

**KIRIKKALE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANA BİLİM DALI**

FATİH ÖNDER

**BORÇLAR HUKUKU AÇISINDAN
ELEKTRONİK İMZA**

Yüksek Lisans Tezi

TEZ YÖNETİCİSİ:

Doç. Dr. Kürşat Nuri TURANBOY

KIRIKKALE – 2007

ÖZET

20. yüzyılın ortalarından itibaren teknolojinin baş döndürücü şekilde gelişmesi, kâğıda dayalı geleneksel iletişimin, dijital iletişim olarak nitelendirilen, modern iletişim yöntemlerine doğru hızlı bir değişim göstermesine, kişi ve kuruluşların, ulusal ve uluslar arası boyutta hukuki ilişkiler kurup, sözleşmeler akdetmelerinde modern iletişim yöntemlerini kullanmasına yol açmıştır.

Sözleşme, iki tarafın bir hukuki sonucu elde etmek üzere iradelerini karşılıklı ve birbirine uygun surette açıklamalarıyla oluşan bir hukuki işlem olup, sözleşmenin elektronik araçlarla kurulmuş veya tamamlanmış olması halinde elektronik sözleşmeden bahsedilir. Yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve taraflarca karşı karşıya gelinmeksizin yapılan sözleşmeler ise mesafeli sözleşme olarak adlandırılır. Bu anlamda elektronik sözleşmeler, mesafeli sözleşmelerin bir türünü oluşturur.

Bir iradeyi açıklamak için kullanılan araca, dış kalıp veya biçime “*şekil*” adı verilir. Kural olarak, bir irade beyanı, hukuki işlem veya sözleşmenin geçerliliği belirli bir şekle tabi değildir. Bu itibarla irade beyanları klasik yöntemlerle yapılabileceği gibi, elektronik ortamda da yapılabilir. Ancak, kanunen veya taraf iradelerince geçerliliği şekil şartına bağlanmış olan bir sözleşme, bu şekil şartına uygun olarak yapılmadığı sürece geçersizdir(BK. m.11/2). Yine belli bir meblağı aşan sözleşmelerin uyuşmazlık halinde ispatı ancak yazılı şekilde yapılmış olmasına bağlıdır.

Resmi bir makamın katılımı veya onayının aranmadığı hukuki işlemlerde şekil şartı metin ve imza ile yerine getirilir. İmza bir irade açıklamasının kendisine ait olduğunu ifade etmek üzere, kişinin kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir kimse tarafından (veya onun namına) kullanılan, herhangi bir işaret veya

kabul edilen herhangi bir güvenlik usulüdür. İmzasız bir belge kural olarak sahibine hak veya yükümlülük getirmedeği gibi bir kıymet de taşımaz.

Klasik yöntemlerde olduğu gibi, elektronik ortamda kurulan sözleşmeler veya yapılan irade beyanlarından şekil şartına bağlı olanların geçerlilik kazanması, şekil şartına bağlı olmayanların ise ispatı, yazılı şekilde yapılmış olmasına, dolayısıyla metin ve imza içermesine bağlıdır. Klasik yöntemlerde kullanılan el yazısı ile imzanın ise yapısı gereği elektronik ortamda kullanılması mümkün değildir.

Bu nedenle geleneksel usulde el yazısı imza ile sağlanan işlevleri ve hukuki korumayı elektronik ortamda yerine geçebilecek, elektronik ortamda bulunan veya gönderilen veri, bilgi ve belgelerin güvenliği ve güvenilirliğini sağlayıp, bütünlüğünü koruyarak, gönderenin ve alanın kimliğini tespit eden bir teknik yöntem olan “*elektronik imza*” ortaya çıkmıştır.

Elektronik imza, elektronik ortamda oluşturulmuş bir mesajın bütünlüğünü ve değişmemişliğini ifade eden, aynı zamanda mesaj sahibinin kimliğini tanımlamaya yarayan her türlü elektronik işarettir. Elektronik imza türlerinden olan sayısal imza ise, açık anahtarlı kriptografi başta olmak üzere, gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bilgilerin, kim tarafından gönderildiğinin belirlenmesini, verileri gönderenlerin gönderdiğini ve alanların aldığını inkâr edememesini, gönderilen veya alınan bilgilerin içeriğinin değiştirilmemesini, başkaları tarafından elde edilse bile içeriğinin anlaşılmasını sağlamayı garanti eden, elektronik ortamda bit katarlarından oluşturulmuş güvenli haberleşme ve tasdik yöntemidir.

İki binli yılların başından itibaren dünyanın pek çok ülkesinde elektronik imza ile ilgili yasal düzenlemelere gidilmiştir. Ülkemizde de elektronik imza ile ilgili yasal düzenleme 5070 sayılı Elektronik İmza Kanunu ile yapılmış ve yasa 24 Temmuz 2004 tarihinde yürürlüğe girmiştir. Yasada yapılan elektronik imza tanımı teknolojik tarafsızlık ilkesi gereği tüm elektronik imza türlerini kapsayacak şekilde yapılmıştır. Ancak elektronik imzanın el yazısı imza ile eşdeğer kabul edilebilmesi için elektronik sertifika hizmet sağlayıcısı tarafından verilmiş nitelikli elektronik sertifikaya dayanan ve yasada güvenli elektronik imza olarak tanımlanan elektronik imzanın niteliklerini

taşıması gereklidir. Buna göre, “*güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*” ve “*..güvenli elektronik imza ile oluşturulmuş elektronik veriler senet hükmündedir.*” Bunun anlamı, güvenli elektronik imza ile ıslak imza gerek fonksiyonel anlamda gerekse şekil ve ispat kuralları bakımından eşittir. Bu hüküm sayesinde, özel hukuk alanında hem şekle tabi sözleşmelerin elektronik ortamda kurulabilmesi, hem de güvenli elektronik imza ile imzalanmış elektronik belgelerin mahkemelerde senet olarak kabul edilmesi mümkün hale gelmiştir.

Güvenli elektronik imza niteliği taşımayan elektronik imza ile imzalan veya elektronik imza ile imzalanmayan elektronik verilerin ise yürürlükteki mevzuat çerçevesinde, şekil şartını yerine getirmediği dahası yazılılık niteliğini dahi taşımadığı kabul edilmektedir. Bu nedenle bu veriler ancak özel hüküm sebepleri kategorisinde değerlendirilebileceklerdir. Buna göre güvenli elektronik imza dışındaki elektronik imzaların ve bunlarla imzalanmış verilerin hukuki değeri yok denecek kadar azdır. Oysa biyometrik yöntemler başta olmak üzere, güvenli elektronik imza kapsamı dışında kalan elektronik imzaların da el yazısı ile imzanın birçok işlevini yerine getirdiği bilinmektedir. Bu itibarla güvenli elektronik imza dışındaki elektronik imza türlerinin hukuki değerini artıran yeni bir hukuki düzenleme yapılması ya da en azından bu nitelikteki elektronik verilerin delil değerini artıran ve yazılık işlevinin kapsamını değiştiren “Türk Borçlar Hukuku” ve “Hukuk Muhakemeleri Usulü” kanun tasarılarının bir an önce yasalaşması gerektiği görülmektedir.

Ülkemizde 5070 sayılı yasa ile birlikte elektronik imza kullanımı hayata geçirilmiş ise de, elektronik imzaya geçiş beklenen düzeyde değildir. Bunda ülkemizin bilişim teknolojilerini kullanma oranının düşük olması ve genel olarak kurumların elektronik ortamda iş yapmaya gerekli düzeyde başlamamış olması etkilidir. Bu sebeple elektronik imzanın yaygınlaşması için devletin öncü rol oynaması ve e-devlet olmanın gereklerini yerine getirmesi gerekmektedir. Yine bilişim teknolojileri kullanımının artırılması ve bunun için toplumsal ve kamusal bilgilendirme ve bilinçlendirme faaliyetlerinin yapılması icap etmektedir.

ABSTRACT

Dazzling development of technology since the second half of the 20. century led to rapid change from the traditional paper-based communication to the modern telecommunication and gave rise to the frequent use of these telecommunication tools in the enactment process of the national and international contracts.

The term contract; stands for a legal process where both side declares their own will in proper manner to reach a legally recognized result, the fact that a contract was enacted through electronic devices constitutes electronic contract. Written, visual, by telephone or electronic- based contracts where parties don't come face to face are called distant contracts. In that sense electronic contracts constitute some sort of distant contracts.

Tool or way used to declare a will called 'process' theoretically, validity of a will declaration, of a legal transaction or of contract is not strictly bound to process. Therefore will declaration can be done either through traditional or in electronic way. But if any given contract has by law or by bilateral will of the parties been bound to process, that contract would not be legally recognized unless it has been done in that particular process.(BK ar.11/2) Additionally contracts acceding a limit put by law have to be proved in written.

In legal transactions, which do not require approval or intervention of any public institution form requirement is meet met by the text and the signature. Signature is any type of sign or security procedure that shows the consent and identity of the relevant person, attached to the text. Any text without signature neither yield any right or obligation to the owner nor does not have any legal effect.

Like classical contracts, electronic contracts or declarations in electronic environment which require form as a condition for validity or proof should include text and signature. Due to nature of the classical signatures they can not be used in electronic environment.

To maintain the same functions and legal protection of the classical signatures in electronic declarations and texts, electronic signatures are existed which protects the integrity and reliability of the text and identity of the sender.

As from the beginning of 2000s, in many countries of the world legal regulations have been put into order. In our country, as well, legal regulation with regard to the electronic signature was made by Law on Electronic Signature of 5070, and the Law has entered into force on 24th July, 2004. The definition of the electronic signature in the Law was determined in a way to cover all types of electronic signature in accordance with the principle of impartiality. Nevertheless, in order that the electronic signature is deemed as equal to hand-written signature, it should bear qualifications of an electronic signature which is based on a qualified electronic certificate provided by an electronic certificate service provider and defined in the law as a reliable electronic signature. According to that, “*a reliable electronic signature results in the same legal consequences like a hand-written signature*” and “*... electronic data which are formed by a reliable electronic signature is equivalent to a deed*”. This means that a reliable electronic signature and a normal signature are equal both functionally and in respect of proof rules. By virtue of this provision, in the field of private law it has become possible both to be able to draw up contracts subject to certain formality rules and those electronic documents signed by means of the electronic signature can be accepted as a deed in courts.

Electronic signature is all kinds of electronic marks meaning the wholeness and invariability of a message created in the electronic environment as well as enabling the identity of the owner of the message. The numerical signature which is one type of electronic signature is a confidential way of communicating and confirmation which is composed of series of *bits* in electronic environment. That form of signature guarantees to provide the determination of the sender of information which is sent or received in electronic environment by using high technology, first of all by cryptography with a key

system, not denial of sending of data by sender and that of received data by receiver, not to be changed the content of the sent or received information, not to understand the content of them even if received by other people.

According to the current Law, electronic records signed with various sorts of electronic signatures which are not meet the standard requirements exactly to be assumed as a reasonable electronic signature and electronic records which are not signed with electronic signatures supposed to accept that they have defect of form and they have not meet the requirements to be accept as a written document. Therefore, these records shall only be determined as “*special terms of a contract*”. Electronic records other than reasonable electronic signatures and records which are signed by these electronic signatures have a little or no legal value. On the other hand, it is known that electronic signatures other than reasonable electronic signatures such as signatures using biometrics methods are legally binding equivalent of the individual’s handwritten signature in some circumstances. As a matter of fact that it seems necessary to make some amendments for improving legal value of many electronic methods of signature or it is necessary to approve “Code of Obligations Draft Law” and “Civil Procedural Code Draft Law” which changes the concept of “written document” and gives more legal value to the electronic records other than reasonable ones as soon as possible.

In Turkish legislation system, with Law 5070, it is provided to practice electronic signatures but it must be noted that the usage of electronics signatures is not in an expected level. One of the reasons of this fact is the percentage number of the population using information techniques is low and the institutions are not started to work in digital system, paper based system is still common in institutions. It is necessary to generalize the usage of electronic signatures by Government and to meet the standart requirements stemming from being e- government. Besides these, it is necessary to increase the percentage of the population using informatics techniques and for this reason it is necessary to raise public awareness in society and public by activities.

KİŞİSEL KABUL / AÇIKLAMA

Yüksek Lisans tezi olarak hazırladığım “Borçlar Hukuku Açısından Elektronik İmza” adlı çalışmamı, ilmi ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazdığımı ve faydalandığım eserlerin bibliyografyada gösterdiklerimden ibaret olduğunu, bunlara atıf yaparak yararlanmış olduğumu belirtir ve bunu şeref ve haysiyetimle doğrularım.

26.12.2007
Fatih ÖNDER

ÖNSÖZ

Bilişim teknolojilerinde yaşanan devrim niteliğindeki ilerlemeler her geçen gün günlük yaşamımızı daha da kolaylaştırmaktadır. Özellikle e-devlet uygulamaları, internet bankacılığı, e-ticaret, internet üzerinden yapılan başvuru işlemleri aracılığıyla saatlerce sıra beklemeden, zaman ve mekândan bağımsız olarak, sadece bir iki dakika içerisinde en hızlı ve en çabuk biçimde istediğimizi elde edebilir hale geldik. İnternet olarak tanımlanan global dünyada hazır bulunanlar yada hazır olmayanlar arasında iletişim kurma imkanlarının bulunması bu kişiler arasında hukuki ilişkiler kurulmasını da doğurmuştur. Ancak bu global dünyanın her an ve herkesin erişimine açık olması ve tarafların birbirleri ile gerçek manada hiç karşılaşmamaları ve kimliklerinden emin olamamaları çeşitli güvenlik kaygılarını da beraberinde getirmiştir. Özellikle elektronik bankacılık ve elektronik ticaret platformlarındaki güvenlik açıkları neticesinde ortaya çıkan kayıplar (ticari casusluk, para aktarımı, yetkisiz erişim v.s.) milyon dolarlar mertebesine ulaşmıştır.

İşte bu güven sorununu ortadan kaldıran ve elektronik ortamda yapılan işlemlerde verilerin bütünlüğünü koruyarak, mesaj gönderen veya işlemi gerçekleştiren kişinin kimliğini belirleyip doğrulayan ve işlemin inkar edilememesini yasal olarak garanti altında alan, ayrıca bu verilerin yasalar önünde delil niteliği taşımasını temin eden elektronik imza uygulaması, 23 Ocak 2004'te Resmi Gazete'de yayımlanarak yasallaşmış ve 23 Temmuz 2004 tarihinde yürürlüğe girmiştir.

Elektronik imzalamada kullanılacak olan gizli anahtar ve elektronik kimlik niteliđi taşıyan elektronik sertifika Elektronik Sertifika Hizmet Sağlayıcısı tarafından verilebilmektedir. Ülkemizde halen Kamu Sertifikasyon Merkezi olarak görev yapan TUBİTAK-UEKAE başta olmak üzere bir resmi, üç adet de özel sertifika hizmet sağlayıcısı faaliyet göstermektedir.

Bu çalışmada elektronik sözleşme, sözleşmelerin şekli, teknik ve hukuki yönleriyle elektronik imza ve elektronik imzanın hukuki sonuçları incelenmiştir.

Bu çalışmanın hukukçulara, ilgilenenlere ve okuyuculara yararlı olmasını diliyorum, bu vesile ile çalışmamda büyük ilgi ve yardımlarını gördüğüm değerli hocam Doç. Dr. Kürşat Nuri TURANBOY'a teşekkür ediyorum. Ayrıca maddi ve manevi desteğini yanımda bulduğum sevgili eşime ve mesai arkadaşlarıma teşekkürlerimi sunarım.

Aralık 2007
Fatih ÖNDER
Hakim

İÇİNDEKİLER

| | |
|--------------------------------|------|
| ÖZET..... | II |
| ABSTRACT..... | V |
| KİŞİSEL KABUL | VIII |
| ÖNSÖZ | IX |
| İÇİNDEKİLER | XI |
| TABLO VE ŞEKİLLER LİSTESİ..... | XVI |
| KISALTMALAR | XVII |
| GİRİŞ | 1 |

BİRİNCİ BÖLÜM

SÖZLEŞMELERDE VE ELEKTRONİK ORTAMDA ŞEKİL ELEKTRONİK İMZANIN HUKUKİ NİTELİĞİ

| | |
|--|----|
| 1.1- Genel Olarak..... | 5 |
| 1.2- Şeklin Fayda ve Sakıncaları | 6 |
| 1.3- Şeklin Türleri | |
| 1.3.1- Kaynaklarına Göre | |
| 1.3.1.1- Kanuni Şekil | 8 |
| 1.3.1.2- İradi Şekil | 9 |
| 1.3.2- Amaçlarına Göre | 9 |
| 1.3.2.1- Geçerlilik Şartı Olarak Şekil | 10 |
| 1.3.2.2- İspat Şartı Olarak Şekil | 10 |
| 1.3.1.1- Kanuni Şekil | 12 |
| 1.3.1.1.1- Sözlü Şekil | 12 |
| 1.3.1.1.2- Yazılı Şekil | 12 |
| 1.3.1.1.3- Resmi Şekil | 14 |

| | |
|---|----|
| 1.3.1.1.4- Tescil | 16 |
| 1.3.1.1.5- İlan | 16 |
| 1.4- Şekil Şartına Uyulmamasının Sonuçları ve Şekil Eksikliğinin Giderilmesi | 17 |
| 1.5- Sözleşmelerde Şekil Şartının Yerine Getirilmesi | |
| 1.5.1- İmza ve Önemi | 19 |
| 1.5.2- İmza Nasıl Atılmalıdır | 22 |
| 1.5.3- Kimler İmza Atmalıdır | 23 |
| 1.5.4- İmzanın Yeri | 24 |
| 1.5.5- El Yazısı İle İmzanın İstisnaları | 25 |
| 1.5.5.1- Alet Vasıtası İle İmza | 26 |
| 1.5.5.2- İmza Yerine Kullanılabilecek İşaretler | 26 |
| 1.6- Elektronik Ortamda Şekil | |
| 1.6.1- Genel Olarak | 28 |
| 1.6.2- Elektronik İmza ve Sayısal (Dijital) İmza Kavramları | 31 |
| 1.6.3- Elektronik İmza Çeşitleri | 36 |
| 1.6.3.1- Basit Elektronik İmza | 36 |
| 1.6.3.2- Gelişmiş Elektronik İmza | 38 |
| 1.6.3.3- Güvenli (Nitelikli) Elektronik İmza | 39 |
| 1.6.3.4- Akredite Edilmiş Sertifika Hizmet Sağlayıcısı Tarafından Verilmiş Sertifikaya Dayanan Elektronik İmza | 40 |
| 1.7- Elektronik imzanın Hukuki Niteliği ve Güveni Elektronik İmza ile El Yazısı İmzanın Fonksiyonel Eşitliği | |
| 1.7.1- Elektronik İmzanın Hukuki niteliği | 41 |
| 1.7.2- Elektronik İmza ve El Yazısı İle İmzanın Fonksiyonel Eşitliği | 44 |
| 1.7.2.1- Sonuçlandırma İşlevi | 45 |
| 1.7.2.2- Devamlılık İşlevi | 45 |
| 1.7.2.3- Kimlik Tespit Etme İşlevi | 46 |
| 1.7.2.4- Gerçeklik İşlevi | 46 |
| 1.7.2.5- Tasdik İşlevi | 46 |
| 1.7.2.6- İspat İşlevi | 47 |
| 1.7.2.7- Uyarı İşlevi | 47 |
| 1.7.2.8- Teklik İşlevi | 47 |

| | |
|---|----|
| 1.8- Elektronik İmza Hakkındaki Uluslararası Düzenlemeler ve Bu Düzenlemelerin Türkiye'ye Yansıması | 48 |
| 1.8.1- UNCITRAL Elektronik Ticaret Model Kanunu | 50 |
| 1.8.2- UNCITRAL Elektronik İmza Model Kanun Tasarısı | 51 |
| 1.8.3- 2000/31 sayılı ve 8 Haziran 2000 tarihli, Avrupa Birliği Elektronik Ticaret Direktifi | 52 |
| 1.8.4- 1999/93/EC sayılı ve 13 Aralık 1999 tarihli, Avrupa Birliği Elektronik İmza Direktifi | 53 |
| 1.8.5- Dünyada Elektronik İmza | 54 |
| 1.8.6- Türkiye'deki Düzenlemeler | 57 |

