isimlendirilen nitelikli elektronik imza şu özellikleri taşımalıdır:

-Sadece imza sahibine bağlı olmak.

-İmza sahibinin kimliğini tespitini sağlamak.

- Sadece imza sahibinin kontrolünde oluşturulmak.

-İmzalanmış veride sonradan değişiklik yapılıp yapılmamış olduğunun tespitini sağlamak.



Şekil 1. E-imza'nın Teknik İşleyişi (Sağıroğlu, Alkan, 2005)

Elektronik imzanın birden çok çeşidi bulunmaktadır. Elektronik imza tiplerinde çeşitlilik, hayal gücü ve teknoloji ile sınırlanmaktadır. Bu bağlamda elektronik imzalar, iki genel yapı altında incelenebilir:

-Dijital İmza Yöntemi ile Oluşturulmayan Elektronik İmzalar.

-Dijital İmzalar.

Bu ayrımın temeli, ıslak imzaya denk elektronik imza ve ıslak imzaya denk olmayan elektronik imza ayrımına dayandırılabilir. "Her ne kadar ABD hukukunda tam bir teknoloji tarafsızlığı prensibi geçerli ise, UNCITRAL ve AB düzenlemelerinde, AB düzenlemeleri doğrultusunda Alman, Fransız ve Türk hukukunda ıslak imzaya denk elektronik imza bakımından dolaylı veya direkt olarak dijital imza işaret edilmektedir."

1.3.1. Dijital İmza Yöntemi ile Oluşturulmayan Elektronik İmzalar

1.3.1.1. Basit Elektronik İmza

Bu yöntem, Açık anahtar teknolojisi dışında kalan elektronik imza teknik ve teknolojilerini kapsamaktadır. Duyarlı bir bilgisayar ekranına özel kalemi vasıtasıyla elle imza atılması veya kağıt bazlı ıslak imzalı bir metnin tarayıcı vasıtasıyla bilgisayara aktarılması başlıca elektronik imza teknikleri olarak sayılabilir. Tarayıcı ile bilgisayara aktarılmış imza ise elektronik bir dokümana resim yapıştırır gibi, ıslak imzanın taranıp resim haline getirilerek dokümana eklenmesidir. Bu yöntem bazı kuruluşlar tarafından seri hazırlanan pazarlama tekliflerini göndermek için kullanılmaktadır. Maddi ortamda hazırlanan ve imzalanan verinin bir bütün olarak da taranması ve bilgisayara aktarılması mümkündür. Bu uygulamanın da yaygın bir elektronik imza uygulaması olduğu belirtilmiştir. Bu noktada ikili bir ayrıma gidilebilir. Tarayıcı vasıtasıyla yalnız imzanın bilgisayara aktarılması halinde, elektronik imzanın ayrı bir veri olarak, başka bir veriye eklenmesi veya mantıksal olarak bağlanması hususu gerçekleşebilir. Çünkü bu halde, birbirinden farklı iki veri söz konusudur. Buna karşılık, ıslak imzalı belgenin tamamının bilgisayara

aktarılması halinde ayrı bir elektronik veri söz konusu olmayacaktır. Her iki hal bakımından da kimlik doğrulama amacı kabul edilebilir ve somut olarak da kısmen dahi olsa imza sahibinin teşhisi mümkün olabilecektir. Islak imzanın veya ıslak imzalı metnin taranması halinde, basit elektronik imza tekniği ile imzalanmış elektronik veri meydana gelir. Böylece, bu verilerin internet vasıtasıyla veya veri depolayıcı belleklerle iletilmeleri mümkündür. Anılan tekniklerin biodinamik versiyonu da bilgisayar ekranına elle atılan imzadır. Bilgisayar ekranına elle imza atılması, uygun donanım ve yazılım vasıtasıyla özel kalemlerle touchpad'e veya dizüstü bilgisayar ekranına el yazısı ile imza atılmasıdır.

1.3.1.2. Biyometrik Yöntemlere Dayalı Elektronik İmzalar

Biyometrik imzalar, "bir kişinin kimliğinin doğrulanması için kullanılan ölçülebilir fizyolojik ve/veya davranışsal özellikler olarak tanımlanabilir."[27] Biyometrik imzalara örnek olarak çok yaygın olarak kullanılan parmak izi, avuç içi izi, ses, retina ve DNA kopyalama sistemleri sayılabilir. Biyometrik imzalar, günümüzde internette yapılacak işlemlerin güvenliği bakımından değil, daha çok bilgisayar sistemine girişte güvenliği sağlamak veya dijital imzalara ek olarak, dijital imzaları aktive eden parolalar yaratmak[28] amacıyla kullanılmaktadır. Yakın bir gelecekte biyometrik yöntemlerin sanal ortamda işlem güvenliği bakımından sıkça kullanılacağını tahmin edilmektedir. Ancak dijital imza kullanımı ile biyometrik yöntemler arasında, bilgisayar tekniği ve hazırlanış ve kullanılış (işleyiş) şekilleri bakımından oldukça büyük farklar mevcuttur. "Biyometrik teknoloji, tek başına, iletilen verinin bütünlüğünü sağlamaz."[29] Kişilerin biyometrik özelliklerinin "dijital imzadaki gibi bir sertifika kurumu tarafından kopyalanması ve sistemin bu tür kurum veya kurumlar aracılığı ile işletilmesi, dijital imzadakinden daha farklı bir alt yapıyı ve güvenliği gerektirmektedir."[30] Bu sebeplerle, günümüzde biyometrik

[27] H. Tarık Erol, Electronic Signatures, Beta Yayınları, İstanbul, 2003, s. 42.
[28] Erol, a.g.e., s.47.
[29] M.H.M. Schellkens, Electronic Signatures Authentication Technology from a Legal Perspective, Netherlands, T.M.C. Asser Press, 2004, s.76.
[30] Leyla Keser Berber/Murat Lostar, Bilişimde Biyometrik Yöntemler, Yetkin Yayınları, Ankara 2006. s.49

imzaların dijital imzaların alternatifi olarak kullanılması düşüncesi düşünülmemesi güvenlik açısından yeterli olamamaktadır.

1.3.2. Dijital İmzalar (Sayısal İmzalar)

"Sayısal imza, gönderilecek (imzalanacak) olan elektronik metnin şifrelenmesi yöntemidir."[31] Elektronik imza çok çeşitli olmakla birlikte şu an için en güvenilir olanı ve güvenilirliği nedeniyle en yaygın olarak kullanılanı sayısal (dijital) imzadır. Bu nedenle daha çok sayısal imza kavramı üzerinde durmak yerinde olacaktır. Literatürde, "sayısal imza" ve "elektronik imza" kavramları aynı anlama gelmek üzere kullanılmaktadır. Oysa sayısal imza, üst kavram olan elektronik imzanın sadece bir çeşidini oluşturmaktadır. Bilgisayar ortamındaki tüm veriler gibi kullanılan teknoloji ne olursa olsun elektronik her imza da sayısal (dijital) verilerden oluşması nedeniyle, bilgisayarın işleyiş tekniği bakımından bütün elektronik imzaları sayısal imza olarak adlandırmanın bilgisayarın teknik terminolojisi açısından yanlış olmadığı iddia edilebilir. Ancak sayısal imza kavramı, farklı bir anlamda ve belli bir şifreleme yöntemine dayanan elektronik imza teknolojisini ifade etmek üzere kullanıldığı için bu iki kavramı birbirinden ayırmak ve elektronik imzayı, sayısal imzayı da kapsayan üst kavram olarak kabul etmek daha isabetli olacaktır. Dış Ticaret Müsteşarlığı bünyesinde kurulmuş Elektronik Ticaret Koordinasyon Kurulu Hukuk Raporuna göre de sayısal imza; "Elektronik imzanın özel bir çeşidi olup bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür. Sayısal imzalar göndericinin kimliğinin açık ve net bir biçimde teyidini, elektronik dokümanın orijinalliğini ve güvenilirliğini mümkün kılar.[32]

[31] E-İmza, E-İmza' nın Toplumsal Boyutu, http://www.e-imza.gen.tr/templates/resimler/File/arastirma_dosyalari/E-IMZANIN_TOPLUMSAL_BOYUTU.doc s.3 erişim tarihi:10.09.2010

[32] http://www.e-ticaret.gov.tr/raporlar/hukuk.htm erişim tarihi:10.09.2006

1.3.2.1. Kapalı Anahtar Şifrelemesine (Single Key Encryption) Dayalı Elektronik İmzalar

Anahtar, şifrelemek veya deşifre etmek için kullanılan sayısal karakter dizisi olarak tanımlanabilir. Açık Anahtar Altyapısında kullanılan asimetrik şifreleme yönteminde, biri "açık anahtar"[33] diğeri "özel anahtar olmak üzere bir anahtar çifti bulunmaktadır."[34] Özel-Kapalı anahtar, sayısal imzanın oluşturulmasında, "açık anahtar ise sayısal imzanın tetkikinde kullanılmaktadır."[35] Başka bir ifadeyle özel anahtar mesajı şifrelemekte, açık anahtar ise deşifre etmekte kullanılır. Bu yüzden özel anahtar sadece kullanıcıda bulunur ve özenle saklanması gerekir. Başkalarının ona ulaşması şifrenin çözülmesi veya yerine imza atmasıyla eşdeğerdir. Bu durumun aksine açık anahtarın üçüncü kişilerce ulaşılabilir olması, onlar tarafından biliniyor olması gerekmektedir.

Söz konusu anahtar çifti, ya elektronik sertifika hizmet sağlayıcıları tarafından üretilir. (5070 Sayılı Elektronik İmza Kanunu 10'uncu maddesinin son fıkrasında "elektronik sertifika hizmet sağlayıcısının üretilen imza oluşturma verisinin bir kopyasını alamayacağını veya bu veriyi saklayamayacağını" hükme bağlamıştır)[36] ve sahibine teslim edilir; "ya da kişiler tarafından bizzat uygun programlar aracılığıyla elde edilir."[37] "Kapalı anahtar ile açık anahtar matematiksel olarak birbiriyle bağlantılıdır."[38] "Ancak, bir anahtarı kullanarak diğerine ulaşmak mümkün değildir."[39] Üçüncü kişilerin mesajı deşifre etmeleri imkansız kabul edilmektedir. Asimetrik şifreleme yönteminde deşifre etme süreci, simetrik şifreleme∗ yöntemine göre daha uzun sürmektedir. Bunun üstesinden gelmek amacıyla Rivest tarafından hash fonksiyonu 61 geliştirilmiştir.

---

[33] 5070 Sayılı, "Elektronik İmza Kanunu", Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004, Madde-3/f.
[34] Calalettin Dönmez, Regulation of Electronic Signatures and Protection of Private Keys, Sheffield: University of Sheffield Department of Law, 2002 s.12
[35] Zarife Şenocak, Zarife: Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması, AÜHFD, C. 50, 2001/2, s.99.
[36] 5070 Sayılı, "Elektronik İmza Kanunu", Kabul Tarihi:15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004, Madde-10.
[37] Leyla Keser Berber, "İmzalıyorum O Halde Varım", Türkiye Barolar Birliği Derigisi, Sayı:2, 2000, s.131.
[38] American Bar Assocation, Digital signature guidelines: legal infrastructure for certification authorities and electronic commerce/Information Security Committee, Electronic Commerce and Information Technology, Chicago: IL, 1996, s.9
[39] Ulvi Altınışık, Elektronik Sözleşmeler, Seçkin Yayınevi, İstanbul 2003, s. 82

Diğer önemli konulardan biri ise, özel anahtarın güvenliğinin sağlanmasıdır. Kapalı anahtar üretildikten sonra ya bilgisayarın diskinde ya da harici bir depolama biriminde tutulur ve erişilmesini önleyici tedbirler alınır. Ancak, erişilmesi kolay olup ataklara maruz kalacağından disk, disket, CD, DVD gibi elektronik ortamlarda tutulması güvenlik açısından tehlikelidir. Özel anahtarın bulunduğu elektronik medya şifre ile korunsa dahi bu şifrelerin bulunması çok zor değildir. "Açık anahtardan yola çıkarak matematiksel yöntemlerle özel anahtarın elde edilmesi imkansız kabul edilmektedir."[40] Ancak, özel anahtarlar akıllı kartlarda veya bilgisayarlarda tutulmaktadır. Gerekli güvenlik önlemlerinin alınmadığı durumlarda özel anahtara ulaşmak mümkün olabilir. Bu durumda, imza özel anahtarla atıldığından ve inkar edilemeyeceğinden bütün sorumluluk özel anahtar sahibine ait olacaktır. Özel anahtarın çok iyi korunması gerektiği konusunda kullanıcılar mutlaka bilinçlendirilmeli, suiistimallerin artmasıyla sisteme olan güven baştan zedelenmemelidir. Kurumsal uygulamalarda özel anahtarın sabit veya geçici disk ortamlarında tutulması yerine akıllı kart gibi güvenlik seviyesi yüksek cihazlar özendirilmelidir. Açık anahtar altyapıları insandan bağımsız olarak düşünülemez. Algoritmalar, protokoller, otoriteler, şifreleme anahtarları gibi unsurların dışında insanlar da bu sistemin bir parçasını teşkil etmektedir.

1.3.2.2. Açık Anahtar Şifrelemesi ve Altyapısı (Public Key Encryption)

Şifreleme, elektronik ortamda iletilen bilginin dönüştürülmesi işlemidir. Bu yöntemde "bilgi, alıcı dışında başka bir kişi tarafından okunamaması ya da değiştirilememesi için kodlanır. Şifreleme ile gönderilen herhangi bir bilginin gizliliği korunmuş ve bütünlüğü bozulmamış olur."[41] Şifreleme yönteminde güvenliği artırmak amacıyla çeşitli şifreleme algoritmaları kullanılmaktadır. Elektronik imza uygulamalarında kullanılan en yaygın kullanılan yöntem Açık (simetrik olmayan) anahtar algoritmasıdır (altyapısı). "Açık Anahtar Alt Yapısı (AAA); 1978 yılında 3 bilim adamı Rivest, Shamir ve Adleman'ın baş harflerinden

[40] Ulvi Altınışık, a.g.e s. 83
[41] Şeref Sağıroğlu, Mustafa Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara 2005, s.43

oluşan RSA matematik algoritmasının onaylanması ile başlar."[42] Geliştirilen ilk asimetrik anahtarlı şifreleme algoritmalarından biridir. Bu teknikte şifreleme ve şifre çözme için farklı kripto anahtarları kullanılır.

AAA teknolojisi İkinci Dünya Savaşından başlayarak belli bir bilimsel temel üzerine oturtulmuş, 1970'li yılların başından itibaren çok önemli gelişmelerle birlikte giderek yoğun şekilde ticari uygulamalarda kullanılmaya başlanmış, dünya üzerinde standartları ve küresel ölçekte güvenlik ve işlerlilik alanları oluşturulmuş en güvenilir güvenlik uygulaması olduğu kanıtlanmıştır. "Küresel düzeyde birçok yapı bu teknolojiyi kullanmakta ülkelerin bu teknolojiyle ilgili şu anda ve gelecek için yatırımları bulunmaktadır. Ülkemizde de gerek devlet gerek özel sektör gerekse de Silahlı Kuvvetler açık anahtarlı altyapı uygulamalarını kullanmakta bu konuyla ilgili AR-GE yatırımları yapılmakta ve bu uygulamanın etkin olacağı kullanım ve güvenlik alanları oluşturulmaktadır."[43] AAA birçok kaynakta "Bilgi iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlamaya yarayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümü" şeklinde tanımlanmaktadır. Günümüzde ağ sistemlerinin çoğu AAA sistemini kullanmaktadır ve bu ağların çoğu kamuya açık ağlar değildir. "AAA, pek çok çalışanı olan bir şirkette, şirket çalışanlarının birbirleriyle olan iletişiminin güvenliği, gizli iletilerin sadece yetkili kişiler tarafından görülebilmesi gibi amaçlarına yönelik olarak kullanılabilir. Böyle bir sistemde şirketin bir sunucusu (server), çalışanlara sertifika dağıtmak görevini üstlenebilir. Ana amacı; sanal dünyada; herhangi bir bilgi taşınırken Gizlilik (Confidentiality), Bilgi Bütünlüğü (Integrity) , Kimlik Doğrulama (Authentication) ve Gönderenin İnkar Edememesi (Non-repudiation) güvenlik özelliklerinin sağlanması olan AAA; bu işlemleri Sayısal İmza ve Sayısal Kripto ile Özel ve Genel anahtar kullanarak gerçekleştirmektedir. Sayısal imza; Kimlik Doğrulama, Bilgi Bütünlüğü ve Gönderenin İnkar Edememesi; Sayısal kripto ise Gizlilik güvenlik fonksiyonlarını sağlamaktadır." [44]

[42] Turhan Yükseliyor, AAA Sayısal Sertifika Karmaşası, www.e-imza.gen.tr/templates/resimler/File/makaleler/AAA_Sayisal_Sertifika_Karmasasi_Turhan_Yukseliyor.doc erişim tarihi: 19.03.2011

[43] Telekomünikasyon kurumu, 2004, s:20-21 www.tk.gov.tr/Yayin/Raporlar/pdf/faaliyet-2004.pdf erişim tarihi 05.04.2011 s.1

[44] Turhan Yükseliyor, AAA Sayısal Sertifika Karmaşası, www.e-imza.gen.tr/templates/resimler/File/makaleler/AAA_Sayisal_Sertifika_Karmasasi_Turhan_Yukseliyor.doc erişim tarihi: 19.03.2011 s.1

Anahtar, şifrelemek veya deşifre etmek için kullanılan sayısal karakterler dizisidir. Simetrik anahtar algoritmasında şifrelemek ve deşifre etmek için aynı anahtar; açık anahtar algoritmasında şifrelemek için açık anahtar, deşifre etmek için ise gizli anahtar kullanılır. Açık anahtar algoritması, çok büyük sayılarla yapılan bazı işlemlerin bir yönde kolay aksi yönde ise zor olduğun gerçeğini kullanmaktadır. "AAA'da çok büyük asal sayılar üretmenin kolaylığına karşın, büyük sayıların asal bileşenlerinin bulunmasının zor olduğu varsayımı ile hareket edilmektedir. Matematikçilerin tamsayıları asal bileşenlerine ayırmanın hızlı bir yolunu henüz bulamamış olmaları, bu varsayımı destekleyici yöndedir."[45] Bu altyapı ile gönderilen mesajın bütünlüğünün korunması, gönderenin belirlenmesi, yetkilendirme gibi birçok amaç gerçekleştirilebilir. Anahtarlar ne kadar uzun seçilirse şifrenin kırılması o kadar zor olmaktadır. "AAA kullanıldığı durumda, açık anahtar genellikle veritabanlarından yayınlanır ve isteyen herkes istediği kişinin elektronik sertifikasını okuyarak açık anahtarını öğrenebilir. Gizli anahtar ise sadece kullanıcının kendisi tarafından bilinir ve kullanılır."[46] Bir anahtarın diğerinden türetilmesi veya hesaplanması mümkün değildir. Açık anahtarın başkaları tarafından bilinmesinin bir sakıncası yoktur fakat gizli anahtar kesinlikle bir başkası bilmemelidir. Dijital anahtarlar açık-gizli anahtar şifreleme algoritması üzerine kurulmuştur. Bir açık-gizli anahtar çifti bir sayı çiftinden ibarettir. "Gizli anahtar sadece sahibi olan kişi ya da kurum tarafından bilinir ve dijital imzayı oluşturmak için kullanılır. Açık anahtar ise dijital imzaların doğrulanması için kullanılır. Bir dijital imzanın doğrulanması mesajın geldiği kişinin kimliğinin doğrulanması anlamına gelmektedir."[47] Dünya pratiği ve Avrupa Birliği ülkelerine bakıldığı zaman % 90 aşan bir oranda elektronik imza uygulamalarında "açık anahtarlı altyapı" (public key infrastructure) teknolojisi kullanıldığı ve kanunlaştırılmalarında da bu teknolojiyi temel alan çözümlemeler üretildiği gözlemlenmektedir.

[45] Şeref Sağıroğlu, Mustafa Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara 2005, s.43
[46] Murat Çak, Dünyada ve Türkiye'de Elektronik Ticaret ve Vergilendirilmesi, İstanbul Ticaret Odası Yayını, İstanbul 2002, s.122
[47] E Lawrance, S. Newton,B Corbitt, R Braithwaite, Technology of Internet Business, John Wiley & Sons Australia Ltd, 2002, s.17

1.3.2.3. Hash Fonksiyonu - Öz Değeri (Hash Value)

Metin şifreleme yöntemlerinde, çok uzun metinlerin şifrelenmesi zaman almakta olduğundan, metin şifreleme kullanışlı değildir. Bu nedenle metnin tamamı değil; metinden belli bir algoritmayla çıkarılan metnin özeti şifrelenir. Metinden özet çıkarma işini hash fonksiyonu yerine getirir. "Bilgisayar terminolojisinde "hash" yazılan bir metnin kısaltılmış şeklini ifade etmektedir. Hash fonksiyonu elektronik imzanın hazırlanmasında son derece önemlidir."[48] Hash fonksiyonu "matematiksel bir algoritmadır."[49] "Hash fonksiyonuyla oluşturulan mesaj özeti verilerin parmak izi olarak düşünülebilir."[50] "Bu algoritmalar geneldir ve özel anahtar gerektirmezler."[51] Hash fonksiyonu sunucu elde edilen değere hash değeri veya mesaj özeti denmektedir. Hash fonksiyonları genel olup orijinal metinden herkes tekrar hesaplama yaptırabilir. "Hash fonksiyonu tek taraflı olarak çalışır. Bunun anlamı metinden elde edilen mesaj özetinden yola çıkarak metni elde etmek mümkün değildir. Farklı iki belge aynı hash değerini vermesi imkan dahilinde olmakla birlikte, imkansıza yakın kabul edilmektedir."[52]

Sayısal imza, bilginin doğruluğunu korumaktadır. Teknik açıdan sayısal imza, imzalanmış belgenin özünü (Hash) içerir. İçerikte yapılacak herhangi bir değişiklik dijital mesaj özetini geçersiz kılacaktır. Çünkü mesaj özeti, metnin karakteristik özelliklerinin tümü dikkate alınarak oluşturulmaktadır. "Yapılacak en küçük bir değişiklik mesaj özetinin değişmesine yol açacaktır."[53]

Burada önemli olan konu, sayısal imza denilen olgunun metnin içeriğinde değil mesaj özeti üzerinde uygulandığıdır. Metni imzalayan kişinin özel anahtarı ve asimetrik şifreleme sistemi vasıtasıyla mesaj özeti şifrelenir ve bu şekilde şifrelenen mesaj özeti elektronik metne

---

[48] Ulvi Altınışık, Elektronik Sözleşmeler, İstanbul: Seçkin Yayınevi, 2003, s. 83

[49] File Hasher (exe), http://downloads.zdnet.com/abstract.aspx?docid=357921, (22 Şubat 2011)

[50] Mario Miccoli, Nadi Günal (çev.), Teknolojik Açıdan Elektronik Ticaret, Noterlik Hukuku Sempozyumu:VII, Elektronikteki Gelişmeler ve Hukuk, Ankara 2001, s.83

[51] Ulvi Altınışık, Elektronik Sözleşmeler, Seçkin Yayınevi, İstanbul 2003, s. 83

[52] A. Michael Froomkin, The Essential Role of Trusted Third Parties in Electronic Commerce, http://74.125.155.132/scholar?q=cache:_vQIrJM-B4UJ:scholar.google.com/+A.++Michael++Froomkin,++The++Essential++Role++of++Trusted++Third++Parties++in++Electronic++Commerce,++&hl=tr&as_sdt=0,5 erişim tarihi: 22 Aralık 2010 s.49.

[53] Mesut Orta, Türkiye'de elektronik imza uygulaması, Konya Barosu Dergisi, Vol:3, Sayı: 5, Temmuz 2006, s. 63.

eklenerek muhataba gönderilir. Şifrelenen mesaj özeti metinden ayrı olarak tutulur. "Mesaj özetinden bir şekilde metne ulaşmak mümkün değildir."[54]

Pratikteki çalışma prensibinde, Hashing (sıkıştırma) ile sıkıştırdığınız veriler (hash value), yani evraka yazdıklarınız, adeta bir sürü yerinden yırtılıp bir küçük boyuta (message digest, mesaj özeti) indirilmekte bir tür yığın teşkil etmektedir. Hashing sonucu elde edilen matematik algoritmik değere; hash value adı verilir. Hash value en büyük özelliği sözkonusu döküman ile sıkı sıkıya bağlı oluşudur. Şöyle ki, o doküman yanlız bir tek tip hash value sonucunu mümkün kılabilir ve bir hash value sadece bir tek dokümana uygulanabilir. Böylece bir kere digital olarak imzalanmakla, dokümanı üzerinde değişiklik yapılması imkânsız olmaktadır. Diğer bir deyişle bir dokümanı tamamlayıp imzaladığınızda oluşan hash değeri, mesaj özeti, onu üreten - ve sayısal imzanızı içeren-bilgisayara özel olarak, geri dönüşsüz ve eşsiz (unique) olarak oluşmaktadır.

1.3.2.4. Onay Kurumu (Sertifika Hizmet Sağlayıcıları)

Sayısal imza kavramının yasal güvenilirlik kazanabilmesi için, kullanıcıların açık anahtarlarını onaylama yetkisine sahip bir kuruluşa, bir otoriteye gereksinim vardır. Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), herhangi bir kullanıcının kimliğini kontrol ederek, bu kimliğin hangi açık anahtara sahip olduğunu belgeleyebilen ve bu belgeyi ESHS'na ait sayısal imza ile onaylayarak, diğer bütün kullanıcıların bu kullanıcının imzasını tanıyabilmelerini, doğrulayabilmelerini sağlayan bir kuruluştur. Elektronik sertifika, ESHS tarafından hazırlanarak kullanıcılara verilir ve bir kopyası ESHS'nın herkese açık olan erişim bölgesine kaydedilir. ESHS tarafından hazırlanarak kullanıcılara verilen elektronik sertifikalar, sahibinin kimlik bilgilerini, açık anahtarını, belgenin kullanım süresini, seri numarasını, belgeyi veren ESHS'nın adını ve sayısal imzasını taşımalıdır. ESHS, kişilerin açık anahtarlarını ve kimliklerini eşleştiren sertifikaların hazırlanmasında çok titiz davranmak, başvuruda bulunanın kimliğinden kesinlikle emin olacak yöntemler geliştirmek durumundadır.

[54] Faruk Günay Özer, Sermaye Piyasalarında Elektronik İmzanın Kullanım Alanları, Bilgi İşlem Merkezi Yöneticileri Semineri (BİMY) 8-11 Nisan 2004, Aksu-Antalya, 2004, s. 6.

5070 sayılı EİK ve ilgili ikincil mevzuat gereğince ıslak imza ile aynı hukuksal etkiye sahip e-imza kullanımı yasal bir tabana oturtulmuş ve 2004/21 sayılı Başbakanlık Genelgesi ile kamu kurum ve kuruluşlarının e-imza ile ilgili sertifika ihtiyaç ve işlemlerinin TÜBİTAK-UEKAE bünyesinde kurulmuş olan Kamu Sertifikasyon Merkezi tarafından yürütülmesi kararlaştırılmıştır. Bu düzenleme ışığında hukuksal açıdan geçerliliği olan e-devlet işlemlerinde e-imza kullanma gerekliliği açıktır. Ayrıca, "kamu kurum ve kuruluşları dışındaki kuruluşlar ve gerçek kişiler için nitelikli sertifika hizmeti Telekomünikasyon Kurumu(TK) tarafından yetkilendirilmiş özel sektör sertifika hizmet sağlayıcıları tarafından yürütülecektir."[55]

Çift (açık) anahtarlı bir kriptografi sisteminde, kullanıcının gizli-açık anahtar çiftinin oluşturulması ESHS tarafından yapılabileceği gibi, kullanıcı tarafından da yapılabilmektedir. Buradaki önemli nokta, anahtar görevini yapacak sayı dizilerinin, belirli bir kriptografik algoritmanın gerektirdiği kurallara uygun olması ve belirli bir uzunluktan daha kısa seçilmemesidir. Bu sayı dizilerinin uzunluğu, sistemin güvenilirliğini, açık anahtar bilgisiyle gizli anahtarın hesaplanamamasını, ayrı kullanıcılara ayrı anahtarlar verilebilmesini ve sayısal imzanın taklit edilememesini sağlayan önemli bir faktördür. Günümüzde 512 ikil uzunluğunda anahtarlar oldukça güvenli kabul edilmektedir. "Çok gizlilik gerektiren uygulamalarda 1024 ikil uzunluğuna kadar çıkılmaktadır." ESHS'nın değil de kullanıcının anahtar çiftini oluşturduğu durumda da, kullanıcının ESHS'na başvurarak elektronik sertifikasını alması, ve bu sertifikayı ESHS'nın açık erişim bölgesine kaydettirmesi atacağı sayısal imzanın diğer kullanıcılar tarafından tanınabilmesi için gereklidir. ESHS'nın hazırladığı ve tüm kullanıcılara açık tuttuğu erişim bölgesinin içinde bulunan elektronik sertifika bilgileri, her değişiklikte (yeni bir kullanıcı, süresi dolan elektronik sertifika, gizli anahtarını kaybettiği için elektronik sertifikasını iptal ettirmesi gerekenler vb.)

[55]Başbakanlık Genelgesi 2005, Resmi Gazete 6 Ocak 2005, s.14

http://docs.google.com/viewer?a=v&q=cache:yCdmms71OakJ:www.puis.org.tr/KURUL_KARARLARI/10.doc+6+Ocak+2005+tarih+ve+25692+say%C4%B1l%C4%B1+Resmi+Gazete&hl=tr&gl=tr&pid=bl&srcid=ADGEESjIZ_0xnbKnc6BbyRlnTVl6NvazBpRX-WVWKcwkQE1BGnh0CbddTQVtT1_aXeQ2RI7DxY7oFSPxEajUW4AB_zCzR6w4JVrw8KzyPoC7T6PxWyqJYVJ1mAce770AdWxp8CLhWWrx&sig=AHIEtbRtyNsSR5x58GCHWfRW7udBmAZyaA erişim tarihi 07.04.2011

hızlı bir şekilde uyarlanmalıdır. Bu uyarlamanın hızı, sistemin güvenilirliğini ve etkinliğini doğrudan etkileyeceği için oldukça önemlidir."[56]

Burada dikkat edilmesi gereken en önemli husus, sertifika ilkelerinin, Yönetmelikte belirtilenin aksine sadece ESHS tarafından yayınlanmak veya onaylanmak zorunda olmayışıdır. "Sertifikaya güvenerek işlem yapacak bir üçüncü taraf, sertifikayı kullanarak imza atacak imzalayan, imza uygulamasını geliştiren ve kullanıma sunan taraf bir sertifika ilkesi yayınlayıcısı olabilir."[57] Zira ESHS'lerin sertifikaları kullanılarak, ESHS'nin ilkeleriyle uyumlu fakat, ESHS'nin ilkelerine göre daha detaylı kriterlerin belirlendiği sertifika uygulama alanları olabilecektir. Örnek vermek gerekirse, Baro aracılığıyla başlatılacak bir elektronik imza uygulamasında, sertifika başvuru prosedürleri, avukatların kullanacağı elektronik imza uygulamaları, avukatların uymaları gereken güvenlik gereksinimleri farklılık arz edebilir. Böyle bir durumda Baro ESHS'nin sertifika ilkeleriyle uyumlu bir ilke yayınlayarak kendi uygulaması için spesifik şartlar ve koşullar belirleyebilir. Ancak burada dikkat edilmesi gereken, Baronun uygulamasında çalışacak sertifikaları yayınlayan tüm ESHS'lerin ilkeleriyle uyumlu bir ilke yayınlanmasının zorunluluğudur. Eğer Baro belirlediği ilkelerde, tüm ESHS'lerin yayınladığı sertifikaların uygulamada geçerli olacağını belirtiyorsa bu durumda tüm ESHS'leri sertifika ilkeleriyle uyumlu bir ilke yayınlamalıdır. Ancak Baro sadece belirli ESHS'lerin sertifikaların kabul edileceği bir uygulama geliştiriyorsa bu durumda kabul edilen sertifikaları kendi sertifika ilkeleri dokümanında belirtmelidir; bu durumda Baro sadece kabul ettiği sertifikaları yayınlayan ESHS'nin ilkeleriyle uyumlu bir ilke yayınlayabilir.

1.3.2.5. Zaman Damgası

Günlük yapılan işlerde, kargaşaya mahal vermemek için yapılan işlemlerden birisi de, işlemlerin çoğunda tarih bilgisi kullanmaktır. Kullanılmadığı taktirde,

[56] TUNEA, 1998 Yılı Çalışma Raporu, www.tbv.org.tr/TBV/Documents/Yayinlar/.../Tbv1998YiliCalismaRaporu.pdf 1998a: 12 erişim tarihi: 07.04.2011

[57] Network Working Group, Internet X.509 RFC 3647 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003 s. 9

"işlemlerde, haberleşmede, ilişkilerde ve işlerde problemler çıkabilmekte, kişiler zarar görmekte ve kurumlarda kayıplar oluşabilmektedir."[58]

Elektronik olarak yapılan yazışmaların bir bölümünde, örneğin bir sözleşme imzalanırken, mutlak zamanın kaydedilmesi de önem taşımaktadır. Sayısal zaman damgası olarak adlandırılan bu kavram, elektronik iletişimin yapıldığı zamanın mesajın bir parçası olarak, elektronik ve değiştirilemeyecek bir şekilde kaydı anlamına gelir. Böyle bir sayısal zaman damgası sayesinde, belirli bir süre sonra, günümüzün anahtar uzunluklarının yeteri kadar olmadığı dönemler gelse, ve eskiye dönük sayısal imza taklitleri yapabilecek teknoloji geliştirilse bile, belgelerin bozulabilmesi, veya imzaların taklit edilebilmesi mümkün olamayacaktır. "Sayısal zaman damgası işlerinin yürütülebilmesi için önerilen yöntemlerden biri, ESHS'ları gibi güvenilir ve mesajlara zaman damgası vurma yetkisi olan elektronik noterlik servislerinin oluşturulmasıdır."[59]

Elektronik bir belgenin ispat gücünü artırmak için, belgenin düzenlendiği zamanın şüpheye yer bırakmayacak şekilde tespiti şarttır. Elektronik ortamda bu fonksiyonu, zaman damgası yerine getirmektedir. "Açık anahtarlı altyapıya sahip bir bilgisayar ağında, kullanıcılar iletişimlerini güvenli hale getirmek için elektronik sertifika kullanabilirler ve bu durumda sistemdeki güvenlik sunucusu sertifika ve zaman damgası hizmeti sağlar."[60]

Zaman damgası ilkeleri ve zaman damgası uygulama esasları, "zaman damgası hizmetlerine ilişkin detaylı açıklamaların yapıldığı, şart ve koşulların belirlendiği dokümanlardır."[61] Esas olarak sertifika ilkeleri ve sertifika uygulama esaslarıyla aynı işleve sahip olmakla birlikte, sertifikaya değil zaman damgasına ilişkin çerçeveyi çizmektedirler. Bunu dışında her iki doküman seti arasında içerik, oluşturulma ve yayınlanma prosedürü, katılımcılar, hukuki statü gibi konularda bir farklılık yoktur. Yurtdışı uygulamalarına bakıldığında da zaman damgası hizmetleri için ayrı ilke ve uygulama esaslarının yaratılmadığı görülmektedir. RFC 3647 sertifika ilkeleri ve sertifika uygulama esasları çerçevesinde de bir bölüm zaman damgası hizmetlerine ayrılmıştır.

