DİJİTAL İMZANIN TİCARİ HAYATTA KULLANILMASI VE DÜZENLENMESİ

The Use And Regulation Of Digital Signature In Business Life

Yrd.Doç.Dr. Salâhattin ALTUNDAĞ*

ÖZET

Elektronik ticaretin en önemli unsuru güvenliktir. Bu güvenliğe ulaşma hususunda, dijital imza günümüzde başvurulan en önemli araçlardan biridir. Ülkemizde bu konuyu içeren bir kanunun bulunmaması dijital imzanın da uygulanmasını mümkün kılmamaktaydı. Elektronik imza kanunun kabulüyle artık bu boşluk giderilmiştir.

Bu çalışmamızda; elektronik imza kanunuyla uygulanması mümkün olacak olan dijital imzanın, ticaret hayattaki kullanımının nasıl olacağı, yararlarının neler olduğu, bu imzanın nasıl elde edileceği ve elde edilirken nelere dikkat edilmesi gerektiği ele alınmıştır.

Anahtar Kelimeler

Dijital İmza, e-İmza, e-Ticaret, e-Ticarette Güvenlik, Elektronik İmza Kanunu.

ABSTRACT

The most important dimension of e-commerce is security. Digital signature is one of most significant instruments applied today to attain this security. Due to the fact that there was no law related to this subject until last year, it was impossible to apply digital signature in out country. By the acceptance of the Law of Electronic Signature, this deficiency has been fulfilled.

In this study, how it will be to use electronic signature in business life, the advantages of it, how to be obtained and what particular paints should be considered while obtaining it will be explained.

Key words

Digital Signature, e-Signature, e-Commerce, Security In e-Commerce, The Law of Electronic Signature.

* Dicle Üniversitesi Diyarbakır Meslek Yüksekokulu Bilgisayarlı Muhasebe ve Vergi Uygulamaları Programı, Program Başkanı. saltundag@dicle.edu.tr

I- GİRİŞ

Elektronik ticaret; 1980'li yıllardan beridir, büyük boyuttaki şirketler için bilinen ve uygulanan bir ticaret yöntemidir. Elektronik sistemler; bu yıllardan itibaren sipariş, stok kontrolü, faturalama ve benzeri pek çok modern işletme unsurlarında kullanılmaya başlanmıştı.

Bu sistemler, bilgisayarların birbirine bağlı olduğu ağlar yoluyla kullanılmaktaydı. Uzun yıllar boyunca birlikte çalışan işletmeler ve güvenilir kişiler arasında oluşturuluyordu. Kontrol, yine bu ağları yönlendirenlerce yapılıyordu. Ödeme ve teslim işlemleri ise yine geleneksel yollarla yapılmaktaydı. Bu nedenle, o dönemlerde güvenliğe büyük önem duyulmamaktaydı.

Bu arada bilgisayar teknolojisi son derece hızlı bir şekilde gelişmekti. Buna paralele olarak; internetin kullanıma açılmasıyla, elektronik ticaret de değişti ve genişledi. Bilgisayarların birbirine bağlı olduğu ağlar kamuya, hatta dünyanın tüm coğrafi bölgelerine açıldı. Ağında, bilgi transferinin ötesinde, artık önemli sözleşmeler ve büyük anlaşmalar akdedilmeye başlandı. Ödemelerin çevrimiçi ve eş zamanlı yapılmasına imkân veren teknolojiler gelişti. Bu gelişim, ticareti inanılmaz boyutlara sürükleye başladı. Birbirlerini hiç tanımayan ve aralarında hiç bir güven unsuru bulunmayan şirketler ve/veya kişiler arasıda ticari akitler yapılmaya başlandı. Geleneksel pazarlara paralel olarak, elektronik pazarlar ortaya çıktı. Teknik gelişmeler doğrultusunda tüketim, üretim, pazarlama, ödeme gibi ticari işlem biçimlerini yeniden şekillendi. Artık küresel bir sayısal ekonomiden söz edilmektedir.[1]

Tüm bu gelişmeler, acil tedbirlerin de alınması şartını ortaya çıkmıştır. İnternet üzerinde yapılan alış verişin güvenliği, güvenirliliği ve bağlayıcılığı, acil tedbirleri gerektirmiştir. Örneğin, sanal ortamda hazırladığımız bir mektup veya bir mesaj nasıl bağlayıcı olacaktır? Şüphesiz bunu hazırlayan kişinin imzası ile… Fakat bir mesajı veya bir mektubu elektronik olarak nasıl imzalayabileceğiz ve bu imza için hukuki geçerlilik mevcut mu?

Bilgisayar ve internet hayatımız her alanını işgal etmiştir. Birbirlerinden kilometrelerce uzakta bulunan kişiler internet üzerinden haberleşme yapmakta, alışveriş yapmakta veya sözleşme akdetmektedir. Bu güncel ihtiyaçlar, kanunların yeniden gözden geçirilmesi zorunluluğunu doğurmuştur.

---

[1] Wolfgang **KILLIAN**, "**Digital Communication and Contract Law**", Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002, s.161.

Sözleşmelerin, şekline ve ispatına ilişkin kanuni hükümler; bu işlemlerin, elektronik yoldan da yapılmasına olanak verecek şekilde yeniden yapılandırılmalıdır. Bu durum, yapılacak sözleşmelerin geçerli olması ve tarafları bağlaması için; sözleşme ile borç altına giren taraf veya tarafların imzalarının, elektronik metinlerde de yer alması gerektirecektir. Bu sorunun cevabını bulmak ise bilgi teknolojisi uzmanlarına düşmüştür. Elektronik belgeleri nasıl imzalanacağı sorusu, günümüzde "**Dijital İmza**" veya "**Elektronik İmza**" olarak adlandırılan teknik işlemle cevaplandırılmaktadır.

Dijital imzalar, hazırlanışı karmaşık olmasına rağmen en güvenilir çözümdür**.** Ancak, günümüzde birçok şirketin web sayfalarının taklit edildiği, Hacker'ların kol gezdiği internet ortamında dijital imzanın % 100'e yakın bir garanti temin edeceği düşünülemez.

İçinde bulunduğumuz yüzyıl "**Bilişim ve Teknoloji Çağı**" olarak adlandırılmaktadır. Bu çağın teknolojisi ise iki ucu keskin kılıca benzemektedir. İnternet'in sunduğu yeni teknolojik olanakların, rekabet ve gelişmişlik adına sevindirici faydalar sağladığı doğrudur. Bu teknolojileri kullanarak insanların; daha kolay zarar verebilmelerini, her türlü yolsuzluğu, aldatma ve hileyi çok daha kolay ve inandırıcı yapabilmelerini de mümkün kıldığını unutmamak gerekir.

Bilişim teknolojilerindeki bu akıl almaz ilerlemelerin, tüm kanun yapıcı ve uygulayıcılarını acil eyleme çağırdığını belirttik. Evet, teknoloji, hukuken sıkıdüzen ve disiplin altına alınmalıdır. Fakat kimilerine göre teknolojik gelişme, hukuk dünyasını zannedildiğinden çok daha fazla etkileyecektir; hukuk, bugüne kadar bilişim ortamına ilişkin düzenlemeler konusunda çok yavaş kalmıştır.

Bütün engellere rağmen; günümüzde ve gelecekte, elektronik ticaret ve dijital imzanın, hayatımızın çeşitli alanlarında yaygın olarak kullanılması kaçınılmazdır. Muhtemel bütün uygulamalarda ise birinci derecede, güvenlik boyutu öne çıkacaktır. Bu durum, doğrudan olduğu kadar dolaylı etkileri vasıtasıyla da elektronik ticaret boyutunu önemli ölçüde etkileyecektir. Bu nedenle, çalışmamızda; güvenlik boyutu ve bunu sağlamada en önemli rolü alan dijital imza üzerinde önemle durduk.