İKİNCİ BÖLÜM

ELEKTRONİK İMZANIN KULLANIM ALANLARI, ELEKTRONİK SÖZLEŞMELER VE ELEKTRONİK İMZANIN HUKUKİ SONUÇLARI

| | |
|---|----|
| 2.1- Genel Olarak | 60 |
| 2.2- Elektronik İmzanın Genel Kullanım Alanları | 61 |
| 2.3- Güvenli Elektronik İmza İle Yapılamayacak Hukuki İşlemler | 65 |
| 2.4- Elektronik Sözleşmeler | 66 |
| 2.4.1- Sözleşme ve Elektronik Sözleşme Kavramı | 67 |
| 2.4.2- Elektronik Sözleşmelerin Konusu | 69 |
| 2.4.2.1- Fiziki Mal Satışına Yönelik Sözleşmeler | 70 |
| 2.4.2.2- Dijital Ürün Satışına Yönelik Sözleşmeler | 70 |
| 2.4.2.3- Hizmet Sunumuna Yönelik Sözleşmeler | 70 |
| 2.4.2.4- Bilgi Teminine Yönelik Sözleşmeler | 71 |
| 2.4.3- Sözleşmelerin Kurulması | 71 |
| 2.4.3.1- İcap ve İcaba Davet | 72 |
| 2.4.3.1.1- Web Sitesindeki Sunumun Hukuki Niteliği | 75 |
| 2.4.3.1.2- İcabin Bağlayıcılığı | 79 |
| 2.4.3.2- Kabul | 82 |
| 2.4.3.3- Sözleşmenin Kurulduğu, Hüküm ve Sonuçlarını Doğurduğu An | 84 |

| | |
|--|-----|
| 2.4.3.4- Sözleşmenin Kurulduğu Yer | 89 |
| 2.4.3.5- Sözleşmelere Uygulanacak Hukukun Tespiti | 90 |
| 2.4.4- Mesafeli Sözleşme ve Elektronik Sözleşme | |
| 2.4.4.1- Genel Olarak | 92 |
| 2.4.4.2- Tanım | 94 |
| 2.4.4.3- Unsurları | 94 |
| 2.4.4.3.1- Tarafların Fiziksel Olarak Karşı Karşıya Gelmemesi | 94 |
| 2.4.4.3.2- Sözleşmenin Kurulmasında Mesafeli İletişim Araçları Kullanılması | 95 |
| 2.4.4.3.3- Organize Bir Mesafeli Sürüm Sisteminin Varlığı | 96 |
| 2.5- Elektronik İmzanın Türk İspat Hukukundaki Yeri | 96 |
| 2.5.1- Güvenli Elektronik İmza İle İmzalanmış Verilerin Delil Değeri | 101 |
| 2.5.2- Elektronik İmza İle İmzalanmamış Verilerin Delil Değeri | 103 |
| 2.6- Elektronik İmza ve Hukuki Sorumluluk | 106 |
| 2.6.1- Elektronik İmza Sahibinin Sorumluluğu | 107 |
| 2.6.2- Elektronik Sertifika Hizmet Sağlayıcısının Sorumluluğu | 111 |

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK İMZANIN UNSURLARI

| | |
|---|-----|
| 3.1- Genel Olarak | 116 |
| 3.2- Elektronik İmza Kanununda Yer Alan Teknik Terimler | 120 |
| 3.3- Kriptografi (Şifreleme) | 124 |
| 3.3.1- Kriptografide Kullanılan Teknikler | 126 |
| 3.3.1.1- Simetrik Anahtar Şifrelemesi | 127 |
| 3.3.1.2- Asimetrik Anahtar Şifrelemesi | 128 |
| 3.3.1.3- Hybrid Şifreleme Yöntemi | 130 |
| 3.4- Açık Anahtar Altyapısı | 130 |
| 3.4.1- AAA'nın Görevleri | 133 |
| 3.4.2- AAA'nın Bileşenleri | 134 |
| 3.4.2.1- Kayıt Makamı | 135 |

| | |
|--|------------|
| 3.4.2.2- Sertifika Makamı(Elektronik Sertifika Hizmet Sağlayıcısı(ESHS)) | 135 |
| 3.4.2.3- Kök Sertifikasyon Makamı | 136 |
| 3.4.2.4- Sertifika Deposu | 137 |
| 3.4.2.5- Arşiv Modülü | 137 |
| 3.5- Elektronik Sertifika | 139 |
| 3.5.1- Bireysel Sertifika | 142 |
| 3.5.2- Sunucu Sertifikası | 143 |
| 3.5.3- Yazılım Sertifikası | 144 |
| 3.5.4- Kök Sertifika | 144 |
| 3.6- Hash Fonksiyonu | 145 |
| 3.7- Zaman Damgası | 146 |
| 3.8- Sistemin İşleyişi ve Örnek Uygulamalar | |
| 3.8.1- Sistemin İşleyişi..... | 148 |
| 3.8.2- Örnek Elektronik İmza Uygulamaları..... | 152 |
| SONUÇ VE ÖNERİLER | 158 |
| KAYNAKÇA | 163 |
| ÖZGEÇMİŞ | 174 |

TABLO VE ŐEKİLLER LİSTESİ

| | |
|--|-----|
| Őekil-1: Simetrik ve Asimetrik Kriptolama | 129 |
| Őekil-2: BaŐbakanlık Genelgesi İle Kabul Edilen TŐrkiye'nin AŐık Anahtar Altyapısı Modeli | 137 |
| Őekil-3: Bireysel GŐvenli (Nitelikli) Elektronik Sertifika ŐrneĐi..... | 143 |
| Őekil-4: Outlook Express'te Elektronik İmzalı Mail GŐnderme ProsedŐrŐ ... | 149 |
| Őekil-5: Outlook Express'te Kimlik DoĐrulama ve BŐtŐnlŐk KontrolŐ | 150 |
| Őekil-6: Outlook Express'te Elektronik İmzalı ve Őifreli Mail GŐnderme ProsedŐrŐ | 151 |
| Őekil-7: Microsoft Word'da Elektronik İmzalama ProsedŐrŐ | 153 |
| Őekil-8: Adobe Acrobat'ta Elektronik İmzalama ProsedŐrŐ | 155 |
| Őekil-9: Uyp Kelime İŐlemci İle Elektronik İmzalama ProsedŐrŐ | 156 |
| Őekil-10: İmzager-MİM Yazılımı İle Elektronik İmzalama ProsedŐrŐ | 156 |

KISALTMALAR

| | |
|-------|--|
| AAA | : Açık Anahtar Altyapısı |
| AB | : Avrupa Birliđi |
| ABD | : Amerika Birleşik Devletleri |
| ASCII | : American Standart Code Information Interchange |
| ATM | : Asynchronous Transfer Mode |
| AÜHFD | : Ankara Üniversitesi Hukuk Fakültesi Dergisi |
| BK | : Borçlar Kanunu |
| BKZ. | : Bakınız |
| C. | : Cilt |
| CD | : Compact Disc |
| Çev. | : Çeviren(ler) |
| Dn. | : Dipnot |
| DVD | : Digital Versatile Disc - Digital Video Disc |
| E. | : Esas |
| EC | : Electronic Commerce |
| EDI | : Electronic Data Interchange |
| EİK | : Elektronik İmza Kanunu |
| ESHS | : Elektronik Sertifika Hizmet Sağlayıcısı |
| F. | : Fıkra |
| ETKK | : Elektronik Ticaret Koordinasyon Kurulu |
| HD | : Hukuk Dairesi |
| Hk. | : Hakkında |
| HUMK | : Hukuk Usulü Muhakemeleri Kanunu |
| HGK | : Hukuk Genel Kurulu |
| IRC | : Internet Relay Chat |
| ITU | : International Telecommunication Union |
| K. | : Karar |
| KM | : Kayıt Makamı |
| KSM | : Kök Sertifikasyon Makamı |
| M. | : Madde |
| MK | : Medeni Kanun |

| | |
|----------|--|
| M.Ö. | : Milattan Önce |
| MÖHUK | : Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun |
| MSUUEHY | : Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmelik |
| NK | : Noterlik Kanunu |
| OECD | : Organisation for Economic Co-operation and Development |
| PC | : Personel Computer |
| PDA | : Personal Digital Assistant |
| PDF | : Portable Document Format |
| PIN | : Personal Identification Number |
| PKI | : Public Key Infrastructure |
| R.G. | : Resmi Gazete |
| S. | : Sayfa |
| SİL | : Sertifika İptal Listesi |
| SM | : Sertifika Makamı |
| SSL | : Secure Sockets Layer |
| S.Y. | : Sayılı Yasa |
| Sy. | : Sayı |
| T. | : Tarih |
| TBMM | : Türkiye Büyük Millet Meclisi |
| TK | : Tapu Kanunu |
| TMK | : Türk Medeni Kanunu |
| TNB | : Türkiye Noterler Birliği |
| TODAİE | : Türkiye Orta Doğu Amme İdaresi Enstitüsü |
| TTK | : Türk Ticaret Kanunu |
| TKHK | : Tüketicinin Korunması Hakkında Kanun |
| UEKAE | : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü |
| UNCITRAL | : Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu |
| USB | : Universal Serial Bus |
| Vd. | : Ve devamı |
| Vs. | : Ve sair |
| YTL | : Yeni Türk Lirası |
| YKD | : Yargıtay Kararları Dergisi |

GİRİŞ

İnsanođlu toplu halde yaşamak zorunda olan bir varlıktır. Toplu yaşamda ise bireylerin bir birleri ile iletişimde bulunmaları ve diyalog kurmaları kaçınılmazdır. Bu diyalogların büyük bir bölümü ise irade beyanı niteliđi taşımaktadır. İrade beyanı, bir iradeyi açıklamak amacıyla yapılan her türlü davranış olarak tanımlanabilir. İrade beyanının belirli bir şekli yoktur. Dolayısıyla yazı, söz, başı eğme veya kabulü gösterir başkaca bir işaret ve hatta bazı istisnai durumlarda susma bile irade beyanı niteliđi taşıyabilir.¹ Karşılıklı ve bir birine uygun irade beyanlarının bir araya gelmesi neticesinde ise sözleşmeler meydana gelir. Başka bir deyişle sözleşmelerin kurulabilmesi için iletişim şarttır.

İnsanlık tarihine baktığımızda uzak mesafelerle iletişim ve haberleşme için boru, duman, güvercin, haberci ve mektup başta olmak üzere pek çok yöntemle başvurulduđu görülmektedir. Günümüze gelindiğinde ise teknolojiye ki gelişmelere paralel olarak telgraf, telefon, radyo, televizyon ve bilgisayar gibi yeni iletişim araçlarının bu işlevi yerine getirdiđini müşahede etmekteyiz. Özellikle son yıllarda ortaya çıkan ve tüm dünyayı kapsayıp, belli bir merkezi olmayan, bir birlerine bađlı bilgisayar ağlarından oluşan bir ağ sistemi olan internet, kısa sürede yaygın bir iletişim aracı haline gelmiştir. Hatta ITU'nun 1999 yılı istatistiklerinde tarihi gelişim açısından diđer haberleşme araçları ile karşılaştırıldığında internetin 50 milyon kişi arasında fiilen kullanılarak

¹ Velidedeođlu-Özdemir, s.9; Eren, s.122; Birsen, s.54

yaygınlaşma süresinin 4 yıl olduğu, oysa bu sürenin, telefonda 74 yıl, radyoda 38 yıl, kişisel bilgisayarlarda 16 yıl ve televizyonda 13 yıl olduğu tespit edilmiştir.

Türk Borçlar Hukuku'na hâkim olan irade özerkliği ilkesi gereğince kişi, hür bir varlık olarak istediği biçimde ve istediği vasıta ile hukuki ilişkiler kurmak, değiştirmek ve ortadan kaldırmak yetkisine sahiptir. İrade özerkliğinin ana unsurlarından biri olan şekil serbestisi ilkesi gereğince de kanunda aksi belirtilmediği sürece sözleşmenin geçerliliği hiçbir şekle tabi değildir. Bu itibarla, sözleşmeyi meydana getiren irade beyanlarının her türlü iletişim aracı ile muhataba iletilmesi ve bu yolla sözleşmenin kurulması mümkündür. Ancak kanunun belirli bir şekle tabi kıldığı sözleşmelerin geçerli olarak kurulabilmesi için aranan şekil şartına uygun surette yapılması zorunludur. Yine, miktar itibarı ile belli bir meblağı aşan sözleşmelerin geçerli olarak kurulmasında herhangi bir şekil şartı gerekmemekle beraber; hukuki uyumsuzluk halinde bu sözleşmelerin varlığının ve hükümlerinin ispatı yazılı şekilde yapılmış olmasına bağlıdır. Bu sebeple sözleşmelerin ve temelde irade beyanlarının yazılı şekilde yapılması, hukuki koruma başta olmak üzere pek çok fayda sağlar. Yazılı şeklin gerçekleşmesi ise beyan sahiplerinden yükümlülük altına giren kişi veya kişilerin buna dair beyanlarını metin olarak belirtmeleri ve bu metnin altına kimliklerini ve iradelerini ortaya koyacak bir işaret koymaları ile olur. İşte bu işaret imza olarak nitelendirilmektedir. Öyleki, insanoğlunun yazıyı bulup kullanmaya başladığı tarihten bu yana sözleşmenin kurulmasında metin ve imza kullanılagelmiştir.

Yazılı şeklin dolayısıyla imzanın yerine getirdiği şekil şartı ve sağladığı hukuki koruma, teknik iletişim araçları ile yapılan irade beyanları ve kurulacak sözleşmelerin de yazılı şekle dönüştürülmesi ihtiyacını ortaya çıkarmıştır. Özellikle halen tüm dünyada yaygın olarak kullanılan ve kullanımı gün geçtikçe artan internetin, zaman ve mekan sınırı tanımaksızın dünyanın her yeri ile yazılı, sözlü ve görüntülü iletişime imkan vermesi ve para ödeme edimini dahi yerine getirebilmesi, yaygın bir sözleşme kurma aracı haline gelmesine neden olmuştur. Ancak, şekle tabi sözleşmelerin geçerli olarak kurulabilmesi, şekle tabi olmayıp belli bir miktarı aşan sözleşmelerin ise ispatı için metin ve imzanın bulunması gerektiğinden ve el yazısı ile imza yapısı gereği elektronik ortamda kullanılamayacağından, bu durumdaki sözleşmeler internet üzerinde kurulamayacak veya ispat edilemeyecektir. Zira el yazısı ile imza, sahibinin karakteristik bir takım özelliklerini taşıdığından, kişi imzalarken görülme dahi tatbiki

imzalarla imza incelemesi yapıldığı takdirde imzanın o kişiye ait olup olmadığı tespit edilebilmektedir. Oysaki elektronik ortamda oluşturulan bir belgeye dijital kalem veya benzer bir aletle kişinin el yazısı imzası atılsa dahi alınacak çıktıdaki bu imza söz konusu karakteristik özellikleri taşımayacağından, imzanın o kişiye ait olup olmadığının tespiti mümkün olmayacaktır. Yine elektronik ortamda iletişim kuran kişilerin bir birlerini fiziksel olarak görmeleri ve kimliklerini öğrenmeleri fiili olarak mümkün olmadığından, sözleşmeciler tarafların birbirlerinin gerçek kimliklerinden emin olmaları da söz konusu değildir. Öte yandan elektronik ortamın sağladığı hız, imkan ve kolaylıkların bir kenara bırakılmayacağı da bir gerçektir. Öyle ise, elektronik ortamda yapılan irade beyanları ve kurulacak sözleşmelerde hukuki şekil şartını ve korumayı sağlayıp, tarafların kimliklerini doğru olarak tespit edecek ve söz konusu irade beyanlarını içeren elektronik verilerin değişmediğini garanti edecek, yani el yazısı imza ile aynı işlevi sağlayacak bir yöntem ihtiyacı olduğu aşikârdır.

İşte bu ihtiyaca çözüm bulmak amacıyla yapılan teknik çalışmalar neticesinde, kriptografik yöntemlerin kullanımı ile elektronik belgenin matematiksel bir özetinin ve imzalayan kişinin elektronik kimlik bilgilerinin elektronik belgeye eklenerek, bu elektronik belgenin bütünlüğünü ve değişmemişliğini garanti edip, aynı zamanda mesaj sahibinin kimliğini tanımlamaya yarayan bir teknik olan “elektronik imza” ortaya çıkmıştır.

Yüksek lisans tezi olarak hazırlamış olduğum bu çalışma ile, halen toplumun büyük bir kesiminde tereddütlerle yaklaşılan elektronik sözleşmeler ve elektronik ortamda imza fonksiyonunu yerine getiren, elektronik imzaya karşı hissedilen tereddütleri bir ölçüde de olsa izale etme ve toplumda elektronik imzanın tanınması ve yaygınlaşmasına katkıda bulunma hedeflenmiştir.

“Borçlar Hukuku Açısından Elektronik İmza” adını taşıyan bu çalışma üç ana bölüme ayrılmıştır. Birinci bölümde genel olarak sözleşmelerde şekil, imza ve elektronik imzanın hukuki niteliği konuları incelenerek uluslararası toplum ve ülkemizdeki mevzuat çalışmalarına değinilmiştir.

İkinci bölümde elektronik imzanın kullanım alanları, ispat hukuku açısından önemi ve hukuki sorumluluk konuları üzerinde durulmuş ve elektronik imzanın en

önemli kullanım alanı olan ancak toplumumuzda halen tereddütle yaklaşılan elektronik sözleşmeler konusu ele alınmıştır.