---

[58] [58] Şeref Sağıroğlu, Mustafa Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara 2005 s.72

[59] TUNEA, 1998 Yılı Çalışma Raporu, www.tbv.org.tr/TBV/Documents/Yayinlar/.../Tbv1998YiliCalismaRaporu.pdf 1998a: 12 erişim tarihi: 07.04.2011

[60] UKK, Elektronik imza hukuk çalışma grubu raporu, s.37 http://www.tk.gov.tr/eimza/doc/diger/e-imza%20hukuk%20calisma%20grubu%20raporu.pdf erişim tarihi: 02.04.2011

[61] ETSI TS 102 023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, V1.2.1, Valbonna – France, 2003 s.7

Ancak, "Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), Avrupa Elektronik İmza Standardizasyon İnisiyatifi içerisinde öngördüğü elektronik imza yapısı içerisinde, elektronik imza hizmetlerinin birbirinden ayrı olarak sunulabileceğini belirtmiştir. Kanaatimizce bu sebepten ötürü zaman damgası hizmetleri için de ayrı bir ilke çerçevesi belirlenmiş ve bu doğrultuda ETSI TS 102 023 Zaman Damgası Hizmet Sağlayıcıları için İlke Gereksinimleri Dokümanı yayınlanmıştır."[62]

Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 31. maddesine göre "ESHS, zaman damgası ve hizmetlerini sağlamakla yükümlüdür. Nitelikli elektronik sertifika sahibi, bu hizmeti talep etmesi halinde alır." Görüldüğü üzere, Yönetmeliğin bu maddesi zaman damgası hizmetlerini ESHS'ler için zorunlu hale getirmiş ve bütün ESHS'lerin hizmetleri sağlamanın yanı sıra zaman damgası uygulama esasları ve zaman damgası ilkeleri yayınlama zorunluluğu doğmuştur.

Yönetmeliğin 3. maddesine göre;

Zaman Damgası İlkeleri: Zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgeyi,

Zaman Damgası Uygulama Esasları: Zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi, ifade eder.

1.3.2.6. Sistemin İşleyişine İlişkin Örnekler

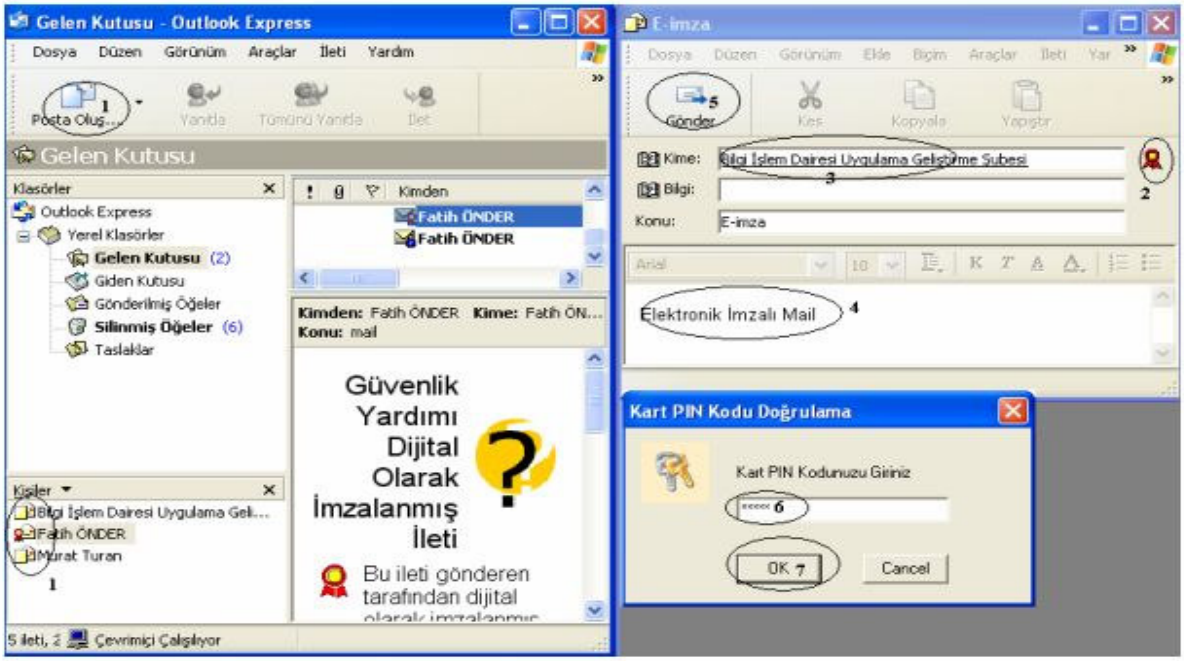
Elektronik imzalı bir belge veya mesajı oluşturmak istendiğinde öncelikle elektronik imzayı destekleyen herhangi bir yazılım kullanılarak daha önceden hazırlanmış belge seçilir veya gönderilecek mesaj oluşturularak dijital imzalama prosedürüne geçilir. Bunun için gönderilecek mesaj ve kişi belirlendikten sonra yazılımın niteliğine göre belgeyi imzalama veya mesajı gönderme butonuna basılır. İmzalama prosedürü çalışmaya başlayınca öncelikle imza sahibinden imza oluşturma aracını isteyecektir. İmza oluşturma aracı bilgisayara takıldıktan sonra da giriş şifresi (PIN) istenecektir. PIN kodu girildikten sonra elektronik imzalama süreci başlar. Bu

[62] ETSI TS 102 023, a.g.e., s. 8

süreçte öncelikle "hash fonksiyonu" kullanılarak gönderilecek metnin bir özeti çıkartılır. Buna "hash değeri" denir. "Anahtardan farklı olarak hash değeri belirli bir mesaj için her zaman aynıdır. Yani mesajda tek bir karakterlik bir değişiklik dahi olsa hash değeri farklı olur. İkinci adım olarak hash değeri göndericinin özel anahtarı ile şifrelenir ve mesaja eklenir."[63] Bu işlemde şifreleme özel anahtar ile yapılıp deşifre de bu anahtara karşılık gelen genel anahtar ile yapılacağından ve genel anahtar mesajın ekinde bulunan sertifikada var olduğundan gönderen veya alıcının başkaca bir işlemde bulunması gerekmemektedir. "Aynı şekilde muhatabın elektronik imza sahibi olmasına ve gönderenin bu kişinin açık anahtarını bilmesine gerek yoktur."[64]

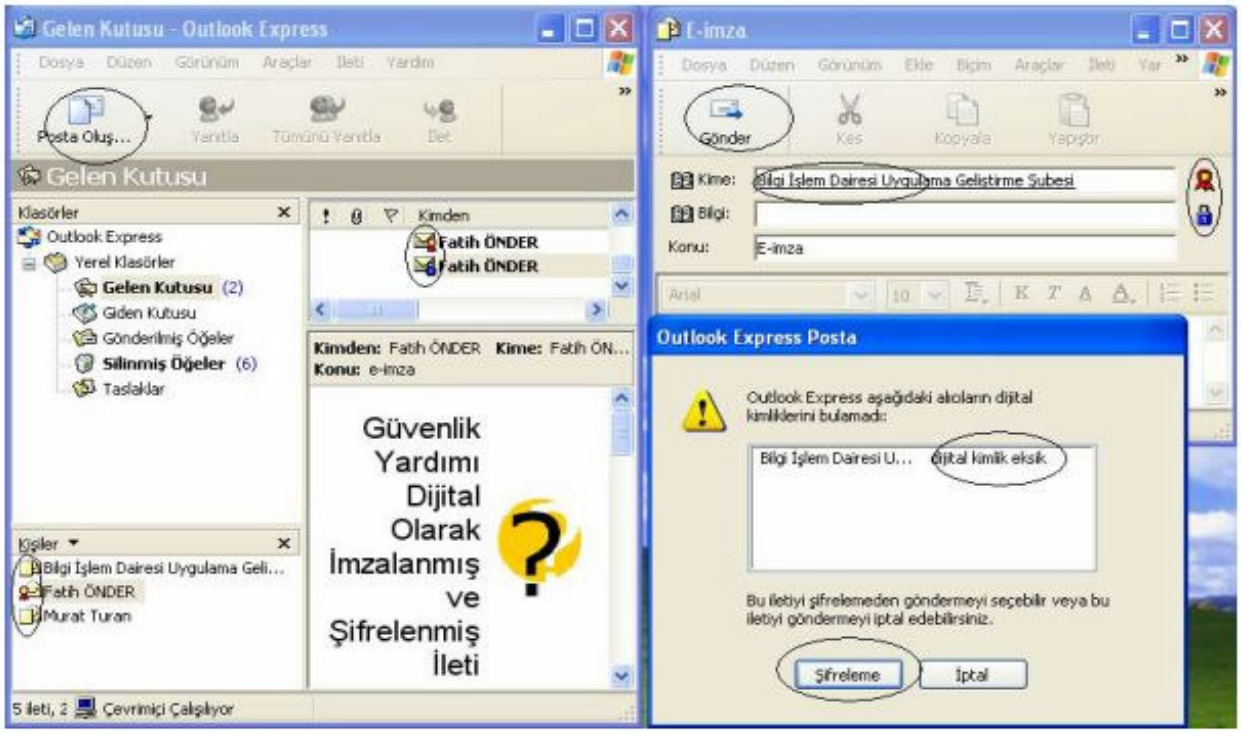
Alıcı mesajı aldığında, bunun gerçekten ilgili şahıstan gelip gelmediğini anlamak için, önce mesajı hash fonksiyonundan geçirir ve mesajın hash değerini elde eder. Daha sonra karşı taraftan gelen imzayı yani mesajın hash değerini gönderenin genel anahtarı ile açarak karşılaştırır. Eğer değerler aynı ise mesaj değiştirilmemiş demektir. En küçük bir müdahale, hash değerlerinin farklı çıkmasına yol açacaktır. "Genel anahtarla şifreyi deşifre etmekle mesajın özel anahtar sahibi tarafından şifrelendiği anlaşılır. Mesaja ekli elektronik sertifika sayesinde de gönderenin sertifika hizmet sağlayıcısının ilan ettiği kişi olduğu anlaşılır."[65] Bu şekilde mesajın bütünlük kontrolü ve kimlik tespiti fonksiyonları gerçekleştirilmiş olur. Ancak bu fonksiyonların yanında gizlilik de isteniyorsa bu durumda şifreleme metodu kullanılabilir.

[63] Ulvi Altınışık, Elektronik Sözleşmeler, Seçkin Yayınevi, İstanbul: 2003, s. 91
[64] Ulvi Altınışık, a.g.e., s.92
[65] Şeref Sağıroğlu, Mustafa Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara 2005 s.71



Şekil.2: Outlook Express'de elektronik imzalı mail gönderme prosedürü. (Leyla Keser Berber 2005)

Şekil 3: Outlook Express'te elektronik imzalı olarak gelen maildeki şifreli ibaresi üzerine kliklenmesi neticesinde yazılım tarafından otomatik olarak yapılan kimlik doğrulama ve bütünlük kontrolü.



Şekil: 4. Outlook Express'te elektronik imzalı mail gönderme prosedürü. Daire içerisine alınmış şifreli işareti gönderilecek mailin elektronik imzalı olacağını kilitli işareti ise alıcının açık anahtarı ile şifreleneceğini belirtmektedir. Alıcı elektronik imza sahibi gözükmüyor ise açık anahtarı sistem tarafından bilinemeyeceğinden şifreleme prosedürü çalışmaz.

"Gönderici oluşturduğu mesajı alıcıya gizli olarak yani sadece alıcı tarafından açılabilecek şekilde göndermek isterse, öncelikle yine yukarıdaki metoda göre mesajın hash değerini elde ederek özel anahtarı ile şifreler ve mesaja ekler. İkinci aşamada ise, bu kez ekinde elektronik imza yani hash değeri de olduğu mesajın tamamını alıcının genel anahtarı ile şifreler ve alıcıya gönderir. Artık bu mesaj alıcının özel anahtarı dışında bir anahtar veya yöntemle açılamayacağından üçüncü şahıslar mesajı okuyamaz veya müdahale edemez (gizlilik)."[66] Alıcı mesajı aldığında önce kendi özel anahtarı ile mesajı deşifre eder. Daha sonra yukarıda anlatıldığı şekilde hash değeri kontrolü yaparak mesajın değişmediğini (bütünlük) ve gerçekten gönderen gözüken kişiden geldiğini (kimlik tespiti) tespit eder. Buradan da anlaşılacağı üzere, elektronik imzalı ve gizli (şifrelenmiş) mesaj veya belge oluşturmak yada gönderebilmek için alıcının da elektronik imzasının bulunması ve açık anahtarının gönderen tarafından bilinmesi daha doğrusu gönderenin

[66] Şeref Sağıroğlu, Mustafa Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara 2005 s.65

bilgisayarında kayıtlı olması gerekmektedir. Aksi halde kullanılan yazılım şifreleme prosedürünü gerçekleştiremeyecek ve hata mesajı verecektir. Bu durumda ya şifreleme işlevinden vazgeçilecek yada alıcının açık anahtarı yani sayısal kimliği sisteme kaydedilerek işleme devam edilecektir.

1.4. TÜRK HUKUKU AÇISINDAN ELEKTRONİK İMZA

"Elektronik kayıtların yazılı şekil şartını sağlamasının ve yargılamada delil olabilmelerinin nitelikli elektronik imza kullanılmasına bağlanmasının sınırlayıcı etkileri Direktifin 5. maddesi 2. paragrafı hükmü ile giderilmeye çalışılmıştır."[67]

Bu düzenlemeyle, üye devletlerin, elektronik imzanın hukuki geçerliliğini ve kanıt olarak kullanılmasını, sadece, a) elektronik formda olması b) nitelikli bir sertifikası bulunmadığı c) akreditasyon belgesi olan bir sertifika hizmet sağlayıcısı tarafından verilmiş nitelikli bir sertifikaya dayanmadığı d) güvenli imza oluşturma araçları ile oluşturulmadığı gerekçeleriyle engellemeyeceği hüküm altına alınmıştır.

Türk Hukuku'nda Elektronik İmza'yı incelemezden evvel, sistemin başlangıcı ve sürecin ilerleyişi hakkında daha net doneler elde etmek için, Dünya'daki öncül E-imza uygulamaları konusunu irdelemek gerekir. Amerikan Hukukunda federal düzeyde uyulması zorunlu elektronik imzalara ilişkin temel düzenleme Federal Global ve Ulusal Ticarette Elektronik İmza Kanunu (The Electronic Signatures in Global and National Commerce Act) [68], bunun yanında, "yeknesak kanun"[69] niteliğindeki 1999 tarihli Yeknesak Elektronik İşlemler Kanunu'nda (Uniform Electronic Transactions Act) da elektronik imzaya ilişkin önemli düzenlemeler yer almaktadır. 30/06/2000 tarihli Amerika Elektronik İmza

[67] Mete Özgür Falcıoğlu, Karşılaştırmalı Hukuk ve Türk Hukukunda Elektronik Satım Sözleşmesi ve Kurulması, Ankara,Yetkin Yayınları, 2004, s. 84

[68] http://uscode.house.gov/lawrevisioncounsel.shtml.

[69] Amerikan hukukunda düzenlemeler, temel olarak federal kanun, yeknesak kanun ve eyalet kanunları şeklinde üç grup altında toplanabilirler. Federal kanunlar, federal devlet tarafından çıkarılan ve her eyalet için uyulması zorunlu kurallar getiren düzenlemelerdir: eyalet kanunları ise her eyaletin kendi iç hukukuna ilişkin olarak çıkardığı ve sadece eyalet sınırları içinde uygulanan kurallardır. Buna karşılık yeknesak kanunlar ise eyalet hukuklarını uyumlaştırmak üzere çeşitli kurumlar tarafından hazırlanan, federal devlet tarafından uyulması zorunlu kurallar olarak belirlenmemekle beraber, kabulleri teşvik edilen düzenlemelerdir. (Falcıoğlu, a.g.e., s. 71 dp. 146)

Kanunu, elektronik işlemlere itimadı arttırmak ve devam eden büyümesine ve güvenirliliğine destek olmak amacıyla kabul edilmiştir.

"1995 tarihli ABD' nin Utah Eyaleti'nin Dijital İmza Kanunundan sonra"[70] Birleşmiş Milletler Uluslar arası Ticaret Hukuku Komisyonunun (UNCITRAL) hazırlanmış olduğu, Elektronik Ticaret Model Kanunu 16 Aralık 1996 tarihinde kabul edilmiştir134. "Bu Kanun, aynen veya milli hukukun ihtiyaçlarına ve özelliklerine göre kısmen veya uyarlanarak milli hukuklarca kabul edilmek üzere hazırlanmış bir örnek kanun niteliği taşımaktadır. Bu Kanunun amacı, özellikle e-posta, internet gibi modern iletişim araçlarının kullanımının arttığı dikkate alınarak bu konudaki hukuki engelleri ortadan kaldırmak, elektronik ticaret alanında hukuki güvence sağlamaktır."[71] UNCITRAL Elektronik İmza Model Kanunu ise Elektronik Ticaret Model Kanununun temel prensiplerinden hareketle, Birleşmiş Milletler Uluslar arası Ticaret Komisyonu tarafından hazırlanmış"[72] ve 05 Temmuz 2001 tarihinde kabul edilmiştir. Elektronik Ticaret Model Kanunu gibi Elektronik İmza Model Kanununun uygulama alanı da ticari faaliyetler olarak belirlenmiş ve tüketicinin korunmasına ilişkin kuralların yürürlükten kaldırılmadığı ifade edilmiştir. "Aynı şekilde, Elektronik İmza Model Kanununda da temel ilkeler olarak, teknoloji tarafsızlığı (m.3), işlevsel denklik (m.6) ve irade özerkliği (m.5, 6/4 bent a ve 12/5) prensipleri esas alınmış bulunmaktadır."[73] "Bu model kanun ülkelerin çıkaracakları elektronik imza kanunları için model olmayı ve elektronik imzanın temel kurallarını oluşturmayı, bu şekilde çeşitli ülkelerin farklı mevzuatlar geliştirme riskini önlemeyi hedeflemektedir."[74] "Bununla birlikte elektronik imzalarla ilgili genel esasları belirlemeyi amaçlayan çerçeve bir yasadır."[75]

"Alman hukukunda elektronik imza hakkında temel düzenleme Alman Elektronik İmza Kanunu (Gesetz über Rahmenbedingungen für elektronische

[70] E-İmza, E-İmza' nın Toplumsal Boyutu, http://www.e-imza.gen.tr/templates/resimler/File/arastirma_dosyalari/E-IMZANIN_TOPLUMSAL_BOYUTU.doc Erişim tarihi:10.09.2010, s.7
[71] Ömer Ergün, Dijital İmza ve Dijital İmzanın Kullanımı, http://ab.org.tr/ab05/tammetin/12.doc erişim tarihi:10.09.2010, s.71
[72] UNCITRAL Model Law on Elektronic Signatures, http://www.uncitral.org, Erişim tarihi:10.09.2010.
[73] İNAL, Tamer, Elektronik İmza' da Hukuki Sorumluluk, Kazancı Hukuk, İşletme ve Maliye Bilimleri, Hakemli Dergi, Ağustos 2004, S.2, s.30
[74] Ayşe İnalöz , Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Uzmanlık Tezi, Ankara 2003 http://www.tk.gov.tr/Yayin/Uzmanlik_Tezleri/tktezler/Ayse_Inaloz_Tez.pdf, Erişim tarihi:10.09.2010, s.59
[75] İnci Demirel, Çeşitli Ülkelerde Uygulanan Elektronik Ticaret ve Elektronik İmza Yasaları Hakkında Not, Hazine ve Dış Ticaret Müsteşarlığı, Elektronik Ticaret Genel Koordinatörlüğü, http://bilisimsurasi.org.tr/dosyalar/7.doc erişim tarihi:10.09.2010, s.2.

Signaturen - SigG)'dur."[76] "AB Direktifinden önce, Almanya'da Dijital İmza Kanunu 13/07/1997 yılında kabul edilmiş idi. Bu kanun AB Elektronik İmza Direktifi ile uyumsuz hükümler içerdiğinden, yaklaşık dört senelik tecrübeyle ve AB Direktifine uygun şekilde"[77] yeniden hazırlanan Alman Elektronik İmza Kanunu 22/05/2001'de yürürlüğe girmiştir. "Alman Elektronik İmza Kanunu'nun 24. maddesine istinaden hazırlanan Elektronik İmza Yönetmeliği (Signaturverordnung – SigV) ise 16/11/2001 tarihinde yürürlüğe girmiştir. Alman Elektronik İmza Kanunu'nda, UNCITRAL, AB ve ABD düzenlemelerinden farklı olarak, yalnız elektronik imzanın işleyişine ilişkin düzenlemelere yer verilmiş; elektronik imzanın hukuki etkisi bu kanunla düzenlenmemiştir. Elektronik imza ve belgelerin hukuki etkileri ve geçerlilikleri mevzuatta yer alan ilgili kanunlarda değişikliğe gidilerek belirlenmiştir."[78]

"Türkiye'deki elektronik imza alanındaki çalışmaların başlangıcı, Bilim ve Teknoloji Yüksek Kurulu'nun 25.08.1997 tarihli kararıyla, Dış Ticaret Müsteşarlığı'nın koordinasyonunda Elektronik Ticaret Koordinasyon Kurulu'nun oluşturulmasına kadar götürülebilir."[79] "Türkiye' de elektronik imzanın hukuki olarak anlam kazanması ve elektronik imza kullanımının hukuken geçerli sayılması 5070 sayılı ve 23 Ocak 2004 tarihli Elektronik İmza Kanununun çıkarılmasıyla sağlanmıştır."[80] Söz konusu Kanunun ülke gerçeklerine uygun olarak uygulamaya geçirilebilmesi için gerekli düzenlemeleri yapma görevi ise yine aynı kanunla Telekomünikasyon Kurumu'na verilmiş bulunmaktadır. Kurum, elektronik imzanın uygulanmasına ilişkin ikincil mevzuatı, diğer ülkelerin ve özellikle AB üye ülkelerinin hukuki düzenlemelerini ve teknik uygulamalarına, konuyla ilgili yetkili ve sorumlu uluslar arası kuruluşlarca belirlenmiş standartları inceleyip, Türkiye' de oluşacak bu yeni sektörün önemli aktörlerinin de görüşlerini değerlendirerek 23 Ocak 2005 tarihinde çıkarmıştır.

"Uygulamalar açısından Türkiye'deki mevcut duruma bakıldığında; kurumsal işlemlerin ve vatandaşa yönelik hizmetlerin elektronik ortama aktarılmakta olduğu, bu anlamda kamu sektöründe birbirinden bağımsız çalışmalar yapıldığı, kurumların bilgi verme

[76] http://bundesrecht.juris.de/bundesrecht/sigg_2001/inhalt.html. erişim tarihi: 02.04.2011
[77] İnci Demirel, Hukuk Elektronik Yaşam ve Ticaretin Hizmetinde veya Siber Uzayda Hukukun Yükselişi, http://www.dtm.gov.tr/ead/DTDERGI/Ekim2002/inci.htm, erişim tarihi: 02.04.2011.
[78] Alman Elektronik İmza Kanunu, http://bundesrecht.juris.de/bundesrecht/bgb/index.html erişim 02.04.2011
[79] Önder Canpolat, Elektronik İmza Kanun Tasarısı neyi düzenliyor?, http://edonusum-demo.tbd.org.tr/demo.tbd.org.tr/demo/index.php?module=bilisim&page=show_content&content_id=160&sid=dd6c2a7212e82f6da08e2310ab0f6c11 erişim tarihi:10.04.2011
[80] M.Emre Civelek, Kağıtsız Ticarete Doğru Adım Adım: Elektronik İmza Yasası ve Dış Ticaret İşlemler, http://www.emrecivelek.com/signature.htm erişim tarihi:04.04.2011

amaçlı olarak ana kapı oluşturduğu, ancak henüz bu ana kapılar üzerinden elektronik işlem yapılması çalışmalarının başlangıç aşamasında olduğu görülmektedir. Türkiye'de oluşturulacak elektronik imza altyapısının ülke çıkarlarına ve uygulama kolaylığına hizmet verecek şekilde olabilmesi amacıyla; elektronik sertifika sağlayıcılarının kök anahtarlarının Türkiye' de üretilmiş olması, kamu kurum ve kuruluşlarının tek bir altyapı ve standart altında toplanması, kıt kaynakların verimli kullanılması ve yapının tek elden koordinasyonunun sağlanması gerekmektedir."[81] Bununla birlikte elektronik imzanın Türkiye'deki kamusal uygulamalarının; her türlü başvurular (ÖSS, KPSS, pasaport başvuruları vb.), kurumlar arası işlemler (emniyet, nüfus ve vatandaşlık işleri), sosyal güvenlik uygulamaları, sağlık uygulamaları, vergi ödemeleri, elektronik oy verme işlemleri oluşturmaktadır. "Ticari uygulamaların ise; internet bankacılığı, sigortacılık işlemleri, e-sipariş ve elektronik sözleşmeler alanlarında olması beklenmektedir."[82] Elektronik imza kamusal alanda her türlü başvurular, kurumlar arası iletişim, sosyal güvenlik uygulamaları, sağlık uygulamaları, vergi ödemeleri gibi uygulamalarda kullanılmasının yanı sıra, ticari alanda da internet bankacılığı, sigortacılık işlemleri, elektronik sözleşmeler, elektronik ticaret gibi alanlarda da kullanılacaktır. Bununla birlikte elektronik ortama ve açık ağ sistemine duyulan güvenin sağlanması için taraflar arası iletilerde, bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu kurulacak olan teknik ve yasal altyapı ile garanti edilebilmelidir.

Elektronik imza ile ilgili hukuki altyapının oluşturulması ile ilgili şu çalışmalar gerçekleştirilmiştir:

Her türlü ikili ve kurumsal iş ve işlemlerde kayıt tutma, standart ve tekniklerinin belirlenmesi,

Elektronik kayıtların kamu kurum ve kuruluşları tarafından belge olarak kabulü ile ilgili standart ve iç mevzuatlarının düzenlenmesi,

[81] E-İmza, E-İmza' nın Toplumsal Boyutu, http://www.e-imza.gen.tr/templates/resimler/File/arastirma_dosyalari/E-IMZANIN_TOPLUMSAL_BOYUTU.doc Erişim tarihi: 10.04.2011, s.9

[82] E-İmza, E-İmza' nın Toplumsal Boyutu, http://www.e-imza.gen.tr/templates/resimler/File/arastirma_dosyalari/E-IMZANIN_TOPLUMSAL_BOYUTU.doc (Erişim tarihi: 10.04.2011, s.9

Ticaret Kanunu, Sayıştay denetim usulleri, Borçlar Kanunu, Bankalar ve Vergi Usul kanunlarının elektronik belge tutma ve gönderme şartları göz önüne alınarak tekrar düzenlenmesi,

Elektronik ortamda oluşturulan yabancı belgelerin geçerliliği konusunda dış ticaret, gümrük ve bankalar kanununda değişiklik, uluslar arası/ulusal olarak yapılan elektronik sözleşmelerde ve sanal ticarette oluşabilecek ihtilaflar konusunda elektronik tahkim yasasının çıkarılması,

Özel ve kurumsal bilgilerin gizliliği, bütünlüğü için Ulusal Bilgi Güvenliği Yasasının çıkarılması buna bağlı olarak SPK gibi kurumların ve ürün borsalarında kontrat bazlı, spot ve opsiyon piyasalarında sanal işlem uygulama yönetmelikleri ile uluslar arası sanal ticaret için akreditasyon kurumları için yeni mevzuatların çıkarılması,

Açık anahtar (public key) ile ilgili onay kurumlarının (Nitelikli Elektronik Sertifika sağlayan kurumların) kurulum izinleri ve denetimi kamu tarafından yapılmalı, %51 hissesi kamu elinde bulunan kurumların bu pazardan ivedi çekilmesi gerekmektedir, uluslar arası kredi ve finans kurumlarının ticarette uyguladığı kriterlerin devlet kurumlarının hizmet ve mal alımında da uygulanması için devlet ihale kanunu, elektronik imza kanunu ile elektronik imza yönetmeliği'ne kesin ve bağlayıcı maddelerin ilave edilmesi,

Elektronik suçların evrenselliği konusunda yapılan uluslar arası mevzuat çalışmaları ve yapılacak ikili anlaşmaların hızlı bir şekilde yapılması, işlerlik açısında delil toplama ve alma/verme standartlarının belirlenmesi.

Elektronik kontrat ve elektronik imza gerektiren sanal işlemlerde tüketicinin korunması ile ilgili mevzuatın elektronik ticaret açısından yeniden gözden geçirilmesi, e-ticaret yapan kurumların uyacağı kuralların ivedilikle yayınlanması, bankacılık kanunu ile ilişkilendirilmeli ve geri ödeme (charge-back) sisteminin sanal ticarette uygulamaya sokulması,

Elektronik ödeme araçları arasında yer alan elektronik paranın (elektronik senet, elektronik çek, elektronik teminat, gibi) uygulanacağı standart, teknikler ve güvenlik kriterleri ile ulusal ve uluslar arası dolaşımı mevzuat ve anlaşmaların yapılması,

Elektronik imza yasası,

Elektronik imza ile ilgili yönetmelik,

Elektronik arşivle ilgili yasal mevzuat.

"Elektronik imzanın kullanımı ile ilgili şu ana kadar çıkmış mevzuatlar ise şunlardır:" [83]

1- 5070 Sayılı Elektronik İmza Kanunu (23 Ocak 2004)

2- Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul Ve Esaslar Hakkındaki Yönetmelik (6 Ocak 2005 R.G. 25692)

3- Kamu Sertifikasyon Merkezi Oluşturulması Hakkında Genelge

4- Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26 Ağustos 2004 RG 25565)

5- Sertifika Mali Sorumluluk Sigortası Tarife Ve Talimatı (27.01.2005 RG 25709)

6- Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (27.01.2005 RG 25709)

7- Elektronik İmza İle İgili Süreçlere Ve Teknik Kriterlere İlişkin Tebliğ (06 Ocak 2005 ve RG 25692)

8- Elektronik İmza İle İlgili Süreçlere Ve Teknik Kriterlere İlişkin Tebliğ'de Değişiklik Yapılmasına Dair Tebliğ.

[83] Mesut Orta, Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı, http://docs.google.com/viewer?a=v&q=cache:z8iujAL0NtoJ:www.e-ticaret.gov.tr/toplanti/t%25C3%25BCrkiyede%2520elektronik%2520imza%2520uygulamari.doc+%C3%87amurdan,+Elektronik+%C4%B0mza+Kanunu+Tasar%C4%B1s%C4%B1+%C3%9Czerine+Bir+De%C4%9Ferlendirme&hl=tr&gl=tr&pid=bl&srcid=ADGEESjrf3nGIXor9c9FqMS0bVyIueRlgi8vSRRVHLLh3icom548DdNHXfXMe8ppGkvGl23DRgwa4_-_vpuBvrWV2GUDhq3fvc42WC2TgzIpgq7PoOeN_CqFS9Le7-MhpQKVwGVxQX-q&sig=AHIEtbSiKvIUrLZhHrOSnyk5OpDuRlnISg erişim tarihi: 03.04.2011

1.5. 5070 SAYILI ELEKTRONİK İMZA KANUNU

Elektronik devlet ve ticaretin en önemli hukuki ve teknik altyapısını oluşturması beklenen "Elektronik İmza Kanunu'nun ilk taslağı, Dış Ticaret Müsteşarlığı'na bağlı Elektronik Ticaret Koordinasyon Kurulu"[84] tarafından hazırlanmış ve tartışmaya açılmıştır. 1998 yılında ETKK bünyesinde hukuk, teknik ve finans çalışma grupları oluşturulmuştur. Hukuk Çalışma Grubu tarafından hazırlanmış olan Temmuz 2000 tarihli çalışma sonuç belgesinde, elektronik imzanın hukuken tanınması için bir kanun taslağının hazırlanmasına değinilmiş ve bu konuda Adalet Bakanlığı'nın çalışmalarının beklenmesine karar verilmiştir. Hukuk Çalışma Grubu Haziran 2001'de tekrar toplanmış; bu toplantıda elektronik imza ile ilgili kanun taslağını hazırlamak üzere Adalet Bakanlığı, Gümrük Müsteşarlığı, DPT Müsteşarlığı, Merkez Bankası, Telekomünikasyon Kurumu, PTT Genel Müdürlüğü ve Dış Ticaret Müsteşarlığı temsilcilerinden oluşan Hukuk Alt Çalışma Grubu kurulmuştur. Hukuk Alt Çalışma Grubu çalışmalarına Temmuz 2001'de başlamış ve "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanunu Tasarısı Taslağı"nı hazırlanmıştır. Hazırlanmış olan taslak, Nisan 2002'de Başbakanlığa gönderilmiştir."[85]

"ETKK Hukuk Grubu'nun çalışmaları devam ederken Adalet Bakanlığı 14 Ocak 2002 tarihli yazısı ile çeşitli kurum ve kuruluşlardan elektronik imzanın düzenlenmesine ilişkin kanun tasarısı taslağının hazırlanması için oluşturulacak komisyona temsilci bildirilmesini talep etmiştir."[86] Adalet Bakanlığı Elektronik Ticaret Koordinasyon Kurulu, elektronik ticaret ağının tesis edilmesi ve elektronik ticaretin yaygınlaştırılması amacıyla Bilim Teknoloji Yüksek Kurulu'nun (BTYK) 25 Ağustos 1997 tarihli toplantısında alınan karar uyarınca Dış Ticaret Müsteşarlığı'nın başkanlığında ilgili kuruluşların katılımıyla oluşturulmuştur. (www.e-ticaret.gov.tr) bünyesinde kurulan komisyon tarafından hazırlanan "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" Bakanlar Kurulu tarafından kabul edildikten sonra 9 Haziran 2003 tarihinde Türkiye Büyük Millet

[84] Elektronik Ticaret Koordinasyon Kurulu, elektronik ticaret ağının tesis edilmesi ve elektronik ticaretin yaygınlaştırılması amacıyla Bilim Teknoloji Yüksek Kurulu'nun (BTYK) 25 Ağustos 1997 tarihli toplantısında alınan karar uyarınca Dış Ticaret Müsteşarlığı'nın başkanlığında ilgili kuruluşların katılımıyla oluşturulmuştur. Kaynak: http://www.e-ticaret.gov.tr erişim tarihi: 02.04.2011

[85] Çiğdem Çamurdan, Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme, TBD Dergisi 2003, http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm erişim tarihi 09.10.2010, s.52-54

[86] Çamurdan, a.g.e, s.55

Meclisi'ne yasalaşması amacıyla gönderilmiş ve meclis komisyonlarından geçerek Genel Kurul'da 15 Ocak 2004 tarihinde yasalaşmıştır. Elektronik İmza Kanunu 23 Ocak 2004 tarihinde Resmi Gazete'de yayımlanmış ve kanunun 25.maddesi doğrultusunda 23 Temmuz 2004 tarihinde yürürlüğe girmiştir.