Elektronik imza e-devlet yolunda çok önemli bir adımdır. e-Türkiye Dönüşüm Projesinin alt yapısının asli unsurunu da "Elektronik İmza" oluşturmaktadır. Elektronik ticaretin de kullanım vasıtası elektronik imza olduğundan, çalışmamızın ana temasını elektronik imza ve onun en güvenli çeşidi olan dijital imza oluşturmuştur.

e-Devletin en zayıf halkası herhalde vatandaştır. Ancak, koordineli bir çalışma ile bu tablo düzeltilirken, en az gayret göstermesi gereken yine vatandaştır. En fazla gayret göstermesi gereken ise politikacılardır. Onlarla beraber daha çok gayret göstermesi gerekenler de bürokratlardır. Bu çalışmamda; kredi kartlarının bile hâlâ yasal düzenlemelerinin tam olarak oturmadığı bir ortamdayken, elektronik imza kanunun ve dolayısıyla dijital imza zemininin sağlam oluşturulması gerektiği, özellikle bu kesimlere vurgulanmaya çalışıldı. Aksi takdirde, elektronik imza vasıtasıyla tüm dünyada gelişen elektronik ticaret, ülkemizde geri saymaya devam edecektir.

Ülkemizde, elektronik ticareti kolaylaştırmasını beklediğimiz Elektronik İmza Yasası, "**müjdeler olsun**" sloganlarıyla kabul edildi. Elektronik İmza Yasası önemli bir dönüşümün anahtarı olacaktır. Bu kesin… Fakat uygulamada bazı problemlerle karşılaşılabileceği ve güvenlik sorunun tam olarak çözümlenmediği, Dijital İmza Sertifika Sağlayıcıları arasında hâlâ uyum sorunları olduğu, vatandaşın ise uygulamaların nasıl yapılacağı hakkında bilgisiz ve şaşkın olduğu, dijital imzayı kullanacakların dahi bu konuda henüz hiç bir şey bilmedikleri de kesindir. Çalışmamızda bu konuları ele almaya çalıştık.

II- İMZA NEDİR VE İMZANIN NİTELİKLERİ:

İmza; bir belgenin veya yazının doğruluğunu göstermek niyetiyle oluşturulan ve bir şahıs tarafından kullanılan her türlü semboldür. İmza, amaçsal açıdan tanımlanmaya çalışıldığında; **"bir belgenin, doğruluğunu gösterme niyetiyle yapılan her türlü işarettir".**[2] İmza söz konusu olduğunda genel kural ise; kâğıttan bir belge üzerine, mürekkepli bir kalemle oluşturulmuş el yazısı bir işaret, imza olarak geçerli sayılmıştır (Klasik/Islak İmza). Evrensel olarak tüm hukukçular, bu şekil şartının gerçekleştiği durumlarda imzanın varlığı için başka bir şart aranmayacağı konusunda görüş birliğine sahiptirler.[3]

Hukuken; bir belgenin doğruluğu, bir şahıs tarafından kendine ait bir sembolle imzalanmasıyla kabul görür. Bu, temel olarak hukuksal bir işlemdir. Ticari açıdan öneme sahip olduğu düşünülen her işleme ait belge imzalanır.

---

2 W. Everett **LUPTON,** "**The Digital Signature: Your Identity by The Numbers**", 6 RICH. J.L. & TECH. 10 (Fall 1999), http://www.richmond.edu/ jolt/v6i2 /note2.html, **Erişim Tarihi:** 10-03-2005.

3 Reed **CHRIS**, "**What is a Signature?**", The Journal of Information Law and Technology (JILT), 2003/3, http://elj.warwick.ac.uk/jilt/00-3/reed.html, **Erişim Tarihi:** 10-03-2005.

İmzanın, yukarıda verdiğimiz amaçsal açıdan tanımlamasının içeriğine uygun "**işaretlemeler**" tarih boyunca kullanılmıştır. Örneğin; Roma Hukukunda, bir sözleşmenin oluşturulabilmesi için sözleşme yapan kişilerin, mühür yüzüklerini balmumu basarak metni mühürlemeleri gerekiyordu. Orta çağ boyunca Avrupa'da, belgeler, topraktan yapılmış mühürlerle mühürlenerek doğrulukları ispat edilmiştir. Daha sonra taraflar, el yazısı ile atılmış imzaları, sözleşmenin geçerliliğini ispat vasıtası olarak kullanmaya başladılar.[4]

Yüzyıllar boyunca oluşan hukuk geleneği; son yüzyıl içindeki değişikleri, "**format**" ve "**araç**" açısından değil "**niyet**" ve "**amaç**" açısından değerlendirmeye başlamış ve bu kapsamda çeşitli sembolleri imza olarak kabul etmiştir. Örneğin; Amerikan hukukunda, mahkeme kararları/içtihat hukuku; telegram ve telekslerdeki isimler, daktilolarda yazılmış isim ve işaretlere, hatta zaman zaman antetli kağıtlara imzaya ilişkin sonuçlar bağlamıştır. Faks kâğıtlarındaki imzalar da geçerli imzalar olarak görülmüştür. Bu çerçeveden olarak bir imzanın oluşabilmesi için temel gerekler şöylece sıralanabilir:[5]

- Mürekkep ve kâğıt, bir imzanın oluşması için temel gerek değildir.
- İmza için, bir belgenin üzerindeki sembolün varlığı yeterlidir.
- Belgenin içeriğiyle, bu belgeyi düzenleyenin niyetinin örtüşmesi gerekmektedir.

Bu durumda; elektronik bir kayıt veya veri üzerindeki bir sembol ya da kod, imza olarak kabul edilebilecektir. Yani, "**Islak veya Klasik İmza**" olarak nitelenen, şahsın kâğıt üzerinde mürekkep ile attığı imza, kabul edilebilecek tek imza olarak görülmemiştir. Hatta bazı yazarlar, bir e-mailin sonuna "**uygun bir niyetle**" yazılmış ismin de imzanın bir çeşidi olan elektronik imza[6] olarak kabul edileceğini savunmuşlardır.

İmzanın özelliklerini belirlemeye çalıştığımızda, şöylece sıralandığını görürüz:[7]

- İmza, öncelikle imzalayanın **kimliğini** belirlemektedir. Bir şahıs el

---

4 W. Everett **LUPTON**, agm.

5 Av.H.Galip **KÜÇÜKÖZYİĞİT**, "**Elektronik Ticaret, Elektronik İmza ve Hukuk**", http://www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc, **Erişim Tarihi:** 11-02-2005.

6 Thomas J. **SMEDINGHOFF** ve Ruth H. **BRO, "e-Commerce in Illionis: Is İt Legal?"**, http://www.bakernet.com/ecommerce, **Erişim Tarihi:** 10-03-2005.

7 Reed **CHRIS,** agm.

yazısı ile bir belgeyi imzalamış ise, bu belgeyi o şahıs tarafından oluşturulduğuna karine oluşturur. Aksinin ispatı imzalayana aittir. Bütün bunlar, kişinin imzasının bir başkası tarafından kolayca taklit edilemeyeceği ve kullanılamayacağı kabulüne dayanmaktadır.

- Belgenin altına imza atan kişinin, belgenin içeriğine **razı olduğu** kabul edilir. Çünkü imza, belge içeriğine ilişkin, imzalayanın niyetini ortaya koyar.
- İmza; imzalayanın, belgenin bu şekilde oluşturulmasını istediğini, belgenin gerçeklik ve doğruluğunu **kabul ettiğini** göstermektedir.

İmzanın bu niteliklerinden dolayı, imzanın son çeşitlerinden olan elektronik imza için; elektronik ortamlarda sunulan mesajlar, başkaları tarafından ulaşılmaz, çözülemez ve değiştirilemez kılınması sağlanmalıdır.[8] Yani, **belge ve imza şifrelenmelidir**. Bu da, "**Dijital (Sayısal) İmzanın**" diğer adıyla, "**Güvenli İmzanın**" kullanılmasını gerektirmektedir. Zira, dijital imza, sunulan belge ile beraber kendisinin de şifrelendiği bir imza çeşididir.

Şifreleme; açık ve anlaşılabilir bir metni, kolayca anlaşılamaz, sadece istenilen kişiler tarafından anlaşılabilir ve erişilebilir kılmayı amaçlayan yöntemdir. Bu yöntem, kişiler arası iletişimde, güvenilirlik, bütünlük, doğruluk, orijinallik sağlar, Şifrelenmiş bir mesaj da; kişiler tarafından gönderildiği anlaşılabilen, bütünlüğü bozulmamış ve değiştirilmemiş olduğuna güven duyulabilecek bir mesajdır. Günümüzde, bu tarz bir şifrelemeyle, taraflar arasında güveni sağlayan ve en çok yaygın olan, ayrıca daha az bir maliyetle kullanılabilen imza çeşidi dijital imzadır.