Üçüncü bölümde ise elektronik imzanın teknik yönü ele alınmış ve güvenli elektronik imzanın unsurlarını oluşturan kriptografi, açık anahtar altyapısı ve elektronik sertifika konuları incelenmiş ve elektronik imzalama sisteminin işleyişi, sertifika yönetimi ve zaman damgası hususunda bilgiler verilerek, mevcut elektronik imzalama uygulamalarından örnekler verilmiştir.

BİRİNCİ BÖLÜM

SÖZLEŞMELERDE VE ELEKTRONİK ORTAMDA ŞEKİL, ELEKTRONİK İMZANIN HUKUKİ NİTELİĞİ VE ULUSLARARASI DÜZENLEMELER

1.1- Genel Olarak

Bir iradeyi açıklamak için kullanılan araca, dış kalıp veya biçime “*şekil*” adı verilir². Her sözleşmenin, her hukuki işlemin ve dolayısıyla her irade beyanının bir şekli vardır. Bu şekil yazılı, sözlü, resmi olabileceği gibi, iradeyi gösteren bir davranış ve hatta yerine göre susma da olabilir.

Bir sözleşmenin geçerliliği veya ispatı için, irade açıklanmasında belli bir şekil şartı bulunup bulunmadığı hususunda, geçmişte ve günümüzde çeşitli hukuk sistemleri farklı hükümlere yer vermişlerdir. Eski hukuk sistemlerinde şekilcilğe son derece önem verilirken, günümüz hukuk sistemlerinde şekilcilik büyük ölçüde önemini kaybetmiştir³.

Borçlar hukukunun en temel ilkesi olan irade özerkliği, akit serbestisi yanında bunun ayrılmaz bir parçası olan şekil serbestisi ilkesini de kapsamaktadır. Şekil

² Eren, s.243; Tunçomağ, s.215; Velidedeoğlu-Özdemir, s.28; Akıncı, s.88; Akıntürk, s.35

³ Tunçomağ; s.215

serbestisi, bir irade beyanı, hukuki işlem veya sözleşmenin geçerliliğinin belirli bir şekle tabi olmadığı, irade beyanının dışarıya aksettirilmesinde kullanılabilecek araçlardan (yazılı, sözlü, resmi, iradeyi gösterir davranış, susma) herhangi biri ile yapılmasının mümkün olduğunu ifade etmektedir⁴. Borçlar Hukukumuz da 11 inci maddesinde “*Akdin sıhhati, kanunda sarahat olmadıkça hiç bir şekle tabi değildir*” hükmü ile bu ilkeyi açıkça kabul etmiştir.

Bununla beraber kanun koyucu, tarafların, üçüncü kişilerin veya kamunun menfaatini korumak amacıyla, bazı hallerde belirli şekil şartları öngörmüştür. Yine taraflar da sözleşmenin kurulması için şekil şartı öngörebilirler.

Bir irade beyanının elektronik ortamda yapılmasının klasik yöntemle aynı hukuki sonuçları doğuracağı doktrin ve uygulamada kabul görmektedir. Buna göre irade beyanları klasik yöntemlerle yapılabileceği gibi, online (internet telefonu, IRC chat) bir görüşme veya e-posta yoluyla yada bir web sitesindeki sipariş formunun doldurulması suretiyle de yapılabilecektir. Dolayısıyla şekil serbestisi ilkesi kural olarak elektronik ortamda yapılan irade beyanları ve sözleşmeler için de aynen geçerlidir⁵. Bu itibarla elektronik yolla iletilen irade beyanının, muhatap tarafından bilgisayara veya harici belleğe kaydedilip kaydedilmemesinin yada sonradan yazılı olarak teyit edilip edilmemesinin bir önemi yoktur. Bu hususlar irade beyanının ve muhtevasının ispatı ile ilgili konulardır. Yine kanunun yada tarafların öngördüğü şekil şartının elektronik ortamda gerçekleştirilen sözleşmeler için de uygulanabileceği kabul edilmelidir. Zira ileride ayrıntılı olarak inceleneceği üzere kanunun resmi şekil veya özel merasim öngördüğü sözleşmeler ile teminat sözleşmeleri dışındaki sözleşmeler, şekil şartı gerektirse de elektronik imza kullanımı ile gerçekleştirilebilecektir.

1.2- Şeklin Fayda ve Sakıncaları

Hukuki muamelelerin belli bir şekle bağlanması ile, bazen tarafların, bazen de üçüncü kişilerin yada kamunun menfaatini korumak ve hukuki güvenli sağlamak amaçlanır. Bu itibarla şekil şartının aşağıda belirtilen faydaları sağladığı söylenebilir⁶.

⁴ Eren, s.244; Karahasan, s.136; Uygur, s.602

⁵ Şenocak, s.124; İnal, s.96; Yıldırım, s.102

⁶ Tunçomağ, s.216; Eren, s.244-246; Renda-Onursan, s.103; Altınışık, s.70; Birsen, s.133; Reisoğlu, s.65; Başyigit, s.7; Yıldırım, s.102; Özdemir Kocasakal, s.93

a) *Şekil akit yapacak tarafları düşünmeye sevk eder.* Acele karar vermelerini önleyerek dikkatsiz davranmaktan alıkoymaz. Bu hali ile tarafları koruyucu ve uyarıcı rol oynar.

b) *Şekil sözleşmeye kesinlik kazandırır.* Tarafların hukuki işlem yapma iradelerinin ciddi olduğunu, muamelenin bir tasarı veya müzakere olmayıp, kesin olarak yapılmak istendiğini gösterir.

c) *Şekil sözleşmeye açıklık getirir.* Tarafların irade beyanlarına açıklık getirerek, hangi konular üzerinde ne şekilde anlaşmaya vardıklarını net bir şekilde ortaya koyar.

d) *Şekil sözleşmenin yorumunu kolaylaştırır.* Uyuşmazlık halinde davaya bakan hâkim, belirli bir şekilde yapılmış sözleşmenin hükümlerini inceleyerek, irade beyanlarını yorumlama imkânı bulur.

e) *Şekil, aleniyet ve güveni sağlar.* Taraflar arasında yapılan sözleşmeler bazen üçüncü kişileri de ilgilendirir. Hatta hak ve menfaatlerini etkiler. İşte bu gibi hallerde üçüncü kişilerin bu işlemlerden haberdar olması şekil sayesinde olur. Yine özellikle resmi senet veya tescil işlemleri sayesinde sözleşmeler daha sağlam temellere dayandırılarak, hukuki emniyet ve güven sağlanmış olur.

f) *Şekil, hukuki muamelelerin ve özellikle sözleşmelerin ispatını kolaylaştırır.* Uyuşmazlık halinde sözleşmelerin veya hükümlerinin ispatı ancak şekil sayesinde mümkün olur. Şekle uyulmadan yapılan sözleşmelerin ispatı son derece güçtür.

Buna karşılık hukuki işlemlerin belirli şekil kurallarına bağlanması, yukarıda belirtilen faydalar yanında bir kısım önemli ve kaçınılmaz sakıncalara da yol açar. Bunları aşağıdaki gibi sıralamak mümkündür.⁷

a) *Şekle uymamak işlemin (sözleşmenin) geçersizliğine yol açabilir.* Şekil zorunluluğu kabul edilen hallerde, konu ve irade uyuşması yönünden bir problem olmamakla beraber, şekil eksikliği nedeniyle sözleşme geçersiz sayılacak; dürüst olan

⁷ Tunçomağ, s.216; Eren, s.248; Altınışık, s.70; Birsen, s.132; Velidedeoğlu-Özdemir, s.30; Başıyigit, s.8; Renda-Onursan, s.103

ve belki de bundan habersiz olan tarafın irade açıklamaları etkisiz kalacak ve mağduriyeti söz konusu olacaktır.

b) *Şekil sözleşme yapılmasını güçleştirir.* Hukuki işlemlerde sürati önler, para ve zaman kaybına neden olur. Söz konusu şekil şartı ne kadar basit olursa olsun, hukuki işlemlerin yapılmasını güçleştirir. Ticari hayatı ağırlaştırır. Resmi şekle bağlı kılınan birçok sözleşme taraflara ekonomik külfet yükler. Taraflar sözleşme yapmak istemelerine rağmen bazen sırf şekilden yıldıkları için vazgeçebilmekte veya sözleşmeyi geciktirmektedirler.

c) *Şekil bazı hallerde ispat hukukunda gerçeğe aykırı karar verilmesine yol açar.* İspat hukuku açısından şekil şartı lazım gelen hallerde şekle uyulmaması tarafların sözleşmeyi veya hükümlerini ispat edememelerine yol açacak ve hâkim tarafından fiili gerçeğe aykırı karar verilmesi sonucunu doğuracaktır.

İşte yasa koyucu bu fayda ve sakıncaları göz önüne alarak, kural olarak şekil serbestisini kabul etmiştir. Ancak çok önemli kabul ettiği bazı istisnai hallerde şekle uyma zorunluluğu koymuştur. Yine bu yönde taraf iradelerine de değer vermiştir. Ayrıca genel olarak şekli de, kendisine uyulması güç olmayacak şekilde düzenlemeye gayret etmiştir⁸.

1.3- Şeklin Türleri

1.3.1- Kaynaklarına Göre

1.3.1.1- Kanuni Şekil

Kanunun, bir hukuki işlemin veya sözleşmenin geçerli olmasını şekil şartına bağladığı durumlarda kanuni şekilden söz edilir. Bu gibi hallerde yapılan hukuki işlem, öngörülen şekle uygun yapılmamış ise geçerli olmaz (BK. m.11/2).

Hukuk sistemimizde yasaların belirlediği değişik şekil türleri bulunmaktadır. Bunları ileride “Kanuni Şekil” ana başlığı altında ayrı ayrı inceleyeceğiz.

⁸ Tunçomağ, s.217

1.3.1.2- İradî Şekil

Hukukî işlemlerin veya sözleşmelerin şekil şartına bağlanmasının her zaman yasadan kaynaklanmaz, taraflar da yasadaki şekil şartına bağlanmamış bir sözleşmeyi şekil şartına bağlayabilirler. Yine taraflar bu şeklin hukukî sonuçlarını, geçerlilik şartı veya ispat şartı olarak kendileri tayin edebilirler. Taraflar bu konudaki iradelerini açıklamamışlarsa, kararlaştırılan şeklin sıhhat şartı olduğu karene olarak kabul edilir ve bu şekle uyulmadıkça sözleşme geçerli olmaz (BK. m. 16/1). İşte bu durumda iradî (kararlaştırılmış) şekilden söz edilir. Ancak bu kural şekil serbestisi olan veya ispatı şekle bağlı yapılmasına bağlı olan sözleşmeler için uygulanabilir. Yoksa kanun sözleşmenin geçerli olmasını belli bir şekle bağlı kılmış ise, taraflar bunun aksine bir şekli kararlaştıramazlar⁹. Örneğin taşınmaz mal ve motorlu taşıt alım satımı yasa gereği resmi şekle bağlanmıştır. Şu halde taraflar bunun aksine bir şekil şartı öngörmüş, hatta buna göre muamele yapmış da olsalar, yapılan sözleşme geçersiz olup, mülkiyet alıcıya geçmez.

Yine BK. m.16/2 ve Türk Borçlar Kanunu tasarısı m. 17/2 gereğince taraflar bir şekil şartı öngörmüş iseler, aksi kararlaştırılmamış ise yasanın bu şekil için aradığı koşullarla uyulması gerekecektir. Örneğin taraflar sözleşmenin geçerliliği veya ispatı için yazılı olarak yapılmasını şart koşmuş iseler. Kanunun yazılı şekil için öngördüğü “borç altına girenlerin imzaları” sözleşmede bulunmak zorundadır. Aksi halde yazılı şeklin şartları tamamlanmamış olacaktır.

1.3.2- Amaçlarına Göre

Hukuk sistemlerinin, hukukî işlemlerin yapılmasında şekle uyulması zorunluluğu öngördükleri hallerde, bu hükümlerde ön görülen amaç ve hukukî sonuçlar da her zaman aynı değildir. Bazen, bir işlemin geçerliliği belli bir şekle uyularak yapılmasına bağlanmış ve bu şekle uyulmadıkça işlemin (sözleşmenin) hüküm ifade etmeyeceği kabul edilmiştir. Bu gibi hallerde şekil “*sıhhat*” (geçerlilik) şartıdır. Buna karşılık, sözleşmenin geçerli olarak kurulması için herhangi bir şekle uyulması ön görülmemekle beraber; anlaşmazlık halinde sözleşmenin varlığının ve hükümlerinin ispat edilebilmesi için, ancak belli bir şekilde yapılmış olması gerektiği hükmüne yer verilmiştir. Bu gibi hallerde, şekil “*ispat şartıdır*” ve bir yargılama usulü kuralıdır.

⁹ Eren, s.250; Akıntürk, s.35; Reisoğlu, s.66; Akıncı, s.94

Buna göre şekil, öngörülen amaç açısından, geçerlilik şartı ve ispat şartı olarak ikiye ayrılır.

1.3.2.1- Geçerlilik Şartı Olarak Şekil

BK. m. 11/2'ye göre: “*Kanunun emrettiği şeklin kapsam ve etkisi hakkında başkaca bir hüküm yoksa, sözleşme bu şekle uyulmadıkça geçerli olmaz.*” Buna göre kanun, bir sözleşmenin belli bir şekilde yapılmasını emretmişse, emredilen şekil, kural olarak “*sıhhat(geçerlilik) şartı*”dır. Dolayısıyla bu şekil şartına uyulmadıkça sözleşme geçerlilik kazanmaz¹⁰.

Kanunun emrettiği şekilde yapılmayan sözleşmeler (aksine bir hüküm mevcut değilse) geçersizdirler, batıldır. Örneğin, gayrimenkullerin alım-satımına ilişkin sözleşmelerin TMK. m. 706 uyarınca resmi şekilde yani (Tapu Kanunu m. 26'ya göre) Tapu Sicil Muhafızlığı tarafından düzenlenmesi gerekir. Yine BK.'nun 163 üncü maddesi gereğince alacağın temlik sözleşmesi yazılı olarak yapılmadıkça geçerli değildir. Şu halde kanunda sözleşmelerin kurulması için öngörülen şekil şartları sıhhat şartı olmakla başka şekilde geçerli olarak kurulamazlar ve yine emredici nitelikte olup, taraflar anlaşarak bu kuralları etkisiz kılamazlar¹¹.

Kanunun şekil şartı öngördüğü sözleşmelerin şekle uygun yapıp yapılmadığını ve dolayısıyla geçerli olup olmadığını hâkim resen göz önüne almak zorundadır. Taraflar da, sözleşmenin kanuni şekle uyulmaksızın yapıldığını ve hükümsüz olduğunu ileri sürmek hakkına sahiptir.

1.3.2.2- İspat Şartı Olarak Şekil

Şeklin sakıncalarını gidermek amacı ile hukuk sistemimizde şekil serbestisi ilkesinin kabul edildiğini belirtmiştik. Buna göre yasanın şekil şartı öngörmediği tüm sözleşmeler, kabul beyanının muhataba ulaştığı anda kurulmuş olur. Sözleşmeyi meydana getiren irade beyanlarının herhangi bir şekilde yapılması yeterlidir. Zira sözleşmede asıl olan, karşılıklı ve birbirine uygun irade beyanlarıdır (BK. m. 1). Şu halde bu tür sözleşmelerin geçerli olarak kurulması için yazılı olmaları gerekmez.

¹⁰ Tunçomağ, s.219; Eren, s.248; Reisoğlu, s.66; Akıntürk, s.36; Orta, s.30; Altınışık, s.71

¹¹ Reisoğlu, s.66; Orta, s.30; Keser Berber (Şekil), s.11

Ancak uygulamada da sık rastlandığı üzere; sözleşmelerin şekil şartına uyulmaksızın geçerli olarak kurulmasına rağmen, ifa aşamasında birtakım anlaşmazlıklar çıktığında, sözleşmenin ispatı sorunu ile karşılaşmaktadır. İşte kanunla veya taraf iradeleriyle, sözleşmenin, ancak kararlaştırılan şekilde ispatlanabileceğinin öngörülmesi durumunda ispat şartı olan şekilden bahsedilir. Bu tanımdan da anlaşılacağı üzere ispat şartı olarak konulmuş şekil, sözleşmenin geçerliliğini etkilememekte, ispatını mümkün kılmakta veya kolaylaştırmaktadır¹². Mevzuatımızda HUMK m. 288 vd. gereğince 400-YTL' nı aşan hukuki işlemler bakımından senetle (kesin delille) ispat zorunluluğu kabul edilmiştir¹³. Ayrıca; senede bağlı iddialara karşı ileri sürülen iddialar da ancak senetle ispatlanabilir(HUMK m.290). Yine bir belgenin senet olarak nitelendirilebilmesi için, onu meydana getirenin imzasını taşıması gerekir. İmzalanmamış hiçbir belge senet niteliği taşımaz.¹⁴

Şu halde, HUMK. 288 inci maddesinde belirtilen miktardan daha fazla alacak veya borç içeren bir hukuki işlem, şekil serbestisi gereğince taraflarca şekle uyulmadan (sözle, davranışla, v.s) yapılmış irade beyanları ile kurulmuş olacaktır. Ancak ifa aşamasında edimlerin yerine getirilmemesi veya başka bir sebeple uyuşmazlık çıkması halinde, “*ispat şartı*” olan yazılı şekle uyulmadığından ispat edilemeyecek ve hak kaybına yol açabilecektir.

HUMK.'nun “belirli bir meblağın üzerindeki işlemlerin ispatı ve senede dayanan her türlü iddianın aksinin senetle ispatlanacağı” hükmünü içeren 288 ve 290 inci maddeleri karşısında, hukuk sistemimizin kabul ettiği şekil serbestisi ilkesinin zedelendiği bir gerçektir. Zira ispat edilemeyen bir hakkın varlığı tartışmalıdır¹⁵.

Usul hukukundaki senetle ispat şartına ilişkin kurallar kamu düzenine ilişkin değildir. Bu nedenle aksi yasada belirtilmedikçe hâkim tarafından resen nazara alınmazlar. Taraflar bu kuralların aksini kararlaştırabilir ve yapacakları sözleşmeyle etkisiz kılabilirler. Yine ispatı yazılı şekle bağlanmış sözleşmeler, kabul, ikrar ve yemin gibi delillerle ispat edilebilirler. Buna karşılık, kanunun belirli bir şekilde yapılmasını öngördüğü sözleşmelerde şekil, sıhhat şartı olduğundan bu şekle uyulmaması

¹² Tunçomağ, s.220 Orta, s. 33; Altınışık, s.33; Reisoğlu, s.78

¹³ Kesin Deliller; “senet, ikrar, yemin, kesin hüküm” dür.