"5070 Sayılı Elektronik İmza Kanunu, Avrupa Komisyonu'nun 99/93/EC numaralı direktifi çerçevesinde hazırlanmıştır. Bu nedenle kendisine kaynaklık eden AB elektronik imza direktifinin temel aldığı açık anahtarlı altyapı teknolojisi üzerinde işlevsellik gösteren elektronik imzayı düzenlemektedir."[87] Bu Kanuna göre elektronik imza "başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"dir. Bu tanım AB elektronik imza direktifinin çevirisi şeklindedir. Çalışmanın ikinci bölümünde açıklandığı gibi elektronik imza bir üst kavramdır. Kanunun elektronik imza tanımının ikinci kısmı ise bu noktada önem kazanmaktadır, çünkü parmak izi, retina, yüz ve ses taraması gibi biometrik yöntemlerle oluşturulan elektronik imzalar her ne kadar kimlik doğrulama amacıyla kullanılabiliyor da olsa eklendikleri veriyle "mantıksal bağlantı"ları yoktur. "Bu anlamda kanunun ismi her ne kadar "elektronik imza kanunu" da olsa kanunla düzenlenen "eklendiği veriyle mantıksal bağ kuran" sayısal imzadır."[88]

"5070 Sayılı Kanun"[89] güvenli bir elektronik imzanın sahip olması gereken özellikleri ise şöyle sıralamaktadır: "münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza". Bu tanımda yer verilmiş olan güvenli elektronik imza oluşturma araçlarına ilişkin düzenlemelerin ise ayrıca düzenlenmesine karar verilmiştir. Elektronik imza uygulamalarının başlayabilmesi için ikincil düzenlemelerin tamamlanması gerekmekte olup, bu görev 5070 Sayılı Kanun'un 24. maddesi ile Telekomünikasyon Kurumu'na verilmiştir. Telekomünikasyon Kurumu'nun, kanunun 13. maddesine göre sertifika, mali sorumluluk sigortası ve 20. maddesine göre güvenli elektronik imza

[87] Telekomünikasyon Kurumu, 2004 a: 18-19
[88] Tolga Tüfekçi, Elektronik İmza Niçin Yaygınlaşmıyor? TÜBİTAK. Bilgi Teknolojileri ve Elektronik Araştırma Enstitüsü, Türkiye Bilişim Haftası, 1-7 Eylül 2003, http://www.uzay.tubitak.gov.tr/tubitakUzay/yayinlar/Elektronik_imza_nicin_yayginlasamiyor-ppt.pdf erişim tarihi: 02.02.2011
[89] http://www.tk.gov.tr/eimza/eimza_yasasi.htm Erişim Tarihi: 09.10.2010

oluşturma araçları, güvenli elektronik imza doğrulama araçları, elektronik sertifika hizmet sağlayıcısı, elektronik sertifika hizmet sağlayıcısının yükümlülükleri, nitelikli elektronik sertifikaların iptal edilmesi ve yabancı elektronik sertifikalar ile ilgili ikincil düzenlemeleri kanunun yürürlüğe girmesinden sonra altı ay içinde yani en geç 23 Ocak 2005 tarihine kadar tamamlaması gerekmektedir. Bu amaçla Telekomünikasyon Kurumu bünyesinde "Elektronik İmza Ulusal Koordinasyon Kurulu" ve bu kurula bağlı "Bilgi Güvenliği ve Standartlar", "Hukuk ve Düzenlemeler" ve "Altyapı" çalışma grupları oluşturulmuştur.

1.6. ELEKTRONİK VERİLERİN DELİL DEĞERİ

Mevcut hukuk sistemimizde deliller ikiye kategoride ele alınmaktadır. Bunlar kesin delil ve takdirli delillerdir. Kesin deliller olarak ikrar; ("Dava evrakında veya hâkim huzurunda iki taraftan birinin veya vekilinin sebkeden ikrarı muteberdir. Ve mukir olan taraf aleyhine delil teşkil eder. Maddi bir hatadan neşet ettiği sabit olmadıkça ikrardan rücu olunamaz. Sulh müzakeresi esnasında sebkeden ikrar muteber değildir. Mahkeme haricindeki ikrarı teyit edecek delail ve emare mevcut ise hâkim buna binaen hüküm verebilir"[90]), kesin hüküm; "Kaziyei muhkeme, ancak mevzuunu teşkil eden husus hakkında muteberdir. Kaziyei muhkeme, mevcuttur denilebilmek için iki tarafın ve müddeabihin ve istinat olunan sebebin müttehit olması lazımdır"[91], senet; "Kanunun muayyen bir delil ile ispatını emreylediği hususlar başka suretle ispat olunamaz. İki tarafça muayyen deliller ile ispatı tahriren kabul edilmiş olan veya muhakeme esnasında olveçhile beyinlerinde karar verildiği ikrar olunan maddeler hakkında başka delil kabul olunmaz"[92] ve yemindir. "Takdiri deliller ise şahit, bilirkişi, keşif ve özel hüküm sebepleridir."[93] Elektronik imza kanununun özündeki düzenleme elektronik belgenin delil vasfının düzenlenmesine yönelik değil; elektronik imzanın düzenlenmesine yöneliktir. Madde 5'in f bendindeki hüküm güvenli elektronik imzaya elle atılan imza ile aynı hukuki sonuç bağlanmıştır.

[90] 1086 Sayılı, "Hukuk Usulü Muhakemeleri Kanunu", Kabul Tarihi:18.06.1927, Resmi Gazete Sayısı:622, Resmi Gazete Tarihi: 02.04.1927, Madde:236
[91] 1086 Sayılı, "Hukuk Usulü Muhakemeleri Kanunu", Madde:237.
[92] 1086 Sayılı, "Hukuk Usulü Muhakemeleri Kanunu", Madde:287.
[93] Seyithan Deliduman, İspat sistemimizin mevcut durumu ve elektronik imzanın bu sistemdeki yeri, e-Akademi Dergisi (elektronik), Sayı:2, Nisan 2002

Uyuşmazlık durumlarında mahkeme öncelikli olarak imza sahibine imzanın kendisine ait olup olmadığını sorması gerekmektedir. Buradaki esas imzanın kişi tarafından ret edilmesine göre düzenlenmiştir. "Kişi imzanın kendine ait olmadığını iddia ederse, mahkeme heyeti imza inceleme yoluna başvurur ve ıslak imzada görülen usul ve esaslar aynen muhafaza edilerek tetkikat bilirkişi heyetleri marifetiyle gerçekleştirilir."[94]

Hukuk Usulü Muhakemeleri Kanunu'muzda senedin tanımı yapılmamıştır. "Doktrinde"[95] medeni usul hukuku bakımından senedin genel kabul görmüş unsurlarına göre, bir tanım yapma gayreti içine girersek; senedi, hukuki bir işlem hakkında, bizzat imzalayan(lar) veya üçüncü bir şahıs tarafından veya bir cihaz yardımıyla yazılı hale getirilen ve bizzat o kimse (veya yetkili temsilci) tarafından imzalanması ile vuku bulan ve aleyhine delil teşkil etme iradesiyle hasma verilen belge olarak tarif edebiliriz. Senedin temel olarak, "hukuki bir işlemi tespit etmek ve belgelemek"[96] yazılı metin ve imza olmak üzere üç temel unsuru olduğu söylenebilir. Senedin tanımında yer alan, aleyhe delil teşkil etme durumunu değerlendirirsek, senedi meydana getirenin, senedi kendi aleyhine delil teşkil etmek iradesiyle meydana getirmesi şart değildir. Senedi meydana getirenin kendi aleyhine delil teşkil etmesini düşünmediği hallerde de yazılı belge senet sayılır.[97] Lakin, bir kimsenin düzenlemiş olduğu belgenin, ticari defterlerdeki durum hariç, kendi lehine delil sayılması mümkün değildir. Aleyhe delil teşkil etme durumu irade beyanının içeriği bakımından değerlendirilebilir. Şöyle ki, aleyhe delil teşkil edebilecek herhangi bir irade açıklaması yoksa bu belge senet niteliğinde sayılmamalıdır kanısındayız. Aleyhe delil teşkil etme hususu yanında, hasma verilmiş olma hususu incelendiğinde de, benzer bir sonuça varılacaktır. Şöyle ki, bir belge senedin diğer unsurlarına sahip ise senet delili olarak kullanılması için karşı tarafa verilmiş olması şart değildir. "HUMK m. 326 vd. uyarınca yargılamada delil olarak kullanılacak belgeler karşı tarafın veya üçüncü kişinin elindeyse hakim tarafından bu belgenin ibrazı emredilebilir. Senetlerin mahkemeye ibrazı zorunluluğuna ilişkin bu hükümler, bir belgenin, senet niteliğine sahip olması için karşı tarafa verilmiş olma unsurunun şart olmadığını göstermektedir."[98]

[94] Haluk Konuralp, Genel Hatlarıyla Elektronik İmza Kanunu, http://www.tbb.org.tr/turkce/konferans.htm erişim tarihi: 03 Haziran 2011
[95] Baki Kuru, Hukuk Muhakemeleri Usulü, C.II, Demir Yayınları, İstanbul 2001, s. 2073-2077
[96] İlhan E. Postacıoğlu, Medeni Usul Hukuku Dersleri, 6. baskı, İstanbul, Sulhi Garan Matbaası, 1975, s. 192
[97] Baki Kuru, Hukuk Muhakemeleri Usulü, C. II, Demir Yayınları İstanbul 2001, s. 2074
[98] Mine Erturgut, Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Yetkin Yayınları, Ankara 2004, s. 192-193

Sonuç olarak, bir belgenin senet sayılması, başka bir deyişle, kesin delil teşkil etmesi yalnız senedin zorunlu unsurlarının tam olarak vuku bulmasına bağlıdır.

Senetler, adi ve resmi senet olmak üzere ikiye ayrılır. Belirttiğimiz üzere, EİK m. 5 uyarınca resmi şekle veya özel merasime tabi hukuki işlemler (basit veya güvenli) elektronik imza ile gerçekleştirilemez. Resmi şekil şartının güvenli elektronik imza ile yerine getirilmesi yasağı, hem düzeleme hem de onaylama şeklindeki resmi senetler için geçerlidir düşüncesindeyiz. Bu bağlamda, Noterlik Kanunu hükümlerine göre belgelendirilen senetler, ihtiyar heyeti tarafından onaylanan senetler (mühürlü senetler), tapu memuru önünde düzenlenen senetler ve diğer resmi senetler güvenli elektronik imza ile meydana getirilemeyecektir. Öte yandan, kanun, resmi şekil şartını saymakla beraber özel bir merasime tabi tutulmuş tüm hukuki işlemlerin de elektronik imza ile düzenlenemeyeceğini belirterek güvenli elektronik imzanın kullanılabileceği alanları daha da daraltmıştır. "Medeni usul hukukunda senet, ispat şeklidir."[99] "Borçlar Hukukundaki geçerlilik şartı ile Medeni Usul Hukukundaki ispat şartı farklı kavramlardır."[100] Kural olarak bir hukuki işlemin, özellikle sözleşmelerin, geçerli olması için herhangi bir şekilde (yazılı şekilde veya resmi şekilde) yapılması şart değildir. Buna karşılık, kural olarak, hukuki işlemler yalnız senetle (kesin delille) yani yazılı şekilde ispat edilebilir. Geçerlilik şartı ile ispat şartının farklı kavramlar olması neticeleri itibariyledir, yoksa her iki şart da yazılı şekil şartında birleşirler. Başka bir ifadeyle, adi yazılı şekil, borçlar hukukunda kanunen veya taraflarca öngörülmüş geçerlilik yazılı şekil şartını yerine getirir, yargılama hukukunda ise diğer unsurlarla birlikte senetle ispat zorunluluğunu yerine getirir.

"Sermaye Piyasası Kanunu"[101]nun 10. maddesinin 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 öngörülmektedir. Kapalı bilgisayar sistemi içinde tutulacak olan kayıtları, sermaye piyasası araçları üzerindeki hak sahipliğine ilişkin bir uyuşmazlık halinde, gerçek sahipliğini öğrenmek üzere kendisine başvurulacak ve bu durum hukuk önünde

[99] Baki Kuru, Hukuk Muhakemeleri Usulü, C. II, Demir Yayınları, İstanbul 2001, s. 2077
[100] Saim Üstündağ, Medeni Yargılama Hukuku, Nesil Matbaacılık, İstanbul 2000, s.649 dp. 15
[101] 4487 Sayılı Sermaye Pisayasası Kanunu, Kabul Tarihi:15.12.1999, Resmi Gazete Sayısı:24622, Resmi Gazete Tarihi: 26.12.2001, Madde:10

doğrudan doğruya delil olarak kabul edilecektir. Bu kayıttan yazıcı aracılığıyla alınan çıktı ise dolaylı bir delildir.

1.7. ELEKTRONİK İMZALI BELGELERİN İBRAZI

Kağıt üzerine kalemle yazılmış ve imzalanmış veya bir cihaz yardımıyla yazılmış ıslak imza ile imzalanmış belgelerde, asıl ve suretin belirlenmesi nispeten kolaydır. Kağıt üzerine yazılı belgenin ilk meydana getiriliği hali yani orijinali ya tektir ya da kaç nüsha hazırlanmış ve imzalanmış ise o kadar orijinal (asıl) belge vardır. El yazısı veya ıslak imza içeren belgenin suretinin çıkarılması halinde, elde edilen kopyanın suret olduğu, çoğu zaman teknik bir inceleme gerekmeksizin dahi anlaşılabilir. Buna karşılık, asıl (orijinal) terimi, bilginin ilk meydana getirildiği hali olarak düşünüldüğünde, veri mesajlarının orijinalliğinden bahsedilemeyecektir, "çünkü veri mesajının alıcısı her zaman bu belgenin ilk meydana getirildiği halin bir kopyasını alır."[102]

"Elektronik ortamda bir belgenin bir kimseden diğer bir kimseye verilmesi, bu belgenin kopyalanması ile gerçekleşir. Elektronik verinin ilk bütün olarak yaratıldığı halin orijinal (asıl) sayılması düşünülse de, bu halde de, asıl ile kopyalar ayırt edilemeyecektir."[103] Örneğin, bir kağıt üzerine yazılmış senet (aynısından birden çok tanzim edilmemişse) ne kadar el değiştirirse değiştirsin tektir, buna karşılık, veri mesajı her el değiştirdiğinde bu mesajın aynısı kopyalanır. Kısaca, kopya (taklit) olmayan anlamıyla orijinal (asıl) belge kavramı, elektronik imzalı belgeler bakımından çoğu zaman kağıt belgeler gibi anlaşılmaya uygun değildir.

Elektronik belgelerin ibrazı bakımından, elektronik belgelerin hangi hallerde aslının ibraz edildiğinin, hangi şartlarda suretinin ibraz edildiğinin belirlenmesi gerekecektir. Bu bağlamda, basit elektronik imzalı belge ve güvenli elektronik imzalı belge ayrı ayrı incelenmelidir.

[102] Uncitral Model Law on Electronic Commerce with Guide Enactment 1996 with additional article 5 bis as adopted in 1998, parag. 62.
[103] M Schellkens, Electronic Signatures Authentication Technology from a Legal Perspective, Netherlands, T.M.C. Asser Press, 2004, s. 82

EİK basit elektronik imzalı belgelere yer vermekle beraber, basit elektronik imzalı belgelerin hukuki etkisi hakkında kanuni bir düzenleme getirmemiştir. Basit elektronik imzalı belgeler, hukuki anlamda, imzasız belgelerdir. Bu bağlamda, basit elektronik imzalı belgeler diğer elektronik belgeler gibi de değerlendirilecektir. Konuralp, bilgisayar ortamında tutulan banka kayıtlarının, kağıt gibi mahkeme huzurunda incelenebilecek bir araçta değil, sayı dili ile bilgisayar ortamında tutulan ve ana sistemin monitöründe izlenebileceğini; ekranda bir kayıt görünmüyorsa delil de olamayacağını; yazıcıdan alınan çıktının, delilin kendisinin değil de, bir anlamda sureti olduğunu ifade etmiştir. "Bilgisayar çıktısının veri taşıyıcısında kayıtlı ve ekranda görülen verinin orijinali olmadığını; aksi kabul edildiği takdirde aynı elektronik veriden birden fazla çıktı alınabildiğinden, alınan çıktı kadar, orijinal (asıl) metin bulunacağını; bu durumda bir metnin orijinalliğinden söz edilemeyeceği" bilgisayar çıktısının suret olarak nitelendirilmesi gerektiği"[104] belirtmiştir.

Bu durum imzanın güvenli imza olması veya bu imza dışında kalan herhangi bir elektronik imza çeşidiyle belgenin oluşturulmuş olması tartışmasından ziyade, elektronik belgelerin senet niteliğine (özellikle yazılılık ve cisim bulmuş olma unsurları açısından) sahip olup olmadığıyla ilgilidir. Elektronik imzalı belgenin senet niteliği kabul edildiği takdirde, senedi imzalayan kişi tarafından imzanın ikrar edilmesi durumunda bu elektronik belge 68. madde anlamında belge olarak değerlendirilebilir. Buna karşılık, imzası ikrar edilmiş elektronik belgenin, senet özelliklerini taşımaması sebebiyle itirazın kaldırılmasında sınırlı inceleme yetkisi olan icra mahkemesi tarafından incelenmesi mümkün olamayacaktır. Çünkü, elektronik formda ibraz edilen, elektronik belgenin icra mahkemesince görülüp algılanabilmesi ve itirazın kaldırılması konusunda kanaat edinilebilmesi için bilirkişinin yardımı zorunludur. Bu sebeple hangi çeşit imzayla imzalanmış olursa olsun, imzası ikrar edilmiş elektronik imzalı belge icra mahkemesinin sınırlı inceleme yetkisi sebebiyle itirazın kaldırılması aşamasında 68/I anlamında belge olarak nitelendirilemez.

Elektronik verilerin mahkemeye ibrazının, "bir veri taşıyıcısının mahkemeye verilmesi ya da elektronik posta yoluyla mahkemeye elektronik belgenin gönderilmesi ile gerçekleştiği"[105] mahkemenin de, elektronik belgeyi başka bir veri taşıyıcısına (taşınır

[104] Mine Erturgut, Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Yetkin Yayınları, Ankara 2004, s.39
[105] Leyla Keser Berber/Murat Lostar, Bilişimde Biyometrik Yöntemler, Ankara, Yetkin Yayınları, 2006. [Dijital İmza], s. 207

ve taşınmaz belleğe) kaydedeceği; böylece, "elektronik belgenin bilgisayarda görülebilir şekilde ibraz edilebileceği belirtilmiştir."[106] Bu noktada, elektronik imzalı belgenin bir veri taşıyıcısına kaydedilerek mahkemeye verilmesi ile bilgisayar ağları vasıtasıyla mahkemeye aktarılması ayrı ayrı incelenebilir.

Elektronik imzalı belgenin (elektronik belgenin), kendisi esasen 0 ve 1'lerden oluşan dijital veridir. Bu belgeden okunan yazı, yalnız bu dijital verinin arayüz programları sayesinde anlamlı hale getirilmiş bir görünümüdür. Elektronik imzalı belgedeki yazı, buz dağının su üstündeki kısmına benzetilebilir. Elektronik belge iki satır yazı içerse dahi, elektronik belge kilobyte'larca veriden oluşabilmektedir. Elektronik verinin kendisinin kağıda aktarılması mümkün değildir. Buna karşılık, monitörde görülen görüntü kağıda aktarılabilir, özellikle elektronik veri yazılı bir metin veya resim ise, resmin veya yazılı metnin (elektronik imza dışında) kağıda aktarılması mümkündür. Bu bağlamda, elektronik verinin yazıcıdan alınan çıktısı ancak suret veya örnek olarak değerlendirilebilir. Yazıcıdan alınan çıktı birebir bir kopya, nüsha veya fotokopi niteliğinde olmadığından, yazıcıdan alınan çıktının suret olarak nitelendirilmesi gerektiği görüşüne katılmaktayız. Bu bağlamda, basit elektronik imzalı belgelerin çıktısının alınarak ve bunların suret niteliğinde olmak üzere mahkemeye sunulması mümkündür. Bu halde, taraflar arasında, basit elektronik imzalı belgenin gerçekliği konusunda ihtilaf yoksa, bu bilgisayar çıktısına delil değeri atfedilmesi mümkündür. İbraz edilen çıktı üzerinde tarafların arasında ihtilaf varsa ve bu ihtilaf başka delilerle giderilemiyorsa, bu halde, tek başına elektronik verinin çıktısı, bu belgenin doğruluğu konusunda kanaat oluşturamayacağından mutlaka aslının (elektronik ortamda) ibrazı gerekir.

Uygulamada, sıkça bir diskete veya CD üzerine kaydedilmiş elektronik postaların veya elektronik belgelerin, bir jelatin içinde dava dosyasına eklendiği görülmektedir. HMK Tasarısı m. 225/I'de, elektronik belgelerin, belgenin çıktısı alınarak ve talep edildiğinde incelemeye elverişli şekilde elektronik ortama kaydedilerek mahkemeye ibraz edileceği, belirtilmiştir. Öncelikle, dava dosyasına eklenmiş bir veri taşıyıcının bozulma riski olduğu gibi, içeriği dışarıdan görülmediğinden dışarıdan aynı görünen başka bir veri taşıyıcıyla değiştirilmesi veya karıştırılması riski de vardır. Bilindiği gibi, kağıt bazlı deliller imzalı bir dilekçeyle ve hakimden havale alınarak dosyaya eklenmekte ve karşı tarafa da tebliğ edilmektedir. İbraz edilen kağıt bazlı belgeler suret ise, ibraz eden bu

[106] Mine Erturgut, Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Yetkin Yayınları, Ankara 2004, s. 296

belgeyi aslına uygun olduğunu belirterek imzalamaktadır. Buna karşılık, elektronik belgenin bir veri taşıyıcısına kaydedilerek ibrazı halinde, ibraz eden ile ibraz edilen veri taşıyıcısı arasında maddi bağı kurmak zor hatta imkansızdır. Veri taşıyıcısının üstünün imzalanmayacağı açıktır. Hukukumuzda bu veri taşıyıcısındaki verinin güvenli elektronik imza ile imzalanması da öngörülmemiştir. Veri taşıyıcısındaki elektronik belgeyi ibraz eden taraf "ben siyah bir disket içinde elektronik belgeyi ibraz etmiştim ama bu disket o disket değil başka bir siyah disket" bildirimleri durumunda, ya da ibraz etmek istediği belgeyi veri taşıyıcısına kaydederek mahkemeye sunan taraf veri taşıyıcısındaki elektronik belgenin sonradan değiştirildiğini, kendisinin böyle bir belge ibraz etmediğini iddia ederse ne yapılmalıdır? Bu sorular dahi tek başına elektronik belgelerin veri taşıyıcına kaydedilerek ibrazını caiz kılmanın yeterli bir düzenleme olmadığını göstermektedir. Mutlaka ibraz edilen veri taşıyıcısı ile ibraz eden arasında maddi bağın kurulmasını sağlayan düzenleme veya düzenlemeler yapılması gerekir. Bu bağlamda en güvenilir yol, elektronik delilin aslını (yani elektronik ortamdaki kopyasını) ibraz eden tarafın, bu belgeyi güvenli elektronik imzası ile imzalayarak veri taşıyıcısına kaydetmesi ve veri taşıyıcısının -içerisindeki veri (elektronik belge) imzalanmış şekilde- mahkemeye verilmesidir. Bunun dışında, bir veri taşıyıcısının dava dosyasına eklenmesinin anlam ifade edebilmesi için ihtilafı gören mahkemenin, bu veri taşıyıcısında saklı bilgiyi görebilmesi gerekir. Veri taşıyıcısında kayıtlı elektronik ortamdaki bilgi, yalnız bilgisayar vasıtasıyla görülebilir. Yalnız, yeterli teknik altyapıya sahip bir mahkeme (hakim), veri taşıyıcısında kayıtlı bilgiyi doğrudan görebilir. Hakimin, dosyaya mübrez veri taşıyıcısını, bilgisayarına yerleştirip bu veriyi tetkik etmesi, keşif çerçevesinde değerlendirilmemelidir. Hakim, tek başına iken dahi, veri taşıyıcısındaki veriyi bilgisayarında inceleyebilmelidir. Bu faaliyet, keşif değil, delillerin değerlendirilmesi çerçevesinde ele alınmalıdır.

1.8. ELEKTRONİK İMZALI BELGELER HAKKINDA SAHTELİK İDDİASI

"Yargılamada ibraz edilen senedin sahteliğinin ileri sürülmesi Hukuk Usulü Muhakemeleri Kanununun 314. maddesinde düzenlenmiştir."[107] Buna göre "Resmi ve

[107] Mine Erturgut, Elektronik İmza Kanunu Bakımından E-belge ve E-imza, Bankacılar Dergisi, Sayı 48, 2003, s.77

gayrı resmi her nevi senedatın sahteliğini iddia eden kimse asıl davayı rüyet eden mahkemede bu iddiasını gerek davayı asliye ve gerek davayı hadise suretiyle ikame edebilir. Usulüne tevfikan icra kılınan tetkikat neticesinde senedin sahte olmadığına dair mahkemeden sadır olan karar kesbi katiyet ettikten sonra iş bu senet hakkında mahakimi cezaiyede dahi sahtelik iddiası mesmu olmaz."[108] "Bu hükme göre, ibraz edilen elektronik imzalı bir belgenin sahteliği ya aynı dava içinde ya da ayrı bir dava açılarak ileri sürülebilecektir. Bu bakımdan elektronik imzalı belgelerin kağıda dayalı adi senetlerden bir farkı bulunmamaktadır."[109]

Güvenli elektronik imza ile oluşturulmuş veriyi, imzaladığı iddia edilen taraf, imza inkarında bulunursa, Hukuk Usulü Muhakemeleri Kanununun 308. maddesi kıyas yoluyla uygulanacaktır. Bu maddenin kıyas yoluyla uygulanması için, yine öncelikle elektronik belgenin güvenli elektronik imza ile imzalanmış olup olmadığının tespiti gerekir. Zira güvenli elektronik imza dışında kalan imzalar bakımından, bu elektronik belgeler senet sayılmadığı için, imza incelemesine ilişkin Kanunun 308. maddesinin uygulanması mümkün olmayacaktır.

Kanunun 308. maddesine göre, "Davanın esnayı tahkikında bir taraf kendisine nispet olunan senette muharrer yazı ve imzayı inkar veya tanımadığını beyan ederse iki tarafın ifadatı ve olbapta serdolunan deliller üzerine hakim kafi derece kanaat hasıl eylediği takdirde senedi kabul veya hükümden ıskat ederek esas hakkında karar verir. Kanaat hasıl olmazsa hakim iki tarafın tayin olunacak günde bizzat ispati vücut etmelerine karar verir. Her iki taraf muayyen günde mütekabilen senet hakkında izahat ita ve medarı tatbik olacak evrakı irae ve tayin ve yazı ve imzanın mevsukiyetini ne şekilde ve ne vasıta ile ispat edebileceklerini beyan ederler."[110]

Kanunun 308. maddesinde, sahtelik iddiasının incelenmesi için izlenmesi gerekli bir sıra bulunmaktadır. Hakim ilk önce tarafların durumlarını ve davadaki açıklamalarını değerlendirerek senet hakkında bir karar verebilir. Bir kanaate varılamamışsa ikinci olarak hakim, tarafları belirlediği bir tarihte duruşmaya davet eder. "Duruşmaya davet, imzayı inkar eden taraf bakımından isticvab"[111] sonuçlarını doğurur. Bu sebeple imza inkarında

[108] HUMK, Madde 314.
[109] Mine Erturgut, Elektronik İmza Kanunu Bakımından E-belge ve E-imza, Bankacılar Dergisi, Sayı 48, 2003, s.78
[110] HUMK, Madde 308
[111] HUMK Madde 234

bulunan taraf, usulüne uygun şekilde çağırıldığı halde duruşmaya gelmezse isticvap konusu imzayı inkar etmiş sayılır. Taraflar çağrıldıkları duruşmaya geldikleri takdirde, senet hakkında açıklama yaparlar ve inkar edilen imza veya yazı hakkında imza karşılaştırılması yapılması için gerekli karşılaştırmaya elverişli imzayı mahkemeye sunarlar. Bundan başka, "taraflar senetteki yazı ve imzanın doğruluğunu nasıl ve hangi vasıtalarla ispat edileceğini açıklarlar."[112]

Adi senetlerde sahtelik incelemesi bakımından, 309. maddede, hakimin belirlediği duruşma gününde, hakimin imza karşılaştırması yapabilmek için imzayı inkar eden tarafa yazı yazdıracağı, yani tarafı istiktap edeceği düzenlenmiştir. Eğer ilk bakışta hakim imzanın o kişiye ait olduğunu tespit edebiliyorsa, imzanın inkar edene ait olduğuna karar verir. "Hakim imza karşılaştırması sonucunda kanaate varamazsa sonraki adımda bilirkişiye başvurur."[113] "Bilirkişinin inceleme yapacağı gün ve karşılaştırmaya elverişli yazılar hakim tarafından belirlenir."[114] Fakat karşılaştırmaya uygun yazılar konusunda mahkeme serbest değildir. Bu yazılar, "iki tarafın üzerinde uyuştukları her çeşit belge ve resmi senetler ile bir kimsenin memuriyeti sebebiyle imzaladığı veya mahkeme huzurunda yazıp imzaladığı belgeler olabilir."[115] Bilirkişi tarafından yapılacak imza incelemesi de kanunda belirtilen sıraya göre yapılır. Buna göre öncelikle mahkeme tarafından belirtilen karşılaştırmaya elverişli yazılar ile imza karşılaştırması yapılacaktır. Eğer "karşılaştırma, kanaate varma konusunda yeterli değilse, bu halde bilirkişi senedi inkar eden tarafa yazı yazdıracaktır."[116] Eğer bilirkişi vasıtasıyla da senetteki imzanın kişiye aidiyeti konusunda bir sonuca varılamamışsa son olarak senedin yazıldığını görenler veya kesin olarak bu konuda bilgisi olanlar tanık olarak dinlenir.

