ELEKTRONİK SİGORTACILIKTA E-İMZA

Ayten ÇETİN*
Zehra Cahide ÇİTLİ**

Özet

İnsanların kullanımına sunulan birçok yeni teknolojik altyapının sergilediği kolaylık ve kullanışlığı gölgeleyebilecek en önemli etkenlerin başında, bilgi ve bilgisayar güvenliği gelmektedir. Elektronik sigortacılık, 1996'da Java'nın kullanıma başlanmasıyla gelişen e-ticaretin bir alt dalı konumundadır. E-sigortacılık, sigortalının ihtiyaçlarına yönelik poliçeler hazırlanmasına, aradaki iletişimin daha kısa zamanda kurulmasına, teminatın esneklikle belirlenmesine ve risk idaresi desteğinin daha etkili olmasına imkân sağlamanın yanında, internetin herkese açık bir ağ olması beraberinde güvenlik sorununu getirmektedir.

Anahtar Kelimeler: Elektronik İmza, Elektronik Ticaret, E-Ticaret, Elektronik Sigorta, E-Sigorta, İnternet Sigortacılığı, Online Sigortacılık.
JEL Sınıflaması: G22

Abstract

The question of security of information and computers is one of the factors overshadowing facilities and efficiencies provided by the modern technology. Electronic Insurance is a sub-department of e-commerce which is developed after begging of Java-usage in 1996. E- Insurance, helps preparation of products of insureds' needs, faster communication, determination of more flexible covers and more effective risk management. However it also brings security problems as the internet being an open source.

Keywords: Electronic Sign, Electronic Commerce, E-Commerce, Electronic Insurance, E-Insurance, Insurance Over Internet, Online Insurance.
JEL Classification: G22

1.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

* Yrd.Doç.Dr., Marmara Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Muhasebe Finansman Anabilim Dalı, acetin@marmara.edu.tr
** Yüksek Lisans Öğrencisi, Marmara Üniversitesi, Bankacılık ve Sigortacılık Enstitüsü, Sigortacılık Anabilim Dalı, cahidecitli@gmail.com

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.

2.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 (Berber, 2001, 503). 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. 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.

2.1 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. 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 (Erturgut, 2003, 66).

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 (Arıkan, 1999, 151).

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 (Arıkan, 1999, 151).

2.2 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 (Topaloğlu, 2006, 120).

3.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 (Yaltı, 2001, 151). Belgenin sözlük anlamı, bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika, dokümandır. 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.

3.1. Sözleşmeler

Elektronik sözleşmeler, elektronik iletişim araçları kullanılarak yapılan sözleşmeler olarak tanımlanmaktadır. Elektronik iletişim araçlarıyla yapılan işlemleri, bu kapsamda elektronik sözleşme olarak saymak gerekmektedir (Topaloğlu, 2005, 46). 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.

3.2. 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.

Elektronik sertifika günlük hayatta kullanılan ehliyet, pasaport gibi kimlik kartlarını elektronik ortamdaki karşılığıdır denilebilir. Elektronik sertifikalar sertifika otoriteleri tarafından düzenlenir (Erzincan, 2004, 32). Elektronik sertifika, kullanıcı adıyla onun açık anahtarını içeren ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik belgedir (Ergün, 2004, 64). 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.

4. 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 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.

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.

4.1. Dijital İmza Yöntemi ile Oluşturulmayan Elektronik İmzalar

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.

Biyometrik Yöntemlere Dayalı Elektronik İmzalar: Biyometrik imzalar, "bir kişinin kimliğinin doğrulanması için kullanılan ölçülebilir fizyolojik ve/veya davranışsal özellikler olarak tanımlanabilir (Erol, 2003, 42). 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 (Erol, 2003, 47) 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 (Schellkens, 2004, 76). 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 (Berber, 2006, 49). Bu sebeplerle, günümüzde biyometrik imzaların dijital imzaların alternatifi olarak kullanılması düşüncesi düşünülmemesi güvenlik açısından yeterli olamamaktadır.

4.2. Dijital İmzalar (Sayısal İmzalar)

Sayısal imza, gönderilecek (imzalanacak) olan elektronik metnin şifrelenmesi yöntemidir. 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 (Sağıroğlu, 2005, 72).

4.3 E-imza 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 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 (Altınışık, 2003, 91).

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 (Altınışık, 2003, 91).

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 (Sağıroğlu, 2005, 71).

Bu şekilde mesajın bütünlük kontrolü ve kimlik tespiti fonksiyonları gerçekleştirilmiş olur. Ancak bu fonksiyonların yanında gizlilik de isteniyorsa bu durumda şifreleme metodu kullanılabilir.

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 (Çamurdan, 2003, 52) 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 (Çamurdan, 2003, 55).

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 (Çamurdan, 2003, 56).

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 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.

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 (Tüfekçi, 2003, 88). 5070 Sayılı Kanun 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 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.