¹⁴ Kuru, s.2076

¹⁵ Tunçomağ, s.220; Acır, s.40; Orta, s.34; Altınışık, s.72

sözleşmeyi hükümsüz kılacağından; kanunun emrettiği şekilde yapılmamış olan bu sözleşmelerin varlığı diğer kesin deliller ile de ispat edilemez¹⁶.

1.3.1.1- Kanuni Şekil

İlgili yasalarda öngörülen şekil şartlarına göre, hukuk sistemimizin hukuki işlemlerin geçerli olarak kurulabilmesi için kabul ettiği şekilleri, aşağıdaki şekilde beş grupta toplamak ve incelemek mümkündür;

- 1) Sözlü şekil
- 2) Yazılı şekil,
- 3) Resmi şekil,
- 4) Tescil,
- 5) İlan.

1.3.1.1.1- Sözlü Şekil

Şekil serbestisi ilkesi gereğince, hukuki işlemlerin ve dolayısıyla sözleşmelerin sözlü olarak kurulması mümkündür. Ancak bu bir sıhhat şartı değildir. Oysa ki, istisnai de olsa, bazı sözleşmelerin geçerli olarak kurulabilmesi için sözlü olarak irade beyanında bulunulması şarttır.

Borçlar kanununda geçerliliği sözlü şekle tabi kılınmış bir sözleşme mevcut değildir. Ancak Medeni Kanunda, evlenme akdinin kurulabilmesi için eşlerin bizzat kendilerinin evlendirmeye yetkili kişi huzurunda sözlü olarak iradelerini açıklamaları gerekmektedir(TMK. m.42). Yine sözlü vasiyetnamede de vasiyetin geçerli olması için yasada belirtilen şartlara uygun olarak sözlü olarak vasiyetin yapılması gerekmektedir(TMK. m.539).

1.3.1.1.2- Yazılı Şekil

Hukuki muamelelerde genellikle uygulama alanı bulan yazılı şekildir. Yazılı şekil bir hukuki muamelenin herhangi bir belgeye bürünerek ortaya çıkmasını ifade

¹⁶ Eren, s.251

eder. Bu belge, el yazısı, daktilo ve bilgisayar gibi vasıtalarla kağıt ve benzeri ortama yazılmış şekilde olabileceği gibi, daha önceki açıklamalarımızda da belirttiğimiz şekilde, kağıtsız olarak elektronik ortamda da bulunabilir. Ancak yazılı şeklin gerçekleşmesi için söz konusu bu belgenin borç altına girenlerce imzalanması gerekir¹⁷.

Bunun yanında kanunu koyucu, çok istisnai bazı hallerde yazılı şekilde vasıflandırma aramış ve bizzat el yazısı ile yazılması gerektiğini belirtmiştir. Örneğin el yazısı ile vasiyetnamede tarih dâhil vasiyetnamenin tamamı, vasiyetçi tarafından el yazısı ile yazılmalıdır(TMK. m.538). Yine kefalette, imza haricinde, kefil olunan miktarın da kefilin el yazısı ile yazılması gerekir(BK. m.484). Kıymetli evrak hukukunda da bazı kıymetli evrakların imza dışında el yazısı ile yazılması gereken bölümleri bulunmaktadır.

Kanun koyucu bazı sözleşmelerin geçerliliğini yazılı olarak yapılmasını şartına bağlamıştır. Yazılı şekil BK. 12-15 arası maddelerde düzenlenmiştir. Ancak burada yazılı şeklin tanımı yapılmamıştır. Ancak BK.m.12 hükmü gereğince yazılı şeklin sözleşmenin tüm esaslı noktalarını kapsaması gerekir. Tamamlayıcı kısımların bu şekil dışında bırakılması sözleşmeyi geçersiz kılmaz. Buna göre sözleşmenin tüm esaslı noktalarını oluşturan irade beyanlarının yazılı bir metinde açıklanması ve beyanda bulunan tarafından imzalanması yazılı şekli gerçekleştirir. Hukukumuzda, alacağın temliki (B.K. m. 163), şuf'a sözleşmesi (B.K. m. 213/2), bağışlama vaadi (B.K. m. 238/2), kefalet (B.K. m. 484), tüketiciye taksitle satış (TKHK. m.6), toplu iş sözleşmesi(2822 s.y. m.4) ve daha pek çok sözleşme için yazılı şekil öngörülmüş bulunmaktadır.

Yazılı şekilde yapılan sözleşme “*metin*” ve “*imza*” olmak üzere iki bölümden oluşur.

Metin; Taraf iradelerini dil araçları ile biçimlendirip yazılı şekilde ifade eden belgeye *metin* denir¹⁸. Metin açısından yazının üzerine yazıldığı maddenin ve yazının ne tarzda ve ne ile yazıldığına herhangi bir önemi yoktur. Metin el ile yazılabileceği gibi, başka bir uzuvla, herhangi bir alet vasıtasıyla herhangi bir yere yazılabilir. Önemli

¹⁷ Uygur, s.807; Eren, s.252; Tunçomağ, s.221; Reda-Onursan, s.105; Velidedeoğlu-Özdemir, s.32

¹⁸ Eren, s.252; Akıntürk, s.37; Akıncı, s.90; Altınışık s.74

olan bu metnin imzalanabilir olmasıdır. Türk Borçlar Kanunu tasarısının 14 üncü maddesinde de bu hususa işaret edilerek, saklanabilmesi koşulu ile “güvenli elektronik imza ile gönderilen” metinlerinde yazılı şekil şartlarını taşıdığı kabul edilmiştir. Metin taraflardan biri tarafından yazılabileceği gibi bir üçüncü kişi tarafından da yazılabilir. Metnin tümünün aynı kağıt veya başka bir madde üzerinde bulunması gerekmez. Ancak, birden fazla metin arasında imzaların bunların tümünü kapsadığını gösteren bir bağlantı bulunmalıdır. Yine metin sözleşme tarzında olmayıp mektup, telgraf v.s tarzda da olabilir. Metnin tarafların anlayabileceği herhangi bir dil ve alfabe ile de yazılması mümkündür¹⁹.

Metin sözleşmenin objektif ve sübjektif yönden bütün esaslı noktalarını kapsamalı ve açık olmalıdır. Şekil şartı yerine geldikten sonra metnin kısmen veya tamamen tahrip olması geçerliliği etkilemez. Önemli olan bu hususun ispat edilebilmesidir.

İmza; bir irade açıklamasının kendisine ait olduğunu ifade etmek üzere, kişinin ismi için kullandığı özel biçimdeki çizgi ve harflerden oluşan işarettir²⁰. Buna uygulamada “ıslak imza” da denmektedir. İmza çok eski zamanlardan beri kullanılmakta olup, geleneksel bir yöntem haline gelmiştir. İmza bir yandan kişinin hüviyetini tespit ederken, diğer yandan da irade beyanını oluşturan metnin içeriğini bildiğini (okuyup anladığını), metnin son şeklini almış olduğunu, metnin içeriğinin imza sahibini hukuken bağladığını, ifade eder.²¹

Eserimizin ana konusunu genel olarak “imza”, özel olarak ise “Elektronik İmza” oluşturduğundan, her iki konu da ileride ayrı başlıklar halinde teferruatlı olarak incelenecek olup²², burada ayrıntıya girmekten kaçınılmıştır.

1.3.1.1.3- Resmi Şekil

Türk ve İsviçre hukukunda bir kısım hukuki işlemlerin, sözleşmelerin geçerliliği resmi şekilde yapılmasına bağlanmıştır. Resmi şekil ile adi yazılı şeklin mahiyet farkı bulunmayıp, her ikisi de yazılı olarak yapılmaktadır. İkisi arasındaki fark belgeyi

¹⁹ Eren, s.252-253; Tunçomağ, s.222; Akıntürk, s.38; Reisoğlu, s.72; Akıncı, s.90

²⁰ Tunçomağ, s.222; Eren, s.253; Altınışık, 74; Başyigit, s.11; Orta, s.25

²¹ Tunçomağ, s.222; Eren, s.253; Altınışık, s.74; Keser Berber (Şekil), s.11, Ensari, s.1; Orta, s. 25

²² Bkz. s.58 vd. ve s.67 vd.

meydana getirenlerin farklı olmasıdır. Bir işlemin resmi şekilde yapılması, taraflara ait irade açıklamalarının ve işlemin yetkili bir makam veya şahıs önünde, kanunların öngördüğü usul ve koşullara uyularak yapılması ya da bu makamlarca onaylanması suretiyle gerçekleşir²³. Örneğin, gayrimenkullerin alım-satımına ilişkin sözleşmelerin geçerli olabilmesi, resmi şekilde yapılmasına (TMK. m. 706), yani tapu sicil memuru veya müdürü tarafından düzenlenmelerine bağlıdır (TK. m. 26). Resmi şekle bağlanmış bir sözleşmeye ilişkin değişiklikler de yine resmi şekilde yapılmalıdır²⁴.

Borçlar Kanunumuzda, resmi şekli düzenleyecek makamlar belirtilmemiştir. Ancak mevzuatımızın incelenmesinde görülecektir ki, bu kişi ve makamlar, noter, sulh hâkimi, köy ihtiyar heyeti ve tapu sicil memuru veya müdürüdür.

Hukukumuzda, resmi şekli yerine getiren makamlar öncelikle noterlerdir. Zira Noterlik Kanunu 82. maddesi gereğince noterler tarafından yapılan bütün işlemler resmi nitelik taşımaktadır. Yine aynı yasanın 60. maddesi gereğince noterler, aksine yasal bir düzenleme yoksa kanunlarda resmi şeklide yapılması öngörülüp de yapılması başka bir kişi, merci veya makama verilmemiş ya da görevlisi belirtilmemiş olan bütün sözleşmeleri düzenlemeye ve/veya onaylamaya yetkilidirler. Bu hükmün açıkça aksini öngören hükme örnek olarak Tapu Kanunu 26 ncı madde gösterilebilir. Zira bu maddeye göre gayrimenkullerin aynına, özellikle mülkiyetinin devrine ilişkin sözleşmeler ancak tapu sicil müdür veya memurları tarafından yapılabilir. Bu tarz sözleşmeleri noterler düzenleyemezler. Aksi halde bu sözleşme geçersiz olur.

Resmi şekilde yapılan hukuki işlemler, diğer yazılı şekillere göre daha yüksek ispat gücüne sahiptir. TMK. 7 nci maddesi gereğince, “*Resmi sicil ve senetler, belgeledikleri olguların doğruluğuna kanıt oluşturur*”. Noterlerin düzenledikleri belgeye “noter senedi” denilmektedir. Noterler düzenleme şeklinde senet yapabilecekleri gibi, onaylama şeklinde senet de yapabilirler. Düzenleme halinde senetler, içeriği de dahil olmak üzere, sahteliği sabit oluncaya kadar geçerlidir ve kesin delil oluştururlar(NK. m.82-HMUK. m.295). Onaylama şeklinde yapılan senette ise, noterce yapılan onaylama belgenin içeriğini kapsamayıp, belgedeki tarihi ve altındaki

²³ Tunçomağ, s.230; Eren, s.261; Ulukapı, s.2; Reisoğlu, s.77; Orta, s.31; Özdilek, s. 28

²⁴ Eren, s.265; Reisoğlu, s.77

imzanın ilgiliye ait olduğunu belirlediğinden, tarih ve imza sahteliği sabit oluncaya kadar geçerlidir²⁵.

Noterler dışında da resmi şekli gerçekleştiren makamlar bulunmaktadır. Resmi şekilde yapılması gereken sözleşme, taşınmazlar üzerindeki aynı haklara ilişkin bulunuyorsa bu sözleşmeyi yapmaya yetkili makam, tapu sicil memuru veya müdürüdür. Yine resmi vasiyetnameyi yapmaya yetkili makam sulh hâkimidir. TMK'nun 532 nci maddesi gereğince resmi vasiyetname, iki tanığın katılımı ile, sulh hakimi, noter veya yasayla kendisine yetki verilmiş başka bir görevli huzurunda yapılır. Ayrıca imza atmaya muktedir olmayan kişilerin kullandığı işaretler köy ihtiyar heyeti tarafından tasdik edilir.

1.3.1.1.4- Tescil

Kanun bazı hukuki işlemlerin geçerliliğini, yasa gereği tutulan resmi sicillere kayıt düşürülmesine bağlamıştır. İşte bu hukuki işlemler söz konusu sicile tescil edilmedikçe geçerlilik kazanamazlar. Bu nedenle bu işlemler için tescil şekil şartıdır²⁶. Örneğin, mülkiyeti muhafaza sözleşmesi, ancak resmi şekilde yapılacak sözleşmenin, menkul malı alan kimsenin yerleşim yerindeki noter tarafından özel siciline kaydedilmesi sonucunda geçerli olacaktır (TMK. m. 764). Aynı şekilde taşınmazlara ilişkin tün aynı haklar tapu siciline tescile tabidir. Vakıfların vakıf siciline, şirketlerin de ticaret siciline kaydedilmesi söz konusudur.

1.3.1.1.5- İlan

İlan, belirli bir durumun, üçüncü kişilerin haberdar olabilmeleri için, herkesin duyabileceği bir şekilde açıklanmasıdır²⁷. Kanun bazı hukuki işlemlerin ilan edilmesini öngörmüş ve bu ilana belli hukuki sonuçlar bağlamıştır. Örneğin, BK. m. 179 uncu maddesi gereğince, bir işletmenin aktifleri ve pasifleri ile birlikte devralınması halinde bu durumun gazetelerde ilanı gerekmektedir. Aynı şekilde Medeni Kanuna göre, vasi tayini, gaiplik, hacir ve kazai rüşd kararlarının ilanı gerekmektedir.

²⁵ Eren, s.265; Ulukapı, s.5-6

²⁶ Eren, s.263; Tunçomağ, s.221;Orta, s. 32; Reisoğlu, s. 78; Akıncı, s.93

²⁷ Eren, s.264

1.4- Şekil Şartına Uyulmamasının Sonuçları ve Şekil Eksikliğinin Giderilmesi

Kanunen veya taraf iradelerince geçerliliği şekil şartına bağlanmış olan bir sözleşme, bu şekil şartına uygun olarak yapılmadığı sürece geçersizdir(BK. m.11/2). Ancak söz konusu geçersizliğin hukuki niteliği hususu doktrinde tartışmalıdır. Bazı yazarların savunduğu “yokluk” görüşüne göre, şekle uyulmamışsa sözleşme geçersiz olmayıp, henüz meydana gelmemiştir. Yani yoktur²⁸. Bir kısım yazarlar ise, söz konusu geçersizliğin kendine özgü (sui generis) geçersizlik olup, şekil şartının amacının tarafları korumak olduğundan bahisle, ancak taraflarca ileri sürülebileceği, üçüncü kişilerce ileri sürülemeyip, hakim tarafından da resen nazara alınamayacağını kabul etmektedirler²⁹. Doktrinde ve uygulamada çoğunlukla kabul edilen ve bizimde katıldığımız görüşe göre ise, şekil eksikliğinin müeyyidesi kesin hükümsüzlüktür (butlan). Yani şekil şartına uyulmadan yapılan bir sözleşme batıldır³⁰. Sözleşme en başından itibaren hüküm ifade etmez, taraflara bir hak veya borç yüklemes. İfa edilen edimler geçerli bir hukuki sebepten yoksun olduğundan geri istenebilir. Ayrıca taraflar veya üçüncü kişiler her zaman bu hükümsüzlüğü ileri sürebilecekleri gibi hâkim de resen nazara almak zorundadır. Sözleşme zamanla veya icazet ile geçerli hale gelmez.

Şu halde, sözleşme şekil noksanlığı nedeniyle batıl olduğundan, geçersizliğini ileri sürmek, kural olarak, ahlaka ve iyi niyet kurallarına aykırı bir davranış olmadığı gibi, haksız fiil de sayılmaz³¹. Bununla birlikte uygulamada ve doktrinde bazı istisnai durumlarda şekle aykırı yapılmış işlemin hukuki sonuç doğurabileceği kabul edilmektedir. Bunlar hakkın açıkça kötüye kullanılması halinde sözleşmeye geçerlilik tanıma ve tahvildir.

Türk Medeni Kanununun 2 nci maddesi gereğince, herkes haklarını kullanırken veya borçlarını ifa ederken dürüstlük kuralına uymak zorundadır. Bir hakkın açıkça kötüye kullanılmasını hukuk düzeni korumaz. Şekle aykırılığı ileri sürmek kural olarak hakkın kötüye kullanılması değildir. Ancak Yargıtay uygulamasında ve doktrinde iki

²⁸ Nomer, s.604

²⁹ Nomer, s.601; Karahasan, s.180; Eren, s.270

³⁰ Tunçomağ, s.236; Nomer, s.621;Renda-Onursan, s.109; Eren, s.268; Uygur, s.603; Akıntürk, s.41

³¹ Renda-Onursan, s.110; Eren, s.268; Uygur, s.604; Reisoğlu, s.66

halde şekil noksanlığına dayanarak sözleşmenin hükümsüzlüğünü ileri sürmenin hakkın kötüye kullanılması sayılabileceği kabul edilmiştir.

İlk olarak, sözleşme şekle aykırı yapılmakla beraber, taraflar her türlü yanılığdan uzak bir şekilde bilerek ve isteyerek edimlerini tamamen veya büyük ölçüde ifa etmişlerse, artık sözleşmenin geçersizliğini ileri sürmek hakkın kötüye kullanılmasını oluşturabilecektir³². Bu durum uygulamada genel olarak *kat mülkiyeti* ve *kat-arsa karşılığı inşaat sözleşmelerinde* karşımıza çıkmaktadır. Zira, Yargıtay uygulamasına göre; kat mülkiyeti kanununa göre yapımına başlanan taşınmazda, bağımsız bölüm satımına ilişkin şekle uygun sözleşme yapılmadan taraflar edimlerini yerine getirmiş yani, alıcı yükümlülüklerini ifa etmiş, satıcı da bağımsız bölümü teslim etmiş ise; yine kat-arsa karşılığı inşaat sözleşmelerinde, sözleşme resmi şekilde yapılmasa dahi taraflar borçlarını büyük ölçüde yerine getirmişler ise; örneğin yapı kullanma izni alınmış, inşaat yüzde doksanın üzerinde tamamlanmış ise, artık şekil noksanı nedeniyle sözleşmenin geçersizliğini ileri sürmek ve bu nedenle mülkiyeti devir borcundan kaçınmak açıkça hakkın kötüye kullanılması sayılmalıdır. Bu durumda şahsi hak sahibi olan yüklenicilerin sözleşmede öngörülen yükümlülüklerini yerine getirdikleri oranda, bu haklarına dayanarak arsa sahibinden mülkiyetin kendilerine devredilmesini isteyebilirler³³.