Güvenli elektronik imzalı belgeler bakımından, 308. maddenin uygulanması konusunda şunlar söylenebilir. Sahtelik incelemesinde yine kanundaki sıraya uyulması gerekecektir. Buna göre, öncelikle taraflar bu konuda dinlenecek ve ibraz edilen deliller incelenecek şayet bir kanaate varılamamışsa, hakim tarafından imzayı inkar eden tarafın isticvabı yoluna gidilecektir. Taraflar çağırıldıkları duruşmaya geldikleri takdirde, hakimin karşılaştırmaya elverişli diğer imzaları dikkate alarak elektronik belgeyi incelemesi, ancak bu konuda yeterli

[112] Mine Erturgut, Elektronik İmza Kanunu Bakımından E-belge ve E-imza, Bankacılar Dergisi, Sayı 48, 2003, s.78
[113]HUMK, Madde 309/I
[114]HUMK, Madde 309/II.
[115] HUMK,Madde 309/III
[116]HUMK, Madde.309/IV

teknik bilgiye ve mahkemenin gerekli araçlara sahip olmasıyla mümkündür. Elektronik olarak karşılaştırmaya elverişli imzalar, tarafın, nitelikli sertifika sayesinde kendisine özgülenmiş olan gizli anahtarla imzaladığı diğer elektronik belgeler olacağı akla gelebilir. Ancak, hemen belirtilmelidir ki, imza inkarında bulunan kişinin imzasının karşılaştırılmasının teknik olarak diğer elektronik belgelerle yapılması mümkün değildir. Çünkü her elektronik belgenin elektronik imzası birbirinden farklı olacaktır. Bu sebeple karşılaştırma yapılabilmesi, kişinin gizli imza anahtarı ile aynı içerikte bir belgeyi imzalaması sayesinde olabilir. Buna karşılık, inkar edilen elektronik belgede kullanılan en az bir karakterin değişik olması durumunda, belgenin içeriği aynı olsa bile teknik anlamda aynı olmayacağı için bu tür bir karşılaştırmayla da bir sonuca varılamaz. Bu sebeple imza karşılaştırması için en iyi yöntem, ibraz edilen ve imzası inkar edilen elektronik belgenin bizzat kendisinin imza kontrolünün yapılmasıdır. Bu şekilde imza kontrolü sonucunda çıkan belgenin değiştirilmediği veya değiştirildiğine ilişkin pozitif veya negatif sonuç, sahtelik konusunda kanaate varılmasına yardımcı olacaktır. Bu imza kontrolü gerekli araçların sağlanması durumunda hakim önünde de yapılabilir. İmza kontrolünde hem belgenin değiştirilip değiştirilmediğinin, hem de imzaladığı iddia edilen kişiden sadır olup olmadığının incelenmesi gerekir. Bu sebeple "hem imzanın kontrolü, hem de sertifikanın kontrolü gerekecektir. Bu konuda hakimin yeterli teknik bilgiye ve donanıma sahip olması beklenemeyeceğinden bilirkişiye başvurulması bir zorunluluktur. Bilirkişi, elektronik imzanın incelenmesinde tekniğin durumuna göre çeşitli saldırı ihtimallerini de değerlendirmelidir. Bu aşamada, 308. maddeye uygun olarak hakim tarafından belirlenen duruşma gününde yapılacak incelemede bilirkişinin bulunması da gereklilik olacaktır."[117]

1.9. E-İMZA İLE YAPILMAYACAK HUKUKİ İŞLEMLER

Kanun'un 5. Maddesinin 2. Fıkrası uyarınca "Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli e-imza ile

[117] Mine Erturgut, Elektronik İmza Kanunu Bakımından E-belge ve E-imza, Bankacılar Dergisi, Sayı 48, 2003, s.78

gerçekleştirilemez."[118] Güvenli e-imzanın uygulama alanın gösterildiği bu maddeye göre noterlerin yapacağı işlemler, noterlerin huzurunda yapılan işlemler, resmi bir makamın katılımını veya tescil zorunluluğu gerektiren işlemler (gayrimenkul, motorlu araç alım satımı v.b.) ile evlenme gibi resmi memur önünde gerçekleştirilmesi zorunlu olan hukuki işlemler güvenli e-imza ile yapılamazlar. Kanun metninde güvenli e-imza ile yapılamayacak hukuki işlemlerin genel bir ifadeyle tanımlanması bazı karışıklıklara sebebiyet verebilecektir. "Özellikle doktrinde tartışmalı olan "teminat sözleşmeleri" türleri ile "kanunun özel bir merasime tabi tuttuğu hukuku işlemler" uygulamada tereddüt yaratacak en önemli hususlardır."[119]

1.10. ELEKTRONİK BELGE

Elektronik belge denildiğinde, en basit ifadesiyle elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler bütünü kastedilmektedir. Bu anlamda karşımıza çıkan elektronik doküman, elektronik belge ve elektronik kayıt gibi kavramlar söz konusudur. Bu kavramlar genel anlamda birbiriyle aynıymış gibi görünse de aslında mesleki terim bakımından aynı şeyleri ifade etmez. Her ne kadar aynı manayı ifade etmese de elektronik ortamda oluşturulan bilgiyi ifade etmek üzere kullanılır. Belgenin sözlük anlamı "bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika doküman"[120]dır. Belge kavramı günümüze kadar, günlük hayatta kullanıldığı şekliyle çoğu zaman, kağıt üzerinde cisim bulmuş olma unsuruyla bağdaştırılmıştır. Çünkü bu şekliyle kâğıt üzerindeki belgelerin istenildiği anda ibraz edilmesi ve her an gözle algılanabilir şekilde bulunması özelliklerinin getirdiği faydalar ve avantajlar, kağıtta tecessüm etmiş belgelerin şimdiye kadar tercih edilmesini ve yaygın kullanımını sağlamıştır. Bu anlamda elektronik belge kavramı algılama yönünde ilk etapta insanlara ters gelen bir

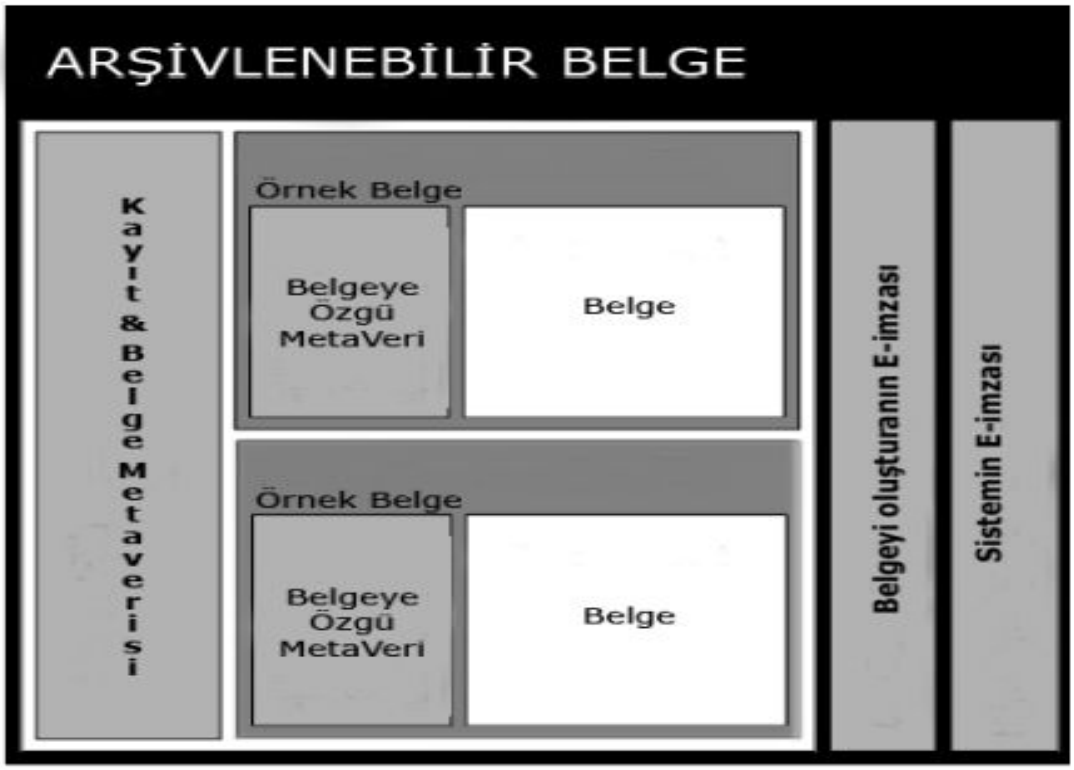
[118] 5070 Nolu Elektronik İmza Kanunu, Kabul Tarihi: 15.01.2004 http://www.tbmm.gov.tr/kanunlar/k5070.html Erişim Tarihi: 10.04.2011
[119] Fevki Beder, Elektronik Belge Yönetim Sistemi ve TCMB Örneği, Uzmanlık Yeterlilik Tezi, Ankara, Nisan 2005, s.35
[120] Türk Dil Kurumu Genel Türkçe Sözlüğü, "Belge", http://www.tdk.org.tr/sozluk, (23 Ağustos 2010)

kavram olabilir. "Belgelerin herhangi bir yardımcı araç olmaksızın görülebilmesi her zaman algılanabilir olduğu anlamındadır."[121]

Elektronik belge terimi, kâğıda dayalı belgeler karşısında bir sınırlamayı ifade eder ve bununla açıklamanın bulunduğu veri taşıyıcısın nitelemesi anlatılır. Sayfa üzerinde, işaretler ve harflerden oluşan bir yığın taşıyan kâğıt belgeler gibi, elektronik belgeler de çoğunlukla o zamanki işletme sistemi anlamında, bir ya da daha fazla veriler formunda, bilgi yığınını içerir. Kâğıt belgelerin aksine, elektronik belgelerde en önemli sorun, belgenin içeriğinin sonradan değiştirilip değiştirilmediğini hakkındaki kaygı ve endişelerdir. Türk Hukuk sistemi açısından da ilerleyen bölümlerde değineceğimiz bu konu Elektronik Belge Yönetim Sistemi Standartlarıyla aşılacak bir durumdur. Çünkü elektronik belge ve elektronik doküman kavramları birbirlerinden farklı kavramları işaret eder.

Elektronik belgede belirtilen sistem kriterleri, belge kriterleri ve üstveri kriterlerini incelendiğinde elektronik imzanın elektronik belgede fonksiyonel ve etkin bir role sahip olduğunu görülmektedir.

[121] Billur Yaltı, "E-imza ve E-Belge: Kâğıtsız ve mürekkepsiz Dünyada Hukuk-I", Vergi Sorunları Dergisi, Sayı.151, Nisan, 2001, s. 131.



Şekil 10- Standart uzun dönemli Elektronik Kayıt yapısı

Kaynak: Ross Gibbs, Justine Heazlewood (hzl.), Electronic Records – Problem Solved?: the Victorian Electronic Records Strategy and the future of electronic record keeping in Victoria, http://www.vala.org.au/vala2000/ 2000pdf/Gib_Hea.PDF, (30 Haziran 2008)

İKİNCİ BÖLÜM

ELEKTRONİK SİGORTACILIK VE ELEKTRONİK İMZA KAVRAMI

2.1.ELEKTRONİK TİCARET TANIMI

İlk çağlardan itibaren insanoğlu ticareti öğrenmiş ve günlük hayatın bir parçası olarak kullanmıştır. İhtiyaçların giderilmesi için, belirlenen nispi bir değer üzerinden mübadele (takas) yapılarak, eldeki mallarla diğer ihtiyaçların karşılanması yoluna gidilmiştir. "Karşılıklı olarak yapılan bu ticarette, insanların güvenini birbirlerini çok iyi tanımaları sağlıyordu. Bu kadar küçük ve güvenin yoğun olduğu bir ortamda ticaret yapmak elbette çok kolaydı."[122]

Ticaretin gelişmesine bakıldığında, akidlerin yani yazılı ve sözlü anlaşmaların çok önemli bir yere sahip olduğunu görüyoruz. Bu akidler sayesinde vade kavramı gelişmiş ve iki taraf arasında yapılan anlaşma ve sözüne ve dürüstlüğüne güvenilir bir tanık ile anlaşma yapılarak, ticaretin gelişmesi sağlanmıştı. Bu anlaşmalar uluslararası boyutlarda da kullanılmaya başlandı. Ve hala ticaretin en önemli araçlarından birisidir. "Günümüze gelindiği zaman ise, sermaye kuruluşları ve şirketlerin gelecek bir yıl içersinde yapması muhtemel sözleşme, anlaşma ve karlılık oranlarına bakarak yatırım yapılmakta buna karşın ilgili kuruluşların hisse senetleri alınmaktadır. Yani daha gelecekte olacak bir takım gelişmelere göre ticaret yapılmaktadır."[123]

Ticaretin gelişmesinde, insanlık olarak epey bir yol kastettiğimiz söylenebilir. Dijital çağ ile birlikte oluşan bilgi ekonomisi, emek yoğun bir sermayeden bilgi yoğun bir sermaye geçişe yardımcı olmuştur.

Elektronik ticaretin Haziran 1995'te Java'nın piyasaya sürülmesiyle başlayan bir başlangıç noktası bulunmaktadır. Elektronik ticaret (e-ticaret), "20. yüzyılın son döneminde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişmelere paralel bir şekilde ve

[122] Hüseyin Kuran, E-imza: Yeni Bir Çağın Başlangıcı, E-imza Paneli, Ankara 2004, s.2
[123] Hüseyin Kuran, a.g.e, s.3

giderek artan ölçüde dünya genelinde tartışılan bir kavram olarak karşımıza çıkmaya başlamıştır."[124]

Elektronik ticaret konusunda pek çok kaynakta farklı ülkelerin kuruluşları ile uluslararası veya uluslarüstü organizasyonlar tarafından yapılan birbirinden farklı tanımlara rastlanmaktadır. Bu tanımlardan bazıları şöyledir:

Dünya Ticaret Örgütü (DTÖ)'ne göre; "elektronik ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır."[125] İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından yapılan bir tanıma göre, "elektronik ticaret, genel olarak birey ve organizasyonların metin, ses ve görsel imajları kapsayan dijital verilerin aktarımına dayalı olarak ticari faaliyetleri yerine getirmeleridir."[126] "Birleşmiş Milletler Yönetim, Ticaret ve Ulaştırma İşlemleri Kolaylaştırma Merkezince (UN-CEFACT) yapılan bir diğer tanımlama ise, "iş, yönetim ve tüketim faaliyetlerinin yürütülmesi için yapılanmış ve yapılanmamış iş bilgilerinin, üreticiler, tüketiciler ve kamu kurumları ile diğer organizasyonlar arasında elektronik araçlar (elektronik posta ve mesajlar, elektronik bülten panoları, www teknolojisi, akıllı kartlar, elektronik fon transferi, elektronik veri değişimi vb.) üzerinden paylaşılması"dır.[127] Bu tanımlamaya göre elektronik ticaret kısaca, elektronik ortamda ticari iş, işlem ve fiillerde bulunmaktır.

Öte yandan Avrupa Komisyonu'nun 1997 yılında yapmış olduğu bir tanımlamaya göre, "elektronik ticaret, işletme faaliyetlerinin elektronik olarak yapılmasıdır. Bu faaliyetler metin, ses ve video verilerinin elektronik olarak işlenmesi ve aktarımına dayanmaktadır. Elektronik ticaret bu boyutuyla mal ve hizmet alım ve ödemelerinin sayısal olarak yapılmasını kapsamaktadır. Bu faaliyetler hem mamulleri (tüketici malları, spesifik ekipmanları) ve hizmetleri (bilgi hizmeti, finansal ve yasal hizmetler) ve hem de geleneksel faaliyetleri (sağlık, bakım ve eğitim) kapsamaktadır."[128]

Japonya Elektronik Ticaret Merkezi'nin (ECOM) 1996 yılında yapmış olduğu bir başka tanım ise, "Elektronik ticaret, her türlü bilgisayar ağları üzerinden, ürünün tasarımı,

[124] Ayşe İnalöz , Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Uzmanlık Tezi, Ankara 2003, http://www.tk.gov.tr/Yayin/Uzmanlik_Tezleri/tktezler/Ayse_Inaloz_Tez.pdf, Erişim tarihi:10.09.2010, s.61
[125] ASO (Ankara Sanayi Odası), Asomedya, Ankara 1998, s.29
[126] Bilgi Ekonomisinde Elektronik Ticaret, ITO Yayınları, İstanbul 1998, s.76
[127] Ekonomik Forum Dergisi, TOBB Yayınları, Ankara 2000, s.51
[128] Bilgi Ekonomisinde Elektronik Ticaret, ITO Yayınları, İstanbul 1998, s.51

üretilmesi ve tanıtımın yapılması ile ticari muameleler ve hesapların ödenmesi gibi tüm faaliyetlerin yerine getirilmesidir."[129]

Elektronik Ticaret Koordinasyon Kurulu (ETKK) Hukuk Çalışma Grubu'nun 8 Mayıs 1998 tarihli raporunda elektronik ticaret; Bireyler ve kurumların, açık ağ ortamında (internet) ya da sınırlı sayıda kullanıcı tarafından ulaşılabilen kapalı ağ ortamlarında (İntranet) yazı, ses ve görüntü şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması temeline dayanan ve bir değer yaratmayı amaçlayan ticari işlemlerin tümünü ifade etmektedir. Bu çerçevede, ticari sonuçlar doğuran ya da ticari faaliyetleri destekleyecek eğitim, kamuoyunu bilgilendirme, tanıtım-reklam vb. amaçlar için elektronik ortamlarda yapılan işlemler de e-ticaret kapsamında değerlendirilmektedir.

E-ticaret temel olarak iki tip faaliyeti kapsamaktadır "dolaylı e-ticaret" gerçek malların elektronik siparişi, posta hizmetleri veya ticari taşıyıcı kullanarak geleneksel kanallar üzerinden fiziksel olarak teslim edilmesi gerekenler. "Doğrudan e-ticaret" bilgisayar yazılımları, eğlence içerikleri veya küresel ölçekte bilgi hizmetleri gibi fiziksel varlığı olmayan malların hizmetlerin on-line sipariş, ödeme ve teslimini içermektedir.

"Kapalı ve açık ağlar kullanılarak yapılabilecek iş ve ticaret aktiviteleri şu şekilde sıralanabilir:"[130]

- Mal ve hizmetlerin elektronik alışverişi,
- Üretim planlaması yapma ve üretim zinciri oluşturma,
- Tanıtım, reklam ve bilgilendirme,
- Sipariş verme,
- Anlaşma/sözleşme yapma,
- Elektronik banka işlemleri ve fon transferi,
- Gümrükleme,
- Elektronik ortamda üretim izleme,

[129] ASO (Ankara Sanayi Odası), Asomedya, Ankara 1998, s.29
[130] S. Çengel, Elektronik Ticaret, Endüstri Mühendisliği Bölümü, Mühendislik Fakültesi, Kocaeli Üniversitesi, Kocaeli 2002

- Elektronik ortamda sevkiyat izleme,
- Ortak tasarım geliştirme ve mühendislik,
- Elektronik ortamda kamu alımları,
- Elektronik para ile ilgili işlemler,
- Elektronik hisse alışverişi ve borsa,
- Ticari kayıtların tutulması ve izlenmesi,
- Doğrudan tüketiciye pazarlama,
- Sayısal imza, elektronik noter gibi güvenilir üçüncü taraf işlemleri,
- Sayısal içeriğin anında dağıtımı,
- Anında bilgi oluşturma ve aktarma,
- Elektronik ortamda vergilendirme,
- Fikri, sınai ve ticari mülkiyet haklarının korunması ve transferi.

"Ticari hayatımızda karşılaşılabilecek tarafların hemen hepsi bu sistem içinde de yer almaktadır. Bunlar;"[131]

- Alıcılar
- Satıcılar
- Ortaklar
- Üreticiler
- Aracılar
- Bankalar
- Banka dışı finansal kurumlar

[131] Cihan Kartal, İnternet Ortamında Pazarlama, Gazi Kitabevi, Ankara 2002, s.25

- Komisyoncular
- Sigorta şirketleri,
- Nakliye şirketleri,
- Vergi, fon vs. ilişkisinin olduğu resmi kurumlar
- Ticari birlikler
- Sistemin çalışmasını sağlayan bilgi işlem kuruluşları vs.dir.

Alternatif Ticaret Sistemlerinin (ATS – Alternative Trading Systems) ve Elektronik İletişim Ağlarının (ECN) hızlı bir şekilde büyümesi, teknoloji evriminin ve yatırım toplumunun arada borsa komisyoncusu (broker) olmadan olumlu ve düzenli bir şekilde yatırım yapma istekliliğinin giderek artmasının bir sonucu olarak gösterilebilir. "Bu hızlı büyüme sayesinde elektronik ticaretteki fiyat verimliliği ve ulaşılabilirlik; özellikle tezgah-üstü takas olmak üzere alışılagelmiş ticaret metodolojilerinin açık bir şekilde güçsüz kaldığını göstermektedir."[132]

[132] Günay Faruk Özer, Sermaye Piyasalarında Elektronik İmzanın Kullanım Alanları, e-Türkiye Sempozyumu, Ankara 2004, s.3

Tablo 1.1: E-Ticaretin Geleneksel ve Yeni Araçları

GELENEKSEL ARAÇLAR	YENİ ARAÇLAR
Televizyon	World Wide Web (WWW)
Radyo Telefon	Dosya Aktarma Protokolü (FTP) Elektronik Posta
Faks	Sözlü Mesaj (Voice Mail)
Elektronik Ödeme ve Para Sistemleri - Bankamatik (ATM) - Kredi Kartları - Satış Noktası (POS) makineleri	Konferans Sistemleri - Telekonferans - Data Konferans - Video Konferans
İntranet: Kapalı Bilgisayar Ağları - EFT - EDI	Mobil İletişim İçin Küresel Sistem Teknolojisi : GSM Kısa Mesaj Servisi : SMS Telsiz Uygulama Programı Protokolü (Wireless Application Protocol) : WAP

Kaynak: Gazenfer Erbaşlar ve Şükrü Dokur, Elektronik Ticaret, Ankara, Nobel Yayınları, 2008, s.9

21.yüzyılda, internet sayesinde rekabetçi avantaj kazanmak için reçete olabilecek "tek bir en iyi strateji" bulunmamaktadır. Her işletme kendine özgü şartları değerlendirerek elektronik ticaret konusunda, hem kendisine hem de müşterilerine değer katacak olan gerekli altyapıyı hazırlamalıdır. Bu altyapıyı hazırladıktan sonra, gerekli iyileştirmeleri sürekli olarak gerçekleştirmeye yönelik stratejiler, sürdürülebilir rekabetçi avantajı kazanmanın en iyi yolu olacaktır.

Bazı yönetim kuramcılar "Bir şirketin küresel olması için yalnızca uluslararası iş yapması değil; aynı zamanda kaynaklarını dünyanın en büyük rekabet avantajı sunacak herhangi bir yerine taşımasına izin verecek bir şirket kültürüne ve değerler sistemine sahip olması gerekir" derken, küresel olmanın sadece ihracat yapmak, yabancı teknoloji kullanmak, lisans vermek, iş gücü veya malzeme almak değil bunun ötesinde mevcut organizasyonların becerilerini ve düşünce yapılarını da geliştirmeleri gerektiğini ileri

sürmüşlerdir. Tüm bunları becerebilen organizasyonlar yaşanan bilimsel ve teknolojik patlama ile üretim organizasyonunu, dağıtımını dolayısıyla ekonomik alanları ve gelir kaynaklarını etkileyen yeni teknolojiler dönemine geçiş yapmaktadır.

E-ticaret, özü itibariyle ekonomik bir olgu gibi algılansa da sosyal ve kültürel alanlarda da etkiler oluşturmaktadır. "E-ticaretin; birey, firmalar ve toplum üzerinde farklı etkiler oluşturduğu görülmektedir. Müşteri beklentilerinin pazarı yeniden tanımladığı veya yeni pazarlar oluşturduğu koşullara E-ticareti benimseyen firmalar, daha hızlı uyum sağlamakta ve rekabet konusunda avantaj elde etmektedir. Bireylere ise alışveriş, bilgi ve hizmetlere erişim, kamu ile etkileşim konularında fiziki uzaklık ve zaman kısıtlarını ortadan kaldıran yeni yollar sunulmaktadır."[133]

E-ticaret kuşkusuz yenidir, ancak geçerli olan esaslar ve ilkeler bakımından geleneksel ticari yöntemlerle benzerlikler içermekte, zaman zaman aynı yöntemleri kullanmaktadır. "Dolayısıyla e-ticaret, her anlamda yeni ve geleneksel ticarete alternatif bir ticari usuller seti değil, iletişim ve bilgi işleme teknolojilerinin gelişimine paralel olarak ortaya çıkan ve ticareti kolaylaştıran bir yeniliktir."[134]

Türkiye'de, özellikle 1999 yılından itibaren internet kullanıcılarında yaşanan artış, Türkiye'deki işletmeleri de internet ortamına girmeye zorlamıştır. Bu sayede işletmeler müşterilerine veya satıcılarına ulaşabilmek için internet kullanarak e-ticaret yapmışlardır. "Türkiye'de bankacılık sektörü e-ticaretin gelişiminde sürükleyici bir faktör olmuştur."[135]

[133] Yücel Özkan, Elektronik Ticaret Yazılım Firmalarında Pazarlama Ve Elektronik Ticaret Uygulamaları, Endüstri Mühendisliği Bölümü, Mühendislik Fakültesi, Kocaeli Üniversitesi 2003, s.83
[134] Murat İnce, Elektronik Ticaret: Gelişmekte Olan Ülkeler İçin İmkanlar ve Politikalar, DPT, www.dpt.gov.tr , Ankara 1999
[135] Gökçen, Ferhat, "İnternet Ve Elektronik Ticaret (E-Ticaret) Üzerine", http:// www.muhasebetr.com/e_İmza, Erişim Tarihi, 10.04.2011

	Geleneksel Ticaret	Elektronik Ticaret
Satın Almayı Yapan Firma		
Bilgi Edinme Yöntemleri	Görüşmeler, dergiler, kataloglar, reklamlar	Web sayfaları
Talep Belirtme Yöntemi	Yazılı form	Elektronik posta
Talep Onayı	Yazılı form	Elektronik posta
Fiyat Araştırması	Kataloglar, görüşmeler	Web sayfaları
Sipariş Verme	Yazılı form, fax	Elektronik posta, EDI
Tedarikçi Firma		
Stok Kontrolü	Yazılı form, fax, telefon	Online Veritabanı, EDI
Sevkiyat Hazırlığı	Yazılı form, fax, telefon	Elektronik Veritabanı, EDI
İrsaliye Kesimi	Yazılı form	Online Veritabanı, EDI
Fatura Kesimi	Yazılı form	Elektronik Posta, EDI
Siparişi Yapan Firma		
Teslimat Onayı	Yazılı form	Elektronik Posta, EDI
Ödeme Programı	Yazılı form	Online Veritabanı, EDI
Ödeme	Banka Havalesi, Posta, Tahsildar	İnternet bankacılığı, EDI, EFT

Geleneksel Ticaret- Elektronik Ticaret Karşılaştırılması

2.2. SİGORTA TANIMI VE KAPSAMI

Kişilerin bazı koşullar altında karşılaşacakları, zarar ve masrafa sebep olan "olayların ekonomik sonuçlarından kendini korumak için önceden tedbir alma ihtiyacından doğan"[136] sigorta kavramı elektronik imza sistemine de yabancı olmaması gerekir. Sigortanın amacı, rastlantıların zararlı sonuçlarını önceden alınacak tedbirlerle ortadan kaldırmaktadır. Bu da "sigortalı"nın zararını "sigortalılar topluluğu"na "dağıtmak suretiyle olur."[137] Keza toplum içinde doğan zararların yine "toplum içinde dağıtılması

[136] Rayegan Kender, Türkiye'de Hususi Sigorta Hukuku, Sigorta Müessesesi-Sigorta Sözleşmesi, Arıkan Basım Yayım, Gözden Geçirilmiş 8. Bası, İstanbul 2005, s.1
[137] Serhat Sayın, Türk Hukukunda Kredi Kartı ve Kredi Kartının Hukuka Aykırı Kullanılmasından Doğan Hukuki Sorumluluk, Kazancı Hukuk Yayımevi, 1. Baskı, İstanbul 2005, s.90

(mutuality) esasına dayanan"[138] sigorta hukuki bir kurum olup, sigorta kurumunun sağlayacağı koruma ya kanunla yada sözleşmeyle gerçekleşir.

Riziko kavramı sigorta hukukunda merkezi bir öneme sahip olmakla birlikte TTK'da tanımlanmamış, fakat sigorta sözleşmesinin esaslı unsurları arasında sayılmıştır. Teknik anlamda riziko, sigorta sözleşmesinin taraflarının münhasır iradeleri dışında kalan, gerçekleşip gerçekleşmeyeceği veya ne zaman gerçekleşeceği belirsiz olan, bir zarar veya başkaca uygun olmayan bir hal doğuran, geleceğe ait ihtimalî bir olaydır. Riziko soyut anlamda "tehlike" demektir. Rizikonun gerçekleşmesi halinde ortaya somut anlamda bir "tehlikeli olay" çıkmakta, bu tehlikeli olayın -ortaya çıkan- zararlı sonucuna da "hasar" adı verilmektedir. Bütün sigorta branşları için, "tehlikeli olay" sigorta bedelinin, "hasar" ise "sigorta tazminatının ödenmesinin bir ön şartıdır.[139] Sigortacı, sigorta sözleşmesini yapmadan önce üstleneceği rizikoyu değerlendirecek, "sözleşmeyi yapıp yapmamaya ve yapacaksa sigorta priminin ne kadar olacağına karar verecektir."[140]

Sigorta sözleşmesi ise, belirlenmiş bir bedel karşılığında, "bir tarafın (sigortacı) diğerinin belirli bir risk nedeniyle belirli bir menfaatinin uğrayacağı zararını gidermeyi taahhüt ettiği bir sözleşmedir."[141] Sigorta sözleşmeleri çeşitli yönlerden sınıflandırılabilmektedir. İhtiyacın karşılanması kıstasına göre yapılan sınıflandırmada, zarar ve meblağ sigortaları; "rizikonun konusuna göre yapılan sınıflandırmada ise malvarlığı ve şahıs sigortaları şeklinde yapılmaktadır."[142]

"Zarar sigortalarında para ile ölçülebilen menfaatlar sigorta altına alınmaktadır."[143] Zarar sigortaları, aktif ve pasif sigortaları şeklinde sınıflandırılmaktadır. "Aktif sigorta; belirli bir değer ile belirli bir şahıs arasındaki münasebet sigorta hukukunda menfaat kavramını teşkil etmektedir. Pasif sigortada ise, sigorta ettirenin malvarlığında bazı pasiflerin ortaya çıkması veya mevcut pasifin artması suretiyle uğrayacağı zararları ödemektedir."[144] Örneğin, sigorta ettiren kanun tarafından veya taraf olduğu bir akitle kendisine yüklenmiş

---

[138] Merih Kemal Omağ, Türk Sigorta Hukukunda Rizikonun Ağırlaşması Sorunu, Sigorta Hukuku Türk Derneği 1985, s.3

[139] Merih Kemal Omağ, Riziko, Türk hukukunda Sigortacının Kanuni Halefiyeti, Türkiye Sigorta ve Reasürans Şirketleri Birliği Yayını, İstanbul 1983, s.23 dipnot (2)

[140] Omağ, a.g.e, s.4.

[141] Huriye Kubilay, Uygulamalı Özel Sigorta Hukuku, Barış Yayınları, 2. Baskı, İzmir 2003, s.3

[142] Rayegan Kender, Türkiye'de Hususi Sigorta Hukuku, Sigorta Müessesesi-Sigorta Sözleşmesi, Arıkan Basım Yayım, Gözden Geçirilmiş 8. Bası, İstanbul 2005, s.140

[143] Işıl Ulaş, Uygulamalı Can Sigortası Hukuku, Turhan Kitabevi, Ankara 2002, s.10

[144] Rayegan Kender, Türkiye'de Hususi Sigorta Hukuku, Sigorta Müessesesi-Sigorta Sözleşmesi, Arıkan Basım Yayım, Gözden Geçirilmiş 8. Bası, İstanbul 2005, s.141

bulunan bir takım borçlar sebebiyle zarara uğrayabilir, bazı masraflar yapmak zorunda kalabilir. Burada rizikonun gerçekleşmesi halinde belli bir değer ile olan ilişkinin ihlali söz konusu olmadığından teknik anlamda bir menfaat yoktur. Menfaat olmadığı için sigorta değeri de yoktur. "Pasif sigortasının çeşitleri; -Kanuni borçlara karşı sigorta (mali mesuliyet sigortası), -Akdi borçlara karşı sigorta ve Zorunlu masraflara karşı sigortadır."[145]

Sorumluluk sigortası, bir şahsın ödeyeceği prim karşılığında, kendisinin tazmin etmekle yükümlü olacağı zararları güvence altına almasını sağlayan bir sigorta türüdür. Böylece sigorta ettiren, başkasının vereceği bir zararın tazmin edilmesi nedeniyle malvarlığında ortaya çıkacak eksilmeye karşı kendisine güvence sağlamış olmaktadır. "Sigorta edilen risk gerçekleştiğinde, zarar, sorumlu kişi tarafından değil, sigorta tarafından karşılanmaktadır."[146]

Yirminci yüzyılın ikinci yarısında yaşanan teknolojik devrim sorumluluk hukukunda yeni gelişmelerin ortaya çıkmasına neden olmuştur. Sorumluluk hukuk alanında tehlike sorumluluğu ilkesinin uygulama alanının gelişmesi: yeni tehlike sorumluluğu hallerinin kabul edilmesi ve modern sorumluluk hukukun zararı giderme veya denkleştirme hukuku niteliğini kazanması teknolojik devrimin belirgin suçlarıdır. "Teknolojik gelişmeler, kazaların artmasına ve dolayısıyla sigortanın gelişmesine yol açmıştır. Sorumuluk sigortası giderek önem kazanmaya başlamış, önce özel sigorta niteliğinde sonraları daha çok zorunlu sigorta niteliğinde yapılagelmiştir."[147]

"Sigorta şirketlerinin sigortacılık faaliyetlerini gerçekleştirmek için birtakım aracılara ihtiyaçları vardır."[148] "Sigorta işlemlerinin tümünün sadece sigorta şirketleri tarafından yapılması mümkün olmadığından sigorta şirketleri sigorta sözleşmelerinin kurulması aşamasını aracıları vasıtasıyla gerçekleştirirler."[149] Sigorta aracılarının en önemli fonksiyonları, müşterilerine danışmanlık hizmeti vererek onları ürünler hakkında bilgilendirmek, primlerin toplanması ve tazminatların ödenmesi konusunda hem sigorta şirketine hem sigortalıya yardımcı olmaktır. Sigorta aracıları, sigorta şirketlerinin en

[145] Rayegan Kender, Türkiye' de Hususi Sigorta Hukuku, 1.Baskı, İstanbul: Arıkan Yayınları, 2005, s.92.
[146] Huriye Kubilay, Uygulamalı Özel Sigorta Hukuku, Barış Yayınları, 2. Baskı, İzmir 2003, s. 112
[147] Huriye Kubilay, a.g.e, s.111
[148] Rayegan Kender, a.g.e, s.143.
[149] Tekin Memiş, "Avrupa Birliği ve Türk Hukukunda Sigorta Aracıları", Reasürör Dergisi, Sayı: 34, 1999, s.7.

önemli ayağı olarak düşünülmelidir. Sigorta aracıları, sigorta acenteleri ile sigorta brokerleri / prodüktörlerinden oluşmaktadır.

2.3.ELEKTRONİK SİGORTACILIK HAKKINDA GENEL BİLGİLER

2.3.1 Gelişme Süreci

1990'lı yıllar sigortacılıkta liberalizme geçiş yılları olarak tanımlanabilmektedir. Bu dönemde yaşanan en mühim gelişme, sigorta sektöründeki "serbest tarife" uygulamaları olarak özetlenebilir. Bu yıllar öncesinde sigorta şirketleri, hazırladıkları tarifeleri, önce ilgili otoritelere onaylattıktan sonra yürürlüğe sokabilmektedirler. Bu dönemde piyasada birbirini benzer tarife ve çeşitlerde sigorta ürünleri mevcut olmuştur. Liberal dönem öncesi kurumsal müşteriler üzerinde yoğunlaşarak büyüme stratejilerini geliştiren sigorta şirketleri, zaman içinde bu stratejilerini bireysel sigortalar üzerine kaydırmışlar ve bu alanda önemli atılımlar yapmışlardır.

Sigorta şirketleri faaliyet gösterdikleri sigorta dallarında tarifelerini kendi portföylerinin büyüklüğüne, dağılımına ve teknik sonuçlarına göre kendileri hazırlamaya başlamışlardır. Buna neden olarak, kurumsal müşteri portföyünün yeterli doyuma ulaşması ve sektörde yaşanan yoğun rekabet gösterilebilir. Ancak "hala deprem, grev-lokavt, kötü niyet ve terör rizikolarında, riziko primini gösteren zorunlu tarifeler uygulanmaktadır."[150]

Kurumsal müşterilerle yapılan işler, daha küçük yatırımla, daha az fakat nitelikli insan kaynağıyla, daha az işlem maliyeti ile, az sayıdaki fakat büyük iş hacimli işletmeler ile iş yapılması prensiplerine dayanmaktadır. Oysa bireysel müşterilere yönelik organizasyonlar daha büyük yatırımlar, daha büyük bilişim teknolojisi, daha çok personel ve daha yüksek işlem maliyetleri gerektirmektedir. Bireysel sigortacılığın en büyük dezavantajı, pazarın derinliği, dinamizmi ve kurumsal pazara göre daha kararlı (stabil) olmasıdır. Rekabet

[150] Temel Sigortacılık Bilgileri, İş bankası Yayınları, İstanbul 2006. s.18

nedeniyle sektörde fiyatlar oldukça düşmüştür. "Bu konuda dünyada büyüyen reasürans kapasitesinin bu durumu destekleyici etkisini de göz ardı etmemek gerekir."[151]

1995 yılında başlayan kasko sigortasındaki önemli fiyat indirimleri, şirketler için önemli sorunlar yaratmaya başlamıştır. Bu dönemde dünyada uygulaması hiç görülmemiş hasarsızlık indirimi, hasarlılık ek primi uygulaması ve diğer yandan ülkede satın alma gücüne oranla artan otomobil sayısındaki ve yedek parça fiyatlarındaki artışlar, sigorta şirketlerinde teknik karlılıkları tehlikeye sokmuştur.

Günümüzde artan rekabet koşulları, fiyatların daha da aşağılara çekilmesine neden olabilecektir. Bu durumda sermaye yapılan güçlü olmayan şirketlerin iflasları ile karşılaşılması mümkündür. Rekabetin daralttığı kar marjlarının genişletebilmesinin bir diğer yolu, giderlerin aşağıya çekilmesidir. Bu amaçla şirket birleşmeleri ya da satışları söz konusu olabilecektir. Bu konunun tüm dünyada yaşanan örnekleri mevcuttur. Ölçek ekonomisinden yararlanarak maliyetlerin, prim gelirlerine oranla düşürülmesi imkanı yakalanmış olacaktır. Yoğun rekabet dönemini sermaye yapısı güçlü büyük şirketlerin sağlıklı bir şekilde geçireceğini, küçük ve orta ölçekli sigorta şirketlerinde ise birleşmelerin ve satışların söz konusu olacağını beklemek hiç de hatalı bir düşünce sayılmamalıdır.