Son olarak imza; kişinin kimliğini teyit ettiği gibi, altına imza atılan metnin de okunduğunu, anlaşıldığını, bu metinden kendisine yüklenen sorumlulukların kabul edildiğini ve kendisini hukuken bağladığını, teyit eder. Bu şekilde imzalanan içerik, imza sahibi tarafından her tür sonucuyla kabul edilmiş sayılır. Bir iddianın ispatı açısından, imzanın önemi büyüktür. Elektronik imza ise; günümüzde, kişinin elektronik ortamda tanınmasına olanak veren en basitten en karmaşığa kadar her türlü teknik çözüm için kullanılan bir üst kavramdır.[9]

---

8 W. Everett **LUPTON**, agm.

9 Yrd.Doç. Dr.Leyla Keser **BERBER**, "**Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi**", http://www. hukukcu. com/ bilimsel/kitaplar/e_imza_tasarielestiri.htm, **Erişim Tarihi:** 12-02-2005.

III- ELEKTRONİK İMZA VE ÇEŞİTLERİ:

Elektronik imza, "Elektronik ortamda yazının/belgenin doğrulanması amacıyla uygulanmış ya da oluşturulmuş, elektronik veya benzer araçlarla ifade edilen her türlü harf, karakter ya da sembollerdir".[10] Elektronik imza, elektronik ortamda oluşturulmuş bir mesajın bütünlüğünü ve değişmemişliğini, ifade eden her türlü elektronik işaret olarak da tanımlanmaktadır.[11] En basit tanımlamasıyla, elektronik imza, bilgisayar tabanlı kimlik belirleyici işaretlerdir.

ABD'nin, Küresel ve Ulusal Ticarette Elektronik İmza Yasasına göre ise: "Bir sözleşmeye eklenmiş ya da mantıksal bağlantı kurabilen ve kaydı imzalamak niyetini güden kişi tarafından oluşturulmuş veya kullanılmış, her türlü elektronik ses, sembol ya da kayıt" olarak tanımlanmaktadır.[12]

AB'nin, elektronik ticareti güvenilir kılmak ve Ortak Pazarda elektronik imza kullanımıyla ilgili genel çerçeve belirlemek amacıyla kabul ettiği, Elektronik İmza Direktifinin 2. maddesinde ise elektronik imza; "Elektronik veri ile bağlı ya da mantıksal ilişkide olarak hizmet veren elektronik formdaki veridir".[13]

Ülkemizin Elektronik İmza Kanunundaki elektronik imza tanımlaması da AB'nin elektronik imza tanımını esas almıştır. Kanunun, tanımlamaları kapsayan 3. maddesinde elektronik imza "bir elektronik veriye eklenen veya veri ile mantıksal bağlantısı bulunan ve imzalayanın kimliğini belirleme aracı olarak kullanılan elektronik veri" olarak tanımlanmaktadır.[14]

Bu durumda, elektronik imza için şunları söyleyebiliriz:

- Genel, belirli bir teknolojiye bağımlı olamayan
- Elektronik kaydın bütünlüğü ve doğruluğunun ispatı ile kaydın sa-

---

10 Florida Eyaleti Elektronik imza Yasası.

11 - Robbie **DOWNING** ve Ross Mc **KEAN**, "**Digital Signatures: Addressing The Legal Issues**", http//www.bakernet.com/ecommerce/robbie, **Erişim Tarihi:** 10-03-2005.
W. Everett **LUPTON**, agm.

12 Marianne **MENNA**, "**From Jamestown to Silikon Valley, Pionering a Lawless Frontier: The Electronic Signatures in Global and National Commerce Act**", Virginia Journal of Law and Technology, Summer, 2001, S.12.

13 - Av.H.Galip **KÜÇÜKÖZYİĞİT**, agm.
Julia **HORNLE**, "**The European Union Takes Initiative in The Field of e-Commerce**", The Journal of Information Law and Technology (JILT), http://elj.warwick.ac.uk/jilt/003/hornle.html, **Erişim Tarihi:** 10-03-2005.

14 5070 nolu Elektronik İmza Kanununun 3. maddesi.

hibi arasında ilişki kurmak için kullanılan tüm metotlara verilen addır.

Böylelikle elektronik imzalar, bir elektronik mesajın doğruluğunu ispatlamaya yönelik tüm elektronik olanakları ifade etmektedir. Bunlar, gönderici tarafından e-mailin sonuna yazılmış isim, basit ama daha az güvenli olan el yazısı imzanın (Islak İmza=Klasik İmza) tarayıcıdan geçirilerek elektronik bir belgenin sonuna iliştirilmiş görüntüsü, gizli bir kod veya şifre, karmaşık ama daha güvenli olan parmak izinin ya da göz retinasının taranması gibi özel bir biyometrik belirleyici şifre elektronik imza çeşitleri olarak sayılabilir.[15]

Teknolojinin gelişmesiyle elektronik imza çeşitlerine yenileri eklenmektedir. En çok kullanılan ve en gelişmiş olan elektronik imza şekli dijital imza denilen, Açık Anahtar Şifrelemesi (PKI) tekniği üzerine kurulan imza şeklidir. Açık anahtar şifrelemesine dayanan dijital imzalar; elektronik imza çeşitleri içinde en çok üzerinde durulan ve kullanılan, en kolay ve verimli, etkin ve düşük maliyetli olduğu belirtilen imzadır.[16]

Elektronik imza kapsamına giren diğer bir gurup ise, biyometrik (yani, kullanıcının parmak izi, avuç içi izi, ses, retina ve DNA kopyalama vb. kişiye has özelliklerin kullanılması gibi) yöntemlerdir. Biyometrik yöntemler; kişinin kendi vücut özelliklerinin gerek bilgisayara girişte, gerek internette yapılacak işlemlerde güvenliği sağlamak amacıyla kullanılmasıdır. Şüphesiz, yakın bir tarihte biyometrik yöntemler sanal ortamda işlem güvenliği bakımından, belki dijital imza yerine daha çok kullanılacak olan yöntemlerdir. Ancak; kişilerin söz konusu özelliklerinin dijital imzadaki gibi, bir sertifika kurumu tarafından kopyalanması ve sistemin bu tür kurum veya kurumlar aracılığı ile işletilmesi, dijital imzadakinden daha farklı bir alt yapıyı ve güvenliği gerektirmektedir.[17]

Son olarak; bu güne kadar, el yazısı kullanılarak atılan imza (Islak İmza=Klasik İmza), taklidi zor olduğundan daha bir kabul görmekteydi. Oysa; taklit edilemezlik açıdan bakıldığında, elektronik imzalar daha güvenlidir.

---

15 - Christina **SPYRELLI**, "**Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication**", The Journal of Information Law and Technology (JILT), http://elj.warwick.ac.uk/jilt/02-2/spyrelli.html, **Erişim Tarihi:** 10-03-2005.
Kiril Speech **KESAREV**, "**Telecommunications Architectures",** Department of Computer Science and Engineering Helsinki University of Technology, 22 November 1998.

16 Thomas J. **SMEDINGHOFF** ve Ruth H. **BRO**, agm.

17 Yrd.Doç.Dr.Leyla Keser **BERBER**, agm.

Retina taraması yoluyla oluşturulmuş bir elektronik imzanın veya parmak izi ya da iris taramasıyla oluşturulan, elektronik imzanın taklit edilmesi, neredeyse olanaksızdır. Fakat, bu imza çeşitleri, yüksek maliyetli olduklarından, günümüzde kullanımları yaygın olamamaktadır.

IV- DİJİTAL İMZA (GÜVENLİ İMZA) VE TİCARİ HAYATTTA KULLANIMI:

a- Dijital İmza Nedir ve Ticari Hayatta Neden İhtiyaç Duyulmuştur?