İkinci olarak ise; şekil eksikliğine, şekle aykırılığı bildiği halde karşı tarafı hile ile aldatarak veya kasten şekle aykırılığa sebebiyet veren taraf şekle aykırılığa dayanarak sözleşmenin butlanını ileri sürerse, bu hakkın kötüye kullanılması olur³⁴. Bu durumda da hâkim geçersiz muameleyi geçerli sayarak aynen tazmine hükmedebileceği gibi, aldatılan tarafın şekil noksanlığı nedeniyle uğradığı zararın tazminine de karar verebilir³⁵.

Hakkın kötüye kullanılması hali dışında şekle aykırı işleme geçerlilik tanınması “tahvil” de karşımıza çıkmaktadır. Tahvil, kanuni gereklerine uyulmaması nedeniyle batıl sayılması gereken bir hukuki işlemin, varlık unsurlarının gerçekleştiği diğer bir hukuki işleme çevrilerek varlığını sürdürme imkânının sağlanmasıdır. Diğer bir ifade ile

³² Karahasan,s.183; Uygur, s. 604-605; Eren, s.268; Tunçomağ, s.237; Nomer, s.608; Reisoğlu, s.67

³³ Yargıtay 14. HD. 7.5.1985 T. 1985/3269 K.; 15. HD 19.02.1992 T. 3622/741 E.K-16.03.1992 T. 4892/1299 E.K sayılı ilamları

³⁴ Karahasan,s.184; Uygur, s.605; Eren, s.269; Tunçomağ, s.236; Reisoğlu, s.67

³⁵ Yargıtay 13. HD. 05.03.1992 T. 10335 E. – 2032 K.

şekil eksikliği nedeniyle batıl olan bir hukuki muamele yerine, bu muamelenin gerçekleştirmek istediği amacı veya doğurmak istediği sonucu başka bir hukuki muamele doğurabilecek ise ve de hali hazırdaki şekil bu muamele için yeterli ise, ayrıca tarafların farazi iradeleri de bu yönde kabul edilebilecek ise, o takdirde batıl muamele geçerli olan bu muameleye yerine geçer³⁶.

Uygulamada bu durum genel olarak gayrimenkul satış vaadi olarak karşımıza çıkmaktadır. Gerçekten de gayrimenkullerin satışının tapu sicil müdürlüğünde yapılmaması halinde söz konusu satış geçersizdir. Ancak taraflar bu satışı noterde resmi şekilde yapmış iseler. Noterlerin gayrimenkul satış vaadi sözleşmesi yapmaya yetkileri olduğu ve taraflarında bu yönde iradelerinin var olduğunun kabul edilmesi halinde, geçerli olmayan bu satış sözleşmesi, gayrimenkul satış vaadi sözleşmesi olarak kabul edilebilir. Aynı şekilde miras sözleşmesi yapmak için hukuki işlem ehliyetine sahip olmak gerekmektedir. Bununla birlikte on beş yaşını doldurmuş ancak henüz hukuki işlem ehliyeti için gerekli yaşa ulaşmamış bir şahsın resmi şekilde miras sözleşmesi yapması halinde, bu sözleşme geçersiz olacaktır. Ne var ki bu işlem resmi vasiyetname olarak kabul edilebilecektir.

1.5- Sözleşmelerde Şekil Şartının Yerine Getirilmesi

1.5.1- İmza ve Önemi

İnsanoğlu, yazıyı bulup kullanmaya başladığı günden bu yana, günlük ticari hayatındaki işlemler için de yazılı sözleşmeler kullanmaya başlamıştır. İnsanlık tarihinde, şu ana kadar bulunmuş en eski yazılı sözleşmelerden biri M.Ö. 2000 yıllarına ait olup, günümüz Güney Irak sınırları içinde kalan bir bölgede gerçekleşen arazi satışı ile ilgilidir. Sözleşmenin metni “*İlı-Eribu nun oğlu Sini İştär ve kardeşi Apil-li, Sini İştär ile Minaninin evine komşu, sokağa cephele, Migrat-Sin oğlu Minaniye ait olup içinde hali hazırda evi olan 1/3 şar araziye anlaştıkları fiyat olan 4.5 sekel gümüşten almışlardır. Minani'nin bu satışdan dolayı hiç bir hakkı kalmamıştır. Kralın huzurunda yemin ettiler. Tebet ayı, Büyük Karra-Şarma duvarı yılı*” şeklindedir. Yine bilinen bir başka yazılı sözleşme ise esir satışına ilişkin ve M.Ö. 2300 yılına ait bulunmaktadır.³⁷

³⁶ Eren, s.274; Uygur, s.606; Renda-Onursan, s.113; Nomer, s.620

³⁷ Babür, s.1

Bu sözleşmelerin konumuz açısından önemi ise, modern zamanın standart sözleşmelerinde olması gereken öğelerin hepsini taşıyor olmasıdır. Gerçekten, bu sözleşmeler, taraflar ve irade beyanları, değiş tokuşun şekli, tarih ve daha da önemlisi imzaları içeriyordu. Her ne kadar bu imzalar günümüzdeki biçiminden farklı olarak, yaş kil üzerine bastırılan üçgen biçimli işaretler olsa da, kullanımındaki amaç günümüz imzaları ile aynı idi³⁸.

İmza; kişinin kimliğini gösteren ve onu diğerlerinden ayıran bir işarettir³⁹. Diğer bir ifade ile bir irade açıklamasının kendisine ait olduğunu ifade etmek üzere, kişinin ismi için kullandığı özel çizgi ve harflerden oluşan işarete imza denir⁴⁰. Hukuki anlamda imza, kişinin kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir kimse tarafından (veya onun namına) kullanılan herhangi bir işaret veya kabul edilen herhangi bir güvenlik usulüdür⁴¹. İmzanın sözlük anlamı ise, “*bir yazının altına bu yazıyı yazdığını veya onayladığını belirtmek için; her zaman, aynı biçimde yazdığı ad ve işaret*” tir⁴². Yazının insanoğlu tarafından bulunmasından sonra imzanın bu tanımlarına uygun “*işaretler*” günümüze kadar kullanılmış ve kullanılmaya devam edilmektedir. Örneğin Roma Hukukunda bir sözleşmenin oluşturulabilmesi için, sözleşme yapan kişilerin mühür yüzüklerini balmumuna basarak metni mühürlemeleri gerekmektedir. Aynı şekilde Avrupa’da ortaçağ boyunca imza olarak, topraktan yapılmış mühürler kullanılmış ve böylece belgelerin doğrulukları ve güvenilirlikleri temin edilmek istenmiştir. Daha sonraları ise, imzanın el yazısı ile atılmasına başlanılmış ve gelişerek günümüze kadar gelmiştir⁴³.

İnsan yaşamında imzanın çok önemli bir yeri vardır. Özellikle günümüz hukuk sistemlerinde maddi varlığımız olsun olmasın, telaffuz dahi edemeyeceğimiz bir borç altına girmek, tüm mal varlığımızı birine bağışlamak ve yine farkında bile olmadan pek çok suçu işlemek atacağımız birkaç imza ile mümkündür. Ancak pek az kişi imzaya gerekli değeri vermektedir. Çoğu kez sayfalarca belgenin altı tam anlamıyla okunmadan imzalanmakta, üzerine ne yazılabileceği hesaplanmadan boş bir belgeye imza atılabilmekte ve daha pek çok riskli durumda imzamızı rahatlıkla

³⁸ Babür, s.1

³⁹ Eren, s.253; Tunçomağ, s.222

⁴⁰ Topaloğlu, s.119; Orta, s.25; Altınışık, s.74

⁴¹ Çanga, s.1

⁴² Tutkun, s.8

⁴³ Küçüközyiğit, s.3; Orta, s.25; Uslu, s.1

kullanabilmekteyiz. Oysa imza, en değerli hukuki varlıklarımızdan biridir. Bu nedenle nerede ve ne için kullandığımıza son derece dikkat etmeliyiz. İmzaladığımız bir belgenin içeriğini tartışmasız olarak kabul etmemiz söz konusu olduğundan, imzalayacağımız belgenin her harfini okuduğumuzdan emin olduktan sonra imzalamalıyız. Yine imzalı bir belgenin aksi ancak benzer nitelikte bir belge ile kanıtlanabileceğinden, imzalı belgeye dayanan ilişkide, örneğin sözleşmelerde yapılacak her türlü değişiklik, yenilik vs. aynı belge üzerinde imzalı düzeltme veya yeni bir belge tanzimi ile yapılmalıdır⁴⁴.

El yazısı ve dolayısıyla imzanın değişmez nitelikleri vardır. Zira her insanın imzası kendine özgüdür ve genellikle benzersizdir⁴⁵. Yine her insanın el yazısı düşüncesinin grafik ifadesi olması nedeniyle kişiliği ve karakteri ile bütünlük göstermektedir⁴⁶. Bunun doğal sonucu olarak da el yazısı ve imza zaman içerisinde değişebilmekte, kişinin imza atarken sarhoş veya yarı uykulu olması halinde dahi farklı olabilmektedir. Kişinin yaşlanması, sakatlanması veya o andaki ruh halinin imza üzerinde etkileri olabilmektedir.

İmza öncelikle imzalayanın kimliğini belirler. Bir belge, bir şahsın imzasını taşıyorsa bu durum, belgenin o kişi tarafından oluşturulduğuna karine teşkil eder. Bu karinenin aksinin ispatı imza sahibine aittir. Burada kişinin imzasının benzersiz oluşu ve bir başkası tarafından kolayca taklit edilip, kullanılmayacağı unsurlarına dayanılmaktadır. Ayrıca imza, imza sahibinin imzaladığı belgenin içeriğine dair niyetini ortaya koyar. Bu sebeple belgenin altında imzası bulunan kişinin belgenin içeriğini kabul ettiği varsayılır ve kanunda aksi belirtilmedikçe⁴⁷ bu yönde sonuç doğurur. Yine imza, üzerinde silinti ve kazıntı gibi bozulmalar olmadığı sürece, belgenin tamamının imzalayanın isteği doğrultusunda ve doğru olarak tanzim edildiğini, diğer bir ifade ile belgenin bütünlüğünü gösterir⁴⁸.

İmza, her türlü resmi veya özel belgenin geçerlilik kazanabilmesi için, üzerinde bulunması gereken en önemli unsurlardan biridir. İmzasız bir belge kural olarak

⁴⁴ Benzer yönde düşünceler için bkz. Öztürk, s.1-2

⁴⁵ Orta, s.26; Altınışık, s.75

⁴⁶ Daha ayrıntılı bilgi için bkz. Evrim-Okan, s.9-17

⁴⁷ BK.'da bahsi geçen irade fesadı halleri (*hata, hile, ikrah*) ile MK.'da bahsi geçen “*tam ehliyetsizler*” tarafından gerçekleştirilen işlemlerde imza sonuç doğurmaz.

⁴⁸ Küçüközyiğit, s.5; Orta, s.27

sahibine hak veya yükümlülük getirmediği gibi bir kıymet de taşımaz. Bu bakımdan imza kişilere hak sağlayıp, sorumluluk yükleyen bir husustur.

1.5.2- İmza Nasıl Atılmalıdır

Borçlar Kanunumuzun 14 üncü maddesi gereğince elektronik belgelerin elektronik imza ile imzalanması istisnası dışında, imzanın kişinin el yazısı ile atılması gerekmektedir. İmzanın el yazısı ile olması demek, imzanın ilgili kişi tarafından bizzat ve şahsen atılması demektir⁴⁹. Dolayısıyla imza, bir el ürünüdür, el yazısıdır. El yazısı, el hareketlerinin bir sonucudur. Ancak yazı yazılırken veya imza atılırken doğal bir şekilde yazı yazılıp, imza atıldığından vücudumuzun bütününün de buna etkisi vardır. Bundan dolayı imza inkârı durumlarında doğal hali temin etmek için, ayakta ve oturarak imza örnekleri alınıp kriminoloji laboratuvarlarında karşılaştırılarak aynı el ürünü olup olmadığı tespit edilir.

Toplumumuzda küçümsenmeyecek oranda bedensel engelli vatandaş bulunduğu düşünüldüğünde, imzanın el yazısı ile atılması geniş yorumlanarak imzayı atana ait olmak koşulu ile el dışında başka bir uzuv kullanılarak, örneğin ayakla atılmış imza da geçerli kabul edilmektedir. Bunun yanı sıra, imzayı atan kişi imza atmak için gerekli el hareketlerini başkasının yardımı ile gerçekleştirmiş olsa bile imza geçerli kabul edilecektir⁵⁰. Burada önemli olan imzanın ilgiliye ait olma özelliğinin gerçekleşmesi ve imzayı atanın üzerinde herhangi bir baskı unsurunun olmamasıdır. Zira Borçlar Kanununun 29 uncu maddesi gereğince baskı altında atılan imza hukukumuzda kabul görmemekte ve diğer tarafın veya üçüncü bir kişinin korkutmasıyla sözleşme yapan kimsenin o sözleşme ile bağlı olmadığı ve fesih hakkı olduğu belirtilmektedir.

Soyadı kanununun 2 nci maddesi gereğince sözlü kullanım, yazılı kullanım ve imzada, önce öz ad sonra da soyadı kullanılacaktır. Dolayısı ile imza önce öz adın sonra da soyadın el yazısı ile yazılması suretiyle atılacaktır. Ancak günümüzde bu kural pek kabul görmemekte ve öz ad veya soy addan herhangi biri, takma ad veya kısaltılmış imza (paraf) kullanılması da geçerli kabul edilmekte ve genelde paraf kullanılmaktadır. Burada önemli olan ne yazıldığı değil, kişinin beyanda bulunma iradesinin tespit

⁴⁹ Eren, s.253; Birsen, 141; Velidedeoğlu-Özdemir, s.35; Topaloğlu, s.119

⁵⁰ Eren, s.254; Velidedeoğlu-Özdemir, s.35; Birsen,s.142; Uygur, s.706

edilmesidir. Ayrıca imzanın okunabilir olması veya kişinin her zaman aynı imzayı atması da şart değildir⁵¹.

1.5.3- Kimler İmza Atmalıdır

Borçlar Kanunumuzun 13/1 inci maddesi gereğince, yazılı şekle bağlı kılınmış sözleşmelerde, borç altına giren tarafın veya tarafların metni imzalaması gerekir. Bağışlama taahhüdü, kefalet ve kıymetli evrakta olduğu gibi yalnız bir taraf borç altına giriyorsa, sadece o tarafın sözleşmeyi imzalaması yazılı şekle uyulmuş olunması için yeterlidir. Her ne kadar, tek tarafa borç yükleyen sözleşmelerde de sözleşmenin kurulması için diğer tarafın da irade beyanı gerekmekte ise de, bunun için borç altına girenin imzasını taşıyan belgenin karşı tarafa verilmesi yeterli görülmektedir. Nitekim Yargıtay, bağışlama yükleniminde, yalnızca bir tarafın borç altına girmesinden bahisle bağışlayanın açıklamasının ve imzasının şekil şartının yerine getirilmesi açısından yeterli olduğunu, bağışlananın kabulünün bir biçime girmesinin gerekmediğini kabul etmektedir⁵².

Her iki tarafa borç yükleyen sözleşmelerde ise, sözleşmenin tamam olması için her iki tarafın da metni içeren belgeyi imzalaması gerekmektedir. Şirket sözleşmeleri gibi çok taraflı sözleşmelerde bütün akitlerin imzalarının bulunması gerekir. Tek bir tarafın imzalaması halinde bu tek taraflı bir irade beyanı niteliği taşıyacağından sözleşme kurulmuş olmaz⁵³. Yine muhataba ulaşması gerekli bir yazılı beyan, karşı tarafa ulaştıktan sonra hüküm ifade edeceğinden, imzalanan metnin de karşı tarafa ulaştırılması gerekir. Tarafların metni aynı anda imzalamaları gerekmediği gibi, imzaların aynı metinde bulunması da gerekmez. Tarafların imzaladıktan sonra belgeleri birbirlerine vermeleri gerekli ve yeterlidir⁵⁴.

İmza, borç altına giren şahsın bizzat kendisi tarafından atılabileceği gibi yetkili temsilcisi tarafından da atılabilir. Yetkili temsilci yetkisini aşmadığı veya azledilmediği sürece, temsilci tarafından atılan imza yetki vereni bağlayacaktır. Ancak bunun için imzalayanın temsilci niteliği taşıdığı metinden anlaşılmalı veya imza atılması esnasında

⁵¹ Eren, s.253; Velidedeoğlu-Özdemir, s.36; Birsen, s.141; Altınışık, s.75

⁵² Yargıtay 4.HD., 26.10.1978 1977/13113 K, Yargıtay 2. HD. 14.04.1998 T. 1998/1981-4282, E-K sayılı ilamları

⁵³ Yargıtay 13.HD. 21.01.2003 T. 2002/12288-E, 2003/459-K

⁵⁴ Karahasan, s.141; Eren, s.254

yazılı olarak belirtilmelidir. Aksi halde temsilci bizzat borç altına girer. Temsilcinin asıl tarafın adını kullanarak imza atamayacağı kabul edilmektedir. Zira imza, imzalayanın kendi adını taşıması halinde bir anlam kazanacaktır⁵⁵.

1.5.4- İmzanın Yeri

İmzanın konulacağı yer hakkında borçlar kanununda herhangi bir hükme yer verilmemiştir. Ancak doktrinde ve uygulamada imzanın tüm metni kapsayacak şekilde metnin sonuna atılması gerektiği kabul edilmektedir. Yine metinde yapılacak ekleme, çıkarma, sime gibi değişikliklerinde altının imzalanması gerekmektedir. Birden fazla sayfa var ise en son sayfaya imzanın atılması yeterlidir. Bununla birlikte, metinle ilişkisi belirtilmek şartıyla metnin başına veya yan tarafına atılacak imzanın da yeterli olacağını savunan yazarlar bulunmakta ise de genel kanı, bu şekilde atılan imzanın sonuç doğurmayacağı yönündedir⁵⁶.