Serbest tarife sisteminin uygulanması ile yukarıda belirtilen kaygıların daha da ötesinde, ürün maliyeti ve bazı branşlarda sigortalının maliyeti daha büyük önem arz etmeye başlamıştır. Serbest tarife sistemi sonucunda ülkemizde fiyatların oldukça düşmesi sonucunda, Hazine ve Dış Ticaret Müsteşarlığı bu duruma müdahale ederek bir minimum tarife zorunluluğu ortaya koymuştur. "Bu sürece müdahale edilmemiş olsaydı, birçok şirketin zararları yüzünden sorunlarla karşılaşacağı da bir gerçektir."[152]

Görülmektedir ki şirketlerin karlılık anlayışları son 20 yıl içerisinde bir yapı değişmesine maruz kalmıştır. "Eskiden belki de zorunlu tarife rejimi nedeniyle teknik karlar ile ayakta durabilen sigorta sektörü, oransal olarak bakıldığında günümüzde sanıldığının aksine, teknik karlılıklarını arttırmadan mali gelirlerini arttırarak faaliyetlerini devam ettirme yolunu seçmişlerdir."[153] Bunun anlamı, ülkemizde sigorta şirketlerinin daha çok sigortacılık

[151] Ali Tümer Akyüz, Rekabet Nereye Kadar? Milliyet Sigorta Sektörü Eki, 5 Haziran 1997, s.10
[152] Enver Yalçınkaya, 3.İzmir İktisat Kongresi, 4-7 Haziran 1992, s.123
[153] Melih Alkgüney, Sigorta Şirketlerinde Maliyet Unsuruları ve Masraf Dağıtımı, 25.02.1997, Türk Sigorta Enstitüsü Konferansı, s.1-2

faaliyeti dışında, yatırım gelirlerinden elde ettikleri mali karlar ile ayakta kalabildikleridir ve bu durum gelecek dönemler açısından umut vermemektedir.

Sigorta sektörü 1995 sonrası dönemde bilgisayar teknolojilerinde yaşanan gelişmelere paralel olarak önemli bir değişim geçirmeye başlamıştır. Özellikle bireysel sigorta müşterilerini hedefleyen pazarlama stratejilerinin uygulanmasında stratejik öneme sahip olan "internet üzerinden sigorta pazarlaması" hayata geçmiştir. Birçok sigorta şirketi teknik altyapılarını bu dönemde oluşturarak, sigorta hizmetlerini internet üzerinden sunmaya başlamıştır. İnternet uygulamalarının sigortacılık dünyasına girişi ve yaygınlaşması oldukça yenidir. Bu dönem Türk sigortacılığında "İnternet Sigortacılığı" olarak anılacak bir dönemin başlangıcı niteliğindedir.

Türk Sigorta Sektöründe özellikle 1990'lı yıllar sonrasında yaşanan liberalleşme eğilimleri, sektördeki faaliyet gösteren sigorta şirketlerinin sayısını 25'lerden 69'lara kadar çıkarmıştır.

E-sigortacılık, bir sigorta poliçesinin pazarlanması sürecinde, sigorta şirketlerinde geçtiği aşamalardan en az birinin elektronik ortamda yapılmasıdır. Günümüzde gelişmekte olan ülkelerde e-sigortacılığa geçiş çok yenidir. Ülkemizde tüm sigorta şirketleri e-sigortacılık uygulamasını kullanmaktadır. Bunlara en genel örnek sigorta poliçelerinin tahsilâtlarının kredi kartıyla yapılmasıdır. On-line sigortacılık uygulaması ise, tüm bu aşamaların internet ortamında yapılmasıdır. Bu uygulama da ülkemizde henüz çok yenidir. On-line sigortacılık bir tür e-sigortacılıktır, e-sigortacılık daha geniş kapsamlıdır ve on-line sigortacılığı da kapsar.

"Sigortacılık sektöründe e-ticaret uygulamaları deyince akla sadece sigorta poliçelerinin internet üzerinden satışı gelmemelidir. E-sigortacılık araştırma ve seçim aşamaları gibi satın alma sürecini etkileyen birçok ara aşamaları kapsayan geniş bir uygulama alanı olarak düşünülmelidir."[154]

[154] Selim Yazıcı ve Serhat Yanık, Elektronik Sigortacılık: Elektronik Ticaretin Sigorta Sektörüne Etkileri, Der Yayınları, İstanbul 2002, s.5

2.3.2. Kapsamı ve Araçları

Bir sigorta poliçesini satın alma süreci, araştırma ile başlamaktadır. Sigorta yaptırmak isteyen kişi istediği ürün, fiyat ve hizmete yönelik bir araştırma yaptıktan sonra almak istediği ürünü ve hizmeti sunan şirket veya şirketlerden teklif isteyebilmektedir. En uygun teklife karar verilerek ödeme yapılmaktadır. Oluşturulan sigorta poliçesi, internet ortamında sigortalıya e-posta yoluyla gönderilmektedir. Böylece sigortalı kendi yazıcısından istediği zaman poliçesini yazdırabilme imkânına sahip olmaktadır. Sigorta poliçesi oluştuktan sonra her türlü teknik destek verilmektedir. Günümüzde, bu işlemlerin tümü internet ortamında gerçekleştirilebilmektedir. Sigorta ürünlerinin doğrudan pazarlanmasında ve tanıtımında kullanılan araçlar televizyon, telefon, faks, bilgisayar, internet, EDI, e-posta ve GSM'dir.

Televizyon: Tek yönlü bir iletişim aracı olduğundan, sigorta şirketleri tarafından reklam, tanıtım ve pazarlama amacıyla kullanılmaktadır.

Telefon: Sigortacılığın en eski araçlarındandır. Telefon sigortacılığı ile üretimde, sigorta poliçesi geleneksel olarak düzenlenerek sigortalıya ulaştırılmaktadır. "Ödeme kredi kartıyla yapılabilmektedir."[155] Telefon ayrıca sigortalıya teknik destek sağlaması açısından önemlidir.

Faks: Tüm sektörlerde olduğu gibi sigorta sektöründe de evrak gönderimi ve bilgi akışını sağlayan bir araçtır. Sigorta teklifleri ve poliçeleri faks yoluyla sigortalıya ulaştırılabildiği gibi, hasar anında hasar dosyasıyla ilgili birtakım evrakın sigorta şirketine iletimi faks ile gerçekleştirilebilmektedir.

Bilgisayar ve Internet: Verilerin kayıt altına alınması açısından bilgisayar sektörde oldukça önemli bir yere sahiptir. İnternet vasıtasıyla, sigorta şirketleri ile acenteleri arasında elektronik ortamda veri akışı sağlanarak, sigorta poliçesi düzenlenebilmektedir.

Sigorta satışında internet kullanımının sağladığı maliyet avantajları şunlardır:

[155] Şebnem URALCAN, Temel Sigorta Bilgileri ve Sigorta Sektörünün Yapısal Analizi, 2.Basım, Bilyay Yayınları, İstanbul 2006, s.208

- Geleneksel ürün fiyatlarında, internet uygulamalarının sağladığı maliyet azaltıcı etkiler nedeniyle önemli ölçüde düşüşler yaşanmaktadır.

- İnternet kullanımı sayesinde sigorta şirketlerinin online satış yapmaları ile acenteler üzerinden yaptıkları satışlar karşılaştırıldığında, internet üzerinden yapılan satışlarla %23′lük bir maliyet avantajı sağlanmaktadır.

- İnternet üzerinden satış ve hizmet sunan sigorta şirketleri, bir müşterinin ömrü boyunca %58 ile %78 arasında değişen bir oranda klasik sigorta şirketlerine göre maliyet avantajına sahip olmaktadır.

EDI: Sigorta şirketleri ve aracıları, veri alışverişini sağlamak için EDI kullanabilmektedir. Acente tarafından kayıt edilen, müşterilere ve sigorta poliçelerine ait her türlü bilgi sigorta şirketine elektronik olarak ulaştırılmaktadır. EDI, özel donanım gerektirdiği ve daha pahalı olduğu için aynı görevi gören Genişletilebilir İşaretleme Dili (XML) tercih edilmeye başlamıştır.

E-Posta: E-posta üretimi ile on-line sigortacılık birbirinden farklıdır. On-line sigortacılıkta sigortalı, sigortasını internet üzerinden yaptıktan sonra ödemesini de on-line yapmaktadır. E-postada ise, müşteri internetten teklifi doldurarak sigorta şirketine göndermektedir. Sigorta şirketi böylece sigortalı adayıyla iletişime geçmekte, anlaşma olduğu takdirde sigorta poliçesini geleneksel usulle düzenleyerek kendisine göndermektedir.

GSM: Daha çok sigorta şirketlerinin müşteriyi bilgilendirmek için kullandıkları bir araçtır. Aynı zamanda kişi, WAP teknolojisiyle internete bağlanarak on-line sigorta poliçesi oluşturabilmekte, poliçesi hakkında bilgi edinebilmekte, hasar dosyasını takip edebilmekte ve teknik destek alabilmektedir. Ancak WAP teknolojisiyle internete bağlanmak oldukça pahalı olduğu için pek tercih edilen bir yöntem değildir. Gelecekte ise, bilgisayarların yerini alacağı yadsınamaz bir gerçektir.

2.3.3. Türleri

Elektronik Sigortacılık'ın iki türü yaygın biçimde kullanılmaktadır:

Şirketler Arası E-Sigorta (B2B - Business to Business): Bu uygulamada, sigorta şirketleri kendi web siteleri üzerinden direkt satış yapmaktansa, aracıları vasıtasıyla on-line sigortacılık yapmaktadırlar. Sigorta şirketleri daha çok bu uygulamayı kullanmaktadırlar. "B2B uygulamalarında acenteler için sigortacılık satış süreçlerini içeren tüm modüller sisteme entegre edilmektedir. Türkiye'de B2B kullanımı açısından web servisi sağlayan şirketlere örnek olarak Axa Sigorta, Ergo İsviçre Sigorta, HDI Sigorta, Ak Sigorta'yı verebiliriz."[156]

Şirket – Tüketici Arası E-Sigorta (B2C): Son yıllardaki web ve wap teknolojilerindeki gelişmelerle ortaya çıkmış yeni bir türdür. Elektronik sigortacılığın en çok bilinen türüdür. Bu yöntemde müşterilere direkt olarak internetten on-line sigorta teklifi veya poliçesi oluşturabilme imkânı sunulmaktadır. Türkiye'de B2C uygulamasını kullanan sigorta şirketlerine örnek olarak Ray Sigorta, Işık Sigorta ve Güven Sigorta'yı sayılabilir. "B2B ve B2C'nin avantajlarını şu şekilde sıralanabilir:"[157]

B2B'nin avantajları: Zaman ve mekân sıkıntısı yaşamadan sigorta şirketleri ve acenteler birbirine kolayca ulaşabilmektedir. Standart ve sık tekrarlanan işlemler elektronik ortamda otomatik hale getirilerek firmalar için zamandan kazanç sağlanmaktadır. Yapılan işlemlerle ilgili takip kolaydır, raporlar kolay hazırlanmaktadır.

B2C'nin avantajları: B2C ile sigorta şirketleri veya acenteler çok büyük bir kitleye satış yapabilmektedir. B2C yapan sigorta şirketleri veya acenteler, müşteriye istediği ortamda ulaşabildiği için rakiplerine oranla daha çok tercih edilmektedirler. Müşterilere ait bilgiler toplanarak bireysel hizmet sunulabilmektedir.

Sigorta şirketlerinden çok sigorta aracılarının kullandığı bu uygulamada, aracılar müşterilerine direkt olarak internetten on-line sigorta teklifi veya poliçesi oluşturabilme imkânı sunmaktadırlar. Acentelerin B2C uygulamalarıyla B2B uygulamalarında kullandıkları tüm sistemler birbirine entegredir. Bu entegre sistemler sayesinde satış sonrası ürünlere ait tek bir bilgi oluşmakta, oluşan bu bilgi sigorta şirketinin ekranına gönderilmektedir. Yapılan araştırmalar sonucu sigorta şirketlerinin B2C uygulamasından çok B2B uygulamasını

[156] Sigortacı Gazetesi, "SigortaPro Sektörde Bir İlk", 12.09.2008, s.30
[157] Jan Devrim ve Adem Özbay, Bilgisayar & İnternet Sözlüğü, s. 29-30

kullandıkları, acente ve brokerleri için web servis hizmeti sundukları sonucuna varılmıştır. "Kanada'daki sigorta şirketlerinin tamamına yakını internet üzerinden satışı acentelerine devrederek yapmaktadırlar."[158]

Bu iki türün haricinde, "E-sigortanın B2B ve B2C'den farklı olarak, işletmeden çalışana (Business to Employee-B2E) şeklinde yapılan türü de bulunmaktadır. Ancak sık olarak kullanılanları B2B ve B2C sistemleridir."[159]

2.3.4. Ödeme Biçimleri

Elektronik ödeme ve para transferi sistemleri, elektronik ticarette kullanılmaları nedeniyle, e-sigortacılığı önemli ölçüde kolaylaştırmakta ve ayrılmaz bir parçası haline gelmektedirler. Bankamatikler (ATM), kredi, borç ve akıllı kartlar nakit aktarılmasında kullanılmaktadırlar.

2.4. ELEKTRONİK SİGORTACILIKTA SÖZLEŞME KAVRAMI

Elektronik Sigortacılık'ta sözleşme, klasik iletişim araçları, sigorta aracıları ve yolları kullanılmadan, tamamen elektronik ortamda internet üzerinden yapılan sözleşmeler olarak genel bir değerlemeye tabi tutulabilir. "Kurulmasında kullanılan yeni ve teknolojik gelişmelerin getirdiği bazı özellikler ile karşılıklı ve uygun irade beyanının imza ile güvenlik altına alınma hali hariç, sözleşme kavramını belirleyen ve tanımlayan bütün unsurlar ve şartlar burada da olmaktadır. Dolayısıyla elektronik sözleşmelerin, yazılı ve imzalanmış sözleşmelerin statüsel şartlarını karşılayacağı belirtilmiştir."[160]

---

[158] Burçin Tanberk, "İnternet Uygulamalarının Türkiye'de Sigortacılık Sektörüne Getireceği Yararlar ve Bu Yararları Sağlayabilmek İçin Hangi Sorunların Ne Şekilde Aşılması Gerektiği", Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2001, s.37.
[159] Belgin Bayır Levent, "E-Sigorta Hazırlığı", Capital Aylık İş ve Ekonomi Dergisi, 01.05.2002, s.11.
[160] H. Edward , J.D. Freeman, "Dijital Signatures and Electronic Contracts",http://www.auerbach-publications.com//ejournals/articles/article.asp?id=81647 Erişim Tarihi, 10.04.2001

2.4.1. Tanımı ve Kapsamı

Sözleşme kavramını izah ederken kullandığımız tanımı göz önüne alırsak, "bir sözleşmenin kurulabilmesi için tarafların karşılıklı irade beyanlarının olması ve bu irade beyanlarının birbirine uygun olması gerekmektedir."[161] Diğer bir ifade ile sözleşmenin kurulabilmesi için tarafların sözleşmenin hükümleri ile bağlı oldukları hususunda anlaştıklarını göstermelidirler. Bu da ancak irade unsuru ile gerçekleşir. "Sözleşmelerin elektronik ortamda, örneğin ağ veya internet ortamında yapılması bu ilkede yeni bir değişiklik veya ekleme yapmayacaktır."[162] Bu nedenle biz klasik sözleşme ile elektronik sözleşmeleri bir bütün olarak inceleyecek ve elektronik sözleşmelerle ilgili akla takılabilecek sorulara yanıtlar arayacağız.

Sözleşmenin kurulumu için gerekli olan irade beyanlarından, "ilk önce yapılan ve sözleşmenin yapılması hususunda öneriyi içeren irade beyanına icap (öneri)"[163], "bu öneriyi uygun gördüğünü bildiren karşı irade beyanına da kabul adı verilir."[164] Bir irade beyanının her koşulda bir insan tarafından gerçekleştirilmesi şart değildir. Günümüzde bilgisayar beyanının yasal olarak geçerli olduğu hususu doktrinde kabul edilmektedir. Bu insanın iradesini doğrudan kullanıp, bilgisayarı aracı kılmak suretiyle, örneğin; web sayfasından siparişte bulunmak, irade beyanını, yazılı, sözlü veya görüntülü olarak muhataba iletmek şeklinde olabileceği gibi, bazen de otomatik olarak bilgisayarlar tarafından, örneğin Elektronik Veri Değişimi (EDI) yöntemi ile gerçekleşir. Bu sistemde bilgisayara yüklenmiş olan bir program araya insan unsuru girmeden otomatik olarak "irade beyanında" bulunur ve bunu yine otomatik olarak muhatabına gönderir. İlk bakışta bu sistemde insan tarafından yapılan aktif bir hareket söz konusu değildir. Ancak şurası bir gerçek ki, bu sistemde dahi, irade beyanının asıl sahibi insan olup, bilgisayar, bir insan tarafından yüklenen program dâhilinde, daha önceden belirlenmiş belli parametreler vasıtasıyla mantıklı işlem yapabilir. "Kendi karar veremez."[165] Burada irade beyanının oluşturulması ve karşı tarafa iletilmesinde bilgisayardan faydalanılmaktadır. Dolayısıyla

[161] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul 2000, s.126
[162] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, Vedat Kitapçılık, İstanbul 2004, s.81
[163]Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul, 1976, s.49
[164] Kenan Tunçomağ, a.g.e, s.60
[165]Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, 1.Baskı, Vedat Kitapçılık, İstanbul 2004, s.84

beyanda bulunanın arzusuna uygundur. Bu nedenle burada da normal insan tarafından yapılmış bir iradenin mevcudiyeti kabul edilmektedir.

Elektronik sigorta sözleşmelerin kurulmasını üç aşamadan oluşmaktadır:

1-İcaba Davet,

2–İcap,

3-Kabul.

İcap, sözleşmenin yapılması teklifini içeren ve zaman itibari ile önce yapılan, muhataba varması gerekli, tek taraflı, kesin ve bağlayıcı nitelik taşıyan, muhatabın kabulü ile "sözleşmenin kurulması sonucunu doğuran irade açıklamasıdır."[166] İcap sözleşme yapılması için gerekli irade beyanlarından ilki olması nedeniyle, sözleşme yapma çağrısı niteliğindedir ve bu nedenle sözleşmenin taraflarından herhangi biri tarafından yapılabilir. "Niteliği itibari ile tek taraflı bir hukuki işlem olup"[167], icap sahibinin belirli bir süre icabı ile bağlı ve istekli olduğunu, "ayrıca teklif ettiği sözleşmenin kurulması hususunda muhataba yetki verdiğini ifade eder."[168] İcap, kural olarak herhangi bir özel şekle tabi değildir. Zira, Borçlar Kanunu 11 inci maddesi, sözleşmelerin kurulması için kural olarak şekil serbestisi ilkesini kabul etmiştir. Buna göre sözleşmenin kurulumu için gerekli irade beyanları olan icap ve kabulün, genel kurala göre, herhangi bir şekli ihtiva etmesi gerekmemektedir. Ancak, şekil serbestisinin istisnaları olan, taraf iradesi veya kanun hükmü ile bu kural geçersiz hale getirilebilir. Şöyle ki, yasa hükmü ile herhangi bir sözleşmenin geçerliliği belli bir şekil şartına bağlanmış ise, icabın da bu şekil şartına göre yapılması gerekir. Yine icapta bulunan sözleşmenin geçerliliğini belli bir şekil şartına tabi tutmuş ise, icabın da bu şekil şartına uygun yapılması gerekir.

İcap belli bir veya birkaç kişiye yöneltilebileceği gibi gazete, televizyon ve internet benzeri vasıtalarla umuma da yöneltilebilir. İcabın tanımından yola çıktığımızda icabın belli özelliklere sahip olması gerektiği sonucuna varmaktayız. Bunları aşağıdaki şekilde kısaca açıklayabiliriz. İcabın hüküm ve sonuçlarını doğurabilmesi için muhataba

[166] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.226
[167] Turgut Uygur, Açıklamalı-İçtihatlı Borçlar Kanunu Sorumluluk ve Tazminat Hukuku, Seçkin Yayıncılık, Ankara 2003, s.451
[168] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.227

varması gereklidir. "Varma tabirinden muhatabın hâkimiyet alanına ulaşması anlaşılmaktadır."[169] Doktrinde kabul edilen görüşe göre, icabın, uygun bir zamanda muhatabın posta kutusuna, "ev veya işyerine varması yada yetkili personel veya aile bireylerince kabul edilmesi halinde hakimiyet alanına ulaşmış sayılır."[170] Bu çerçeveden bakıldığında icabın muhatabın elektronik posta adresine ulaşması, online olarak kullanıcının bilgisayarına ulaşması veya telesekreterine mesaj olarak bırakılması hallerinde de hakimiyet alanına ulaştığı kabul edilmelidir. İcap ciddi olmalı, icabı yapan icabı ile bağlanma niyetinde olmalıdır. İcapta sözleşme yapma niyeti açık ve kesin olmalıdır. İrade beyanı bağlanma niyeti ile yapılmamışsa, mesela espri veya şaka ile yapılmış ise icap sayılmaz. Ancak bazen şartları var ise icaba davet olarak telakki edilebilir. İcap, sözleşmenin objektif ve sübjektif yönden tüm esaslı noktalarını kapsamalıdır. Dolayısı ile icap öyle olmalıdır ki muhatabın peki, evet, kabul gibi bir söz söylemesi veya elektronik ortamda bir tuşa basması, fareyi tıklaması ile sözleşmenin kurulmasını sağlayacak nitelikte olmalıdır. "Sözleşmenin hangi noktalarının esaslı hangi noktalarının ikinci derecede olduğunu ayırmak için kesin bir ölçü yoktur. Bu husus her sözleşmenin niteliğine, tarafların maksatlarına ve teamüllere göre tayin edilir."[171] Sözleşme yapma çağrısı yukarıda belirtilen özelliklere sahip değilse, sözleşme yapılmasına yönelik teklif, icap olmayıp, "icaba davet niteliğinde kabul edilecektir."[172] Gerçekten icap, sözleşme yapılması için gerekli bütün esaslı noktaları ihtiva ettiğinden, muhatabın kabulü ile sözleşme kurulmuş olur. İcaba davette ise beyan sahibi nihai ve kesin işlem iradesini açıklamamakta muhataba sözleşme yapmaya hazır olduğunu açıklamakta ve "muhatabı icapta bulunmaya veya sözleşme şartlarını müzakere etmeye davet etmektedir."[173]

Bir irade beyanının icap mı yoksa icaba davet mi olduğunu ayırt etmek her zaman kolay olmayabilir. "Bu durumda beyanın icap olup olmadığı genel hükümler çerçevesinde yorumlanması ve beyanda bulunanın maksadının ve durumunun tespiti ile anlaşılabilecektir."[174] Bu sebeple Borçlar Kanunu bazı hükümlerinde irade beyanının icap mı yoksa icaba davet mi kabul edileceği hususunda yorumlayıcı kurallar koymuştur. "Buna göre reklam broşürü, tarife, katalog, fiyat listesi v.s. göndermek veya yayımlamak icap

[169] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.226
[170] Turgut Uygur, Açıklamalı-İçtihatlı Borçlar Kanunu Sorumluluk ve Tazminat Hukuku, Seçkin Yayıncılık, Ankara, 2003, s.452
[171] Turgut Uygur, a.g.e, s.452
[172] Safa Reisoğlu, Borçlar Hukuku, 13. Baskı, Öngören Hukuk Yayınları, İstanbul, 2006, s.58
[173] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.228
[174] Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul 1976, s.186

olmayıp, icaba davettir."[175] "Yine üzerinde fiyatı gösterilmek suretiyle herkesin görebileceği çarşı, pazar, mağaza gibi yerlerde mal sergilenmesi icap sayılır."[176] Ancak bu hükme göre malın bizzat kendisinin fiyatı ile sergilenmesi gerekir. Malın resminin veya maketinin sergilenmesi ya da fiyat konulmadan malın sergilenmesi icap sayılmaz. "Keza araç veya ev satışı gibi geçerliliği şekil şartına bağlanmış sözleşmelerde, malın üzerine fiyatı konularak teşhir edilmesi icap sayılmamaktadır."[177] Borçlar Kanunu, fiyatı gösterilmek suretiyle eşya teşhirini kural olarak icap saymış ise de, bu durum yasa gereği kesin bir hüküm olmayıp karine teşkil etmektedir. Dolayısı ile bir malın üzerine fiyatı konularak sergilenmesinin icapta bulunmak niyetini taşımadığı iddia ve ispat olunabilir. "Yine doktrinde kabul edilen görüşe göre bu şekilde yapılan icap teşhir edilen mal ile sınırlıdır."[178] Bununla beraber kanun koyucu bazı istisnai durumlarda fiyatı gösterilmese de alıcıya, satıcının elinde bulunduğu sürece dilediği miktarda alma hakkı tanımaktadır. Gerçekten de Tüketicinin Korunması Hakkında Kanun'un 5 inci maddesi gereğince; aksine bir teamül yada ticari adet yoksa alıcı, "satıcının elinde var olduğu sürece bir mal veya hizmetten dilediği kadar alabilir."[179] Burada fiyat belirtme zorunluluğu olmaması, icabın sözleşmenin bütün esaslı unsurları içermesi gerektiği ve icabın teşhir edilen mal ile sınırlı olduğu kuralına ters düşmektedir. "Dolayısı ile bu şekilde ürün teşhiri bir icap olmayıp, sözleşme yapma ya da yapılacak icabı kabul etme zorunluluğu olarak anlaşılmalıdır."[180] Web sitelerinde mal veya hizmet sunumuna ilişkin bilgilerin yayımlanmasının, yine elektronik posta kullanılarak muhatabın e-mail adresine teklif gönderilmesinin, icap mı yoksa icaba davet mi sayılacağının tespiti özellik arz etmektedir. "Öncelikle, bireysel elektronik posta kullanılarak muhatabın e-mail adresine teklif gönderilmesinin, fonksiyonları itibari ile mektupla yapılan tekliften pek farkı yoktur."[181] Bu nedenle normal posta ile olduğu gibi, elektronik posta ile de icapta bulunulabilir. Ancak, web sitesinde yer alan ürün sunumları, nitelik itibari ile umuma yapılmış olması nedeniyle, uygulamada ve öğretide farklı değerlendirmektedir.

[175] Borçlar Kanunu, Madde 7/2
[176] Borçlar Kanunu, Madde 7/3
[177] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul 2000, s.51
[178] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.230
[179] Borçlar Kanunu, Madde 7/3
[180] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul 2000, s.51
[181] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.70

Elektronik ortamda yapılan irade beyanlarının hazırlar arasında olup olmadığının tespitinde iletişimin niteliği önem arz etmektedir. Söz konusu iletişimde taraflar, aynı anda diyalog kurarak, belirsiz konuları karşılıklı sorularla çözebilecek konumda değil iseler, "hazır olmayanlar arasında irade beyanından söz edilecektir."[182] Bunun en çarpıcı örneği elektronik postadır. "Zira e-postada tarafların doğrudan iletişim söz konusu olmayıp, klasik posta kutusunda olduğu gibi gönderilen beyanı geri almak mümkün olmadığı gibi, bu beyanın irade beyanın okunup okunmayacağı ya da ne zaman okunacağı tamamen alıcının iradesindedir."[183] Web sitelerinde yer alan sunumlar vasıtası ile sözleşme kurulmasında da doğrudan diyalog ve müzakere imkânı mümkün olmayıp, genelde sitede yer alan formun doldurulması veya ilgili butonun kliklenmesi ile sözleşme kurulduğundan, burada da hazır olmayanlar arasında iletişim söz konusudur. Aynı şekilde EDI yöntemi ile kurulan sözleşmeler de taraflar yüz yüze olmayıp diyalog imkânı olmadığından hazır olmayanlar arasında cereyan etmektedir. Bu nedenle elektronik ortamda, hazır olmayanlar arasında icabın varlığı kabul edilen hallerde muhataba kabul için uygun bir düşünme süresi tanınmalı ve "icabın bu sürenin sonuna kadar bağlayıcı olduğu kabul edilmelidir."[184] Tarafların elektronik ortamda, doğrudan diyalog kurarak ve karşılıklı etkileşime girerek, gerektiğinde sorular sorup, anında cevaplandırabilme yani müzakere etme imkânlarının var olduğu iletişim durumlarında ise, hazırlar arasında iletişimin varlığı kabul edilmektedir. İnternette, chat, sesli veya görüntülü internet telefonu, video konferans gibi iletişim yöntemleri, bu kategoride kabul edilmektedir. "Dolayısı ile bu tür iletişimde yapılan icap, hazırlar arasında gerçekleştiğinden, derhal kabul edilmemesi halinde bağlayıcılığını kaybedecektir."[185]

"Kabul, icapçı tarafından yapılan icaba karşılık, muhatap tarafından icapçıya yöneltilen ve icaba uygun olarak sözleşmenin kurulmasına imkân sağlayan, tek taraflı irade beyanıdır"[186] Kabul, sözleşmenin kurulması için gerekli olan irade beyanlarından zaman itibari ile ikincisidir. Kabul beyanının içeriği icaba uygun olmalı, icabın içerdiği esaslı noktalarda değişiklik, daraltma ya da genişletme yapmamalıdır. Aksi halde bu, "duruma

[182] Çiğdem Kırca, İnternette Sözleşme Kurulması, Banka ve Ticaret Hukuku Dergisi, Sayı:4, Ankara 2000, s.74
[183] Ergun Özsunay, Uluslararası Çalışmaların ve Bazı Ulusal Düzenlemelerin Işığında Elektronik Ticaret ve E-Sözleşmelerin Temel Sorunları, Uluslararası İnternet Hukuku Sempozyumu, İzmir 2002, s.121
[184] Özsunay, a.g.e, s.130
[185] Özsunay, a.g.e, s.131
[186] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul 2000, s.27

göre icabın reddi veya yeni bir icap sayılmaktadır."[187] Mesela muhatap, yapılan icaba karşı icapta bulunana bir ısım şartlar ileri sürer ise, bu yöndeki beyan yeni bir icap sayılır. Ancak, icap muhataba tercih hakkı tanıyor ve muhatap bu hakka dayanarak miktar, renk vs. yönden bir tercihte bulunuyorsa, "bu yöndeki beyan yeni bir icap olmayıp, kabul sayılır."[188] İcapta olduğu gibi, kabul için de kural olarak şekil serbestisi geçerlidir. Kanun, sözleşmenin geçerliliği için bir şekil şartı öngörmemiş ya da icapta bulunan kabul için bir şekil şartı koymamış ise, kabul beyanı, sözlü yada yazılı olabileceği gibi, muhatabın kabul iradesini gösteren bir hareketi, bir davranışı ile de olabilir. Yine kabul her zaman açık bir irade beyanı ile yapılmak zorunda değildir. "Zımni olarak da yapılabilir."[189] Örneğin, icapta bulunan tarafından gönderilen mal veya hizmet, muhatapça kullanılmaya, tüketilmeye başlanırsa, icap kabul edilmiş olur. Yine yapılan icap üzerine karşı bir beyanda bulunulmadan, muhatapça icabın gereği ifa edilir ise, söz konusu ifa kabul anlamına gelir. Örneğin, yapılan sipariş üzerine sipariş edilen malın gönderilmesi, tamir için bırakılan bir eşyanın muhatapça bir beyanda bulunulmadan tamir edilmesi, durumlarında zımni kabul söz konusudur.