Günümüzde, elektronik imza; kişinin elektronik ortamda tanınmasına olanak veren, en basitten en karmaşığa kadar, her türlü teknik çözüm için kullanılan **bir üst kavramdır**.[18] Elektronik imzaların, Açık Anahtar Şifrelemesi (PKI) yöntemine dayanan, alt bir grubu da dijital imzadır.

Elektronik ticaretin, bir anlamda uygulama vasıtası dijital imzalardır. Dijital imzaların kapsamında yer alan temel güvenlik hedefleri arasında:

- Kişinin kimliğinin teyidi (authentication),
- Kişisel bilgilerin gizliliği (confidentiality),
- Verilerin bütünlüğünün sağlanması (integrity),
- İnkâr edememezlik (non-repudiation)

yer almaktadır. Bu kriterler elektronik ticaretin de vazgeçilmez güvenlik kriterlerinden olan dört temel unsurdur. Sayılan bu temel unsurlar ise; "**Asimetrik Kripto Teknolojisi**" olan "**Açık Anahtar Şifrelemesi (PKI)**" sayesinde, yani dijital imzalarla sağlanabilmektedir.

Dijital imzayı tanımlamaya geçmeden önce, dijital imzada kullanılan ve önemli bir kavram olarak kullanılan "**anahtar**" sözcüğüne açıklık getirelim: Anahtar; imzayı şifrelemek veya deşifre etmek için kullanılan sayısal karakterler dizisine denmektedir. Dijital imza, imza sahibinin gizli anahtarı kullanılarak oluşturulan ve imza sahibinin açık anahtarı kullanılarak alıcı tarafından kontrol edilen bir yapıya sahiptir.[19]

Genel bir tanımlamayla dijital imza; bir bilgisayar tarafından oluşturulan ve kullanılan, el yazısı bir imza (Islak=Klasik İmza) ile aynı etkiye sahip olması niyeti ve bilgisine sahip olan bir elektronik imzadır.[20]

---

18 Yrd.Doç.Dr.Leyla Keser **BERBER**, agm.

19 Arş.Gör.Ömer **ERGÜN**, "**Dijital İmza ve Dijital İmzanın Kullanımı**", İnternet Hukuku, 06-02-2004, http://www.law.ankara.edu.tr/yazi.php?yad=856, **Erişim Tarihi:** 12-02-2005.

20 Virginia Eyaleti Ticaret Yasası.

Dijital imzanın diğer bir tanımı ise şöyle yapılmaktadır: Elektronik imzanın özel bir çeşidi olup, bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür.[21]

Elle atılan imzayla (Islak=Klasik İmza) eşit hukuki statüde tutulan dijital imza, teknik bir tanımlamayla; internet üzerinden gönderilen her türlü bilgi ile ilgili olarak gönderenin kimliğini ve yine gönderenin gönderi içeriğini bildiğini doğrulayan; iletilen bilginin taşınma sırasında değişmediğinin ve gönderen kişinin bilgiyi gönderdiğini inkâr edemeyeceğinin garantisini sağlayan, kişiye ya da kuruma özgü işarettir.

Sahibinin, elektronik ortamdaki nüfus cüzdanı ya da pasaportu olarak algılanan dijital imza, güvenilir kabul edilen ve sertifika otoritesi olarak adlandırılan, kurumlar tarafından dağıtılıyor ve izleniyor. Dijital imza, teknik olarak iki anahtar yapısı üzerinde çalışıyor. Birisi, kişisel ve bireyin bildiği "**kapalı**", öteki de "**açık**" anahtardan oluşuyor. Kapalı ve açık anahtar birleşince, ilgili kişinin kimliği, hiçbir şüpheye gerek kalmayacak biçimde öğrenilmiş oluyor. [22]

Dijital imzaya şu nedenlerden dolayı gereksinim duyulmuştur:[23]

1. Öncelikle; oluşturulan bilgi ve verinin içeriğini dışımızdaki kimselerin, izinsiz öğrenme ve görmelerini önlemek; yani, bilgi ve verinin gizliliğini korumak amacıyla, gereksinim duyulmuştur.

2. İkincisi; bilgi ve verinin yine dışımızdaki kimselerin izinsiz değiştirmesi veya oluşturulan bilgi ve verinin gideceği yere varıncaya kadar geçen süre içerisinde, yolda değiştirilmesini veya bozulmasını önlemek amacıyla, gereksinim duyulmuştur.

3. Diğer bir gereksinim neden de; internet ortamında bir işlem yapılırken, tarafların karşılıklı olarak kimliklerini güvenli bir biçimde doğrulayamamalarıdır.

4. Ayrıca; işlemi yapan kimsenin yaptığı işlemi, kısmen veya tamamen reddetmesi durumunda, ispat aracı olarak, dijital imzaya gereksinim duyulmuştur.

Dijital imzaların esasını oluşturan, güvenli şifreleme tekniğinin (secure encryption technology) işleyişi şu şekildedir: İki ayrı, fakat matematiksel olarak ilişkili, anahtar vardır; kamusal anahtar ve kişisel yani gizli anahtar. Bunlar; dijital imzanın oluşturulmasında, belgenin kodlanmasında,

---

21 http://www.turkpoint.com/e-yasam/sayisal_imza.asp, **Erişim Tarihi:** 20-01-2005.

22 http://www.turkpoint.com/e-yasam/sayisal_imza.asp, **Erişim Tarihi:** 20-01-2005.

23 Arş.Gör.Ömer **ERGÜN,** agm.

imzanın doğrulanması ve şifrenin çözülmesinde kullanılır. Uygulamada, elektronik bir belgeyi oluşturan kişi, daima gizli olan kişisel anahtarıyla bu belgeyi şifreler.[24] Bu şifreleme ile mesajın içeriği, özel bir algoritma ile korunur. Bu şifreleme sırasında, ne alıcı ne de gönderici özel bir gayret göstermez ve şifreleme, bir yazılım sayesinde kolayca uygulanır. Alıcının açık anahtarı ve göndericinin gizli anahtarı ile şifrelenen bu mesaj ancak göndericinin kamusal anahtarı ve alıcının gizli anahtarı ile çözümlenebilir. Mesaj, alıcının kamusal anahtarına gönderilir ve alıcı, göndericinin açık anahtarı ve kendi gizli anahtarı ile mesajı okuyabilir. Bu metod ile üç şey sağlanmış olacaktır:[25]

- İlk olarak, mesaj; değiştirilmemiş, yani bütünlüğü bozulmamış, göndericinin istediği ibare ve ifadeleri içeren mesajdır (data integrity),
- Göndericinin gizli anahtarı taklit edilemeyeceğinden, bu mesajın belirtilen göndericiden geldiği kesindir (gönderici doğrulanması) (sender authentication),
- Gönderici de bu mesajın kendisi tarafından ve iradesiyle gönderildiğini inkar edemeyecektir(non repudiation).

Sonuç olarak; elektronik ticarette tüketiciden, elde edilen bilgiler, çok iyi bir şekilde korumalıdır. Bu noktada da; elektronik ticaret üzerinden yapılan işlemlerin inkâr edilememesi için dijital imza gündeme gelmiştir. Dijital imzanın temel hedefi elektronik ortamda yapılan işlemlerin hukuksal geçerliliğini ortaya koyabilmektir. Hâlâ kapsamlı çalışmalar devam etmektedir. Dijital imza yasasının getirdiği çok önemli iki husus var:

- Birincisi; dijital imza ile imzalanmış belgeler elle imzalanmış belgelerle eşit hukuki geçerliliğe sahip olacaklar,
- İkincisi de; güvenli dijital imza ile imzalanmış veriler, aksi ispat edilene kadar kanun karşısında kesin delil olacaklardır.

Önemli olan, tamamen güvenli bir elektronik ticaret ortamının oluşturulmasıdır. Bunun için de, güvenli bir dijital imza oluşturulmalıdır. Güvenli bir dijital imza oluşturmanın yolu da nitelikli elektronik sertifikalamadan geçmektedir. Burada asıl iş uygulama konusunda çalışmaları yürüten Telekomünikasyon Kurumu'ndadır.

---

24 Christina **SPYRELLI**, agm.

25 Graham **GREENLEAF**, "**Privacy Implications of Digital Signatures**", http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html, **Erişim Tarihi:** 10-03-2005.