İmza, metnin yazılmasından önce de atılmış olabilir. Uygulamada bu durum “açığa imza” olarak bilinmektedir. Açığa (beyaza) imza, önceden yazılmış bir sözleşme metni olmaksızın, imza edenin karşı tarafa duyduğu güvene dayanarak, üzeri taraflar arasında yapılan anlaşmaya uygun olarak doldurulmak üzere, borçlu tarafından boş bir kâğıdın veya kısmen doldurulmuş bir senedin imzalanıp karşı tarafa veya üçüncü şahsa verilmesi suretiyle gerçekleşmektedir⁵⁷. Burada taraflar arasında daha önceden var olan bir anlaşma olup, açığa atılan imzanın bu anlaşmaya göre doldurulması söz konusudur. Ancak uygulamada açığa atılan imzanın üzerinin anlaşmaya aykırı olarak doldurulduğu ve/veya bu yönde iddiada bulunulduğu sık karşılaşılan bir durumdur. Yargıtay uygulamasında⁵⁸ ve doktrinde de kabul edildiği üzere, açığa imza atan kimse, imzanın üzerinin diğer tarafla kararlaştırılan anlaşmaya aykırı olarak doldurulduğunu ispat etmedikçe, imzalı metin geçerli kabul edilecek ve imza atan borçlandığı edimi yerine getirmek zorunda kalacaktır⁵⁹. Bu durumun ispatı ise çok zor ve hatta çoğu kez imkânsız olmaktadır. Zira burada güvene dayanan bir işlem söz konusu olduğundan, irade fesadı hallerinden olan hata ve hileden söz edilemeyecek ve HMUK’nun 293/son

⁵⁵ Karahasan, s.142; Eren, s.255; Reisoğlu, s.73

⁵⁶ Eren, s.260; Karahasan, s.142; Keser Berber (Şekil), s.59; Altınışik, s.75; Reisoğlu, s. 73

⁵⁷ Ulusoy, s.472; Eren, s.256; Karahasan, s.143

⁵⁸ Y. 13.H.D., 25.12.1986 T. 1986/5422-6629 E.K. sayılı ilamı

⁵⁹ Eren, s.256; Karahasan, s.143; Tunçomağ, s.228

maddesi uygulanamayacaktır. Dolayısıyla ortada yazılı bir belge olduğundan, buna karşı tanık dinlenemeyecek ve bu şekilde tanzim edilmiş bir belgenin aksi ancak eşdeğer bir yazılı delille (senetle) ispat edilebilecektir (HMUK. m.290). Ancak imzalı boş kağıt imza atanın rızası dışında örneğin hile ile elinden alınmış veya çalınmış ise bu durumda tanık dinletilebilecektir.

1.5.5- El Yazısı İle İmzanın İstisnaları

El yazısı ile imza atmanın mümkün olmadığı bazı özel durumlarda yasa koyucu istisnai bazı düzenlemeler getirmiştir. Ancak şunu da hemen ifade etmek gerekir ki, ileride ayrıntılı olarak inceleyeceğimiz “*Elektronik İmza*” el yazısı ile imzanın bir istisnası değildir. Zira el yazısı ile imzanın istisnaları fiziki belge üzerine şahıslardan kaynaklanan bir sebeple el yazısı ile imza atmanın çok zor veya imkânsız olduğu durumlarda uygulanır ve fiziki belge üzerine yasanın öngördüğü çerçevede konulan işaret, onay veya buna benzer bir tasdiki oluşturur. Elektronik imza ise, fiziki ortamda bulunmayan dolayısıyla el yazısı ile imza atmanın fiilen imkânsız olduğu durumlarda, sanal(elektronik) ortamda bulunan belgenin doğruluğunu, bütünlüğünü koruyan ve beyan sahibinin bu belgenin içeriğini kabul edip onayladığını belirtmesine diğer bir ifade ile imzalamasına imkân tanıyan bir teknik terim olup, el yazısı ile imzanın elektronik ortamdaki karşılığıdır. Bu anlamda elektronik imza, ıslak imzanın istisnası olmayıp, alternatifidir.

Borçlar Kanunumuzda el yazısı ile imzaya ilişkin genel kurala iki istisna öngörülmüştür. Bunlar bir alet vasıtasıyla imza atılması ve imza yerine kullanılacak işaretlerdir.

Körlerin (âmâların) imza attıkları belgeleri görme imkanları olmadığından, atmış oldukları imzaların hukuken geçerli olabilmesi için ya imzasının noterde tasdik edilmesi ya da amanın imzaladığı belgenin içeriğini bildiğinin ispat edilmesi gerektiğine dair düzenleme bulunmakta idi (BK. m.14/3 “mülga”). Ancak bu hüküm 01.07.2005 tarih ve 5378 sayılı yasanın 50. maddesi yürürlükten kaldırılmıştır. Aynı şekilde ticari senetlerde âmâların imzasına ilişkin benzer düzenleme de aynı madde ile yürürlükten kaldırılmıştır. Şu halde el yazısı ile imza hususunda âmâlara ilişkin istisnai bir

düzenleme kalmadığından, bu kişilerin de imzaları diğer kişilerle eşit ölçüde hak ve sorumluluk doğuracaktır.

1.5.5.1- Alet Vasıtası İle İmza

Alet vasıtasıyla imza, imza atmaya muktedir bir kişinin el yazısı ile atmış olduğu imzasının mekanik veya elektronik bir alet vasıtası ile evrak üzerine atılmasıdır. El yazısı ile imza atmak kural olmakla birlikte, bazı istisnai durumlarda el yazısı ile imza atmanın çok zor ve hatta imkânsız olduğu nazara alınarak bir alet aracılığı ile imza atılabileceği kabul edilmiştir. Hukukumuzda alet vasıtasıyla imza, ancak örf ve adetçe kabul olunan hallerde ve özellikle çok miktarda tedavüle çıkarılan kıymetli evrakın imzalanması gereken durumlarda kabul edilir (BK. m.14/2). Örneğin binlerce hatta milyonlarca çıkarılan hisse senetleri, tahviller, tedavüle çıkarılan para gibi kıymetli evrakların tamamının borç altına giren kişi veya kişilerin tamamınca imzalanması mümkün değildir. İşte bu gibi durumlarda bu kişilerin el yazısı ile imzaları bir alet vasıtası ile atılmaktadır. Ancak kanun ticari senetlere ilişkin düzenlemeleri bu istisna kapsamı dışında tutmuştur (BK. m.15). Buna göre ticari senetlerdeki (bono, çek, poliçe) beyanların el yazısı ile imza edilmesi gerekmektedir. El yazısı ile imzanın mekanik yoldan kopya edilmesi yani bir alet vasıtasıyla atılması mümkün değildir(TTK. m.668/2).

1.5.5.2- İmza Yerine Kullanılabilecek İşaretler

Ülkemizde halen okuma yazma bilmeyen insan sayısı son derece fazladır. Doğal olarak bu insanların çok büyük bir bölümü imza atmasını da bilmemektedir. Yine bedensel özrü nedeniyle imza atamayan kişiler de bulunmaktadır. İşte kanun koyucu bu gibi durumları göz önüne alarak, imza atmasını bilmeyenler veya bedeni bir özrü nedeniyle el yazısıyla imza atamayanların imza yerine “*usulen tasdik olunmuş ve el ile yapılmış bir alamet*(işaret)” veya “*resmi bir şahadetname*” (belgeleme-onaylama) kullanabilirler (BK. md.15). Bu işaret el ile yapılan bir çizgi, geometrik şekil, yazı şeklinde kullanılmayan bir harf rakam ve benzeri şeyler olabilir⁶⁰. Parmak izinin de bu kapsamda yer aldığı doktrin ve Yargıtay uygulamasında kabul edilmektedir. Ülkemizde okuma yazma bilmeyen pek çok insan mühür kullanmaktadır. Borçlar Kanununda

⁶⁰ Eren, s.258

mühürden söz edilmemiştir. Ancak Noterlik Kanunu'nun 75 ve HUMK'nun 297 nci maddelerinde mühür kullanma yöntemi kabul edilmiştir. Bu nedenle mühür de BK.'nun 15 inci maddesi kapsamında değerlendirilmektedir⁶¹.

İmza yerine kullanılabilir işaretlerin geçerli kabul edilebilmesi için bunun resmi bir makam tarafından onaylanması gerekmektedir. Bu makam hukukumuzda noterler ve köy ihtiyar heyeti olarak düzenlenmiştir. Örneğin parmak basmanın imza yerine geçebilmesi için noter veya köy ihtiyar heyetince tasdik edilmesi gerekmektedir. Aynı şekilde mühürün geçerli olabilmesi için HUMK'nun 297 nci maddesi hükmü gereğince köy ihtiyar heyeti ve mahallince tanınan iki şahit tarafından tasdik edilmiş olmalıdır. Yargıtay uygulaması da bu yöndedir⁶². Madde metninde belirtilen ihtiyar heyeti borç altına giren kişinin ikamet ettiği yerin ihtiyar heyetidir.

BK. 15 inci maddesinde el ile yapılmış işaretin yanında resmi bir şahadetnameden de bahsedilmiştir. Buradaki resmi şahadetnameden kastedilen imza atamayan bir kişinin resmi bir memura giderek, memura, beyan ettiği hususların imzalanması gereken belge veya senette yer aldığını ve bu beyanın kendi iradesine uygun olduğunu söylemesi ve memurun da bu beyanı metnin altına yazarak imza ve tasdik etmesidir⁶³.

İmza yerine kullanılabilir işaret ve resmi şahadetnamenin geçerli olabilmesi için kanunun aradığı ön şart bu yola başvuran kişinin imza atmaya muktedir olmamasıdır. Yani kişi imza atmaya bilmemeli veya bedensel özrü nedeniyle imza atamamalıdır. Dolayısıyla imza atmasını bilen ve buna bedensel olarak gücü yeten bir kişinin imza yerine el işareti, parmak izi, mühür veya resmi şahadetname kullanması halinde bu geçerli olmayacak, hüküm ve sonuç doğurmayacaktır⁶⁴.

⁶¹ Eren, s.258-259; Karahasan, s.153; Reisoğlu,s.74; Akıncı, s.91; Orta, s.28

⁶² Yargıtay HGK. 12.11.1930 T. 1930/29-30 E.K. sayılı ilamı

⁶³ Karahasan, s.153; Tunçomağ, s.225; Eren, s.258; Reisoğlu, s.75

⁶⁴ Eren, s.258; Reisoğlu, s.75; Orta, s.29

1.6- Elektronik Ortamda Şekil

1.6.1- Genel Olarak

Hukumumuzda sözleşmelerin geçerliliği herhangi bir şekil şartına uyulmasına bağlı değildir(BK. m.11). Ancak kanunun şekil şartı öngördüğü sözleşmelerin şekle aykırı yapılması halinde, aksine yasal hüküm bulunmadığı sürece geçerliliği söz konusu olamaz. Yine belli bir meblağı aşan sözleşmelerin ispat edilebilmesi için yazılı olmaları gerekmektedir. Şu halde elektronik ortamda akdedilen sözleşmeler yazılılık işlevini taşımakta mıdır? Yine kanunun şekil şartı öngördüğü sözleşmeler elektronik ortamda geçerli olarak kurulabilir mi?

Bir irade beyanının yazılı kabul edilebilmesi için, istenildiğinde ibraz olanağının olması ve değiştirilmezliğinin temin edilmiş olması gerekmektedir⁶⁵. Bu nedenle yakın tarihe kadar, belgenin istenildiğinde ibraz edilebilmesi ve değiştirilmezliğinin temini için sürekli ve dayanıklı bir madde üzerine yazılması ve taşınabilir olması gerektiği görüşü hakimdi. Bu anlamda elektronik belgelerin, öncelikle doğrudan algılanabilir olmayıp, algılanabilmesi için verileri yazıya dönüştürebilen teknik bir araca (bilgisayar ekranı, yazıcı) ihtiyaç duyduğu, içeriğinden her an bilgi sahibi olma ve ibraz edilebilme imkânı bulunmadığı gibi bilgisayar ve veri taşıyıcılarındaki verilerin iz bırakmadan değiştirilebilir olması nedenleriyle yazılı metin özelliğini taşımadığı kabul edilmekteydi⁶⁶.

Yine 5070 sayılı Elektronik İmza Kanunu yürürlüğe girmeden önce Borçlar Kanununun 14 üncü maddesi hükmü gereğince yazılı şeklin unsuru bulunan imzanın, el yazısı ile atılması gerektiğinden ve elektronik ortamda bunu gerçekleştirme imkânı olmadığından, şekle bağlı sözleşmelerin elektronik ortamda geçerli olarak kurulması da mümkün değildi.

Elektronik ortamda kurulan hukuki ilişkilerde tarafların birbirleri ile hiç karşılaşmadıkları ve muhtemelen ileride de karşılaşmayacakları bir gerçektir. Böyle olunca internet ortamında hazırlanan bu belgelerin senet niteliği taşıyıp taşımadığı,

⁶⁵ Pekcanitez, s.400; Eren, s.252; Erturgut, s.202

⁶⁶ Eren, s.252; Pekcanitez,s.401-402; Özdemir Kocasakal, s.93;Gezder, s.143; Altınışık, s. 95; Erturgut, s.204

sözleşme taraflarının belirlenmesi, kimliklerinin doğrulanması ve kimliklerinin sözleşme ile ilişkilendirilmesi önemli bir problem olarak karşımıza çıkmaktadır. Zira elektronik ortamda hazırlanan bir mektup veya bir mesajın daha genel ifade ile bir irade beyanının güvenilir ve bağlayıcı olması ancak bunu hazırlayan kişinin imzası ile mümkündür. Aynı şekilde sözleşme ile borç altına giren tarafların sözleşme metninde imzasının bulunması gerekir. Peki, elektronik ortamda bu nasıl yapılacaktır? Bilgisayara takılı bir çizim kalem veya tarayıcı vasıtasıyla kişinin imzasının metne eklenmesi halinde, bu imzanın gerçek olup olmadığının ve sahteliğinin denetlenmesinin mümkün olmadığı bilinmektedir. Bir başka problem ise herkese açık olan internet ortamında karşı tarafa gönderilen mesajın içeriğinin değiştirilip değiştirilmediğidir. O halde sanal ortamda hazırlanmış bir belge elektronik olarak nasıl imzalanabilecektir? Daha da önemlisi bu imza hukuken geçerli olacak mıdır? Yine imzalamış olan belgenin içeriğinin değişip değişmediğinden veya başka kişilerin eline geçip geçmediğinden nasıl emin olunacaktır? Görüldüğü gibi elektronik ortamda yapılan veya yapılacak işlemlerde ihtiyaç duyulan en önemli şey güvenlidir. İşte söz konusu bu güvenliği sağlayıp, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu, garanti edebilmek amacıyla yapılan uluslararası çalışmalar neticesinde çözüm olarak elektronik imza tekniği geliştirilmiş ve bu tekniğin yasal geçerliliğine yönelik yasal düzenlemelere gidilmiştir. Ülkemizde de bu yöndeki düzenleme 5070 sayılı Elektronik İmza Kanunu ile yapılmıştır.

5070 sayılı Elektronik İmza Kanunu'nun 5 inci maddesinde “*güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*” hükmüne yer verilmiş; 22 nci maddesi hükmü ile, Borçlar Kanunu'nun 14 üncü maddesine “*güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir*” cümlesi eklenmiştir. Yine kanunun 23 üncü maddesi hükmü ile HUMK'na güvenli elektronik imza ile imzalanmış bir elektronik belgenin, senet hükmünde olduğu ve aksi ispat edilinceye kadar kesin delil teşkil edeceği hükmünü içeren 295/a maddesi eklenmiştir. Ayrıca, Türk Borçlar Kanunu ve Hukuk Muhakemeleri Kanunu tasarılarında yazılık işlevi ve şekil şartlarına ilişkin yer verilen hükümlerle de bu yöndeki tereddütlerin giderilmesi hedeflenmiştir. Zira, Borçlar Kanununun 14 üncü maddesinde yapılan değişiklik ile güvenli elektronik imza ile el yazısı ile atılan imzanın ispat gücü açısından eş değer olduğu kabul edilmiştir. Yine Borçlar Kanunu tasarısında buna paralel olarak güvenli elektronik imzanın el

yazısı imza ile aynı hukuki sonuçları doğuracağı belirtilmiş(m.15), yürürlükteki yasadaki farklı olarak, güvenli elektronik imza ile imzalanan elektronik belgelerin de **metin** olarak kabulü ve yazılılık işlevini yerine getireceği hükme bağlanmıştır(m.14).

Bu açıklamalar doğrultusunda kanımızca, elektronik ortamda bulunan belgelerin yazılılık özelliğinin olmadığı söylenemez. Zira Borçlar Kanununun 14 üncü maddesinin eski halinde, yazılı şeklin gerçekleştirilmesi için metnin el yazısı ile imzalanmasının zorunlu olduğu hükmüne yer verilmişti. Söz konusu maddede yapılan değişiklik ile güvenli elektronik imza ile el yazısı ile imza eşdeğer kabul edildiğine göre, bu hükmün anlam ifade edebilmesi için elektronik belgelerin de metin unsurunu ve yazılık işlevini içerdiği kabul edilmelidir. Aynı sonuca Borçlar Kanunu tasarısı (m.14-15) ve Hukuk Muhakemeleri Usulü Kanunu tasarısı (m. 203 vd.) hükümlerinin incelenmesi neticesinde ulaşılabilecektir. Sonuç olarak, güvenli elektronik imza ile imzalanması ve istenildiğinde ibraz edilmek üzere saklanabilmesi koşuluyla elektronik belgeler de yazılı şeklin şartlarını taşır ve Elektronik İmza Kanununun 5 inci maddesindeki istisnalar dışında şekle bağlı sözleşmeler de elektronik ortamda geçerli olarak kurulabilir.

Hukuk kurallarının genelde, sosyal vakıanın ortaya çıkıp tamamlanarak, hukuki problemin ortaya çıkmasını, teşkil ve teşhisini beklemek zorunda olduğu kabul edilmektedir⁶⁷. Ancak, Elektronik İmza Kanunu bu genel kurala aykırı şekilde gelişmiştir. Zira ülkemizde, gerek özel sektörde gerekse kamuda, henüz Elektronik İmza kullanılmaya başlanmadan bu yönde bir düzenlemeye gidilmiş ve sosyal vakıa ortaya çıkmadan bunun yasal düzenlemesi yapılmıştır. Aslında Elektronik İmza Kanunu bizim dışımızda gelişen sürecin yasal mevzuatımıza uyarlamasından ibarettir⁶⁸. Gerçekten elektronik ticaretin gelişmesine paralel olarak, Avrupa Birliği üyesi ülkelerde ve ABD başta olmak üzere birlik üyesi olmayan ülkelerde elektronik imzaya ilişkin düzenlemelere gidilmesi, her ne kadar elektronik imzanın fiilen ve yaygın olarak kullanımının söz konusu olmamasına rağmen, Avrupa Birliği yolunda ilerleyen ülkemizde, internet kullanımının büyük bir hızla artması ve elektronik ticaret hacminin genişlemesi de nazara alınarak Avrupa Birliği'ne uyum yasaları çerçevesinde, Avrupa Komisyonu'nun 99/93/EC sayılı direktifi baz alınarak bu yönde bir düzenlemenin yapılması gereğini doğurmuştur. Böyle olunca da uyarlama sürecinde bir takım eksiklik

⁶⁷ Kalpsüz, s. 60-61

⁶⁸ Turan, s.2

ve yanlışlıkların ortaya çıkması da söz konusu olabilecektir. Yine uygulamanın sonuçlarını görmeden elektronik imza ile imzalanmış verilere hüküm ve sonuçlar bağlanması da tartışmalara yol açacak ve uygulamada karşılaşılan sıkıntıları artıracaktır⁶⁹. Ancak bu durum olumsuz bir gelişme olarak algılanmamalıdır. Aksine dünyada örnekleri görülen ve ülkemizde de gündemden hiç düşmeyen e-ticaret, e-devlet ve e-dönüşüm benzeri projelerin hayata geçirilebilmesi için çok önemli bir adım ve fırsat olarak değerlendirilmelidir.