Elektronik sözleşme kurulum araçları vasıtası ile kurulan sözleşmelerde de kabul beyanı çeşitli şekillerde iletilebilmektedir. "Sohbet (chat) ve e-posta da yazılı olarak, sesli ve görüntülü internet telefonu aracılığı ile sesli olarak ve nihayet internet sitelerinde sözleşmeye ilişkin formu doldurarak yada sözleşmeyi kabule ilişkin butonu tıklayarak kabul beyanında bulunulabilmektedir."[190] Kural olarak, susma bir irade beyanı değildir. Dolayısıyla icaba karşı susan muhatap, icabı kabul etmiş sayılmaz216. Hatta icapta bulunan, susma halinde icabın kabul etmiş sayılacağına dair kayıt bile koysa sonuç değişmez. Zira hiç kimse "kendi sebep olmadığı bir beyanı cevaplamak zorunda değildir."[191] Ancak bazı istisnai durumlarda muhatabın icapta bulunana cevap verme yükümlülüğü vardır. "Bu gibi hallerde susma, kabul sayılır."[192] Gerçekten, Borçlar Kanunu 6'ncı maddesi gereğince, icapta bulunan, kanun veya işin özelliği ya da durumun gereği, açık bir kabulü beklemek zorunda değilse, öneri uygun bir sürede reddedilmediği

[187]Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.235
[188] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul 2000, s.60
[189] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.236
[190] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul 2003, s.74
[191] Turgut Uygur, Açıklamalı-İçtihatlı Borçlar Kanunu Sorumluluk ve Tazminat Hukuku, Seçkin Yayıncılık, Ankara 2003, s.454
[192] Fikret Eren, Borçlar Hukuku Genel Hükümler, Cilt 1, 3.Baskı, Beta Basım Yayın, İstanbul 1998, s.237

takdirde, sözleşme kurulmuş sayılır. Örneğin, bir kişiye yapılan bağışlama teklifi, durumun özelliği gereği, muhatap tarafından uygun sürede reddedilmez ise, susma kabul anlamına gelir ve sözleşme kurulmuş olur. "Kabul, yenilik doğuran bir işlemdir. Kabul beyanı ile sözleşme kurulmuş olur."[193]

Bu nedenle kural olarak kabul geri alınamaz. Ancak, Borçlar Kanunu 9 uncu maddesinde zikredilen istisnai durum burada da geçerlidir. Buna göre, "hazır olmayanlar arasındaki işlemlerde, kabul beyanından önce kabulün geri alınması beyanının icapta bulunana ulaşması veya kabulden sonra ulaşmakla beraber, icapta bulunanca kabul beyanından önce kabulden dönme beyanının öğrenilmesi halinde, kabul geçersiz olur"[194]. "Hiç yapılmamış sayılır."[195]

2.4.2. Sözleşmenin Kurulması, Hüküm ve Sonuç Doğurduğu An

Sözleşmenin meydana geldiği anın tespiti ile ilgili olarak doktrinde dört farklı görüş bulunmaktadır. Açıklama teorisine göre, sözleşme muhatabın kabul beyanını açıklaması ile kurulur. Dolayısıyla kabul haberinin icapta bulunana gönderilmesine gerek yoktur. Gönderme teorisine göre sözleşme, muhatabın kabul beyanını icap sahibine gönderdiği anda kurulmuş olur. Varma teorisine göre sözleşme, kabul beyanının icapta bulunanın hâkimiyet alanına ulaştığı, vardığı anda kurulmuş olur. Öğrenme teorisinde ise sözleşmenin kurulabilmesi için icap sahibinin kabul beyanını öğrenmesi gerekir. Buna göre "icap sahibinin kabul beyanını öğrendiği anda sözleşme kurulmuş olur."[196] Hukuk sistemimizde sözleşmenin meydana geldiği anın tespitinde, sözleşmenin hazırlar arasında olup olmadığına göre ayrıma gidilmiştir. Hazırlar arası sözleşmelerde, iradenin açıklanması, ulaşması ve öğrenme aynı anda gerçekleştiği için sözleşmenin kurulum anının tespitinde bir problem bulunmamaktadır. "Hazırlar arasındaki icabın derhal kabulü gerektiği için, muhatabın kabul beyanında bulunduğu anda sözleşme kurulmuş

[193] Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul, 1976, s.200
[194] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul, 2000, s.63
[195] Turgut Akıntürk, Borçlar Hukuku, 1.Basım, Beta Basım Yayın, İstanbul, 2006, s.29
[196] Şahin Akıncı, Borçlar Hukuku Bilgisi, 3.Basım, Bahçıvanlar Basım, Konya, 2006, s.85

olur."[197] Sözleşme yazılı olarak yapılıyorsa muhatap sözleşmeyi imzaladığı anda sözleşme kurulmuş olacaktır. "Elektronik sözleşme kurulum araçlarından olan, chat ve internet telefonu benzeri iletişim hazırlar arasında kabul edildiğinden kabul beyanında bulunulduğu an sözleşme kurulmuş olur."[198] Hazırlar arasında meydana gelen sözleşmelerde sözleşmenin kurulduğu an ile hüküm ve sonuçlarını doğurduğu an aynıdır. "Bu itibarla sözleşme, kabul beyanının açıklandığı anda kurulmuş ve de hüküm ve sonuçlarını doğurmaya başlamıştır."[199] Hazır olmayanlar arasında kurulan sözleşmelerde hukukumuz, kurulum anı olarak, varma teorisini kabul etmiştir. Bilindiği gibi İsviçre-Türk hukukunda, varma anı olarak irade beyanının muhatabın hâkimiyet alanına girdiği an kabul edilmektedir. Buna göre, "kabul beyanının icap sahibinin hâkimiyet alanına ulaştığı anda sözleşme kurulmuş olur."[200] Açık bir kabule ihtiyaç bulunmayan hallerde ise "uygun bir bekleme süresinin sonunda sözleşme kurulmuş olur."[201] Görüldüğü üzere varma teorisi, icapta bulunanın kabul beyanını öğrenip öğrenmemesine değer vermemektedir. Buna göre kabul beyanı icapta bulunanın hâkimiyet alanına ulaştıktan sonra icapta bulunanca öğrenilmeden, kayıp veya zayi olsa da sözleşme kurulacaktır. Bu sonuç bazı yazarlarca ağır bulunmakla eleştirilmiş ve bu kuralın tüm sözleşmelerde uygulanamayacağı, varma teorisinin sadece tarafların menfaatleri arasında denge olan sözleşmelerde uygulanacağı, "somut olaya göre icapta bulunandan muhatabın beyanını öğrenmesi beklenmiyorsa ve kabul beyanı kayıp ya da zayi olmuş ise ulaşmamış sayılması gerektiği savunulmaktadır."[202]

Hazır olmayanlar arasında gerçekleşen sözleşmelerin hüküm ve sonuçlarını doğurmasında ise hukukumuz, gönderme teorisini benimsemiştir. Buna göre sözleşme, "kabul haberinin icapta bulunana gönderildiği andan itibaren hüküm ve sonuçlarını doğurmaya başlayacaktır."[203] Açık bir kabule ihtiyaç bulunmadığı durumlarda ise sözleşme, "icabın muhataba ulaştığı andan itibaren hükümlerini doğuracaktır."[204]

---

[197] Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul, 1976, s.204
[198] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, 1.Baskı, Vedat Kitapçılık, İstanbul, 2004, s.121
[199] Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul, 1976, s.207
[200] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul, 2000, s.166
[201] Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul, 1976, s.204
[202] Kemal Oğuzman, Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, Filiz Kitabevi, İstanbul 2000, s.66-68
[203] Borçlar Kanunu Madde 10 / 2
[204] Kenan Tunçomağ, Türk Borçlar Hukuku, 1.Basım, İstanbul Barosu Yayınları, İstanbul, 1976, s.205

Web sitesi ve elektronik posta kullanılarak irade beyanı gönderiminin, kural olarak hazır olmayanlar arasında iletişim kategorisinde bulunduğunu, daha önce ifade etmiştik. Dolayısıyla, bu hallerde sözleşme, kabul beyanının icapta bulunanın hâkimiyet alanına girdiği anda kurulmuş olacaktır. Ancak, internet üzerinden gönderilen irade beyanları genel itibari ile, tarafların sahibi olmadığı internet servis sağlayıcısı yada elektronik posta hizmet sunucusu aracılığı ile muhataba ulaşmaktadır. Söz konusu "hizmet sağlayıcıları tarafların hâkimiyet alanı kabul edilemez."[205] Hizmet sağlayıcısının taraflara tahsis ettiği e-posta kutusu ise hâkimiyet alanı dâhilindedir. O halde, irade beyanı ne zaman hâkimiyet alanında kabul edilecektir. E-posta kullanımında, gönderilen mesaj önce hizmet sağlayıcı vasıtası ile mail sunucusu (server) bünyesinde bulunan muhataba ait posta kutusuna kaydedilir ve muhatap bu sunucuya bağlanarak gelen mesajı öğrenir. Şu halde ulaşma anı, mesajın muhatabın e-posta kutusuna ulaştığı an mı, yoksa muhatabın sunucuya bağlanarak mesajı öğrendiği, yani bilgisayarına indirdiği an mıdır? Doktrinde her iki durumu da savunanlar vardır. Ancak hâkim olan görüş, "beyanı içeren mesajın muhatap tarafından erişilmek üzere, muhatabın e-posta kutusuna kaydedildiği anda mesaj muhatabın hâkimiyet alanına ulaşmıştır."[206] Yine "beyanın muhatabın hâkimiyet alanına varması yeterli olmayıp, muhatabın bunu öğrenme imkânının da olması aranmaktadır."[207] Buna göre muhatap, başka kişilerin yardımı veya müdahalesi olmadan kendi elektronik posta kutusuna girerek, beyanı içeren mesajı öğrenebiliyor ise mesaj muhatabın hâkimiyet alanına ulaşmıştır. Ancak günümüzde, elektronik posta adresi olduğu halde bunu hiç kullanmayan, kontrol dahi etmeyen kişiler olduğu gibi, birden çok elektronik posta adresi kullanan ve bunlardan bazısını özel işlerinde, bazılarını ise ticari ve hukuki işlerinde kullananlar da bulunmaktadır. Yine elektronik posta adresi kullanımına rağmen, posta kutusunun boşaltılmamasından veya posta kutusuna spamming yolu ile çok sayıda mail gelmesinden dolayı posta kutusunun kapasitesinin dolması nedeniyle, gelen mesajın kaydedilemediği durumlarda olmaktadır. O halde posta kutusuna kaydedilemeyen veya muhatabın haberi olmadan posta kutusuna kaydedilen ama muhatabın öğrenmediği maillerin durumu ne olacaktır sorusu önem kazanır. "Doktrinde e-mail ile iletişimin klasik iletişim yolları ile aynı hukuki sonucu doğurabilmesi için elektronik posta adresi

[205] Birsen Acır, Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, SPK Yeterlilik Etüdü, Ankara, 2000, s.15
[206] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.183
[207] Özdemir Kocasakal, a.g.e., s.84

sahibinin, bu yönde bir kullanıma izin vermesinin aranması gerektiği ifade edilmektedir."[208] Buna göre e-posta adresi ticari bir işletmeye veya ticari bir kullanıcıya ait ise, e-posta adresinin evrak, web sitesi, reklâm broşürü gibi herhangi bir yolla açığa vurulması halinde bu yönde kullanıma izin verilmiş demektir. Buna paralel olarak da "ticari işlerde tacirlerin e-posta adreslerini günlük bir veya birden çok kez kontrol etmeleri gerektiği kabul edilmektedir."[209] E-postanın mesai kavramından bağımsız olarak, günün 24 saati gönderilebildiği nazara alındığında, tacirler açısından e-posta mesajı muhatabın e-posta kutusuna kaydedildiği anda muhataba ulaşmıştır. Bu an muhatabın posta kutusunu kontrol yükümlülüğü olmadığı bir zaman, örneğin gece ise, "en geç gönderildiği günü takip eden günün sabahı muhataba ulaşmış kabul edilecektir."[210]

Elektronik posta adresinin bir tüketiciye ait olması durumunda ise, mesajın e-posta kutusuna ulaşmasının, "kullanıcının hâkimiyet alanında kabul edilebilmesi için, tüketicinin, bu adresini hukuki işlemlerinde kullandığını muhatabına bildirmesi gerekmektedir."[211] Bu bildirim, tüketici tarafından sözleşme kurulmasına yönelik girişimin e-mail aracılığı ile başlatılması şeklinde olabileceği gibi, web sitesine kayıt yapılırken e-posta adresinin belirtilmesi şeklinde de olabilecektir. Bu şekilde bir bildirimde bulunulmuş ise, kullanıcının e-posta adresini günlük kontrol etmesi gerektiği kabul edilecek ve "irade beyanı posta kutusuna kayıt anında veya en geç gönderilen günü takip eden gün tüketiciye ulaşmış sayılacaktır."[212] Kullanıcı tarafından böyle bir bildirimde bulunulmamış ise irade beyanı ancak, kullanıcı tarafından "mesajın içeriğinin öğrenildiği an ulaşmış kabul edilecektir."[213] Elektronik posta adresi sahibinin, posta kutusunu kontrol yükümlülüğünün olduğu kabul edilen hallerde, irade beyanının gönderilmesine rağmen, ulaşma engelleri nedeniyle posta kutusuna kaydedilememesi durumlarında ise, bizim de katıldığımız görüşe göre, ulaşma engelinin kaynağına göre değerlendirme yapılacaktır. Söz konusu engel, muhatabın etki alanında bulunmayan harici bir sebepten kaynaklanıyor ise, örneğin, virüs, hacker saldırısı veya hizmet sağlayıcısının sisteminin çökmesi yada

[208] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, 2004, s.122
[209] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.83
[210] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, 1.Baskı, Vedat Kitapçılık, İstanbul, 2004, s.124
[211] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.85
[212] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, 2004, s.124
[213] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, 1.Baskı, Vedat Kitapçılık, İstanbul, 2004, s.124

spamming tarzı bir saldırı ile e-posta kutusunun dolması gibi nedenlerle, mesajın posta kutusuna kaydedilememesi halinde, "riziko göndericiye yüklenerek mesaj ulaşmamış kabul edilecektir."[214] Buna karşılık, alıcının etki alanındaki bir sebepten; örneğin, posta kutusunu düzenli kontrol ve gerektiğinde boşaltma yükümlülüğü olduğu halde, posta kutusunun boşaltılmaması nedeniyle, kapasitesinin dolması ve bu nedenle mesajın kaydedilememesi veya mesaj posta kutusuna kaydedilmekle beraber, alıcının bilgisayarındaki arıza yada başka nedenle silinmesi halinde, "riziko alıcıya ait olacak ve mesaj muhataba yani alıcıya ulaşmış olacaktır."[215]

Web sayfaları üzerinden gönderilen irade beyanlarında ise, tarafların doğrudan diyalogu olmamakla beraber, elektronik posta iletişiminden farklı olarak irade beyanı, genelde "üçüncü bir bilgisayara (mail server) kaydedilmeyip doğrudan muhatabın bilgisayarına gönderilmektedir."[216] Yani bir nevi doğrudan iletişim söz konusudur. Bu nedenle irade beyanının gönderilmesi ile muhataba ulaşması neredeyse aynı anda olur. Ancak ulaşma engelleri ve iletişim kopukluğu gibi sebepler dikkate alınarak diyebiliriz ki, "web sayfaları üzerinden gönderilen irade beyanları, muhatabın bilgisayarına kaydedildiği anda ulaşmış sayılmalıdır."[217] Şu halde sözleşmenin kuruluş anı da, web sayfasındaki sunumun icap veya icaba davet olarak nitelendirilmesine göre değişecektir. Web sayfasındaki sunumun icap kabul edildiği hallerde, "muhatabın kabul beyanının icapta bulunana ulaşma anında sözleşme kurulmuş olacaktır."[218] Web sayfasında ki sunumun icaba davet kabul edildiği durumlarda ise, sunumu yapanın kabul beyanının icapta bulunana ulaştığı anda sözleşme kurulacaktır. Yine bu halde sunumu yapanın sözleşme yapmaya hazır olduğunu belirtmesi nedeniyle, "açık kabule ihtiyaç bulunmayan hallerde sunumu yapan kabul beyanında bulunmayıp susarsa uygun bir bekleme süresi sonunda sözleşme kurulmuş olacaktır."[219] UNCITRAL tarafından hazırlanan, Elektronik Ticaret Model Kanunu (m.15) ve Veri Mesajları Aracılığıyla Kurulan veya Tespit Edilen Sözleşmelere İlişkin Konvansiyon Ön Tasarısı (M.8,11) mesajların muhataba ulaşma anını, muhatabın

[214] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, 2004, s.123
[215] Ümit Gezder, Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, 1.Baskı, Vedat Kitapçılık, İstanbul, 2004, s.123
[216] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.85
[217] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.88
[218] Özdemir Kocasakal, a.g.e, s.85
[219] Çiğdem Kırca, İnternette Sözleşme Kurulması, Banka ve Ticaret Hukuku Dergisi, Sayı:4, Ankara, 2000, s.113

haberleşme sistemi bildirip bildirmemesine göre, iki şekilde düzenlemiştir. Buna göre, muhatap elektronik haberleşme adresini bildirmiş ise mesajların bu adrese ulaştığı an muhataba ulaşma anıdır. Aksi halde, yani adres bildirilmemesi veya bildirilen adresten başka bir adrese mesaj gönderilmesi durumunda ise ulaşma anı, "muhatabın mesajı öğrendiği andır."[220] Elektronik Ticaret Model Kanununa göre, elektronik sözleşme kuruşlum araçları ile yapılan irade beyanları, "onu gönderenin kontrolü dışında olan bir elektronik ortama girdiği anda gönderilmiş sayılır"[221] Bu doktrinde de benimsenmiştir. Bu ilkeden hareketle denebilir ki, elektronik sözleşme kurulum araçları ile kurulan sözleşmeler, açık bir kabule ihtiyaç olan hallerde, kabul beyanının gönderenin kontrolü dışındaki bir elektronik ortama girdiği andan, "açık bir kabule ihtiyaç olmayan durumlarda ise, icabın muhataba ulaştığı andan itibaren hüküm ve sonuçlarını doğurmaya başlar."[222] Ancak, elektronik ortamda kabul beyanının icapta bulunana gönderilme anı ile ulaşma anı arasında çok kısa bir zaman geçmektedir. Bu nedenle de "genel olarak elektronik ortamda yapılan bir sözleşmenin kurulma anı ile hüküm ve sonuçlarını doğurmaya başladığı an aynı olmaktadır."[223]

[220] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.87
[221] Elektronik Ticaret Kanunu, Madde 15 / 1
[222] Çiğdem Kırca, İnternette Sözleşme Kurulması, Banka ve Ticaret Hukuku Dergisi, Sayı:4, Ankara, 2000, s.113
[223] Özdemir Kocasakal, Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti, 1.Baskı, Vedat Kitapçılık, İstanbul, 2003, s.85

2.5. ELEKTRONİK SİGORTACILIKTA KARŞILAŞILAN SORUNLAR

Tüm dünyada e-sigortacılık uygulamalarının diğer sektörlere oranla daha az gelişim göstermesinin nedenlerini aşağıdaki gibi sıralanabilmektedir:

- Karmaşık Yapıdaki Poliçeler
- Hasar İle İlgili Sorunlar
- Güven Sorunu
- Yasal Düzenlemeler ve Hukuki Eksiklik.

Sigorta ürünleri yapısı gereği biraz karmaşık ürünler olduğu için bütün ürünlerin internet üzerinden satışının yapılması mümkün olmamaktadır. Hayat, sağlık, ticari yangın gibi karmaşık ürünlerin danışman/aracı yardımı olmaksızın anlaşılması güç olduğundan internet üzerinden satışa sunulan ürünler daha anlaşılabilir, basit ürünlerdir. Bu nedenle sigorta şirketleri hayat, sağlık, emeklilik, ticari yangın poliçelerinin internet üzerinden sadece tanıtımını yapabilmektedir. "Elektronik olarak ürün tanıtımı yapılması da bir tür e-sigortacılıktır. Bunun dışında poliçelerin iptal süreci de birtakım prosedürler içerdiğinden bazı durumlarda bu işlemler fazladan zaman alabilmektedir. Bu da e-sigortacılığın önündeki engellerden biridir."[224]

Hasar ve ekspertiz işlemleri bazen uzun sürebilen işlemlerdir. Bu işlemleri belirli bir standarda oturtmak mümkün değildir. Hasar incelemesi ile ilgili gerekli evrakların bir kısmı internet vasıtasıyla sigorta şirketine ulaştırılabilse dahi, hasar işlemleri ve ekspertiz çalışmalarının internet üzerinden yalnızca durumun gidişatı takip edilebilmektedir. Sigorta güvene dayanan bir sistemdir. İnternetin herkese açık bir ağ olması nedeniyle, sigortalılar interneti güvenilir bir araç olarak görmemekte, bu sebeple de internet sigortacılığı yaygınlaşamamaktadır. Geleneksel yöntemdeki güven duygusu internet sigortacılığında henüz oluşmamıştır. Çalışanların eğitimsizliği, yazılımlardan kaynaklanan hatalar ve çalışanların teknolojik değişimlere karşı direnmesi de e-sigortacılıkta karşılaşılan sorunlar arasındadır. İnternet sigortacılığında dünyanın çeşitli ülkelerinde çeşitli

[224] Selim Yazıcı ve Serhat Yanık, Elektronik Sigortacılık: Elektronik Ticaretin Sigorta Sektörüne Etkileri, Der Yayınları, İstanbul 2002, s.12

kurallar ve düzenlemeler mevcuttur. Örneğin, "ABD' de tüm eyaletlerde faaliyette bulunma ruhsatı alan kurum internet üzerinden pazarlama ve satış yapabilmektedir. Ðnternet sigortacılığının önündeki engellerden bir tanesi de yasal düzenlemelerdeki eksikliktir. Tüm ülkelerde geçerli olabilecek bir e-sigortacılık anlaşması henüz bulunmamaktadır"[225]

"Yukarıda sayılanlarla birlikte, internet sigortacılığının önündeki engelleri şu şekilde sıralayabiliriz:"[226]

- "Ekspertiz işlemlerinin internet üzerinden yapılması mümkün olmamaktadır."[227]
- Genel ve özel şartların müşteri tarafından tam olarak okunmaması sonucu, herhangi bir hasarda anlaşmazlıkların ortaya çıkma ihtimali bulunmaktadır. Sigortayı anlatmak ve satışını yapmak sigortanın önemini bilen kitlelere yapılabilmektedir. "İkna edici bir etkinin olmaması sigorta şirketleri ve aracıları açısından bir kayıptır."[228]
- İnternet ortamındaki sigorta ve tahsilâtlarda güven sorunu bulunmaktadır.
- Kasko poliçelerinde, hasarlı araca sigorta yapılabilmesi ihtimali bulunmaktadır.
- Her ihtiyaca uygun poliçe henüz tam olarak yapılandırılamamıştır.

Çok fazla işlem detayı olmasında dolayı poliçe yapmanın çok fazla uzaması ve uzun zaman alması zor karar veren alıcılar için caydırıcı olabilmektedir. Sanal ortamdaki güvenliğin yeterli düzeyde olmaması da e-sigortacılığın aşması gereken engellerdir.

[225] Sigma - Swiss Re, The Impact of E-Business on the Insurance Industry, Pressure to Adapt-Chance to Reinvent, s.3
[226] Ebru Öztürk, Elektronik Sigortacılık ve Türkiye'deki Türleri, Yayımlanmamış Tezler, s.70
[227] Şebnem Uralcan, Temel Sigorta Bilgileri ve Sigorta Sektörünün Yapısal Analizi, 2.Basım, Bilyay Yayınları, İstanbul, 2006. s.207.
[228] Meral Özel, Sigorta Sektöründe İnternet Aracılığı ile Satış, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, İstanbul, 2000. s.117

2.6. KİŞİSEL VERİLERİN KORUNMASINA YÖNELİK YAPTIRIMLAR

"Demokrasi ve şeffaflığın bulunduğu ülkelerin anayasalarında, uluslararası belgelerde ve BM Birleşmiş Milletler Genel Kurulu'nun 10 Aralık 1948 tarih ve 217 A(III) sayılı Kararıyla ilan edilen İnsan Hakları Evrensel Beyannamesinde özel yaşamın gizliliği güvence altına alınmıştır."[229] Kişinin izni ve bilgisi olmadan kişi hakkında fiziksel özelliklerini, fikir ve düşüncelerini, vicdan ve inançla ilgili bilgilerini, sağlık, öğrenim, istihdam durumu ile ilgili bilgilerini, fert olarak sürdürdüğü yaşamın mahremiyetini, aile yaşantısını, başkaları ile yapılan haberleşmelerini ifşa etmek, bilgisi dışında bu bilgilere erişmek ya da kullanmak bir ahlak zaafı ve suç unsuru olarak görülmektedir. "Aynı zamanda kişinin kendi hakkında verdiği bilginin çarptırılarak, amaç dışı kullanılması da bu kapsam dâhiline girmektedir."[230] Bilgi çağında, kişisel bilgilerin yaygın bir şekilde toplanarak işlenmesini kolaylaştırmak ve bunları ilgililerin yararlanmasına sunmak bir zorunluluk haline gelirken, diğer taraftan hakkında bilgi toplanan kişi ve kurumlara ait bilgilerin korunması ve saklanması önemli bir sorun haline gelmiştir. "Medeni Kanunun 24. maddesinde kişilik haklarına aykırı bu tür fiil veya faaliyetlere karşı kişiyi koruma vardır."[231] Fakat son yıllarda kişisel verilerin elektronik bilgi işlem yöntemleri ile derleme, sınıflandırma, saklama işlemelerine tabi tutulması ve istendiğinde istenen biçimde sunabilmesi olanağı ortaya çıkmış ama bunun sonucu olarak özel yaşamla ilgili bu gibi bilgilerin veya teknik deyimi ile kişisel verilerin haksız kullanılması riskini arttırmış, "kişinin rızası olmadan başkasına açıklanmasını ve bilginin bulunduğu yerden başka yerlere aktarmayı kolaylaştırmıştır."[232] Hal böyle olunca teknolojinin "getirdiği yeniliklere bağlı olarak kişisel verilerin ihlali söz konusu olmuştur."[233] Özel Yaşamın Gizliliğin Korunması Hakkı ile Bilgiye Erişim Özgürlüğü Hakkı birbirine taban tabana zıt kavramlar olarak karşımıza çıkmaktadır. Uygulamada her iki hakkında gereğince güvence altına alınabilmesi ve bu özgürlükleri düzenleyen kurallar konulurken özen gösterilmesi gerekmektedir. Bütün özgürlükler gibi özel yaşamın gizliliği hakkı

[229] Birleşmiş Milletler, İnsan Hakları Evrensel Beyannamesi, 10 Aralık 1948 tarih ve 217 A(III) sayılı Karar.
[230] 4982 Sayılı, Bilgi Edinme Hakkı Kanunu, Kabul Tarihi: 09.10.2004, Resmi Gazete Sayısı: 25269, Resmi Gazete Tarihi: 24/10/2003.
[231] İlknur Uluğ, Sanal Sigortacılık, Sosyal bilimler Araştırma Dergisi, Sayı:2, Eylül 2003, s.230
[232] Gökçe Üzel (edt.), Kişisel Verilerin Korunması, Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası, Ankara, Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.315
[233] Gökçe Üzel (edt.), a.g.e., s. 317

mutlak olmayıp bazı sınırlamalara tabidir. Diğer bir deyişle diğer bütün özgürlüklerde olduğu gibi kişisel verilerin korunması hakkının kapsamının belirlenmesi ve sınırlarının çizilmesi sırasında bazı ilkelere uyma zorunluluğu vardır. 1990 yılında Birleşmiş Milletler Genel Asamblesi bilgisayarla işlenen kişisel veri dosyaları hakkında yönlendirici ilkeler adını taşıyan belgede bu ilkeleri detaylı olarak incelemiştir. Bu ilkeleri kısaca incelersek;

"Yasalara Uygunluk ve dürüstlük: Kişisel veriler kanunlara aykırı yollarla toplanmamalı ve toplanmış bilgiler amaç doğrultusunda kullanılmalıdır.

Doğruluk ve Tutarlılık: Toplanan verileri doğruluğu ve tutarlılığı kontrol edilmeli; bütünlüğü ve güncelliğini sağlamak için saklandığı süre zarfında düzenli olarak kontrole tabi tutulmalıdır.

Haklı ve Belirli Amaçlara Yönelik Olması: Kişisel verilerin hangi amaç uğruna toplanacağı baştan kesin olarak belirlenmeli ve bütün ilgili kişilere açık bir şekilde bildirilmelidir.

İlgili Kişilerin Erişim Hakkı: Kişi kimliğini ispatlamak koşuluyla kendisi hakkında toplanan bilgilerin ne gibi bir işleme tabi tutulduğunu öğrenebilmeli ve bunların bir anlaşılabilir nüshalarını aşırı masraf ve zaman kaybı olmadan elde edebilmelidir.

Ayrımcılıktan Kaçınma: Kişinin kökeni, ırkı, cinsiyeti, dini veya felsefi inançları, cinsel yaşamı ve benzeri gibi konularda bilgiler ancak yasaların izin verdiği haklı ve gerekli durumlarda toplanabilmelidir.

Güvenlik ve Koruma: Kişisel verilerin toplanması, saklanması ve işlenmesi ile görevli bütün kurum ve kişiler, bu verilerin doğal afetler ve kazalar ile insanların işleyecekleri hata, kusur ve suçların yaratacağı tehlikelere karşı korunması için her türlü önlemi almalıdırlar.

Denetim ve Yaptırım: Kişisel verilerin korunması ile ilgili düzenlemelerle öngörülen ilke ve kuralların uygulanmasının, önlemlerin alınmasının ve gerekli denetimlerin yapılmasının sorumluluğu tarafsız, yetkin ve adil bir makama verilmelidir.

Uluslararası Veri Aktarımı: Kişisel verilerin saklanmakta olduğu ülkeden başka bir ülkeye aktarılması için her iki ülkenin ulusal mevzuatlarının bu aktarma işlemine

izin vermesi yanında bu veriler için, verinin gönderileceği ülkeni bu veri için sağladığı korumanın verinin bulunduğu ülkede sağlanan korumadan daha aşağı düzeyde olmaması da gerekir."[234]

"Şahsiyet hakkı, kişinin hayatı, vücut tamlığı, sağlığı, şeref ve haysiyeti, ismi, resmi, hürriyeti, özel hayatı ve sırları, kısacası tüm kişisel değerleri üzerinde söz konusu olan mutlak bir haktır."[235] Yukarıda bahsedilen günümüzün hızlı gelişen teknolojisi ve toplum hayatındaki değişmeler, her türlü ihlale açık olan kişilik hakkının korunmasının önemini giderek arttırmaktadır. Bunun en net göründüğü yer şüphesiz internettir. İnternet bu bahsedilen ihlalleri artıran ve hızlandıran bir etkiye sahiptir. İnternet sitelerinde yazı ve resim yoluyla kişinin gerek şeref ve haysiyeti ve gerekse de özel hayatı, sırları ihlal edilebilmektedir. Günlük gazeteler geceden basılıp dünün haberini ya da gündemini aktarırken elektronik ortamda çıkan gazeteler anında her haberi dakikalarla kitlelere ulaştırabilmektedir. Başka amaçlarla oluşturulan web sitelerinde de şahsiyet hakkını ihlal edecek, özellikle reklâm amacıyla resmin yayımlanması ve benzeri yayınların yapıldığı görülmektedir. Bunlara ek olarak elektronik posta yoluyla da şahsi varlıklara yönelik saldırılar gerçekleşebilmektedir. "İnternet yoluyla şahsiyet hakkı ihlali çok çeşitli şekillerde gerçekleşebilmektedir."[236] "Elektronik posta göndericinin bilgisayarı tarafından bir mail/server aracılığıyla alıcının mail servisine iletilir. Alıcının genellikle bir elektronik posta alma protokolü vardır."[237] Bu şekilde ulaşan e-posta, alıcının mail sunucusu tarafından yine alıcının mail kutusuna konur. Bunların en başında elektronik posta yoluyla ve web sitesi yoluyla gerçekleştirilenleri görebiliriz. Elektronik ortamda gerçekleşen ihlallere kısaca incelersek;

a) Mail Adresine gönderilen e-postalar: Bir kişi kendi e-mail adresini, göndericiye vermediği halde, kişinin şahsiyetine, şeref ve onuruna, sırlarına ya da özel yaşamına dair elektronik posta gönderilebilir. Benzer şekilde, bir kimse, e-posta adresine gönderilen ve doğrudan şahsiyetine yönelik olmamakla birlikte rahatsız edici haber, reklâmlarla da taciz edebilir. Bu göndericiler kişinin mail adresini ortak forumlardan, bilgi

[234] Gökçe Üzel, Kişisel Verilerin Korunması, Bilgi Toplumuna Doğru, Türkiye Bilişim Şurası, Ankara, Başbakanlık, 10-12 Mayıs 2002, ODTÜ, s.315
[235] Yaşar Karayalçın, Türk Hukukunda Şeref ve Haysiyetin Korunması, Ankara Üniversitesi Hukuk Fakültesi Dergisi, CXIX, n.1-4, 1962, s. 251-253, 274
[236] 97/7 Sayılı Tüketicinin Korunmasına Dair AT Yönergesi, http://www.turkhukuksitesi.com/makale_168.htm (Erişim Tarihi: 23.04.2011)
[237] Yargıtay Dergisi, İnternet Üzerinde yapılan hukuki işlemler, c.27, 2001, s.749-788

bankalarından elde edebilir. Bu tür gönderilere spamming ya da spam adı verilir. Bununla birlikte gönderilen e-postalar sadece reklâm mahiyeti taşımayabilir, bazı durumlarda bozuk dosya formatları ile alıcının bilgisayarına zarar veren virüsler gönderilir. Son olarak başka bir kişinin özel hayatını ilgilendiren fotoğraf, metin ya da ses dosyaları da bu yolla ifşa edilip gerçek veya tüzel kişileri rencide edici dosyalar gönderilebilmektedir.

b) Web Sitesi Yoluyla Gerçekleştirilen ihlaller: Web siteleri yoluyla kişilik hakkı ihlali internette önemli bir yer tutmaktadır. Kişi hakkında herhangi bir yazı, resim veya ses dosyası kişiyi rencide edici, özel yaşamına müdahil bir şekilde kullanılabilir. Bu durum reklâm amacıyla da kullanılsa da aynıdır. Mevzu bahis olan kişinin herhangi bir izni olmaksızın yapılan bu tür eylemler son zamanlar artış göstermiş, hacker olarak tanımlanan kötü niyetli kişiler tarafından bazı eylemler internette vuku bulmuştur. Kişisel hakların internet yoluyla ihlali olarak link ve frame yolu gösterilebilir. Bu yolla gerçekleşen ihlallerin basın medya yoluyla gerçekleşen ihlallerden temel nitelik olarak pek bir farkı yoktur.

Bu temel ihlallerin dışında bir kişiye ait ismin internette alan ismi olarak tescil ettirilmesiyle gerçekleşen ihlaller gösterilebilir. Bu durumda gerçek kişi sanal ortamda kendi adına alan ismi alamayacaktır. Bir başka ihlalde bir kimsenin adı, soyadı, yaşı, cinsiyeti, medeni durumu, ailesi, işi, adresi, e-posta adresi, geçirdiği hastalıklar, nitelikleri, hobileri, fobileri ve benzeri bilgileri kişinin şahsi bilgilerini oluşturur. Bu bilgiler kişinin ilgili formu doldurması ile alakalı şirket tarafından arşivlenebilir. Fakat üçüncü bir şahısa ya da başka bir firmaya satılması, sunulması ya da güvenlikten kaynaklanan sebeplerle zikredilen şahıs veya firmalara verilmesi de kişilik haklarının ihlali olarak sayılabilir.

Bilgilerin Korunması ve bu konuya yönelik yaptırımlar, Elektronik İmza Kanunu'nun 12.maddesinde incelenmiştir. Buna göre:

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

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

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

"Öncelikle belirtelim ki, EİK m. 12/b bendi, açık anahtar altyapısına aykırı bir düzenlemedir. Nitelikli elektronik sertifika, imza sahibinin kişisel bilgilerini içerdiği gibi (EİK m. 9/c, h ve g), güvenli elektronik imza doğrulama verisini de içerir (EİK m. 9/d), EİK m. 12/b bendi uyarınca, imza sahibinin sertifikasına üçüncü kişilerin erişimini engellediği düşünüldüğünde, güvenli elektronik imzalı belgenin alıcısı imza doğrulama verisini kullanamayacaktır."[238] Dolayısıyla, alıcı kendine gelen güvenli elektronik imzalı belgenin değiştirilip değiştirilmediğini de göremez. Buna karşılık, EİK m. 12 gerekçesinde, hüküm daha iyi ifade edilmiştir. Gerekçeden anlaşılacağı üzere, amaç, kişisel bilgilerin (EİK m.9/c, h ve g) korunmasıdır. Bu nedenle, "EİK m. 12/b'nin, imza sahibinin sertifikasında yer alan tüm bilgilerine erişimi engelleyebileceği şeklinde değil de, yalnız kişisel bilgilerine erişimi engelleyebileceği şeklinde anlaşılması gerekir düşüncesindeyiz."[239] Bu noktada, belki de önemli husus, imza sahibinin imzaladığı belgeye dair biçim, içerik gibi bilgilerin, güvenli elektronik imzanın ne kadar ve ne sıklıkla kullanıldığı gibi bilgilerin 212 veya imza sahibinin kimlere veri gönderdiği gibi bilgilerin ESHS tarafından ifşa edilmesinin önlenmesi ve gönderinin içeriği gibi bazı bilgilerin kayıt altına alınmasının engellenmesi konusunda herhangi bir düzenlemenin yapılmamış olmasıdır. Bu bağlamda, EİK m. 12 yeterli olmayacaktır. Çünkü bu madde sertifikada yer alan kişisel bilgilere özgü bir düzenlemedir.

AB Elektronik İmza Direktifi Madde 8/I'de, "ESHS'lerin kişisel verilerin korunması hakkındaki 95/46/AB sayılı ve 24/10/1995 tarihli AB Direktifi'ne"[240] uygun davranması gerektiği düzenlenmiştir. AB Elektronik İmza Direktifi m. 8/II'de, ESHS'lerin kişisel verileri sadece doğrudan veri konusu kişinin kendisinden, veya açık rızasının temininden sonra ve ancak sertifika verilmesi ya da sürdürülmesi için gerekli olduğu takdirde, toplayabilecekleri; verilerin ilgili kişinin açık rızası olmaksızın bir başka amaçla toplanamayacağı veya işlenemeyeceği düzenlenmiştir. Türk hukukunda, hem kişisel verilerin korunmasına ilişkin bir düzenleme olmaması hem de EİK m. 12'nin kısıtlı bir koruma sağlaması karşısında, önemli bir boşluk olduğu söylenebilir. Buna karşılık, ülkemizde kişisel verilerin korunması hakkındaki düzenleme tasarı aşamasındadır. Bu

[238] Mehmet Ertan Yardım, Elektronik İmza Ve Medeni Usul Kanunumuza Etkileri, Yayımlanmamış Yüksek Lisans Tezleri, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, s.74
[239] Mehmet Ertan Yardım, a.g.e., s.74
[240] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" direktif metni için bkz. http://eur-lex.europa.eu/en/index.htm. Erişim Tarihi, 20.04.2011

Tasarının kişisel veri, veri kütüğü sistemi ve kişisel bilgileri işleyen gibi tanımlar oldukça geniş tutulmuştur. Bu tasarının yasalaşması, andığımız sakıncaları ortadan kaldırabilir.