Elektronik Sertifika; kullanıcı adıyla, onun açık anahtarını içeren ve gizli anahtarının kullanıcıya ait olduğunu doğrulayan elektronik dokümandır.[26]

b- Dijital İmzanın Kullanımı ve Ticari Hayat İçin Güvenli Üçüncü Taraf

Herkesin kendi anahtarını oluşturması mümkün olmadığına göre, bu anahtar çifti, kişilere hangi usulle verilecektir? Bu anahtarlar; güvenilir kurumlar tarafından verilmelidir ve düzenlemeleri hukuksal açıdan güvenli ve sıkı bir şekilde yapılmalıdır. Zira kişilerin alacağı gizli anahtarların başkalarınca kullanılabilmesi ya da öğrenilebilmesi telafi edilmesi neredeyse olanaksız zararlara sebep olabilir. Bu tekniğin güvenilir bir şekilde uygulanabilmesi sisteme güvenilir üçüncü tarafların (trusted third parties) dâhil edilmesini zorunlu kılar.[27] Yürürlüğe giren yeni Elektronik İmza Kanunumuzla, bu sağlanmıştır.

Kural olarak; dijital imza alabilmek için öncelikle, bir "**Dijital İmza Sertifika Sağlayıcısından**", "**Sayısal İmza Sertifikası**" alınması gerekmektedir. Bu sertifikaları düzenleyen kurumlar, "**Sertifikasyon Otoritesi**", "**Onay Makamı**" ya da "**Onay Kurumu**" olarak adlandırılmaktadır. Sertifika, Onay Makamı tarafından düzenlenir ve sayısal olarak imzalanır. Sertifika verilirken Sertifika Sağlayıcısı:

- Önce, talepte bulunanın "**kimliğini tespit**" edecektir.
- Sertifika ile birlikte talep edene temin edeceği "**Anahtar Şifre**" ve "**Şifre Oluşturma Yazılımlarını**" sağlayacaktır.
- Bir takım teknik yöntemler aracılığıyla, yalnızca talepte bulunana ait olan, bir "**dijital imza**" hazırlayacaktır.
- Verilecek imzanın, elektronik ortamda düzenlenecek belgelerde "**kullanılmasını sağlayacaktır**".
- İmzanın, başkaları tarafından "**doğrulanmasını**" sağlayacaktır.

Genel olarak, Sertifikalandırma Kurumu (Certification Authority) olarak da adlandırılan bu, güvenilir üçüncü taraflar; Avrupa Birliği Elektronik İmzalar Direktifinde, Sertifika Hizmet Sağlayıcıları (Certification Service Provider) olarak anılmış, yasa taslağımızda da sertifika hizmet sağlayıcısı olarak belirtilmişlerdir**.** Bu sertifika hizmet sağlayıcıları; kamusal anahtar

---

[26] http://turk.internet.com/haber/yazigoster.php3?yaziid=8084, **Erişim Tarihi:** 20-01-2005.

[27] Billur Y. **SOYDAN**, "**e-İmza ve e-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-1**", Vergi Sorunları Dergisi, S.151, Nisan-2001, s.132.

sahibinin kimliğini sertifikaya bağlar, yani onaylar, kamusal anahtarların yayınlanma görevini yüklenir, gizli anahtarların güncellenmesi, sertifika bilgilerinin saklanması gibi görevleri üstlenirler ve bu konularda hukuksal sorumluluk altındadırlar. Kısacası; dijital imza kullanmak isteyen bir kişinin, kimliğinin tam olarak belirlenebileceği belgeleri alır, bu kişiye bir anahtar çifti verir, sonrasında da bu şifrelerin kullanımları ile ilgili her türlü değişiklikler konusunda kamusal sorumluluk taşır.

c- Dijital İmzanın Özellikleri

Dijital imzanın özelliklerini şöyle açıklayabiliriz:[28]

1. Dijital imza; gönderilen bilgilerin, kesinlikle o kuruma veya kişiye ait olduğunu doğrulayarak, verinin başkası tarafından yollanmadığını garanti eder.

2. Dijital imza, veri akışı sırasında bilgilerin içeriğini korur.

3. Dijital imza, bir başka kişinin eline geçmesini ya da değiştirilmesini engeller.

4. Dijital imza, bilginin sadece alıcıya gittiğini ve sadece alıcı tarafından okunacağını garanti eder.

5. Dijital imza, gönderilen bilgilerin, gönderenin ve alanın kim olduğunun kanıtlanmasına imkân tanır. Yani, imzalanmış bir dokümanı yollayan kişi onu yolladığını ve alıcı da aldığını inkâr edemez.

d- Dijital İmzanın Ticari Hayattaki Yararları

1. Bir kullanıcı tarafından gönderilen bilgi veya verilerin, kesinlikle o kişi tarafından gönderildiğini teyit edilir. Gönderici göndermediğini, alıcı da almadığım iddia edemez.

2. Bir kullanıcı tarafından gönderilen bilgi veya verilerin, bir başkasının eline geçmesi veya değiştirilmesi engellenir.

3. Bir kullanıcı tarafından gönderilen bilgi veya verilerin içeriği, gönderici tarafından veya alıcı tarafından inkâr edilemez. Çünkü değil başkası, gönderici dahi gönderdikten sonra içeriğini değiştiremez. Bir uyuşmazlık durumunda ise, elektronik belgenin bir kopyası, üçüncü güvenilir kişi olan Sertifika Sağlayıcısında da bulunduğundan reddi imkansızdır.

4. Gönderilen veriler, tarih açısından damgalandığı gibi, arşivleme kolaylığı da sağlanır.

5. Gönderilen verilerin çabuk ulaşmasını sağlanır.

---

[28] http://www.alfabim.com.tr/cankaya_web/smartcard.html-1k, **Erişim Tarihi:** 01-06-2003.

6. Baskı, kâğıt, posta ve arşivleme maliyetlerini en aza indirgenir.

7. Artık nispeten azalan, ama tam olarak yok olmayan sigorta primi ve vergi yatırma kuyrukları gibi kuyrukların ortadan kaldırılmasına neden olacaktır.

8. Para ile ilgili işlemler, internet ortamına daha bir güvenle taşınabilecektir.

9. Günümüzde internet bankacılığı alanında yoğun bir altyapı yatırımı çalışması var. Zira parasal işlemler; daha fazla güvenlik gerektirmektedir. Dijital imzanın kullanıma başlaması, hazır bazı çalışmaları tamamlayıcı olacaktır.

10. İnternetin önemi artacaktır.

11. Yeni bir sektörün ve dolayısıyla istihdam alanının açılmasına neden olacak ve böylece, ülke ekonomisine yeni bir katkı sağlayacaktır.

12. Güvenli elektronik imza dijital imza ile elle atılan imza, hukuki olarak aynı düzeyde görülecektir.

13. Elektronik İmza Yasasında; elektronik imzanın tanımı yapılarak hukuki ve teknik kullanımı düzenlenirken, güvenli elektronik imzayla oluşturulan veriler, senet hükmünde olacaktır.

e- Dijital İmzanın Ticari Uygulamalarda Yerine Getireceği Fonksiyonlar

Dijital imzalar, hukuk bilimi açısından sonuçlar doğurmaya yarayacak şu fonksiyonları yerine getireceklerdir:

1. Doğrulama (Verification): Gönderilen veriyi, dijital olarak imzalayan kişinin kimliğinin doğrulanması yoluyla, işleme katılan tarafın kim olduğunun kesin bir şekilde bilinmesi sağlanacaktır. Bu özellik; dijital imza sahibinin, imzasının (gizli anahtarı) üzerinde kontrolü kaybetmedikçe taklidini yapmanın mümkün olmaması mantığına dayanmaktadır.[29]

2. Erişim Kontrolü (Access Control): Elektronik olarak gönderilen bilgilere ve kaynaklara, sadece izin verilmiş kişiler tarafından erişilebilmesi garanti edilecektir. İzin verilen kişi de, okuduğu mesajı bir başkasına gönderecek olduğunda kendi imzası ile şifreleyebilecektir. Bu aşamada; üçüncü kişi de gelen mesajın, bir aracı yoluyla geldiğini anlayacak ve gerekiyorsa doğruluğu konusunda teyit alabilecektir. Ancak, mesaj içeriğinin değişmesinden mesajı üçüncü kişiye gönderen sorumlu olacaktır.