1.6.2- Elektronik İmza ve Sayısal (Dijital) İmza Kavramları

İmza, yukarıda açıklandığı üzere, ait olduğu belgenin doğruluğunu göstermek niyetiyle oluşturulan ve kullanılan her türlü işaret olup⁷⁰, genel bir kavramdır. Bu tanımlamaya göre imzanın oluşabilmesi için, mürekkep ve kâğıt şart olmayıp, bir sembolün varlığı ve belge içeriği ile bu belgeyi düzenleyen niyetinin örtüşmesi yeterli olacaktır. Bu açıdan bakıldığında elektronik bir kayıt veya verideki herhangi bir sembol ya da kod da imza olarak kabul edilebilecektir⁷¹.

Elektronik imza da genel bir kavram olup, bilgisayar tabanlı kimlik belirleyicileri olarak kullanılan, elektronik ortamda oluşturulmuş bir mesajın bütünlüğünü ve değişmemişliğini ifade eden, aynı zamanda mesaj sahibinin kimliğini tanımlamaya yarayan her türlü elektronik işarettir. Bu işaretlerin herhangi bir şekli veya sınırlaması yoktur. Bu itibarla, el yazısı ile imzanın tarayıcı vasıtasıyla elektronik ortama aktarılması, bilgisayara takılı bir alet vasıtasıyla el yazısı imzanın bilgisayar ekranına atılması, kredi kartlarında kullanılan PIN kodları, kişilerin biyometrik özelliklerine dayalı ses, göz retinası taraması, parmak izi taraması gibi yöntemler ve çift anahtarlı kriptografiyle oluşturulan sayısal imza birer elektronik imza türüdür. Buna göre elektronik imza, bir kimsenin bir belgeyi elektronik ortamda imzalayabileceği yöntemlerin tümünü ifade eden bir üst kavramdır⁷². Genel anlamıyla elektronik imza, imza sahibinin kimliğini ve ekli bilgiye onay verildiğini göstermek niyetiyle bir kimse

⁶⁹ Turan, s.2; Deliduman, s. 2

⁷⁰ Altundağ, s.60, Çanga, s.1; Küçüközyiğit, s.3; Özgül,s.2

⁷¹ Altundağ, s.61; Küçüközyiğit, s.3

⁷² Küçüközyiğit, s.5; Erturgut, s.54; Altınışık, s.79; Ahi, s.2; Orta, s.36

tarafından (veya onun namına) kullanılan herhangi bir işaret veya kabul edilen herhangi bir güvenlik usulüdür⁷³.

Elektronik imza, konuyla ilgili pek çok çalışmada ve yasal düzenlemede tanımlanmıştır. Amerika Birleşik Devletleri Küresel ve Ulusal Ticarete elektronik İmza Yasasında (Electronic Signatures in Global and National Commerce Act) elektronik imza; “bir sözleşmeye doğrudan eklenmiş ya da mantıksal bağlantı kurulabilen ve kaydı imzalamak niyetini güden kişi tarafından oluşturulmuş veya kullanılmış, her türlü elektronik ses, sembol ya da kayıt”⁷⁴ olarak tanımlanmıştır. Elektronik imza 13 Aralık 1999 tarihli Avrupa Birliği Direktifinde ise; “*başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan, kimlik teşhisine yarayan elektronik formda bulunan veriler*” olarak tanımlanmıştır. Bu tanıma benzer olarak, ülkemizde 23 Temmuz 2004 tarihinde yürürlüğe giren 5070 sayılı Elektronik İmza Kanununda da “*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*” şeklinde tanımlanmıştır.

Yasal düzenlemelerdeki bu tanımlar haricinde pek çok çalışmada da elektronik imza tanımlamaları yapılmıştır. Bu tanımlar genelde elektronik imzanın ıslak imza ile fonksiyon eşitliği prensibi nazara alınarak yapılmıştır. Bunlardan birkaçını şu şekilde sıralayabiliriz. Elektronik imza; “*kişinin el yazısı ile attığı imzanın sahip olduğu özellikleri elektronik ortamda gerçekleştirmeye yarayan matematiksel formüllere veya şifreleme programlarına verilen bir isimdir*⁷⁵”, “*ıslak imzanın fonksiyonlarını da 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*⁷⁶. “*bir bilginin üçüncü kişilerin erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir settir*⁷⁷.

⁷³ Orta, s.37

⁷⁴ Küçüközyiğit, s.6

⁷⁵ Keser Berber (Tasarı Değerlendirmesi), s.1

⁷⁶ Arıkan, s.151; Orta, s.36

⁷⁷ ETKK, Hukuk Çalışma Grubu Raporu, s. 8; İnalöz, s.23

Yukarıdaki tanımlarda görüldüğü üzere elektronik imzaya bir sınırlama getirilmemiş, herhangi bir teknolojiye üstünlük tanınmamış, sadece ondan beklenen fonksiyonlar dikkate alınmıştır. Bu durum “teknolojik tarafsızlık” olarak nitelendirilmektedir⁷⁸. Böylece elektronik imza alanında ortaya çıkabilecek yeni teknikler veya değişiklikler yasal mevzuat değişikliğine gerek olmaksızın uygulanabilirlik kazanmaktadır. Yine bu sayede yasal düzenlemeler, bu anlamda teknolojinin gerisinde kalmayacak ve her değişikliğe uygulanabilir bir durumda olacaktır. Buna örnek olarak yasal düzenlemelerden sonra ortaya ve giderek yaygınlaşan mobil elektronik imza gösterilebilir. Elektronik imza, şimdiye kadar imzalamada kullanılan ve ileride kullanılabilecek tüm yöntemleri kapsar bir şekilde tanımlanmıştır. Hal böyle olunca elektronik belgede kullanılan imzaların güvenilirliği imzanın çeşidine göre farklılık arz etmektedir.

Elektronik ortamda bağlayıcı işlem yapma olanağı sağlamayı amaçlayan bir elektronik imza tekniği de sayısal imza, diğer adıyla dijital imzadır. Sayısal imza teknik olarak bir yazılımdır ve verinin (belgenin) anahtar olarak tanımlanan özel bir veri kullanılarak şifrelenmesi temeline dayanır.

Bu anlamda Sayısal (Dijital) İmza, elektronik imzanın özel bir türü olup, düşük maliyeti ve yüksek güvenlik standardı nedeniyle dünyada en çok kullanılan türdür. Sayısal imza, başka bir dijital belgeye eklenmiş yada mantıken ilişkilendirilmiş bitlerden⁷⁹ oluşan bir seriyi ifade eder. Teknik olarak tanımlanacak olursa, sayısal imza; asimetrik şifreleme yöntemi ve hash fonksiyonu kullanılarak, bir mesajın imzalayanın açık anahtarına karşılık gelen bir özel anahtar kullanılarak oluşturulup oluşturulmadığını, mesajın dönüşüm esnasında değiştirilip değiştirilmediğini ve mesaja sahip olan kişinin kimliğinin tam olarak saptanabildiği bir yöntemdir⁸⁰. Dış Ticaret Müsteşarlığı bünyesinde kurulmuş Elektronik Ticaret Koordinasyon Kurulu Hukuk Raporunda; “Elektronik imzanın özel bir çeşidi olup, bir anahtar çifti (açık ve gizli anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühürdür⁸¹. Sayısal imzalar göndericinin kimliğinin açık ve net bir biçimde teyidini, elektronik dokümanın orijinalliğini ve güvenilirliğini mümkün kılar. Gönderici için ve mesajın gönderildiği

⁷⁸ Erturgut, s.60; Altınışık s.78-79, dn. 61

⁷⁹ Bit: En küçük veriyi ifade eder. İkilik (binary) sisteme dayanan bit, her zaman 0 yada 1 değerini alır.

⁸⁰ Winn Jane, s.3; Orta, s.37; Erturgut, s.69

⁸¹ Pekcanitez, s.395

taraf için tek olan sayısal imzalar doğrulanabilir ve inkar edilemez.” Biçiminde tanımlanmıştır.⁸²

Bu tanımlamalardan da anlaşılacağı üzere sayısal imza, daha geniş ve genel kapsamlı olan ve elektronik ispat yöntemlerinin tamamını içine alan elektronik imza kavramından farklılık arz etmektedir. Zira elektronik imza, bir elektronik belgenin kimden satırında yer alan bir isim, bazı elektronik sistemlerinde kullanılan el yazısı imzanın dijitalize edilmiş hali veya el ile atılan kâğıt tabanlı imzanın elektronik ortama aktarılması şeklinde de karşımıza çıkabilmekte, dolayısıyla hukuki bağlayıcılık açısından zaruri olan veri bütünlüğü ve inkâr edilemezlik işlevleri açısından yetersiz olabilmektedir. Sayısal imza da ise, bir açık şifre altyapısı içinde yerleşik asimetrik şifreleme yöntemi ile ıslak imzanın kâğıt üzerinde gerçekleştirdiği tüm işlevleri ve fazlasını herhangi bir tereddüde mahal vermeyecek şekilde elektronik ortamda gerçekleştirecek şartları ve teknik gereksinimleri içeren bir elektronik ispat metodudur.

Elektronik imza genel ve üst bir kavram olmasına ve sayısal (dijital) imzayı da kapsamasına karşın, uygulamada elektronik imza ifadesi ile genelde sayısal imza kastedilmekte ve bu anlamda kullanılmaktadır. Halen çeşitli ülkelerde yürürlüğe girmiş ve girmek üzere olan yasa metinlerinde de dijital imza veya elektronik imza terimlerinden birinin seçildiği görülmektedir.

Ülkemizde de “elektronik imza” kavramı kabul edilmiş ve ıslak imzanın tüm işlevlerini elektronik ortamda karşılayan sayısal imza “güvenli elektronik imza” olarak tanımlanmıştır. Ancak bu tanımlama doktrinde eleştirilmiş ve sayısal imza kavramının kabul edilmesinin gerektiği ileri sürülmüştür.⁸³

Buna göre “*münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli*

⁸² ETKK, Hukuk Çalışma Grubu Raporu

⁸³ “...Yapı itibariyle birbirinden tamamen farklı olan dijital imza ile biyometrik yöntemlerin, elektronik imza üst kavramı altında, aynı kanunda aynı hüküm ve sonuçlara bağlı olarak düzenlenmesi mümkün değildir. Tasarıdaki hükümler dikkate alındığında, bu hükümler ile kanun koyucunun sadece dijital imza ile ilgili olarak düzenleme yaptığı anlaşılmaktadır. Dolayısıyla bu tasarının adının “TÜRK DİJİTAL İMZA KANUNU” olması ve böylece tasarıdaki hükümler ile tasarının adı arasındaki çelişkinin giderilmesi yerinde olacaktır” Keser Berber (Tasarı Değerlendirmesi), s.2

*elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapıp yapılmadığının tespitini sağlayan, elektronik imza” güvenli elektronik imzadır*⁸⁴. Burada imzanın güvenli sayılması için güvenli elektronik imza oluşturma aracı ile oluşturulması şartına yer verilmiştir. Zira güvenli elektronik imza oluşturma aracı; imzanın bir eşinin bulunmamasını, gizliliğini ve güvenliğini garanti etmektedir. Bu husus yasanın 6 ncı maddesinde irdelenmiştir. Bu tanımdan da anlaşılacağı üzere dijital imzanın kullanılabilmesi için öncelikle onay kurumundan dijital bir sertifika alınması gerekmektedir.

Bu açıklamalar ışığında güvenli elektronik imza olarak da adlandırdığımız sayısal imzayı hukuki anlamda “gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun *doğrulanmasını*, iletilen veya alınan verilerin bilinmeyen kişiler (başkaları) tarafından gönderilmediğini veya bildiğimiz kişiler tarafından gönderildiğinin *belirlenmesini*, verileri gönderenlerin gönderdiğini ve alanların aldığını *inkâr edememesini*, gönderilen veya alınan bilgilerin *içeriğinin değiştirilmemesini*, başkaları tarafından elde edilse bile, içeriğin başkaları tarafından *anlaşılamamasını* sağlamayı garanti eden, elektronik ortamda bit katarlarından oluşturulmuş *güvenli haberleşme ve tasdik yöntemi*”⁸⁵ olarak tanımlayabiliriz.

Bu tanımlamalar doğrultusunda diyebiliriz ki, sayısal (dijital) imzanın işlevi, elektronik ortamda aslından ayrılması güç, hatta neredeyse imkânsız olan sahte imzayı önlemek ve dokümanların orijinal hali ile herhangi bir tahrip ve tahrife uğramaksızın iletilmesini sağlamaktır. Bu nedenle sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir⁸⁶. Zira elektronik ortamda yapılacak her tür sözleşme, mektup veya başka tür belgelerin hukuki koruması ancak ve ancak sayısal imza ile mümkün olmaktadır. Sayısal imza, elektronik ortamda üretilen bilgilerin gönderilmesi sırasında, göndericinin kimliğini kesinlikle teyit edecek, verinin başkası tarafından

⁸⁴ Elektronik İmza Kanunu, m.4 ; Orta, s.37

⁸⁵ Sağıroğlu-Kabasakal-Alkan (Sempozyum), s.23

⁸⁶ Orta, s.38

gönderilmediğini garanti edecek ve bu verilerin güvenliğini sağlayıp, başkası tarafından değiştirilemeyecek bir uygulamadır⁸⁷

1.6.3- Elektronik İmza Çeşitleri

Gerek Avrupa birliği direktifi ve birliğe üye ülkelerin yasal düzenlemelerinde, gerekse Türk hukukundaki düzenlemelerde ve konu ile ilgili çalışmalarda elektronik imza, taşıdığı özelliklere göre çeşitli ayırmalara tabi tutulmuş ve mevcut yasal düzenlemelerde çeşitli sebeplerle ve özellikle hukuki işlem güvenliğinin sağlanması bakımından çeşitli kriterler ve nitelikler öngörülmüştür. Bu kriterleri karşılayabilme özelliklerine göre elektronik imzalar, basit elektronik imza, gelişmiş elektronik imza, güvenli (nitelikli) elektronik imza ve akredite edilmiş sertifika hizmet sağlayıcısı tarafından verilmiş elektronik imza şeklinde sınıflandırılmıştır.

Bu sınıflandırmalar kimlik doğrulama amacıyla başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan her türlü işaretin elektronik imza kapsamında bulunması hususu dikkate alınarak, bu esasa çeşitli nitelik ve kriterlerin eklenmesi suretiyle yapılmıştır. Bu tür bir düzenleme tarzı, teknikteki gelişmelerin dikkate alınmasına olanak vermesi bakımından uygun bir tutumdur. Bu sayede mevcut yasal düzenlemeler, baş döndürücü bir hızla gelişen bilim ve teknoloji neticesinde ortaya çıkacak yeni teknik gelişmelerin gerisinde kalmayacak ve var olan yada ileride ortaya çıkacak bütün elektronik imza türleri, teknik nitelikleri nazara alınmaksızın hukuki bağlayıcılık, geçerlilik ve güvenlik bakımından öngörülen şartları taşımaları yönünden değerlendirileceklerdir.

1.6.3.1- Basit Elektronik İmza

Basit Elektronik imza, genel anlamda elektronik imza tanımının karşılığıdır ve bu tanım içerisine giren tüm yöntemleri kapsamaktadır. Ancak yasal düzenlemelerde elektronik imzanın, hukuki geçerlilik, bağlayıcılık ve güvenlik gereksinimleri açısından taşınması gerektiği öngörülen şartları kısmen veya tamamen karşılamayan elektronik imza türleri bu kapsamda değerlendirilmektedir.

⁸⁷ Keser Berber (İmzalıyorum O Halde Varım), s.503

Basit elektronik imza kapsamında bulunan elektronik imza türleri, yasal düzenlemelerdeki bazı şartları taşımadıklarından, hukuki işlemlerde şekil şartını yerine getirmeye elverişli olmadıkları gibi (şu an için⁸⁸) yargılamada geçerli delil olarak kullanılamazlar⁸⁹. Oysa Avrupa Birliği Direktifine göre, bir elektronik imzanın, sadece elektronik formda olması veya nitelikli bir sertifikaya dayanmaması ya da akredite edilmiş bir sertifika hizmet sağlayıcısı tarafından verilmiş nitelikli bir sertifikaya dayanmaması yahut güvenli bir imza oluşturma aracıyla üretilmemiş olması, onun hukuki etki doğurmasına veya yargılamada caiz delil olarak kullanılmasına engel teşkil etmemelidir (m.5).

Bilgisayar ekranına dijital kalemle atılan imza, el yazısıyla atılan imzanın tarayıcıdan geçirilerek elektronik belgelere eklenmesi ve biyometrik yöntemler ile sadece veri bütünlüğünü garanti eden sayısal imza türleri basit elektronik imza sınıfında değerlendirilebilir.

Bilgisayar ekranına imza atılması veya el yazısı ile atılan imzanın tarayıcı benzeri bir araçla bilgisayara aktarılması durumlarında, bu işlemin gerçekten irade beyanında bulunan kişi tarafından yapıldığı tespit neredeyse imkansızdır. Bu tür bir imzalamanın herkes tarafından oluşturulması veya kopyalanması mümkündür. Dolayısıyla bir belgeye bu şekilde eklenmiş imza veri bütünlüğünü garanti etmediği gibi kimlik tespiti işlevini de kesin olarak sağlayamaz. Yine bu şekilde oluşturulmuş imza otomatik bir usulle metnin altına eklendiği için uyarı işlevini de tam olarak gerçekleştirdiği söylenemez⁹⁰.

Biyometrik imza, bir kişinin kişisel, fiziksel veya davranış özellikleri ile teknik olarak tanınmasını sağlar. Zira bir şahsın parmak izi, sesi, göz retinası, yazı yazarken ve imza atarken oluşturduğu dinamikler ve daha başka pek çok biyometrik özellikleri kendine özgüdür. Biyometrik yöntemler kimlik tespiti işlevini yerine getirirler. Ancak veri bütünlüğünün korunmasını sağlamazlar. Bu nedenle genellikle bir sisteme girişte kullanılırlar⁹¹. Sayısal imza ise genel olarak veri bütünlüğünün korunması ve kimlik

⁸⁸ Halen yürürlüğe girmemiş olan “Hukuk Muhakemeleri Kanun Tasarısı”nın 203 ve devamı maddeleri gereğince basit elektronik imza ile imzalanmış belgeler de karşıladıkları niteliklere göre delil başlangıcı olarak kabul edilebilecek ve tanık delili ile desteklenmesi halinde geçerli delil olarak ileri sürülebilecektir.