Elektronik İmza Kanunu'ndan kişisel bilgilerin korunması ile ilgili maddeler haricinde, hukuki düzenleme adına Kişisel Veriler'in Korunması Kanunu yürürlükte bulunmaktadır. Kişisel Veriler'in Korunması Kanunu, Avrupa Konseyinin 28 Ocak 1981 tarihinde imzaya açtığı , "108 sayılı Otomatik Olarak İşlenen Kişisel Veriler Bakımından Bireylerin Korunması Hakkında Sözleşme" 1985 yılında yürürlüğe girmiştir. Kanun üzerinde 1999 yılında bazı değişiklikler yapılmıştır. Türkiye, Kişisel Veriler'in Korunması Kanunu imzalamış fakat onaylanmamıştır. Bir başka deyişle "onay" kanununu çıkaramamıştır. Çünkü bu Sözleşmenin Türkiye tarafından onaylanabilmesi için Sözleşmeyi imzalayan devletin bu Sözleşmede öngörülen ilkelere uygun olan bir kanun çıkarması zorunludur. Ama Türkiye kişisel veriler ve bireylerin korunması hakkında herhangi bir kanunu henüz kabul etmemiş durumdadır. Resmi Gazetede yayımlanan, Bakanlar Kuruluna ait "Avrupa Birliği Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programı" ile "Avrupa Birliği Müktesebatının Üstlenilmesine İlişkin Türkiye Ulusal Programının Uygulanması, Koordinasyonu ve İzlenmesine Dair Karar"ı içinde "Kişisel Veriler" ile ilgili düzenleme vardır.[241] 2009 yılının içinde kişisel verilerin korunması kanunu yasalaşmamıştır.

Bu noktada, internet aracılığıyla yapılan her bilginin kişisel bilgi sayılıp sayılmayacağı sorusu akla gelebilir. Bu konuda, Verilerin Korunmasına İlişkin 95/46 sayılı AB Yönergesi'nin[242] ikinci maddesinde, "kişisel bilgi, belirli veya belirlenebilir bir kişiye ait her türlü bilgi anlamına gelir." şeklinde bir tanım yer almıştır. Kişi, adının verilmesi gibi doğrudan belirlenebileceği gibi, özel kimlik numarası, fiziksel, psikolojik, fikri, ekonomik, kültürel veya sosyal kimliğe ait özellikler gösterilmek suretiyle dolaylı olarak da belirlenebilir.[243]

Türk Ceza Kanunu, 2004 yılından itibaren, teknolojik gelişmelere paralel olarak ortaya çıkan "kişisel verilerin kaydedilmesi, ele geçirilmesi, başkasına verilmesi ve yayılmasını" 135 ve devamındaki maddeler ile düzenlemiştir. Bu suçun kişilik haklarından özel hayatın gizliliğini ihlal etmeme ilkesi ile ilgili olduğu kadar ayrıca kişilerin ekonomik hakları ile de ilişkisi vardır. Özellikle pazarlama tekniklerinin gelişmesi sonucu; mal ve hizmet üreten

[241] 31.12.2008 tarihli ve 5.Mükerrer 27097 sayılı Resmi Gazete
[242] Official Journal of The European Communities, L 281, 23.11.1995
[243] Gürsel Öngören, İnternet Hukuku, Öngören Hukuk Yayınları, İstanbul 2006, s.64

kuruluşlar, her bir tüketicinin tercihlerini belirleyen kişisel bilgilere ve verilere, yüksek miktarlar ödemeye hazır olmaktadırlar. Telekomünikasyon mevzuatına baktığımızda, kişisel veriler / bilgiler; tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasal bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve – veya tüzel kişilere ilişkin herhangi bir bilgiyi ifade etmektedir.[244]

Sağlıktan haberleşmeye ve ticareti hayatın değişik yönlerine ilişkin kişisel verilerin özel ve kamu kurumları tarafından elektronik ortamlarda tutulabilmesi, ülkeleri hem bu verilerin toplanma şekli ve yapısı ile ilgili kurallar koymaya hem de bu kuralların ihlali sonucu uygulanacak cezai yaptırımların açıkça düzenlemeye zorlamıştır. "Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir."[245] Hukuka aykırılık önşart olduğundan, izin, bir kanun gereği bunların kayıt edilmesi veya suçların önlenmesi için emniyet ya da istihbarat emriyle bunların kaydı, kişinin kendine veya başkalarına yapılan saldırıları durdurmak için veya normalde Yargı yolu ile elde etmesi gereken bir hakkını elde etmek için Yargıyı aradan çıkartıp bizzat hakkını alma için bu işi yapması kişisel bilgilerin kaydının hukuka aykırılığını ortadan kaldırır. Bu nedenlerle varlığı halinde suç oluşamaz. Ancak, "sebebi ne olursa olsun kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine ilişkin bilgilerin kaydı suçtur."[246] Burada hukuka uygunluk sebeplerine bakılmaz. Öte yandan kişilerin ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri hukuka uygunluk şartları olmadan kişisel veri olarak kaydeden kimse, altı aydan üç yıla kadar hapis ile cezalandırılır.

Kişisel Verilerin Korunması için, Kişisel Verilerin Korunması Hakkında Yasa Tasarısı olarak 47 maddelik bir tasarı hazırlanmıştır. Tasarının amacı, 1.maddede şu şekilde özetlenmektedir: "Bu Kanun, kişisel verilerin işleme tâbi tutulmasında kişiliğin, temel hak ve özgürlüklerin korunmasını ve kişisel verileri işleme tâbi tutan kişi ve kurumların uyacakları esas ve usulleri düzenler."[247] Kanunun Kapsamı ise ikinci maddede, "Bu Kanun hükümleri, kişisel verileri işleme tâbi tutulan kişiler ile bu verileri işleme tâbi tutan kamu kurum veya kuruluşları ile gerçek ve özel hukuk tüzelkişileri hakkında uygulanır." şeklinde belirlenmiştir.

Kanun tasarısı ile hedeflenenler şöyle özetlenebilir:

[244] Gürsel Öngören, a.g.e, s.65
[245] Türk Ceza Kanunu, Mad. 135, Fıkra 1
[246] Türk Ceza Kanunu, Mad. 135, Fıkra 2
[247] http://www.adalet.gov.tr/kanun/newfolder/kisiselveri.htm alıntı 27.05.10

- Kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetleri ile ilgili kişisel veriler ise işlenememesini sağlamak.

- Kişisel verilerin, aktarmayı isteyen gerçek ve tüzel kişilerin belirli bir olayda, kanundan doğan bir görevini yerine getirmesi için bu bilgiye ihtiyaç duyması ve kanunda belirtilen uygun haller dışında üçüncü kişilere açıklanmaması.

- Herkesin, veri kütüğü sahibine başvurarak; kendisiyle ilgili kişisel veri kaydedilip kaydedilmediğini öğrenme hakkı, kaydedilmişse bunları talep etmek, verinin muhtevasının eksik veya gerçeğe aykırı olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesini veya aktarımının engellenmesini ve yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini istemek hakkına sahip olması.

- Kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkumiyetleri ile ilgili kişisel veriler işlenmemesini sağlanması. Özel hayatın ve aile hayatının gizliliğine dokunmamak şartıyla, temel kamu yararlarının gerektirmesi halinde, ilgili mevzuatta yeterli koruma tedbiri bulunması kaydıyla, Kişisel Verileri Koruma Kurulu özel niteliği olan kişisel verilerin işlenmesine karar verilmesi.

- Kişisel verilerin, aktarmayı isteyen gerçek ve tüzel kişilerin belirli bir olayda kanundan doğan bir görevini yerine getirmesi için bu bilgiye ihtiyaç duyması ve kanunda belirtilen uygun haller dışında üçüncü kişilere açıklanmaması. Milli güvenliğin ve milli savunmanın sağlanması, suçun önlenmesi veya soruşturulması amacıyla yapılan istihbari faaliyetlerle ilgili olarak kanundan doğan bir görevin yerine getirilmesi için gerekli olması halinde de kamu kurum ve kuruluşlarınca kişisel verilerin, ilgili kamu kurum ve kuruluşuna aktarılabilmesi.

Artan saldırılar konusu, amaçları açısından iki ana bölümde incelenebilir. Bunlardan birincisi kişisel bilgilerin ele geçirilerek elektronik ortamda yapılan bankacılık, e-ticaret v.b. alanlarda başkasının adına sahte işlemler yapılmasıdır. İkincisi ise, bu illegal işlemlerin yanı sıra, kişilere ait özel bilgilerin kişilerin izni olmadan çeşitli ortamlarda açığa vurulmasıdır. Birinci gruba giren saldırılara karşı teknik ve prosedürel yaklaşımlar kullanılarak karşı önlemler geliştirilebilmekte olup, yasalarla da desteklenmesi büyük önem arz etmektedir. “İkinci gruba ait ihlallerde ise kişisel verilerin korunması ve gizliliğinin sağlanması için

yasaların çıkarılması AB uyum süreci içerisinde önem kazanmıştır. Türkiye bu konuda Avrupa Birliği Konseyinin kabul ettiği 108 sayılı sözleşmeyi imzalayarak gerekli önlemlerin alınması için çalışmalar başlatmıştır."[248] Bu çerçevede, kişisel nitelikteki verilerin otomatik işleme tabi tutulması dolayısıyla bireylerin kişilik haklarının himayesine ilişkin Kanun Tasarısı hazırlamak üzere 13/9/1995 tarihinde kurulmuş olan ve çalışmalarını tamamlayamayan Komisyonun yerine yeniden oluşturulan Komisyonca hazırlanan Kişisel Verilerin Korunması Kanunu Tasarısı Adalet Bakanlığı tarafından bakanlıklar ile ilgili kamu kurum ve kuruluşlarının görüşüne gönderilmiştir. Tasarı Haziran 2004'de Başbakanlığa sevk edilmiştir. Tasarı, Başbakanlığın 14/03/2005 tarih ve 1113 sayılı yazısı gereği "Üzerinde Çalışılanlar" bölümüne alınmıştır. Adı geçen tasarı, "veri korumasında genel kabul gören temel uluslararası metinlerin izini taşımaktadır ve ülkemizde kişisel verilerin işlenmesinde hukuka uygunluk denetimi yapacak olan "Kişisel Verileri Koruma Kurumu"na yer vermektedir. Bu doğrultuda, kamu tüzel kişiliğini haiz idari ve mali özerkliğe sahip "Kişisel Verileri Koruma Kurumu" kurulmasını da öngörmekte olup, Kurumun, Başbakanlığın "ilişkili" kuruluşu olmasını da ifade etmektedir. Kurum, Kişisel Verileri Koruma Kurulu ile Kişisel Verileri Koruma Kurumu Başkanlığı ve hizmet birimlerinden oluşacaktır."[249]

Günümüzün gelişen teknolojisi dikkate alındığında kişisel verilerin eskisine oranla daha büyük bir hızda ve oranda gizliliğinin, mahremiyetinin ve bütünlüğünün riske girdiği aşikardır. Dolayısı ile kişilerin bu hususa yeterince özen ve önem göstermeleri son derece önemlidir. Bu çerçevede kişilerin ve kurumların bilgi güvenliği konusunda bilinçlendirilmesi ve bilgilendirilmesi, olabilecek muhtemel sorunların en aza indirilmesine katkı sağlayacaktır.

2.7. KİŞİSEL VERİLERİN KORUNMASININ ELEKTRONİK TİCARETE ETKİSİ

Kişisel verilerin korunmasının elektronik ticaretin gelişmesi ile doğrudan ilişkisi vardır. Kişiler elektronik ortamda kendilerine ait bilgilerin korunacağına ne ölçüde güvenirlerse o ölçüde yeni bir iş modeline yöneleceklerdir. Zira online müşteriler, kişisel bilgilerin 3.kişilere açıklanmayacağından net olarak emin olurlarsa, kendilerini güvende ve

[248] Bilişim Şurası, http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01K___SEL_VER_LER_N_KORUNMASI.doc erişim tarihi: 26.05.2010
[249] Bilişim Şurası, http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Mar/att-0044/01K___SEL_VER_LER_N_KORUNMASI.doc erişim tarihi: 26.05.2010

rahat hissederler. Buna karşın web sitesinin bilgilerini korumada yetersiz görürlerse, alışveriş yapmakta tereddüt ederler.

Buna karşın, kişisel verilerin aşırı şekilde korunmasının internette serbest pazarın gelişmesine engel olacağı öne sürülmüştür. Bu görüşte olanlara göre, bu konudaki uyulması zorunlu olan kurallar, kişisel bilgilerin kullanılmasına bağlı olan yeni iş modellerinin ve ürünlerin ortaya çıkmasına olumsuz baskı yaparak, elektronik ticaretin hacminin azalmasına neden olurlar.[250] Bunlara ek olarak, bilgi işleme ve saklama konusunda ek masraf yaparak bilişim sistemi kurulması ve bu sistem için de personel istihdamı yapılarak ekonomiye artı katkı yapılacaktır.

[250] Gürsel Öngören, İnternet Hukuku, Öngören Hukuk Yayınları, İstanbul, 2006, s.64

ÜÇÜNCÜ BÖLÜM

E İMZA KAVRAMI VE ÖNEMİ

3.1. ELEKTRONİK SİGORTACILIKTAKİ E- İMZA UYGULAMASINDA İLGİLİ TARAFLAR

Elektronik imza uygulamasında farklı işlevlere ve farklı hak ve yükümlülüklere sahip taraflar bulunmaktadır. Elektronik imza uygulamasının özelliklerine göre katılan taraflar değişebilecek olmasına rağmen her uygulamada en azından, elektronik sertifika hizmet sağlayıcı (kayıt makamı ile birlikte), imzalayan ve doğrulayan bulunmaktadır. Elektronik imza uygulamasının bir topluluk uygulaması olması veya üçüncü bir taraf tarafından sağlanıyor olması halinde, uygulama sağlayıcı ve/veya ilke/politika belirleyici de taraflar arasında sayılabilecektir. Ayrıca uygulamada dinamik bir etkileri olmamasına rağmen elektronik imza ürün sağlayıcıları (güvenli elektronik imza oluşturma aracı, güvenli elektronik imza doğrulama aracı, güvenli elektronik imza oluşturma uygulamalarında kullanılan yazılımlar) da çeşitli yükümlülükleri sebebiyle elektronik imza uygulamasındaki taraflardan sayılabilecektir.

3.1.1. Elektronik Sertifika Hizmet Sağlayıcısı

İmzalayan kişinin uygulamada imzalayan olarak yer alabilmesi için öncelikle ESHS'ye kimliğini kanıtlaması ve "ESHS'den nitelikli elektronik sertifika alması gereklidir." [251]

[251] T. Collins. DESS Droit de l'Internet - Administration – Entreprises, Aspects techniques et juridiques des infrastructures de gestion de clés publiques, Septembre 2004, s.23

Ülkemizde ESHS'lerin hak ve yükümlülükleri 5070 sayılı Elektronik İmza Kanunu, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenmektedir. 5070 sayılı Elektronik İmza Kanunu ile Telekomünikasyon Kurumu konuyla ilgili regülasyon yetkisine sahip olmuştur. Yasaya göre Elektronik Sertifika Hizmet Sağlayıcısı (ESHS), elektronik sertifika, zaman damgası ve e-imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir.

Serbest rekabet koşulları içinde ticari faaliyet gösterecek bu kişiler, bir düzenleyici kurumun belirlediği koşullarda hizmet verir. Düzenleyici kurum, ESHS'lerin hizmet koşullarını belirlemek ve denetlemenin yanı sıra, kişilerin kullanacağı araçlarla ilgili standartları belirleme ve yayınlamaktan da sorumlu olmaktadır.

Elektronik sertifikada yer alan bilgilerin doğruluğundan emin olunması için bir güven modeline ihtiyaç duyulmaktadır. E-imza yasasında tanımlanan ESHS'ler, sertifika veren kuruluşlar olarak tanımlanmaktadır. ESHS, güven ve itibarın tesisi için belirlenmiş kurallara bağlı olarak faaliyetlerini yürütmek ve yasa ile belirlenen bir kuruluş tarafından denetime açık olmak zorundadır. Türkiye'de ESHS faaliyetlerini düzenleyici kurum olarak Telekomünikasyon Üst Kurulu (TK) görevlendirilmiştir.

ESHS yapacağı bildirimde;

- Güvenli ürün ve sistemleri kullanmak,
- Hizmeti güvenilir bir biçimde yürütmek,
- Sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile ilgili şartları sağladığını ayrıntılı bir biçimde gösterir.

ESHS ile noterler arasında bir takım benzerlikler bulunmakla beraber aslında hizmet yapılarında farklılıklar bulunmaktadır. Noterler, bir işlemin vaki olduğunun resmi kaydını zaman mührüyle birlikte tutarlar. Bu anlamda işlem ve/veya kişilere güvenilir tanık durumundadırlar. Örneğin noterde bir sözleşme yapıldığında, noter açısından sözleşme içeriğinin hukuki boyutları önemli değildir. Önemli olan, evrakın ilgili taraflarca belirtilen tarihte noterin huzurunda ve tanıklığında imzalandığıdır. Noterin kimlik tespiti de beyan usulünde çalışır. Kimliği doğrulamak yerine evraktaki kimlikle kişinin beyan ettiği

kimlik belgesini karşılaştırır. Bir noter, noterlik hizmeti alan bir vatandaşla daha önce çalışmış olmak zorunda değildir.

Kimlik doğrulamada ESHS, noterde olmayan bir sorumluluk taşımaktadırlar. ESHS, işlemi gerçekleştiren şahsın kimliğinin doğruluğunu da kontrol eder. Bununla birlikte gerçekleştirilen işlemle ilgisi yoktur. Gerçekleştirilen işlem veya gönderilen belge tamamen iletişim kuran tarafları ilgilendirir. ESHS, bir kimyasal tepkimede, uygun ortam şartlarını sağlayan bir katalizör gibi görev yapar.

İletişim esnasında, e-imzanın onaylanması aşamasında sertifikanın geçerliliğinin kontrolüne ihtiyaç duyulabilir. Ayrıca belgeye eklenmek üzere zaman damgası hizmeti alınabilir. Bu hizmet, belgeyi görmeden zaman bilgisinin belgeye iliştirilmesi olarak düşünülebilir. Bu işlemde de ESHS, tam olarak noter gibi davranmaz. Çünkü noter, noterlik hizmeti alınan belgenin bir kopyasını alır, içini görür, yapılan sözleşmenin/anlaşmanın miktarına bağlı olarak bir hizmet bedeli ve devlet adına damga vergisi alır. Bununla birlikte ESHS belgenin içeriği ile ilgilenmez. "Ancak mesaj sahibi, mesajı imzalamakta kullanacağı NES için ya da zaman damgası hizmeti için ESHS'ye bir ücret ödediğinden, dolaylı olarak da olsa bir ücretlendirme söz konusudur."[252] Kısaca, hem işlevsel olarak hem de Türk Hukuku açısından, noterler ile ESHS'ler birbirine benzer ve farklı yanları olan ve birbirlerini tamamlayan işlevlere sahip iki kurum gibi düşünülmelidir.

Her elektronik sertifikanın belli bir kullanım süresi vardır. Bir kişi için bir ESHS tarafından yayınlanan elektronik sertifika, sertifika sahibi tarafından hayatı boyunca kullanılamaz. Sertifikanın kullanımının bir başlangıç bir de bitiş tarihi vardır. E-imza uygulamaları, elektronik sertifikalarla işlem yapmadan önce sertifikanın geçerlilik süresini kontrol ederler. Genellikle bu süre bir yıldır.

"Bir ESHS'nin iptal olma nedenleri ise şu şekilde listelenmektedir:"[253]

- Sertifikaya ait anahtarın kaybedilmesi veya çalınması,
- Sertifika politikalarının değişmesi,
- SM'nin anahtarının çalınması,

[252] Man Young Rhee, Internet Security: Cryptographic Principles Algorithms and Protocols, John Wiley & Sons Inc., England, s. 123-138
[253] Man Young Rhee, a.g.e, s.139

- SM'nin iptal edilmesi,
- Kullanıcının kendi isteği ile sertifikasını iptal ettirmesi,
- Kullanıcı bilgilerinin (ad, soyad, e-posta adresi vb.) değişmesi,
- Kullanıcının yetkilerinin askıya alınması.

3.1.2. İmzalayan

"Elektronik imza uygulamasında, "imzalayan" süreci başlatan dinamik taraftır."[254] İmzalayan, imza uygulamasının özelliklerine göre, imza uygulaması içerisinde çeşitli roller ve sorumluluklar edinebilir. İmza uygulaması, imzalayan kullanıcı tarafından esnekliğe uğratılabilir özellikte ise veya uygulama içerisinde kullanıcıya çeşitli seçenekler sunuyorsa, imzalayanın uygulamaya aktif katılımı artmakta ve buna göre sorumluluk yapısı değişmektedir. Örnek vermek gerekirse, web tabanlı basit bir form doldurma ve bu formu imzalama uygulamasında, imzalayan sadece formu doldurmak vebu form üzerindeki bilgileri imzalamak yetkisine sahiptir. Ancak son kullanıcının daha önceden yarattığı bir dokümanı, harici bir elektronik imza oluşturma yazılımı ile imzalaması ve bu yazılımın içerisinde; "imza taahhüdü"[255] (signature commitment), imza ilkeleri (signature policy) belirleme gibi seçenekler bulunması halinde, imzalayanın uygulamaya katılımı artacak ve imzalama ile ilgili sorumluluk yapısı değişecektir.

Burada imzalayanın sorumluluk yapısını değiştiren, imza uygulamasında kendisine sunulan seçeneklerdir. Şöyle ki, imza uygulaması, imzalayana imza taahhüdünü belirleme yetkisi veriyorsa, imzalayan belirlediği taahhüde göre imzasıyla sorumlu olacaktır. İmzalayan, imza taahhüdünü, onay, alındı, yaratma gibi farklı amaçlar doğrultusunda belirleyebilir. İmzalayan, taahhüdü belirledikten sonra, imzalı belge ile, belirlediği taahhüt doğrultusunda sorumlu olacaktır. Yani alındı amacıyla belgenin imzalanması, imzalayana

[254]Forum of European Supervisory Authorities for Electronic Signatures (FESA), Working Paper on Qualified Certificates for Automatically Signing Systems, October 2004 s. 1 http://www.fesa.eu/public-documents/WorkingPaper-AutomaticallySigningSystems-20041012.pdf (Erişim Tarihi, 10.04.2011)
[255] ETSI TS, Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES), V1.6.3, Valbonna – France, 2005 s. 28

belgeyi yaratan ve imzalayan sorumluluğunu getirmez, imzalayan sadece belgeyi teslim almış olduğunu belirtmekte ve belgeyi teslim almış olmakla sorumlu olmaktadır. İmzalayan, imza ilkesi belirleme seçeneğini kullanarak ise imza uygulamasında seçtiği imza ilkelerinin hükümleriyle bağlı olacağını kabul etmekte ve doğrulayanın da imzalı belgeye dayanarak işlem yaptığı takdirde, imzalayanın seçtiği imza ilkeleri hükümleri ile bağlı olacağını belirtmektedir. İmza ilkeleri, yine imza oluşturma yazılımının niteliklerine göre, imzalayan tarafından yaratılabilir veya mevcut imza ilkeleri içerisinden seçilebilir.

İmzalayan, 5070 sayılı Elektronik İmza Kanunu'nun 3. maddesinde "imza sahibi" olarak tanımlanmıştır. Bu tanıma göre imza sahibi; elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişidir. Güvenli elektronik imza uygulamasına bakıldığında imza sahibi/imzalayan aynı zamanda nitelikli elektronik sertifika sahibi olarak karşımıza çıkmaktadır; zira güvenli elektronik imza uygulamasında, güvenli elektronik imza sadece güvenli elektronik imza oluşturma aracı ve nitelikli elektronik sertifika ile oluşturulabildiği için; imza sahibi/imzalayanın aynı zamanda nitelikli elektronik sertifika sahibi olması da gerekmektedir. Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik ile nitelikli elektronik sertifika sahibinin yükümlülükleri belirlenmiştir. Bu yükümlülükler yukarıda belirtilen uygulamalı kaynaklı yükümlülüklerin yanında mevzuattan kaynaklanan yükümlülükler olarak ele alınmalıdır. Yönetmeliğin 15. maddesine göre nitelikli elektronik sertifika sahibi/imzalayan;

a) Nitelikli elektronik sertifika almak için gerekli tüm bilgi ve belgeleri eksiksiz ve doğru olarak sağlamakla,

b) ESHS'ye vermiş olduğu bilgilerde değişiklik meydana gelmesi halinde ESHS'yi derhal bilgilendirmekle,

c) İmza oluşturma verisini kendisi üretmesi durumunda Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenen algoritmaları ve parametreleri kullanmakla,

d) İmza oluşturma ve doğrulama verilerini sadece elektronik imza oluşturma ve doğrulama amaçlı olarak ve nitelikli elektronik sertifikanın içerdiği kullanıma ve maddi kapsama ilişkin sınırlamalar dahilinde kullanmakla,

e) İmza oluşturma verisini başkalarına kullandırmamakla ve bu konuda gerekli tedbirleri almakla,

f) İmza oluşturma verisinin gizliliğinden veya güvenliğinden şüphe etmesi durumunda ESHS'yi derhal bilgilendirmekle,

g) Güvenli elektronik imza oluşturma aracını kullanmakla,

h) İmza oluşturma ve doğrulama verilerinin ESHS'ye ait olmayan yerlerde ve araçlarla üretilmesi durumunda gerekli güvenliği sağlamakla,

i) İmza oluşturma aracının veya erişim verisinin kaybolması, çalınması ve güvenilirliğinden şüphe edilmesi durumunda ESHS'yi derhal bilgilendirmekle yükümlüdür.

3.1.3. Doğrulayan / Üçüncü Taraf

"Elektronik imza uygulamasında doğrulayan, imzalı belgeye güvenerek işlem yapan ve imzalı belgeyi alan taraftır."[256] Elektronik imza uygulamasına göre doğrulayan bir gerçek kişi olabileceği gibi aynı zamanda bir sunucu (server) da olabilir. Burada dikkat edilmesi gereken nokta doğrulama işlemini, ister gerçek kişi gerçekleştirsin ister bir sunucu gerçekleştirsin, doğrulamaya ilişkin sonuçların imzalı belgenin gönderildiği şahsa ilişkin olarak doğacak olmasıdır. Bu durum elle (manuel) olarak doğrulamanın yapıldığı anlardan çok bir güvenli elektronik imza doğrulama aracı kullanıldığı zamanlarda ortaya çıkmaktadır. Güvenli elektronik imza doğrulama aracı, Elektronik İmza Kanunu'nun 7. maddesinde şu şekilde tanımlanmıştır; Güvenli elektronik imza doğrulama araçları;

a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,

b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

[256] Sabo J.T., Dzambasow Y.A., PKI Policy White Paper, PKI Forum, March 2001, s.3

c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,

d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,

e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan, imza doğrulama araçlarıdır.

Görüldüğü üzere Kanun'da güvenli elektronik imza doğrulama araçlarına ilişkin nitelikler teknoloji - nötr bir şekilde tanımlanmıştır. "Uygulamaya bakıldığında ise, güvenli elektronik imza doğrulama araçlarının sunucu veya kullanıcı tabanlı yazılımlar olduğu görülmektedir."[257]

Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ve daha sonra çıkan Telekomünikasyon Kurumu Kararları ile eğer araçlar ESHS tarafından sağlanıyorlarsa, araçların standartlara uygunluğunun, ESHS tarafından taahhüt edilmesi gerektiği belirtilmiştir. Burada regülatörün amacı, piyasanın kendi iç dinamikleri içerisinde kendi kurallarını belirlemesi ve akreditasyon ile ilgili bir nevi self-regulation yapısının kurulmasıdır. Bu durum uygulamada araç sağlayıcıların, ESHS'ler ile çalışmasına ve yazılımlarının ilgili standartlara uyumluluğu konusunda ESHS'lerden taahhüt almasına yol açmaktadır. Böylece Kanun ile yetkilendirilen güvenilir üçüncü parti ESHS'ler, araçların standartlara uyumluluğu konusunda da sorumluluk sahibi durumuna gelmektedirler.

3.1.4. Uygulama Sağlayıcı, Politika İlke Belirleyici

Elektronik imza uygulamasında, uygulama sağlayıcı elektronik imza uygulamasını oluşturan ve imzalayanın (uygulamanın çeşidine göre doğrulayanın) kullanımına sunan

[257] CEN Workshop Agreement, CWA 14171 General guidelines for electronic signature verification, 2004, s.42

taraftır. Burada bahsedilen uygulama, imzalayanın elektronik imza atmasını sağlayan yazılım/ortam'dır. Şunu belirtmek gerekir ki; burada bahsedilen uygulama, güvenli elektronik imza oluşturma aracı değildir. "Güvenli elektronik imza oluşturma aracı, elektronik imza uygulamasının bir parçası olmakla birlikte, uygulama/yazılım güvenli elektronik imza aracının da yardımıyla elektronik imzanın oluşturulmasını sağlar."[258] Bu doğrultuda elektronik imzanın atılmasını sağlayan yazılım ve ara yüzler, Elektronik İmza Kanunu ve ilgili ikincil mevzuattaki güvenli elektronik imza oluşturma aracının tanımlarına dahil olmayıp burada belirtilen nitelikler haiz olmak zorunda değildirler. Bu uygulamalar/yazılımlar, ESHS'ler tarafından sağlandığında, Telekomünikasyon Kurulu'nun 01.06.2006 tarihli Kararı doğrultusunda, uygulamaların CWA 14170 standardına uyumluluğunun sağlanması gerekmektedir. Elektronik imza uygulamasının güvenliği veya işleyişi ile ilgili bir sorun ortaya çıktığında, uygulama sağlayıcının kusurundan bahsedebilmek için uygulama sağlayıcının objektif sorumluluğunu yerine getirip getirmediği tespit edilmelidir. Böyle bir durumda, uygulama sağlayıcının objektif sorumluluğunu yerine getirip getirmediğinin tespiti ilk bakışta oldukça zor olacaktır; zira uygulama sağlayıcının objektif sorumluluğunu yerine getirmesi için yapması gerekenler temel bilgi güvenliği kriterleri dışında çok da belirlenebilir değildir; çünkü mevzuatta elektronik imza uygulama sağlayıcının hak ve yükümlülüklerine ilişkin hükümler bulunmamaktadır. Burada Elektronik İmza Kanunu'nun 8. maddesi uygulamamaktadır, çünkü 8. madde metni içerisinde her ne kadar elektronik imza ile ilgili hizmetleri sağlayanlar da ESHS olarak kabul edilse de madde metni bütünü ile okunduğunda ve konuyla ilgili uluslararası standartlar göz önüne alındığında elektronik imza uygulaması sağlayanların elektronik sertifika hizmet sağlayıcısı olmadıkları açıklıkla ortaya çıkmaktadır. Bu sebeple, elektronik imza uygulama sağlayıcılarının, elektronik sertifika hizmet sağlayıcıların tabi oldukları hak ve yükümlülüklere tabi olmaları mümkün değildir.

[258] CEN Workshop Agreement, CWA 14170 Security requirements for signature creation applications, May 2004 s.14

3.1.5. Araç Sağlayıcılar

Elektronik imza uygulamasında, araç sağlayıcılar, güvenli elektronik imza oluşturma ve doğrulama araçlarını, son kullanıcılara ve ESHS'lere sağlayan donanım üreticileri ve satıcılardır. Bilindiği üzere ülkemizde elektronik imza oluşturma aracı üreticisi bulunmadığı için bütün elektronik imza oluşturma araçları ithalatçı firmalar tarafından sağlanmaktadır. Bu durum, uygulamada "elektronik imza oluşturma araçlarına ilişkin uygunluk sertifikalarının ithalatçı firmalar tarafından temin edilmesi sonucunu doğurmaktadır. Bilindiği üzere, Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 8. maddesine göre, elektronik imza oluşturma araçları, CWA 14169 standardına uygun ve TS ISO/IEC 15408 (-l,-2,-3)'e veya ISO/IEC 15408 (-1,-2,-3)'e göre en az EAL 4+ seviyesinde olmalıdır. Uygulamada güvenli elektronik imza oluşturma araçlarının EAL 4+ uygunluk belgeleri Telekomünikasyon Kurumu'na verilmektedir." [259]

"Elektronik imza oluşturma araçlarının uygunluk belgeleri için, hem aracın çipine (crypto processor) hem de işletim sistemine ait olmak üzere iki adet uygunluk belgesi veya aynı belge içerisinde her iki konunun birden kapsanması durumunu gerekli görülmektedir."[260] Ancak, ne Telekomünikasyon Kurumu ne de ESHS'ler, EAL 4+ seviyesine sahip elektronik imza oluşturma araçlarını deklare etmedikleri için kamuoyunda bu konuda bilgisizlik bulunmaktadır. Güvenli elektronik imzanın oluşturulması için güvenli elektronik imza oluşturma aracı ve nitelikli elektronik sertifika zorunlu unsurlar olmasına ve ESHS'lerin kamuoyuna açıklanmasına rağmen, güvenli elektronik imza oluşturma araçlarına ilişkin bu belirsizlik, güvenli elektronik imza altyapısının oluşturulmasına ve kullanıma ilişkin problemlerin ortaya çıkmasına sebebiyet verebilecektir.

[259] Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, İstanbul, 2004

[260] Déler-Castro G., Cruellas-Ibarz J., Electronic Signature Functionality and Security Requirements, Upgrade, Vol. 5, No. 3, June 2004 s. 23

3.2. ELEKTRONİK SİGORTACILIKTA E İMZA'NIN KULLANIM ALANI

3.2.1. E İmzada Güven Kavramı

Güven ve güvenlik konusu, nasıl kişiler arası ilişkilerde önemliyse, toplumların kullanımına sunulan teknolojik ürünlerin, verimli, bilinçli ve yaygın olarak kullanılabilmesi açısından da önemlidir. Bilgi ve sistem güvenliği kavramı, kişisel ve kurumsal güvenlik kapsamında, bilgiyi güvenli saklama, bilgi taşıma güvenliği, iletişim ağı güvenliği, işletim sistemi güvenliği, veri tabanı güvenliği, internet erişimi güvenliği ve sistem güvenliği gibi pek çok önemli konuyu kapsamaktadır. Genel olarak değerlendirildiğinde ise, elektronik imza ve açık anahtar altyapısının bu güvenliği sağlamakta en etkin yöntemlerden birisi olduğu görülmektedir. Bununla birlikte, bilgi ve iletişim teknolojileri alanında bilgi güvenliği ve mahremiyetin korunmasına yönelik olarak, gerek AB ülkeleri ile diğer bazı ülkelerde, gerekse ABD'de ortak olarak kullanılabilecek birçok uluslararası güvenlik standardı oluşturulmuş olsa da, bilişim teknolojileri her zaman yüksek risk altındadır. Bu itibarla öncelikle elektronik imzaların güvenli olabilmesi için, önceki bölümlerde belirtilen teknik kriterler ve güvenlik gerekleri mutlaka karşılanmalıdır. Bu işlemler için kullanılan şifreleme teknikleri ve diğer teknik kriterlerin, güvenliği sağlayacak şekilde seçilmesi ve teknolojik gelişmeler paralelinde güncellenmesi ve artırılması gerekmektedir.