3. Bütünlük (Integrity): Dijital imza ile imzalanıp gönderilen, verinin bütünlüğü korunacaktır. Veriler, dijital imza ile imzalanıp gönderildiği

---

[29] Christina **SPYRELLI**, agm.

andan itibaren; mesajın içeriğinin hiç değişmemiş olduğu, mesajın hangi amaç ile olursa olsun hiçbir şekilde alıcının gizli anahtarına sahip olmayan bir başkası tarafından açılamayacağı ve hatta göndericinin de aynı mesajı değiştiremeyeceği garantisi altına alınmıştır.[30] Dijital imzalar; Asimetrik Kriptografi Teknolojisi ve Açık Anahtar Altyapısı (PKI) teknolojisiyle çalıştıklarından, internet ve diğer açık ağlar üzerinde gerçekleşen elektronik haberleşme ve işlemlerde, çok üst düzeyde bir güvenlik ve güvenilirliği mümkün kılmaktadır. [31]

4. İnkâr Edilememe (Non-Repudiation): Dijital imza ile imzalanıp gönderilen bilgiler, üçüncü güvenli kişiler tarafından devamlı olarak kontrol edilmekte ve dijital imza ile imzalanıp gönderilen her verinin bir sureti, üçüncü güvenli kişi tarafında saklanmaktadır. Bu nedenle; taraflar arasında bir anlaşmazlık vücut bulduğunda, bu üçüncü güvenli kişiye başvurulmakta ve güvenli kişinin verisi, reddedilememekle beraber, taraflar da bu veriyi inkâr edememektedirler. İnkâr edilememe; hukuksal bir anlaşmazlık ortaya çıktığında, gönderici tarafın mesajdan sorumlu tutulabilmesini sağlamaktadır. Karşı tarafın; bir mesaja, sözleşmeye ya da ödemeye ilişkin isteği, bu mesajın karşı tarafın tek taraflı iradesiyle reddedilemeyeceğine güvenebilmesi ile yakından ilişkilidir.[32] Gönderilen mesajın, gönderen tarafından reddedilememesi ve bu yolla işlemi gerçekleştiren açısından hukuksal yükümlülük oluşturması sağlanacaktır.[33] Uzaktan iletişimde, çok büyük bir öneme sahip bu fonksiyon, elektronik ticaretin gelişimini olumlu yönde etkileyecektir.

5. Verimlilik ve Lojistik (Efficiency and Logistics): Dijital imzalar, işlemlere kolaylık, ucuzluk ve hız kazandıracaktır.

Dijital imzaların, hukuk dünyasında sonuçlar doğurmaya yarayan yukarıda saydığımız fonksiyonlarıyla, el yazısı imzalara (Islak=Klasik İmza) bağlanan aşağıdaki hukuksal sonuçlar, dijital imzalara da bağlanabilecektir:

- Delil Olma Özelliği,
- Resmiyet ve Şekil Şartı Olma,

---

30 John **ANGEL**, "**Why use Digital Signatures for Electronic Commerce?"**, The Journal of Information, Law and Technology (JILT), Commentary-1999.

31 Christina **SPYRELLI**, agm.

32 Thomas J. **SMEDINGHOFF** ve Ruth H. **BRO,** "**Moving With Change: Electronic Signatures Legislation As a Vehicle for Advancing Electronic Commerce**", The John Marshall Journal of Computer and Information Law, Vol. XVII, No. 3, Spring 1999 at 723, http://www.bakernet.com/ecommerce, **Erişim Tarihi:** 10-03-2005.

33 John **ANGEL**, agm.

- Onaylama.

Nitekim, Avrupa Birliğinin Elektronik İmza Yönergesi, 'Elektronik İmzanın Hukuksal Etkileri' başlığı altındaki 5. maddesine göre gelişmiş elektronik imzalar;

- Kâğıt üzerindeki bilgiler açısından, el yazısı imzaya bağlanan tüm sonuçların, elektronik ortamdaki bilgiler açısından doğmasına ilişkin, hukuksal gerekleri haizdir.
- Hukuksal uyuşmazlıklarda delil olma özelliğine haizdir.
- Elektronik imzaların hukuksal etkileri sadece elektronik formatta olduklarından dolayı, reddedilemeyecektir.

Sonuç olarak; dijital imza oluşturma, kullanım ve doğrulama hukuksal amaçlar açısından önemli fonksiyonlar yerine getirecektir.[34] Dijital imza ile doğacak sonuçlar, dijital imzanın, ticari hayat açısından önemini ve vazgeçilmezliğini ortaya koymaktadır.[35]

f- Ticari Hayatta Dijital İmzanın Kullanımında Karşılaşılabilecek Problemler

Dijital imzanın oluşturulmasında ve kullanımında ortaya çıkan bazı problemleri şöyle sıralayabiliriz:[36]

1. Sertifika veren kurumun; güvenirliği, güvenliği ve ortaya çıkacak problemlerden dolayı bir zarar söz konusu ise, bunun nasıl karşılanacağı vs. gibi konuların, yasal bir düzenleme ile düzenlenmesi gerekmektedir.[37]

2. Uluslararası düzeyde, dijital imzanın kodlanmasına ilişkin kabul gören bir standardın gelişmemiş olması, dijital imza açısından büyük bir handikaptır. Uluslararası alanda birçok standart vardır ve bunlar birbirleriyle uyumlu değildir. Dijital imzanın kullanımının yaygınlaşması için bu alanda da bir uluslararası entegrasyona ihtiyaç vardır.[38]

3. Aynı problem, oluşturulan dijital imzanın; imzalanmış bir veriyle

---

34 **ABA**, "**Legal Acceptance of Digital Signatures**", http://www.abanet.org/rppt/meetings_cle/2002/2002spring/RealProperty/Thursday/TechnologyandtheRealEstate/OnlineTransactionManagement.pdf, **Erişim Tarihi:** 10-03-2005.

35 Christina **SPYRELLI**, agm.

36 Tolga **TÜFEKÇİ**, http://www.bilten.metu.edu.tr/Web_2002_v1/ common/yayinlar/Elektronik_imza_nicin%20_yaygınlaşamıyor, **Erişim Tarihi:** 15-05-2003

37 http://turk.internet.com/haber/yazigoster.php3?yaziid=8084, **Erişim Tarihi:** 20-01-2005.

38 http://turk.internet.com/haber/yazigoster.php3?yaziid=8084, **Erişim Tarihi:** 20-01-2005.

birlikte nasıl oluşturulacağı, nasıl taşınacağı ve nasıl korunacağına ilişkin yerleşmiş bir standardın olmayışında da karşımıza çıkmaktadır. Dolayısıyla, farklı biçimlerde kodlanmış imzaların karşılıklı olarak doğrulanmasında zorluklar yaşanacaktır.

4. Ayrıca, şunu da ifade etmek gerekir ki; tüm bu problemler çözülse bile, bu teknolojiyi kullanabilecek eğitim seviyesinde, bilgisayar kullanabilen kimselere ihtiyaç vardır. Ülkemizde, bu niteliklerde insan sayısının giderek artmasına rağmen yeterli olmaması, devlete bu konuda büyük bir yükümlülük yüklemektedir.

5. Doğal olarak, her teknolojiyi kullanmanın bir bedeli olduğu gibi, bu teknolojinin kullanımının da bir maliyeti olacaktır. Özellikle gelişmekte olan ülkelerde bu maliyet, kullanıcıları caydıracak kadar yüksek bir meblağa ulaşabilmektedir. Bu bağlamda, devletin özellikle bu tür yeni teknolojinin kullanımını teşvik etmesi, sübvansiyonda bulunması gerekir. Aynı zamanda, özel kuruluşların da buna destek olması, örneğin, bankaların bu konuda düşük faizli kredi vermesi gibi, devlet-özel kuruluş ortak çalışması yapılması gerekir.[39]

g- Dijital İmza Alınırken Dikkat Edilmesi Gerekenler

Hiç kuşkusuz, elektronik ticaretin gelişimi ve yaygınlaşmasında internetin çok büyük katkısı bulunmaktadır. Ancak, günümüzde dijital imzaya geçmek amacıyla "**Dijital İmza Sertifika Sağlayıcısından**", "**Sayısal İmza Sertifikası**" almak isteyecek kullanıcıların, dikkat etmeleri gerekli bazı teknik hususlar da vardır. Bunları şöylece sıralayabiliriz:

1. Elektronik İmza Kanununun yürürlüğe girmesi sonrasında dijital imza uygulamalarına geçişte kurumlar, "**hukuki geçerliliği olan sertifika**" almalıdırlar.