6. ELEKTRONİK TİCARET

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 giderek artan ölçüde dünya genelinde tartışılan bir kavram olarak karşımıza çıkmaya başlamıştır (İnalöz, 2003, 64).

Dünya Ticaret Örgütü (DTÖ)'ne göre; elektronik ticaret, mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılmasıdır (ASO, 1998, 29). 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 (ITO, 1998, 76).

"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 paylaşılmasıdır. Bu tanımlamaya göre elektronik ticaret kısaca, elektronik ortamda ticari iş, işlem ve fiillerde bulunmaktır.

7. ELEKTRONİK SİGORTACILIK

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. 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. Rekabetnedeniyle sektörde fiyatlar oldukça düşmüştür. 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.

7.1. Kapsamı ve Araçları

Bir sigorta poliçesini satın alma süreci, araştırma ile başlamaktadır (Uralcan, 2006, 208). 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.

7.2. 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 verilebilir. 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: (Tanberk, 2001, 37) 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.

7.3. Elektronik Sigortacılıkta Sözleşme Kavramı

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.

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 (Oğuzman, 2001, 126). 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 (Gezder, 2004, 81). 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) (Tunçomağ, 1976, 49) bu öneriyi uygun gördüğünü bildiren karşı irade beyanına da kabul adı verilir. (Tunçomağ, 1976, 49) 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 (Gezder, 2004, 84). Burada irade beyanının oluşturulması ve karşı tarafa iletilmesinde bilgisayardan faydalanılmaktadır. Dolayısıyla beyanda bulunanın arzusuna uygundur. Bu nedenle burada da normal insan tarafından yapılmış bir iradenin mevcudiyeti kabul edilmektedir. "Elektronik sigorta sözleşmelerin kurulması için; icaba davet, icap, kabul aşamalarının gerçekleşmesi gerekmektedir." (Altınışık, 2003, 42)

7.4. Elektronik Sigortacılıkta Karşılaşılan 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. (Yazıcı, Yanık, 2002, 142)

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. (Yazıcı, Yanık, 2002, 12) Bu da e-sigortacılığın önündeki engellerden biridir.

8. E İMZA KAVRAMI VE ÖNEMİ

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. (Öngören, 2006, 64) 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.

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 (Collins, 2004, 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.

8.1. Elektronik Sigortacılıkta E İmza'nın Kullanım Alanı

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.

8.2. 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 (ETSI, 2005, 28).

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 (FESA, 2004, 1). 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.

8.3. Elektronik İmzanın Gelişmesi İçin Uygulanabilecek Yaptırımlar

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. (Dzambasow, 2001, 3) 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: (Dumortier, 2004, 5)

• 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.

• 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.

9. 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.

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.

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

Çamurdan, Ç. (2003) Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme, TBD 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.

Ergün, Ö. (2004) 5070 sayılı Elektronik İmza Kanunu ve Dijital İmza, Türkiye Noterler Birliği Hukuk Dergisi, Sayı:122.

Erturgut, M. Elektronik İmza Kanunu, e-Belge ve e-İmza (Hukuki Açıdan Tanıtım Ve Değerlendirme) Bankacılar Dergisi, 2003, Sayı. 48

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).

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

Haşıloğlu, (2001) S. Sigortacılık Sektöründe Sanal Organizasyon Teknolojileri: İnternet, Intranet ve Extranet, İstanbul: 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.

Oğuzman, K. (2000) Borçlar Hukuku Genel Hükümler, Gözden Geçirilmiş ve Genişletilmiş 3.Baskı, İstanbul: Filiz Kitabevi.

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

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.

Schellkens, M.H.M (2004) Electronic Signatures Authentication Technology from a Legal Perspective, Netherlands.

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.

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.

Yaltı, B. (2001) E-İmza ve E-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-I, Vergi Sorunları Dergisi, s.151

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, Dergi, Rapor, Yönetmelik ve Tebliğler

ATO (Ankara Ticaret Odası)

İTO (İstanbul Ticaret Odası)

Collins. T. (2004) DESS Droit de l'Internet - Administration – Entreprises, Aspects techniques et juridiques des infrastructures de gestion de clés publiques, Unıversıte Parıs-I Pantheon-Sorbonne, France.

Dzambasow Y.A., Sabo, J. (2001) PKI Policy White Paper, PKI Forum, USA.

Dumortier J., Kelm S., (2004) The Legal and Market. Aspects of Electronic Signatures, European Commission, Brussels.

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

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

İnalöz, A. (2003) Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Uzmanlık Tezi.

Tüfekçi, T. (2003) Elektronik İmza Niçin Yaygınlaşmıyor? TÜBİTAK. Bilgi Teknolojileri ve Elektronik Araştırma Enstitüsü, Türkiye Bilişim Haftası.

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.

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.

Tanberk, B. (2001) "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.