Günümüzde, devletin, tüm vatandaşlarına elektronik ortamda etkin, verimli, hızlı, şeffaf, ucuz ve güvenilir hizmetler sunması ve bunu vatandaşlarının kullanımına aktarması için, her alanda bilgi ve iletişim teknolojilerinin yaygınlaştırılması şarttır. Ekonomik imkanları sınırlı olan ülkemizde, bu teknolojilerin yaygın olarak kullanılması önemli olduğu kadar, etkin kullanımı, karşılaşılabilecek tehlikelerin önceden bilinmesi ve gerekli tedbirlerin alınması da bir o kadar önemlidir. Yapılan bir araştırmada, kurum ve kuruluşların %90'dan fazlasının, hukuken geçerli olmasından dolayı, iş süreçlerini, kağıt belge ile yürüttüğü, dokümanların azımsanmayacak bir kısmının yanlış yerleştirilmiş ve bir daha bulunamayacak durumda olduğu, kullanıcıların haftanın bir gününü bedensel kayıt için kullandığı, belgelerin zaman içinde çok sayıda kopyasıyla karşılaşıldığı ve çalışanların zamanlarının büyük bir kısmını doküman yönetimine yönelik çalışmalara harcadığı

anlaşılmıştır. Bu ve buna benzer kayıpları azaltmak ve önlemek, ancak bilişim teknolojilerinin bilinçli ve etkin bir şekilde kullanılmasıyla mümkündür. Bunun için, herkesin belgelere ve verilere hızlı ve kolay erişiminin sağlanması, her zaman ulaşılabilen ve güvenilir arşiv sistemlerinin oluşturulması, iş süreçlerinin hızlandırılması ve belgelerin güvenliğinin sağlanması şarttır. Ancak bu sayede kurum ve kuruluşların iş verimlilikleri artırılabilecek, işlemler hızlandırılabilecek, maliyetler düşürülebilecek, müşteri memnuniyeti arttırılabilecek, zamandan ve mekandan tasarruf sağlanarak hayat daha yaşanılabilir bir hale gelebilecektir. Bunun sağlıklı olarak yapılabilmesinin tek yolu ise, bilgi güvenliği unsurlarını tamamıyla sağlayan ve hukuken de geçerli olan, elektronik imza ve açık anahtar altyapısının kullanılmasıdır. Bu teknolojilerinin kullanımının ve üretiminin artması, bilinçli internet kullanımının yaygınlaştırılmasıyla olacaktır. Ülkemizin mevcut haberleşme altyapısının genel olarak değerlendirildiğinde çok iyi durumda olmadığı ve bilişim teknolojileri kullanımının yeterli düzeyde olmadığı bilinmektedir. Devlet İstatistik Enstitüsü'nün 2004 yılı raporunda, bu oranın %14 seviyelerinde olduğu açıklanmıştır. Bu itibarla yeni politikalar ve yaklaşımlar üretilerek, mevcut altyapının hızının arttırılması, internet ve bilişim teknolojileri kullanımının yaygınlaştırılması için yeni stratejilerin geliştirilmesi gereklidir. Zira ancak haberleşme altyapısının geliştirilmesiyle, elektronik imza ve AAA yapıları, daha sağlıklı olarak kurulabilecek, işletilebilecek ve yaygınlaştırılabilecektir. Yine bilişim teknolojileri kullanımının artırılması için toplumsal ve kamusal bilgilendirme ve bilinçlendirme faaliyetlerinin yapılması önem arz etmektedir. Mevcut hukuki düzenlemeler değerlendirildiğinde, 5070 sayılı Elektronik imza Kanunu'nun bugünkü ihtiyaçları karşılayabilecek şekilde düzenlendiği ve özellikle Borçlar Kanunu ve Hukuk Usulü Muhakemeleri Kanunu'nda yapılan değişikliklerle Türkiye'de elektronik imzanın kullanımı için yasal altyapının hazır hale getirildiği söylenebilir. Ancak elektronik ortamdaki metinlerin yazılık işlevi ve nitelikli elektronik sertifikaya dayanmayan elektronik imzaların hukuki niteliği ve değeri hususlarında herhangi bir düzenlemenin mevcut olmayışı da önemli bir eksiklik olarak karşımıza çıkmaktadır. Oysa nitelikli bir elektronik sertifikaya dayanmayan elektronik imzaların da veri bütünlüğü dahil, el yazısı ile imzanın birçok işlevini yerine getirebildiği görülmektedir. Yine Elektronik İmza Direktifi'nin 5 inci maddesi gereğince elektronik imzaların nitelikli bir sertifikaya dayanmaması onun hukuki etki doğurmasına veya yargılamada delil olarak kullanılmasına engel teşkil etmemelidir.

Ülkemizde ESHS'lerin faaliyete başlaması, kullanılacak standartların ve sağlanması gereken teknik şartların belirlenmiş olması da düşünüldüğünde, elektronik imzaya geçmek için hiçbir engelin olmadığı görülmektedir. Ancak, buna rağmen elektronik imzaya geçiş beklenen düzeyde değildir. Bunun en önemli nedeni ise genel olarak kurumların elektronik ortamda iş yapmaya başlamamış olmasıdır. Bu itibarla, elektronik imzanın yaygınlaşmasında devlet öncü rol oynamalı, gelişmeler zamanında takip edilerek kamu kurum ve kuruluşlarının iş süreçlerini gözden geçirmesi sağlanmalı, e-devlet kurumu olmanın gerekleri yerine getirtilmelidir.

3.2.2 E-imza Kullanımının Yaygınlaşmasının Sigorta Sektörüne Etkileri

Elektronik sigortacılık, internet üzerinden yapılan bir ticari işlemdir. Bu ticari işlem, iki tarafa da sorumluluk yüklemektedir. Sigortayı talep edenler bu ticari işlemler üzerindeki sorunlar açık çözümlere kavuşmadan, çok büyük oranlarda elektronik sigorta işlemleri yapma konusunda çekingen davranmaktadırlar. Dünyanın pek çok bölgesinde, mevcut hukuksal çerçeve, güvenlikli ve güvenilebilir bir online (çevrimiçi) ticaret ortamı için yeterli garantileri sağlayamamaktadır. Buna bağlı olarak güvenlik ile ilgili konular; elektronik sigortacılığın daha yüksek boyutlara ulaşabilmesi için, hem ulusal hem uluslararası platformda çözüme kavuşturulmalıdır. Eğer bu sağlanırsa, nirbirlerini hiç görmemiş, coğrafi konumlarından habersiz, ticari durumlarını tespit edemeyecek kişi ve kuruluşlar, elektronik sigortacılık yapabileceklerdir. Dolayısıyla elektronik sigortacılıkta güvenliğin arttırılması, her türlü işlemin güvenilirliğinin sağlanması, elektronik iletişimde doğrulanabilirliğin tespiti önemli olacaktır.

Geleneksel üretimde poliçeler, merkezi üretim sistemi tarafından üretilmektedir. Üretilen bu poliçeler, müşteriye doğrudan postalama yoluyla ulaştırılmaktadır. İletişimin yüz yüze olmasından dolayı sorunları yerinde ve daha kolay çözme imkânı sağlanmaktadır. Müşteriyle yüzyüze iletişim kurulmasından dolayı, müşteriyi ikna etme olasılığı daha yüksektir. Geleneksel sigortada güven ortamının oluşması daha kolaydır. İnternet sigortacılığının sağladığı;

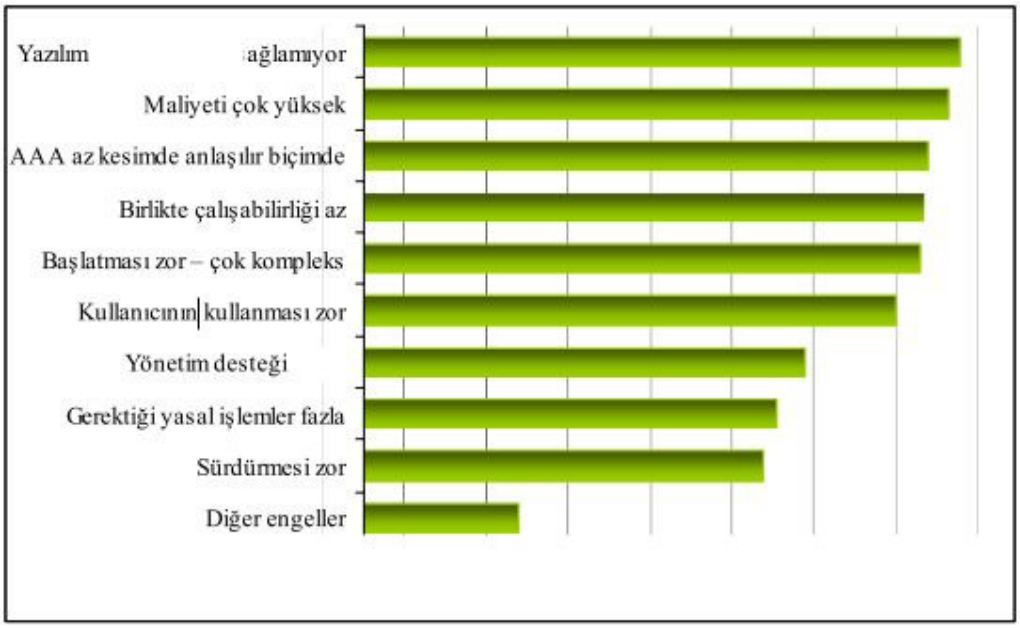
- İsteğimize uygun ürün oluşturabilme imkânı
- Rekabet yaratarak maliyet avantajı
- Kolay erişilebilirlik
- Müşterilerle ilgili veri tabanı oluşturabilmek
- Zaman ve iş gücü tasarrufu sağlamak
- Karşılaştırmalı teklifler oluşturulabilmek
- Şeffaflık
- İletişim kolaylığı

olarak pek çok avantaj olmasına rağmen; geleneksel sigortanın internet sigortacılığına tercih edilmesinin nedeni, alışkanlıklar ve güven duygusudur.

E-imza, elektronik sigortacılığa karşı duyulan güveni arttırabilecek önemli araçlardan birisidir. Güvenli bir altyapı ile oluşturulmuş e-imza kullanımının yaygınlaşması, kişilerin güven duygusuna etki edebilecektir. Güvenli bir ortamın oluşması halinde, sigortacılık uygulamalarının internet üzerinden yapılması da artabilecektir. E-imza kullanımının yaygınlaşması ve doğru kullanımı, elektronik sigorta sektörüne duyulan güvene olumlu katkı yapabilecektir.

3.3. ELEKTRONİK İMZANIN GELİŞMESİ İÇİN UYGULANABİLECEK YAPTIRIMLAR

Elektronik İmza, açık anahtar alt yapısı üzerinden işleyen bir sistemdir. Açık anahtar altyapısında mevcut bazı sorunlar, elektronik imzanın kullanım alanını da sınırlamaktadır. Açık Anahtar Altyapısının (AAA) temel görevi; elektronik ortamlarda haberleşen, işlem gören ve çalışan kişiler, kurumlar veya cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır. Yapısal Enformasyon Standartları İlerleme Kuruluşu (OASIS), AAA kullanımı ve devreye sokulması önündeki engelleri tanımlamak ve öncelikler belirlemek atamak üzere bir araştırma gerçekleştirmiştir.



2003 yılında yayınlanan bu raporda J. Dumortier, e-imza kullanımının yaygınlaştırılmasına olan yönelik açık konular ile Avrupa Komisyonunun etkinlikleri dikkate alınarak önemli hususlar aşağıda sunmuştur:

• Nitelikli sertifikalar ve ilgili hizmetler için doğal bir pazar talebi bulunmamaktadır. Avrupa'da e-imzaların en büyük uygulama alanı genel olarak kapalı kullanıcı ortamındaki elektronik bankacılık uygulamalarıyla bağlantılıdır ve böylece Direktifin kapsamı dışındadır. Direktifin kapsamı içerisinde, çok az sayıda uygulama kullanımdadır ve bunlar hemen hemen tamamıyla e-devlet uygulamaları ile sınırlıdır.

• Pek çok US'ları, uygulamalarının yasal olarak uyumlu olması için minimum Nitelikli E-imzalar gerektirdiğine inanmaktadır. Bu gerekli olsa da sertifikaların nitelikli olmadan da kullanabileceği bilinci olmadığından maliyet artışı ve karmaşıklıklara karşılaşabilmektedir.

• Hem ulusal hem de uluslararası boyutta e-imzanın uygulanması için isteksizlikler ve pazar boyutunun azlığı, e-imza uygulamalarının artırılmasının önündeki büyük engellerdir.

• Kısmen AB Direktifinin şu anda SSCD'ler hakkında çok yüksek gereksinimleri belirlemesi nedeniyle, bu gibi aygıtlar nadiren piyasada bulunmakta ve bu günden yeni artmaya başlamıştır.

• AB İmza Direktifin düzenleyici çerçevesi sertifika sağlayıcılar için oldukça ayrıntılı kurallar içerirken, sertifika sağlayıcıların diğer kategorileriyle ilgilenmemektedir.

Açık anahtar Altyapısı üzerinde yapılacak yeni düzenlemeler ile bu altyapının gelişmesi sağlanabilecektir. Bu altyapının geliştirilmesiyle, e-imza kullanımının yaygınlaşması da gözlenebilecektir.

Elektronik imzanın gelişmesi için mühim bir konu olan Açık Anahtar Altyapısı sistemlerinin e-imzalar ya e-devlet hizmetleri açısından uygulaması yalnızca başlangıç aşamasında olup bu konuda şu engellerle karşılaşılabilmektedir:

• Altyapıyı oluşturmak için gereken karmaşıklık ve başlangıç yatırımının yüksek olması.

• Maliyetlerin (kart okuyucu, yazılım) yüksekliği ve mevcut e-uygulamaların azlığı.

• Sertifika yönetiminde karşılaşan güçlükler, zaman damgası konusundaki standartların eksikliği, farklı platformda kullanılabilirlik gibi sorunlar.

• SM'leri ve ülkeler ve de ilgili yetki alanları arasında karşılıklı güven tanıma oluşturmanın yasal ve usul düzenleme yönleri yani, (e-imzalar ve akdi sorumluklar hakkındaki) politikaların, akdi sözleşmelerin ve yasal çerçeveler,

• Farklı SM'leri arasındaki teknik olarak uyumsuzluklarla karşılaşma ve özellikle uygulama düzeyinde kriptografik tekniklerin, sertifika özelliklerinin, akıllı kart teknolojilerinin ve sertifika yönetiminin oluşturulmasındaki zorluklar.

Açık ağ anahtar yapısının;

- Maliyetlerinin düşürülmesi
- Anlaşılabilir olması
- Kolay başlatılabilir

- Daha anlaşılabilir

olması sağlanırsa, anahtar yapısının kullanımında bir artış gözlenebilecektir. Bununla berbar de , e-imza kullanımı da daha güvenli bir şekilde yaygınlaşabilecektir.

Nitelikli e-imzaların kullanımı beklenenden daha düşüktür ve pazar bugün çok iyi gelişmiş değildir. Bugün için e-imza uygulamalarının e-devlet ve kişisel e-bankacılık hizmetleri ile bağlantılı olması ve ekonomik getirilim bugün için fazlaca olmasını bunun ana nedenlerinin başındadır. Hizmet sağlayıcılar birden fazla uygulama için e-imza geliştirmek üzere çok az teşvike sahiptir. Sadece bankacılık gibi paralı sektörlere çözümler sunmayı tercih etmektedirler. Devletin, e-imza kullanımı konusunda şirketleri ve bireyleri teşvik etmesi, e-imza kullanımının yaygınlaşmasına yardımcı olacaktır.

Elektronik imzanın içinde bulunduğu bir diğer sorun, elektronik arşivler için kapsamlı çözümlerin hala olmamasıdır. Elektronik arşivlerin düzgün saklanabilmesi, ulaşılabilir olması, 3. kişilerden gizli kalması şeklinde; varolan arşivleme ile ilgili sorunlar, e-imzanın kullanımı da etki edebilmektedir.

Bütün bunların dikkate alınmasıyla, e-imza kullanımının düzgün kullanımı ve yaygınlaştırılması sağlanabilecektir. E-imzanın yaygınlaşması, elektronik sigortacılıkta sıklıkla karşılaşılan güven sorununa olumlu bir etki yapabilecektir. Böylece, elektronik sigortacılığın yaygınlaşması sağlanabilecektir.

Sonuç

2004 yılında yürürlüğe giren "Elektronik İmza Kanunu" ile artık elektronik ortamda yapılacak iş ve işlemler de hukuken bağlayıcı hale gelmiştir. Zira, elektronik imza ile imzalanan bir elektronik belge, kanunda senet hükmünde kabul edilmiştir. Elektronik imzanın, gerçek ve güvenli bir yöntemle düzenlenmesi, ESHS tarafından oluşturulan sertifika, sertifika yönetimi ve denetimi ile hukuken ispatlanmaktadır. E-imzanın sağladığı en önemli fonksiyonlardan biri de ulusal boyutta güvenli haberleşmenin yanında, uluslararası boyutta da güvenli işlem yapılabilmesini sağlayabilmesidir. Bu itibarla ülkelerin elektronik imza konusunda işbirliği yaparak ortak düzenlemeler ya da uluslararası sözleşmeler yapmaları sistemin sağlıklı işleyişi açısından zorunlu görünmektedir. Çünkü elektronik sertifika, ülke içinden alınabileceği gibi yabancı bir elektronik sertifika sağlayıcısından da elde edilebilir, elektronik imza internet ortamında yurtdışındaki bir web sitesinden alışveriş yapmada da kullanılabilir.

Kanunumuzda yabancı elektronik sertifikalarla ilgili hükümler, yasanın 14 üncü maddesinde düzenlenmektedir. Bu maddede, yabancı bir ülkede kurulu bir ESHS tarafından verilen elektronik sertifikaların, hukuki sonuçlarının, milletlerarası anlaşmalarla belirleneceği belirtilmiştir. Ayrıca, yabancı bir ülkede kurulu bir ESHS tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir ESHS tarafından kabul edilmesi durumunda, bu elektronik sertifikaların nitelikli elektronik sertifika sayılacağı ve bu elektronik sertifikaların kullanılması sonucunda doğacak zararlardan, Türkiye'deki ESHS'nin sorumlu olacağı hüküm altına alınmıştır. Elektronik imza, başta elektronik satın alma ve satış işlemleri olmak üzere, belge hazırlama ve onaylama gibi işlemlerin birçoğunda kullanılacak olduğu için, elektronik uygulamaların olmazsa olmazını oluşturan bir altyapıdır.

Öte yandan elektronik imza kullanımı ile karşılıklı imzalanması gereken belgelerin ve yine kağıt ortamındaki kopyalarının, taraflar arasında fiziksel olarak taşınması gerekmeyecektir. Bilgi ve belgeler, kullanıcıların izni dahilinde çevrimiçi olarak elektronik ortamda taşınabilecek ve böylelikle, kağıt tasarrufu sağlanabilecektir. Bu bilgi ve belgelerin taraflar arasında taşınması elektronik ortamdan yapılacağı için zaman ve hizmet tasarrufu da sağlanacaktır. Yine elektronik imza ve AAA'nın kullanılması, elektronik ortamlarda yapılan dolandırıcılığı çok az seviyelere düşürebileceğinden, elektronik ticaretin, e-iş ve e-devlet uygulamalarının önü açılacaktır. Bu yapının

kullanılmaya başlanması ve yaygınlaşmasıyla, iş ve iş süreçleri bundan olumlu yönde etkilenecektir. İş ve ticarette sınırlar ortadan kalkacak, iş yapış ve sunuş metodolojileri değişecek, hizmetler hızlanacak, hizmet alış ve sunuş türleri farklılaşacak, karşılaşılacak problemler azalacak ve ticari yaşam boyut değiştirecektir.

Elektronik imza, eskiden filmlere konu olan ancak günümüz dünyasında artık bir ihtiyaç haline gelen dijital ortamlarda bilgi alışverişinin temelinde yerini almıştır. Artık devletler vatandaşına daha fazla imkan sağlayabilmek için daha hızlı iletişim araçlarını tercih etmektedir. Bu da elektronik ortamın güvenilir olarak kullanılması, daha korunaklı hale getirilmesi yoluyla olmaktadır. Elektronik imza tam bu noktada iletişimin güvenliğini sağlamak için devreye girmektedir. Dağıtımın ve ulaştırmanın güvenliğini koruma görevi üstlenen sistem tam bir kapalı kutu olarak çalışmayı sürdürmektedir. Bünyesinde dış etkenlerden etkilenmeyecek bir sistem barındırması gereken elektronik imzanın kullanıcıların;

- İmzalayanın tanımlanması

- Veri bütünlüğünün kontrol edilmesi

- Gizliliğin korunduğunun teyidi

- İnkar etmenin engellenmesi

- Zamanlama bilgisi

gibi ihtiyaçlarını da karşılaması gerekmektedir. Bunlar elektronik imza üreticilerince kullanıcılara sağlanan hizmetlerdir. Günümüzde elektronik imza her alanda faaliyet gösterme adayı olup teknoloji ile içiçe yaşayan kurum veya bireylerin kaçınılmazı olmuştur. Elektronik imza sadece yüksek maliyeti ile sınırlı kullanıcılara hitap eden bir sistem bütünü olmaktan çıkarılıp herkes tarafından kullanılabilecek seviyeye getirilmesi gereklidir. Bunun önündeki bazı büyük engeller;

- Teknolojiden kaynaklanmakta olan uygulama güçlükleri

- Yüksek uygulama maliyetleri

- Bilgi ve bilinç eksikliği olarak sıralayabiliriz. Bu engellerin aşılarak elektronik imzanın toplum hayatına geçirilmesi durumunda bir bütün olarak devlet daha fazla verimli bir hale gelecektir.

Keza, elektronik imza ve AAA, ihtiyaç duyulan güvenliği, gizliliği, veri bütünlüğünü, kimlik doğrulamasını, inkar edilememezliği ve iş sürekliliğini sağladığından; güvenli elektronik iletişimi sağlayacaktır. Elektronik ortam kullanıcılarının kimliklerinin doğrulanması e-postaların ve dosyaların şifrelenmesi ve imzalanması mümkün olacaktır. Yazılımların güvenli olarak alınıp kullanılmasıyla sahte yazılım kullanımı önlenebilecek, sunucuların gerçek sunucular olduğunun teyidi yapılabilecek, daha güvenli haberleşmelerin önü açılarak, güvenli elektronik ortamların veya merkezlerin oluşturulması bu sayede sağlanabilecektir.

Bu yaptırımlardan bir diğeri de, e-imzaya olan güvenin arttırılması olacaktır. e-devlet hizmetlerinin yaygınlaşması ve internet kullanımın artmasıyla beraber ortaya çıkan güvenlik açıkları, elektronik işlemlere karşı talebe etki etmektedir. Güven sorununun düzeltilmesi, e-imza uygulamalarının yaygınlaşmasına ve genelce kullanılmasını sağlayacaktır.

E-imza uygulamalarının yaygınlaşması, bir elektronik ticaret türü olan elektronik sigortacılığı da etkilecek, internet üzerinden yapılan işlemlerin güvenliğinin sağlanması nedeniyle internet üzerinden sigorta işlemlerinin yapılması daha sıklıkla gözlemlenebilecektir. Böylece, güvenli e imza uygulamalarının artması, elektronik sigorta işlemlerini de etki edecektir.

Kısaca; yapılması gerekenler olmakla birlikte, mevcut elektronik imza ve AAA uygulamaları, toplumsal değişim ve dönüşümde önemli bir rol oynayarak, ekonomik, teknik, hukuki ve sosyal gelişmeler açısından müspet sonuçlar doğuracak, elektronik sigortacılık sektörününün yapılanmasına ve yaygınlaşmasına büyük katkılar sağlayacaktır.

Kaynakça

Altınışık, U. (2003) Elektronik Sözleşmeler. İstanbul: Seçkin Yayınevi.

Akıncı, Ş. (2006) Borçlar Hukuku Bilgisi, İstanbul: Bahçıvanlar Basım.

Arıkan, S. (1999) Dünyada ve Türkiye'de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım, Ankara: Yetkin Yayınları.

Berber, K. A. (2001) Şekil ve Dijital İmza, Elektronikteki Gelişmeler ve Hukuk, Ankara: Bankacılar Dergisi.

Berber, L. K. Lostar, M. (2006) Bilişimde Biyometrik Yöntemler, Ankara: Yetkin Yayınları.

Biçkin, İ. (2004) Elektronik İmza Kanunu ve Getirdiği Düzenlemeler, Ankara: Yargıtay Dergisi.

Bozbel, S. (2006) Internet Alan Adlarının (Domain Names) Korunmasında Icann Tahkim Usulü, Ankara: Seçkin Yayıncılık.

Bozbel, Savaş, (2001) İnternet Üzerinden Yapılan Hukuki İşlemler, Ankara: Yargıtay Dergisi.

Çak, M. (2002) Dünyada ve Türkiye'de Elektronik Ticaret ve Vergilendirilmesi, İstanbul: İstanbul Ticaret Odası Yayını.

Çeker, M. (2003) Yargıtay Kararları Işığında Sigorta Hukuku, Adana: Karahan Yayınları.

Ertaş, S, (2000) Elektronik Ticaretin Tanımı, Gelişimi, Avantajları, Güvenliği, Ekonomik, Toplumsal, Teknik ve Yasal Yönleriyle Elektronik Ticaret, Derleyen Veysel Bozkurt, İstanbul: Alfa Yayınları.

Devrim, J (2000) Bilgisayar & İnternet Sözlüğü, İstanbul: Hayat Yayınları.

Dönmez, C. (2002) Regulation of Electronic Signatures and Protection of Private Keys, Sheffield: University of Sheffield Department of Law.

Erol, H.T. (2003). Electronic Signatures, İstanbul: Beta Yayınları.

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

Erturgut, M. (2004). Elektronik İmza Kanunu Bakımından E-belge ve E-imza. İstanbul: Bankacılar Dergisi.

Eren, F. (1998) Borçlar Hukuku Genel Hükümler. İstanbul: Beta Basım Yayın.

Erzincan, Ö. D. (2004) E-imza Deneyimi, İstanbul: Telekom Dünyası Dergisi.

ETSI TS, Electronic Signatures and Infrastructures (2005) Valbonne, France: CMS Advanced Electronic Signatures (CAdES).

Falcıoğlu, M. K (2004) Karşılaştırmalı Hukuk ve Türk Hukukunda Elektronik Satım Sözleşmesi ve Kurulması. Ankara: Yetkin Yayınları.

Ford, W. (2000) Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption

Genç, H.(2006) http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/PKI-problems.pdf

Gezder, Ü. (2004) Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması, İstanbul: Vedat Kitapçılık.

Grant, G.L. (1997) Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks

Haşıloğlu, (2001) S. Sigortacılık Sektöründe Sanal Organizasyon Teknolojileri: İnternet, Intranet ve Extranet, Reasürör Dergisi, Sayı: 39.

Haşıloğlu, S. (1999) Enformasyon Toplumunda Elektronik Ticaretin ve Stratejileri, İstanbul: Türkmen Kitabevi.

İnal, E. (2005) E-Ticaret Hukukundaki Gelişmeler ve Internette Sözleşmelerin Kurulması, İstanbul: Vedat Kitapçılık.

Katz, J. (2008) Digital Signatures (Advances In Informatıon Security)

Kayıhan, Ş. ve Yıldız, H. (2004) Habib, Elektronik Ticaretin Hukuki ve Vergi Boyutu, Ankara: Seçkin Yayıncılık.

Kepenek, Y. (2000) Ekonomik Yönleriyle Ekonomik Ticaret, İstanbul: Alfa Basım Yayım.

Keser, L. B. (2000), İmzalıyorum O Halde Varım, Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler Dijital İmzalı Belgelerin Hukuki Değeri. İstanbul: TBB Dergisi Yayınları

Keser, L. B. (2002) İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza

Kender, R. (2005) Rayegan Kender, Türkiye'de Hususi Sigorta Hukuku, Sigorta Müessesesi-Sigorta Sözleşmesi, İstanbul: Arıkan Basım

Kubilay, H. (2003) Uygulamalı Özel Sigorta Hukuku, İzmir: Barış Yayınları.

Kocasakal, (2003). Ö. Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti. İstanbul: Vedat Kitapçılık.

Kuru, B. (2001) Hukuk Muhakemeleri Usulü, İstanbul: Demir Yayınları.

Memiş, T. (1999). Avrupa Birliği ve Türk Hukukunda Sigorta Aracıları, İstanbul: Reasürör Dergisi Yayınları. Sayı: 34

Nomer, C. (2000) Sigortanın Genel Prensipleri, İstanbul: Ceyma Matbaacılık.

Orta, M. (2007) E – kavramlar, Uygulamalı Elektronik İmza Semineri.

Öngören, G. (2006). İnternet Hukuku. İstanbul: Öngören Hukuk Yayınları.

Özer, F.G. (2004) Sermaye Piyasalarında Elektronik İmzanın Kullanım Alanları, Bilgi İşlem Merkezi Yöneticileri Semineri (BİMY) 8-11 Nisan 2004, Aksu-Antalya.

Özceylan C. (2002) E-Bankacılık, İstanbul: Türkiye İş Bankası Yayınları.

Sayın, S. (2005) Türk Hukukunda Kredi Kartı ve Kredi Kartının Hukuka Aykırı Kullanılmasından Doğan Hukuki Sorumluluk. İstanbul: Kazancı Hukuk Yayınevi.

Sevim, T. (2004) Elektronik İmzanın Hukuksal Boyutları (Mevcut Durum, Eksiklikler ve Çözüm Önerileri), İstanbul: II. Türkiye Bilişim Şurası, Hukuk Çalışma Grubu.

Sevimli, K. (2001) Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası, Prof.Dr.Hayri Domaniç' e 80. Yaş Günü Armağanı, İstanbul: Beta Basım Yayım.

Sözer, B. (2002) Elektronik Sözleşmeler, İstanbul: Beta Basım Yayım.

Şenocak, Z. (2001), Dijital İmza ve İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması, Ankara: AÜHFD.

Sağıroğlu, Ş. Alkan. (2005) Her Yönüyle Elektronik İmza. Ankara: Grafiker Yayınları.

Schellekens, M.H.M. (2004) Electronic Signatures: Authentication Technology from a Legal Perspective Piper, Digital Signatures Security and Controls.

Sigma-Swiss Re. (05/2006) World Insurance in 2005.

Sigma-Swiss Re. (04.2007) World Insurance in 2006.

Pekcanıtez, H. (2001) Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri. İzmir: Uluslararası İnternet Hukuku Sempozyumu.

Timur, N. Banka ve Sigorta Pazarlaması (2007) Eskişehir: Anadolu Üniversitesi Yayını.

Topaloğlu, M. (2006). Bilişim Hukuku. İstanbul: Karahan Kitabevi Yayınları.

TBD, Kamu BİB. (2005) Kamu Bilişim Platformu, E-İmzanın Toplumsal Boyutu.

Ulaş, I. (1992) Uygulamalı Sigorta Hukuku Mal ve Sorumluluk Sigortaları, Ankara: Turhan Kitabevi.

Uralcan, Ş. (2006) Temel Sigorta Bilgileri ve Sigorta Sektörünün Yapısal Analizi, İstanbul: Bilyay Yayınları.

Topaloğlu, M. (2005) Bilişim Hukuku, Ankara: Karahan Kitabevi.

Tunçomağ, K. (1976) Türk Borçlar Hukuku, İstanbul: İstanbul Barosu Yayınları.

Yazıcı, S. Yanık, S. (2002) Elektronik Sigortacılık: Elektronik Ticaretin Sigorta Sektörüne Etkileri. İstanbul: Der Yayınları.

Yenidünya, C. Değirmenci, O. (2003) Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul: Legal Yayıncılık.

Diğer Kaynaklar

Kanun, Rapor, Yönetmelik ve Tebliğler

Elektronik Ticaret Koordinasyon Kurulu (ETKK) Hukuk Alt Çalışma Grubu.

Elektronik Veri, Elektronik Sözleşme Ve Elektronik İmza Kanunu Tasarısı Taslağı, 2002.

Telekomünikasyon Kurumu. Elektronik İmza ile ilgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, 6 Ocak 2005.

4487 Sayılı. Sermaye Piyasası Kanunu. Kabul Tarihi: 15.12.1999, Resmi Gazete Sayısı:24622, Resmi Gazete Tarihi: 26.12.2001.

5070 Sayılı. Elektronik İmza Kanunu. Kabul Tarihi: 15.01.2004, Resmi Gazete Sayısı:25355, Resmi Gazete Tarihi:23.01.2004.

4982 Sayılı. Bilgi Edinme Hakkı Kanunu. Kabul Tarihi: 09.10.2004, Resmi Gazete Sayısı:25269, Resmi Gazete Tarihi: 24/10/2003.

1086 Sayılı. Hukuk Usulü Muhakemeleri Kanunu. Kabul Tarihi: 18.06.1927, Resmi Gazete Sayısı:622, Resmi Gazete Tarihi: 02.04.1927.

Elektronik Ticaret Koordinasyon Kurulu Raporları

Tezler

Akıncı, S. (2002) Elektronik Ticarette Pazarlama Stratejileri ve Bir Uygulama, Yayınlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya.

Çatak, S. (2002) Elektronik Ticaret ve Uygulamaları, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Karaca, D. (2006) Avrupa Birliği'nde E-Ticaret Kavramı, AB'de ve Türkiye'de Bu Konuda Yapılan Hazırlıklar, Çalışmalar ve E-Ticaretin Vergilendirilmesi, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul.

Canberk, G. (2005) Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yayımlanmamış Yüksek Lisan Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

Çifti, Ç. (2005) Legal Aspects Of Ict Implementatıon In Turkısh Constructıon Industry; Applicability Of Elegal Framework, Thesis Submitted To The

Graduate. School Of Natural And Applied Sciences Of Middle East Technical University, Ankara.

Yalçınkaya, B. (2008) Elektronik İmzalı Belgelerin Yönetimi ve Arşivlenmesi, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi, Türkiyat Araştırmaları Entitüsü Bilgi ve Belge Yönetimi, İstanbul.

KISALTMALAR

AAA Açık Anahtar Altyapısı

BK Borçlar Kanunu

CA Certification Authority (Sertifika Otoritesi)

CEN European Committee for Standardisation

COBIT Control Objectives for Information and Related Technologies

EC European Commission

ETSI European Telecommunications Standards Institute

f. Fıkra

FIPS Federal Information Processing Standards

HUMK Hukuk Usulü Muhakemeleri Kanunu

ISACA Infornation Systems Audit and Control Association

İİK İcra İflas Kanunu

ITSEC Information Technology Security Evaluation Criteria

md. Madde

PDA Personal Digital Assistant

PIN Personal Identification Number

PKI Public Key Infrastructure

RFC Request For Comments

RSA Rivest, Shalmir, Adleman

SigG Signaturgesetz (İmza Kanunu)