2. Alınan sertifikaların, "**EAL 4+ güvenlik seviyesine sahip cihazlar"** üzerinde tutulması önemli bir husustur.

3. Sertifikaları "**akıllı kartlar üzerinde saklama**" konularına dikkat edilmelidir.

4. Dijital imzanın kullanım aşamasında sertifika; "**akıllı kart**" ve "**akıllı kart**" okuyucusu olmak üzere üç bileşen bulunduğu bilinmelidir.

5. Dijital imza kullanımı için, üç tip terminal bulunmaktadır: Birinci tip terminallerde, PIN girişi yok, PIN klavyeden girilmektedir. İkinci tip terminallerde, PIN girişi cihaz üzerinden yapılmaktadır. Üçüncü tip termi-

---

[39] http://turk.internet.com/haber/yazigoster.php3?yaziid=8084, **Erişim Tarihi:** 20-01-2005.

nallerde, PIN girişi cihaz üzerinden yapılmakta ve standartlar değiştiğinde uygulama güncellenebilmektedir. Uygulaması güncellenemeyen cihazlar **İLERİDE ÇÖPE ATILACAKTIR**. Dijital imza kullanıcıları cihaz alırken bu noktaya dikkat etmelidir. Uzmanlar kullanıcılara, üçüncü tip terminalleri tavsiye etmektedirler

6. Dijital imzada karşılaşılan en büyük sorunlardan biri, imza için sadece o bilgisayara bağımlı kalma mecburiyetidir. Bu konuya dikkat edilip mobil halde kullanılan dijital imza çeşitlerini tercih etmek lazımdır. Mobil dijital imza konusunda, yeni çözümler ve platformlar sunan firmalar vardır. Örneğin **mIDentity** gibi ürünler mobil hale getirilmiştir. Bu tip ürünler, **flash hafızaya** sahip olup **OTP (Tek Kullanımlık Şifre)** çözümlerine de destek vermektedirler.

V- SONUÇ

Elektronik ticaretin, gelişim ve yaygınlaşmasında internetin çok büyük katkısı olmuştur. Fakat elektronik ticarette, uzaktan erişimle elde edilen bilgilerin, çok iyi bir şekilde koruması gerekmektedir. Zira, elektronik ticaretin gelişmesinin en önemli öğelerinden biri, bu ortamda gönderilen bilginin güvenliği konusudur.

"Kişinin Kimliğinin Teyidi", "Kişisel Bilgilerin Gizliliği", "Verilerin Bütünlüğünün Sağlanması" ve "İnkâr Edememezlik" elektronik ticaretin vazgeçilmez güvenlik kriterlerinden olan dört temel unsurdur. Uzaktan iletişimde çok büyük bir öneme sahip bu unsurların oluşturulması, elektronik ticaretin gelişimini olumlu yönde etkileyecektir. Önemli olan, tamamen güvenli bir elektronik ticaret ortamının oluşturulmasıdır.

Elektronik ticarette yapılan işlemlerin; güvenlik kriterlerinden olan dört temel unsurun oluşturulması için, dijital imza gündeme gelmiştir. Çünkü elektronik ticaretin, vazgeçilmez temel unsurlarını karşılayabilen ve dolayısıyla bir anlamda, elektronik ticaretin uygulama vasıtası, dijital imzalar olmuştur.

Elektronik imzalar, elektronik ticaret işlemlerinin güvenlik ve güvenilirliğine katkı sağlayarak, elektronik ticaretin gelişiminde önemli bir rol oynayacaktır. Güvenli bir elektronik ticaret ortamının oluşturulması, güvenli bir dijital imza oluşturulmasından, güvenli bir dijital imza oluşturmanın yolu da nitelikli elektronik sertifikalamadan geçmektedir. Bu noktada asıl iş, uygulama konusunda çalışmaları yürüten Telekomünikasyon Kurumundadır.

Türkiye'de internet, daha çok haberleşme, oyun oynama veya müzik dinleme gibi faaliyetler için kullanılmaktadır. İnternette paraya bağlı, risk içeren işlemler yapılamamaktaydı. Dijital imzayla; kimlik doğrulama, inkâr edilememezlik, bilgi bütünlüğü ve gizlilik sağlanabildiği için internet ortamında yapılamayan mal alım satımları, ihaleler, gümrük beyannamelerinin doldurulması vs gibi işlemler; artık yapılabilecek, böylelikle internet kullanımı çok yaygınlaşacak, şeffaflık, verimlilik, hız artacak, ucuzlama gelecektir

Dünyada internet üzerinden işlem yapma eğilimi göz önünde bulundurulduğunda, dijital imzanın önemi daha net anlaşılmaktadır. Dijital imza, önümüzdeki dönemde dünyaya paralel olarak Türkiye'de de önem kazanacaktır. Gelecekteki beklenti, herkesin dijital imzasının olması ve işlemlerini bununla yapmasıdır. Dolayısıyla endüstriye, elektronik ticaret hâkim olacak ve dijital imza her tarafa yayılacaktır.

Elektronik ticaretin; tüm bu olumlu yapısına, ülkemizde bu konuda çok büyük çabalar harcanmasına ve bu konuda nihayet bir elektronik imza kanununa kavuşmamıza rağmen, dijital imza ile ilgili sorunlar, gerek teknik ve gerekse hukuki anlamda, tam olarak bitmiş ve çözümlenmiş değildir. Hatta eğitim ve alışkanlıklarımız olarak da hazır değiliz.

Hiç kuşkusuz, elektronik ticaretin gelişimi ve yaygınlaşması üzerinde internetin çok büyük katkısı bulunmaktadır. Bugüne kadar; özellikle elektronik ticaretin güvenliği alanında, çok ciddi paralar harcanmış ve harcanmaya devam edilmektedir. Bu yatırımların tamamlanması asla mümkün değildir. Çünkü insanın içinde bulunduğu bir sistemde, yüzde 100 güvenli bir ortam oluşturmak mümkün değildir. Evet, dijital imza kullanım kolaylığı getirecek, hayatımızı birçok açıdan kolaylaştıracak, özellikle banka gibi kurumlar için ciddi bir iş potansiyeli oluşturacaktır. Ancak güvenli dijital imza ve nitelikli sertifikalama konularında hâlâ netleşmeyen bir takım sorunlar var.

Örneğin, günümüzde internette halen 32 bitlik IPv4 kullanılmaktadır. Halbuki, 128 bitlik IPv6; güvenlik, hizmet kalitesi, mobil internet uygulamalarında esneklik sağlanması ve otokonfigürasyon açısından IPv4'e göre birçok üstün yönleri bulunmaktadır. Otokonfigürasyon; son kullanıcı hizmet sağlayıcısını değiştirdiğinde ya da bir şebeke başka bir şebeke ile birleştiğinde ya da genişletildiğinde her bir "router" ve "host"un manuel olarak konfigürasyonu yerine, IPv6'da bu işlemin otomatik olarak yapılması sağ-

lama özelliğidir. Ayrıca 32 bit'lik IPv4'ler 4 milyar IP adresine sahip iken, 128 bit'lik IPv6 3,4 x 10^{38} adet IP adresine sahiptir.[40]

Dijital imzanın teknik yapısını oluşturan Açık Anahtar Şifrelemesi (PKI) yöntemi olan Asimetrik Kripto Tekniğinin kullanıldığı dijital imzada açık ve gizli anahtar olmak üzere iki temel anahtar kullanılmakla beraber, dijital imza teknolojisi henüz gelişim sürecini tamamlamamıştır. Zira üzerinde mutabakata varılmış tek bir dijital imza standardı bulunmaktadır. Bu nedenle farklı üreticilerin hazırladıkları sertifikalar birbirlerini tanımamaktadır.[41]

Bununla beraber, elektronik ticarete diğer bir engel de dünyada güvenli elektronik ticaretin nasıl yapılacağına dair ortak bir mutabakat henüz geliştirilememiş olup, bu çerçevede halen, WTO (World Trade Organization-Dünya Ticaret Örgütü) ve ICC (International Commerce Chamber-Uluslararası Ticaret Odası) gibi çeşitli kuruluşlarca çalışılmalar sürdürülmektedir.[42]

Unutulmaması gereken bir nokta da, kredi kartlarının bile hâlâ yasal düzenlemelerinin tam olarak oturmadığı bir ortamdan söz etmekteyiz. Ancak bunların hepsinin teker teker aşılacağına inanıyoruz.

Dijital imza büyük bir fırsattır. Fakat Pazar, henüz bu konuya hazır değildir. Dijital imza için 2005 yılının, bilincin oturması için gerekli birtakım uygulamaların görüleceği bir yıl olacağı, 2006 yılı itibariyle de elektronik imza ile ilgili uygulamaların piyasada görülmeye başlayacağı tahmin edilmektedir.

Güvenlik konusunda, teknolojik olarak birçok yenilikler yapılıyor olsa da, hukukun felsefesi gereği statik bir yapıda olması nedeniyle hukuki uygulamalar beklendiğinden yavaş ilerlemektedir.

Dijital imzanın temel hedefi elektronik ortamda yapılan işlemlerin hukuksal geçerliliğini ortaya koyabilmektir. Bu bağlamda, hukuksal düzenlemeler, eğer doğru yapılabilirse, elektronik ticareti daha çok geliştirecek ve cesaretlendirecektir. Ayrıca, elektronik ticaretin daha iyi gelişebilmesi için her şeyden önce geleneksel ticaret ve elektronik ticaret

---

40 Mustafa **ALKAN;** Köksal **ÖZENÇ, "e-Ticareten M-Ticarete Doğru Süreçteki Yeni Yansımalar",** Telecommunications International, Telekomünikasyon Kurumu-Ankara, Mayıs 2002, http://www.inet-tr.org.tr/inetconf9/bildiri/86.doc, **Erişim Tarihi:** 10-03-2005.

41 Mustafa **ALKAN;** Köksal **ÖZENÇ, agm.**

42 Mustafa **ALKAN;** Köksal **ÖZENÇ, agm.**

arasında ayırım yapılmaması, kanunların bu anlamıyla teknolojik tarafsız olması gerekir.[43]

Sonuç yazımızda; yapıcı birer eleştirici olarak sunduğumuz bu görüşlerimizden, dijital imzaya karşı olduğumuz anlaşılmamalıdır. Çalışmaları sonuna kadar destekliyoruz ve kullanmaya başlayacağız.

KAYNAKÇA:

1. **ABA**, "Legal Acceptance of Digital Signatures", http://www.abanet.org /rppt/meetings_cle/2002/2002spring/RealProperty/Thursday/TechnologyandtheRealEstate /OnlineTransactionManagement.pdf, Erişim Tarihi**:** 10-03-2005.
2. **ALKAN** Mustafa**; ÖZENÇ** Köksal**, "**e-Ticareten M-Ticarete Doğru Süreçteki Yeni Yansımalar", Telecommunications International, Telekomünikasyon Kurumu-Ankara, Mayıs 2002, http://www.inet-tr.org.tr/inetconf9/bildiri/86.doc, Erişim Tarihi: 10-03-2005.
3. **ANGEL** John, "Why use Digital Signatures for Electronic Commerce?", The Journal of Information, Law and Technology (JILT), Commentary-1999.
4. **BERBER** Leyla Keser Yrd.Doç.Dr., "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi", http://www. hukukcu. com/ bilimsel/kitaplar/e_imza_tasarielestiri.htm, Erişim Tarihi: 12-02-2005.
5. **CHRIS** Reed, "What is a Signature?", The Journal of Information Law and Technology (JILT), 2003/3, http://elj.warwick.ac.uk/jilt/00-3/reed.html, Erişim Tarihi: 10-03-2005.
6. **ÇOBAN** Çağrı**; TURHAN** Serhat; **UYSAL** A. Bora**,** "Sayısal İmza Sunumu", Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü Bil342 Programlama Laboratuarı, ÇSB. Yazılım Ltd. Şti. Sayfa:4.
7. **DOWNING** Robbie ve **KEAN** Ross Mc, "Digital Signatures: Addressing The Legal Issues", http//www.bakernet.com/ecommerce/robbie, Erişim Tarihi: 10-03-2005.
8. Elektronik İmza Kanununun.
9. **ERGÜN** Ömer Arş.Gör., "Dijital İmza ve Dijital İmzanın Kullanımı", İnternet Hukuku, 06-02-2004, http://www.law.ankara.edu.tr/yazi.php?yad=856, **Erişim Tarihi:** 12-02-2005.
10. Florida Eyaleti Elektronik imza Yasası.
11. **FRIEDEN** Robert M., "Universal Service When Technologies Converge and Regulatory Models Diverge", Harvard Journal of Law & Technology, Volume: 13, Number: 3, Summer 2000.

[43] John **ANGEL**, agm.

12. GREENLEAF Graham, "Privacy Implications of Digital Signatures", http://www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html, Erişim Tarihi: 10-03-2005.
13. HORNLE Julia, "The European Union Takes Initiative in The Field of e-Commerce", The Journal of Information Law and Technology (JILT), http://elj.warwick.ac.uk/jilt/003/hornle.html, Erişim Tarihi: 10-03-2005.
14. http://turk.internet.com/haber/yazigoster.php3?yaziid=8084, Erişim Tarihi: 20-01-2005.
15. http://www.alfabim.com.tr/cankaya_web/smartcard.html-1k, Erişim Tarihi: 01-06-2003.
16. http://www.turkpoint.com/e-yasam/sayisal_imza.asp, Erişim Tarihi: 20-01-2005.
17. KESAREV Kiril Speech, "Telecommunications Architectures", Department of Computer Science and Engineering Helsinki University of Technology, 22 November 1998.
18. KILLIAN Wolfgang, "Digital Communication and Contract Law", Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002, s.161.
19. KÜÇÜKÖZYİĞİT.H.Galip Av., "Elektronik Ticaret, Elektronik İmza ve Hukuk", http://www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc, Erişim Tarihi: 11-02-2005.
20. LUPTON W. Everett**,** "The Digital Signature: Your Identity by The Numbers", 6 RICH. J.L. & TECH. 10 (Fall 1999), http://www.richmond.edu /jolt/v6i2/note2.html, Erişim Tarihi: 10-03-2005.
21. MENNA Marianne, "From Jamestown to Silikon Valley, Pionering a Lawless Frontier: The Electronic Signatures in Global and National Commerce Act", Virginia Journal of Law and Technology, Summer, 2001, S.12.
22. SMEDINGHOFF Thomas J. ve **BRO** Ruth H.**,** "e-Commerce in Illionis: Is İt Legal?", http://www.bakernet.com/ecommerce, Erişim Tarihi: 10-03-2005.
23. SMEDINGHOFF Thomas J. ve **BRO** Ruth H.**,** "Moving With Change: Electronic Signatures Legislation As a Vehicle for Advancing Electronic Commerce", The John Marshall Journal of Computer and Information Law, Vol. XVII, No. 3, Spring 1999 at 723, http://www.bakernet.com/ecommerce, Erişim Tarihi: 10-03-2005.
24. SOYDAN Billur Y., "e-İmza ve e-Belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk-1", Vergi Sorunları Dergisi, S.151, Nisan-2001, s.132.
25. SPYRELLI Christina, "Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication", The Journal of Information Law and Technology (JILT), http://elj.warwick.ac.uk /jilt/02-2/spyrelli.html, Erişim Tarihi: 10-03-2005.
26. TÜFEKÇİ Tolga,http://www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar/Elektronik_imza_nicin%20_yaygınlaşamıyor, Erişim Tarihi: 15-05-2003
27. Virginia Eyaleti Ticaret Yasası.