⁸⁹ Orta, s.106; Erturgut, s.61

⁹⁰ Erturgut, s.63;

⁹¹ Erturgut, s.61, dn. 125- s.67; Özkaya-Sağiroğlu, s.285

tespiti işlevlerini yerine getirdiği için, gelişmiş ve güvenli elektronik imza kategorilerinde değerlendirilecektir. Ancak bu işlevlerden birini garanti edemeyecek durumda olursa, o zaman basit elektronik imza olarak sınıflandırılabilir.

1.6.3.2- Gelişmiş Elektronik İmza

Gelişmiş elektronik imza, elektronik imzanın genel tanımı yani basit elektronik imza esas alınarak, bu tanımlamaya bazı unsurların eklenmesi suretiyle tanımlanmıştır. Gelişmiş elektronik imza, veri bütünlüğünü koruyan, aynı zamanda da kimlik tespiti işlevini yerine getiren elektronik imzadır⁹².

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

Alman ve İsveç Elektronik İmza Kanununda da gelişmiş elektronik imza AB direktifindeki nitelendirmeye benzer şekilde tanımlanmış ve dört unsur öngörülmüştür. Buna göre gelişmiş elektronik imza; sadece imza anahtarı sahibi adına özgülenmiş, imza anahtarı sahibini tanımaya imkân veren, imza anahtarı sahibinin kendi kontrolü altında bulunan araçlarla yaratılan, imzanın bağlantılı olduğu verilerin sonraki değişikliklerini tespiti imkân veren elektronik imzadır(Alman EİK - İsveç EİK, m.2).

Gelişmiş elektronik imzaya örnek olarak, güvenli elektronik imza oluşturma aracı ile oluşturulmayan ve/veya nitelikli elektronik sertifikaya dayanmayan sayısal imzalar gösterilebilir. Doğrudan bilgisayarın hard diskinde kayıtlı veya CD/DVD, disket gibi üçüncü kişilerin erişme imkânı olan veri taşıyıcıları üzerinde bulunan, bazı sertifika hizmet sağlayıcılarının deneme sertifikası ve benzeri adlarla kullanıcıya sunduğu, nitelikli elektronik sertifika kapsamında bulunmayan sertifikalarla kullanılan sayısal imzalar bu kapsamda değerlendirilebilirler.

Gelişmiş elektronik imzalar, basit elektronik imza ile güvenli elektronik imza arasında bir güvenlik derecesine sahiptir. Ancak istenilen güvenlik şartlarını tam olarak sağlamadığından ve kötüye kullanım ihtimalleri mevcut olduğundan, gerek Avrupa

⁹² Erturgut, s.89; Orta, s.106

Birliđi düzenlemelerinde gerekse başka ÷lkelerde el yazısı ile imzaya eşdeđer kabul edilmemiřtir. Hukukumuzda ise geliřmiř elektronik imza tanımına yer verilmemiř, geliřmiř elektronik imzanın unsurları, güvenli elektronik imzanın unsurları ierisinde tanımlanmıřtır.

1.6.3.3- Güvenli (Nitelikli) Elektronik İmza

Nitelikli elektronik imza, geliřmiř elektronik imzanın güvenlik gereksinimleri yönünden bir kısım ek nitelikleri taşıyan halidir. AB Direktifinde nitelikli (güvenli) elektronik imzanın tanımı yapılmamıřtır. Ancak Direktifin 5 inci maddesi geređince üye devletlerin, nitelikli bir sertifikaya dayanan ve güvenli imza oluřturma araçları ile yaratılan ileri teknolojik imzaların, el yazısı imzaya eşdeđer kabul edilmesi ve yargılamada delil olarak kullanılmasını temin etmeleri gerekmektedir.

Alman Elektronik İmza Kanununda “nitelikli elektronik imza” kavramına da yer verilmiř ve geliřmiř elektronik imzadan hareketle tanımı yapılmıřtır. Buna göre nitelikli elektronik imza, geliřmiř elektronik imzanın unsurlarını taşıması yanında, imzanın oluřturulması anında geçerli bir nitelikli sertifikaya dayanan ve güvenli elektronik imza oluřturma bileřenleri ile üretilen elektronik imzadır⁹³.

Hukukumuzda ise, nitelikli elektronik imza kavramı yerine “güvenli elektronik imza” kavramına yer verilmiř ve 5070 sayılı Elektronik İmza Kanununun 4 üncü maddesinde tanımlanmıřtır. Buna göre güvenli elektronik imza, “*münhasıran imza sahibine bađlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluřturma aracı ile oluřturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliđinin tespitini sađlayan, imzalanmıř elektronik veride sonradan herhangi bir deđiřiklik yapılp yapılmadıđının tespitini sađlayan,* elektronik imzadır.

Bu tanımlamadan da anlařıldıđı üzere, AB Direktifi ve diđer yabancı mevzuatta geliřmiř elektronik imza tanımında zikredilen dört unsur, hukukumuzda güvenli elektronik imzanın unsurları arasında belirtilmiřtir. Diđer bir ifade ile 5070 sayılı yasada yapılan tanım, Direktifin 2. maddesinde yer alan ileri(geliřmiř) elektronik imza tanımında belirtilen unsurlar ile 5 inci maddesinde zikredilen üye devletlerin el yazısı ile

⁹³ Erturgut, s.90; Orta, s.107

imzaya eşdeğer kabul edecekleri elektronik imza için belirtilen gereksinimlerin birleştirilmesi sonucu oluşturulmuş ve ayrıca gelişmiş elektronik imza şeklinde bir ayırım yapılmamıştır. Güvenli elektronik imza, Avrupa Birliği Direktifinde belirtildiği üzere, el yazısı ile imzaya eşdeğer kabul edilmiş ve yargılamada geçerli delil olarak kullanılması temin edilmiştir. Zira yasa ile Borçlar Kanunu ve Hukuk Usulü Muhakemeleri Kanununda yapılan değişiklikler neticesinde, güvenli elektronik imza, el yazısıyla imzaya eşdeğer kabul edilmiş (EİK m.22 – BK m.14) ve elektronik imza ile oluşturulmuş verilerin senet hükmünde olacağı belirtilmiştir (EİK m.23 - HUMK m.295/A).

5070 sayılı Elektronik İmza Kanunda, elektronik imza ve güvenli elektronik imza ayrımı yapılmış ve genel elektronik imza tanımı dışında sadece güvenli elektronik imza düzenlenmiştir. Güvenli elektronik imza kapsamı dışında kalan elektronik imza türlerine herhangi bir hukuki değer atfedilmemiştir. Bu nedenle mevcut mevzuat çerçevesinde basit ve gelişmiş elektronik imza türlerinin hukuki anlamda bağlayıcılıkları ve delil değeri bulunmamaktadır.

Yabancı mevzuatlarda el yazısıyla imza ile eşdeğer hukuki etkiye sahip elektronik imzalar çeşitli adlarla (kalifiye, üniversal, e-imza vs.) ve değişik teknik gereksinimlerle tanımlanmıştır. Ancak bütün bu imzaların ortak noktası, nitelikli bir sertifikaya dayanmaları ve güvenli elektronik imza oluşturma aracıyla oluşturulmalarıdır.

1.6.3.4- Akredite Edilmiş Sertifika Hizmet Sağlayıcısı

Tarafından Verilmiş Sertifikaya Dayanan Elektronik İmza

Bu elektronik imza kalıbının güvenli (nitelikli) elektronik imza kalıbından tek farkı, nitelikli sertifikayı veren sertifika hizmet sağlayıcısının, yetkili bir makamdan teknik ve kurumsal güvenliğinin, yetkili kurum tarafından kontrol edildiğine dair bir belge veya sertifika almasıdır. Bu sayede ilgili sertifika hizmet sağlayıcısının nitelikli sertifikaya dayalı elektronik imzası için kapsamlı teknik ve kurumsal güvenlik araştırması yapıldığı yönünde bir ispat sağlanmış olur.

Hukukumuzda elektronik sertifika hizmet sağlayıcıları bakımından akreditasyon sistemi kabul edilmemiştir. Buna karşılık, AB Direktifinde, Alman ve Avusturya Elektronik İmza Yasalarında ihtiyari akreditasyona yer verilmiştir. İhtiyari akreditasyon, sertifikasyon hizmeti sunulmasıyla ilgili tüm hak ve yükümlülükleri belirleyen, ilgili sertifikasyon hizmeti sunucusunun isteği üzerine bu hak ve yükümlülüklerin geliştirilmesi ve denetimi ile ilgili kamuya da, özel nitelikli kurum tarafından verilen ve sertifikasyon hizmeti sunucusunun bu izinden kaynaklanan haklarını kullanmasına ilgili kararın kendisine ulaşmasına dek engel olan her türlü izindir (Direktif m.2/13). Buna göre sertifika hizmet sağlayıcısı, yetkili makama başvurarak akredite edilmek ister ve ilgili yasa ve bu yasaya dayanarak çıkartılmış olan diğer mevzuattaki şartları taşıdığını ispat ederse, söz konusu yetkili makam, ilgili sertifika hizmet sağlayıcısının akreditasyonunu sağlar(Alman EİK m.15 – Avusturya EİK m.17).

Akreditasyon yapılmakla sertifika hizmet sağlayıcısının teknik ve kurumsal güvenliği yetkili kurumca onaylandığından, ilgili sertifika hizmet sağlayıcısı akredite edilmiş sertifika hizmet sağlayıcısı olarak adlandırılır ve bu sayede akredite edilmemiş sertifika hizmet sağlayıcılarına nazaran daha fazla güven duyulması sağlanmış olur.

Akredite edilmiş sertifika hizmet sağlayıcıları tarafından verilmiş nitelikli elektronik sertifikaya dayanan nitelikli elektronik imzaların, hukuki anlamda şekil veya ispat kuralları açısından, diğer nitelikli elektronik imzalardan bir farklılığı veya üstünlüğü bulunmamaktadır. Zira kanundaki, elektronik imzanın elektronik belgelerdeki şekil şartını yerine getirmesi ve elektronik imzalı belgelerin delil olarak kullanılmasına ilişkin düzenlemelerde akredite edilmiş sertifika hizmet sağlayıcılarından bahsedilmemektedir. Dolayısıyla Türk hukuku açısından nitelikli elektronik sertifikanın akredite edilmiş bir sertifika hizmet sağlayıcısı tarafından ya da akredite edilmemiş bir sertifika hizmet sağlayıcısı tarafından verilmiş olması arasında bir fark yoktur.

1.7- Elektronik imzanın Hukuki Niteliği ve Güveni Elektronik İmza İle El Yazısı İmzanın Fonksiyonel Eşitliği

1.7.1- Elektronik İmzanın Hukuki niteliği

Yukarıda ayrıntılı olarak açıklandığı üzere, elektronik imzanın çeşitli türleri ve birbirinden farklı nitelikleri bulunmaktadır. AB Direktif'inin 5/1 inci maddesine göre

nitelikli sertifikaya dayanan ve güvenli imza oluşturma aracı ile oluşturulan imzaların hukuki etkisi kağıda elle atılmış imza ile aynı olmalıdır. Ayrıca bu imzanın delil niteliği inkar edilmemelidir. Yabancı mevzuatlarda elektronik imzanın hukuki değerinin farklılık arz ettiği görülmektedir. Alman Elektronik İmza Kanunu'nda elektronik imzanın geçerliliği ile ilgili bir hüküm bulunmamaktadır, geçerlilik hükümleri çeşitli kanunlarda yer almaktadır (Medeni Kanun, Medeni Usul Kanunu). Bulgar Elektronik İmza Kanunu'nda ise normal, kalifiye ve üniversal elektronik imza çeşitleri bulunmaktadır. Bunlardan kalifiye imza, özel hukuk kişileri arasında elle atılmış imza ile aynı sonucu doğururken üniversal imza, kamu kurumları ve gerçek kişiler arasında elle atılmış imza ile aynı hukuki sonucu doğurur. Üniversal imzanın kalifiye imzadan farkı, kullanılan sertifikaların akredite edilmiş bir hizmet sağlayıcı tarafından sağlanıyor olmasıdır⁹⁴.

Ülkemizde de elektronik imzanın niteliği hukuki etkisi açısından farklılık arz etmektedir. Zira 5070 sayılı Elektronik İmza Kanununda 3 üncü maddede yer alan genel anlamdaki “Elektronik İmza” tanımı haricinde, özel olarak “Güvenli Elektronik İmza” düzenlenmiş ve bu nitelikteki elektronik imzaya hukuki değer verilmiştir. Buna göre “Güvenli Elektronik İmza, elle atılan imza ile aynı hukukî sonucu doğurur”(m.5/1). Bunun anlamı, güvenli elektronik imza ile ıslak imzanın gerek fonksiyonel anlamda gerekse şekil ve ispat kuralları bakımından eşit olduğudur. Bu hüküm sayesinde, özel hukuk alanında hem şekle tabi sözleşmelerin elektronik ortamda kurulabilmesi, hem de güvenli elektronik imza ile imzalanmış elektronik belgelerin mahkemelerde senet olarak kabul edilmesi mümkün hale gelmiştir.

Ayrıca kanunun 22 nci maddesi hükmü ile, Borçlar Kanunu'nun 14 üncü maddesine “*güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir*” cümlesi eklenmiştir. Şüphesiz, BK'nun 14 üncü maddesi, yazılı şekil şartının unsuru olan imzanın ne olduğu ve nasıl tatbik edilmesi gerektiğine ilişkin olup, bu hükmün ispatla veya ispat gücüyle bir ilgisi bulunmamaktadır. Zaten kanunun 23 üncü maddesi hükmü ile HUMK'na güvenli elektronik imza ile imzalanmış bir elektronik belgenin, senet hükmünde olduğu ve aksi ispat edilinceye kadar kesin delil teşkil edeceği hükmünü içeren 295/a maddesi eklenmiştir. Bu sebeple, maddede yer alan “ispat gücü”

⁹⁴ Berber-Sevim-Beceni, s.32; Sevim, s.8

ifadesine rağmen bu hükmü, güvenli elektronik imzanın, elle atılan imza ile hukuken eşdeğer olduğu, yani yazılı şekil şartı için gerekli imza unsurunu yerine getirdiği şeklinde anlamak gerekecektir⁹⁵.

Güvenli elektronik imza ile ilgili bu düzenleme Direktif'in 5/1inci maddesine uygundur. Ancak, yukarıda da bahsedildiği üzere elektronik imza, Kanun'un 3/b maddesinde "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*" şeklinde, diğer bir ifade ile tüm elektronik imza türlerini kapsayacak tarzda yapılmasına rağmen, elektronik imza ile ilgili diğer tüm düzenlemeler güvenli elektronik imza baz alınarak yapılmıştır. Güvenli (nitelikli) elektronik imza özelliklerini taşımayan elektronik imzaların hukuki niteliği hususunda ise herhangi bir düzenleme yapılmamıştır. Dolayısıyla, elektronik imza tanımı kapsamında bulunmalarına rağmen, bu nitelikteki elektronik imzaların hukuki bağlayıcılık ve ispat gücü açısından mevcut düzenlemede hiçbir değeri bulunmamaktadır. Oysa ki Direktif'in 5/2 nci maddesi gereğince bir elektronik imzanın, sadece elektronik formda olması, nitelikli bir sertifikaya dayanmaması veya akredite edilmiş bir sertifika hizmet sağlayıcısı tarafından verilmiş nitelikli bir sertifikaya dayanmaması ya da güvenli bir imza oluşturma aracıyla üretilmemiş olması, onun hukuki etki doğurmasına veya yargılamada caiz delil olarak kullanılmasına engel teşkil etmemelidir. Şu halde 5070 sayılı yasada güvenli elektronik imza kapsamı dışında bulunan elektronik imzalara ilişkin herhangi bir düzenleme veya hukuki nitelendirme yapılmaması önemli bir eksikliklerdir. Zira şu durumda yukarıda kısaca değindiğimiz hukuki bağlayıcılık ve ispat sorunları Güvenli Elektronik İmza dışında bulunan elektronik imza türleri için devam etmektedir. Bu yöndeki eksikliklerin giderilebilmesi için yukarıda da izah edildiği üzere, Türk Borçlar Kanunu ve Hukuk Muhakemeleri Kanunu tasarılarında elektronik kayıtları da içerir yeni hükümlere yer verilmiş ise de söz konusu problemler bu tasarılar yasalasınca kadar devam edecek gibi gözükmektedir.

Bu durumda güvenli elektronik imza kapsamı haricinde bulunan elektronik imzaların ıslak imzanın fonksiyonlarını eda etmesi mümkün değildir. Dolayısıyla bu tür elektronik imzalar ile şekle bağlı sözleşmeler geçerli olarak kurulamazlar. Yine şekil

⁹⁵ İnal, s.144

şartı bulunmayan sözleşmeler de bu tür elektronik imzalarla geçerli olarak kurulabilseler bile bu kez de ispat şartlarını yerine getiremezler.

Diğer taraftan güvenli elektronik imza, el yazısı ile imzanın gerek fonksiyonel gerekse hukuki anlamdaki fonksiyonlarını tam anlamıyla yerine getirebilmektedir. Diğer bir deyişle ıslak imza ve güvenli elektronik imza hukuki ve fonksiyonel anlamda eşittir. Dolayısıyla temelde ıslak imza ile gerçekleştirilebilecek her türlü işlem elektronik ortamda güvenli elektronik imza ile gerçekleştirilebilir. Bununla beraber Kanun, güvenli elektronik imzaya da birtakım istisnalar getirmiş ve kanunen resmi şekle veya özel bir merasime tabi tutmuş olduğu hukuki işlemler ile teminat yani kefalet, garanti ve rehin sözleşmelerinin güvenli elektronik imza ile imzalanmış olsalar dahi elektronik ortamda geçerli olarak akdedilemeyeceklerini hükme bağlamıştır(EİK. m.5/II).

Güvenli elektronik imzanın el yazısı (ıslak) imza ile hukuki bakımdan eşdeğer olduğu yukarıda zikredilen yasal hükümlerden anlaşılmaktadır. Bunun haricinde az önce de belirttiğimiz üzere, güvenli elektronik imza el yazısı ile imzanın kağıt üzerinde yerine getirdiği tüm fonksiyonları da elektronik ortamda yerine getirdiğinden fonksiyonel anlamda da eşdeğerlik söz konusudur. Bu fonksiyonların ne şekilde yerine getirildiği aşağıda açıklanacaktır.

1.7.2- Elektronik İmza ve El Yazısı İle İmzanın Fonksiyonel Eşitliği

Elektronik imza, fiziki olarak el yazısı ile imza değildir. Yine elektronik imza ile imzalanmış bir belgenin bilgisayar çıktısında el yazısı ile imzada bulunan karakteristik kişiselleştirme özelliği yoktur. Buna karşılık elektronik imzada imza sahibinin kimliğini tespit eden sertifikanın ve belgenin bütünlüğünü garanti eden özet değerinin (hash) imza sahibine özel bir anahtarla şifrelenmesi söz konusudur. Bu nedenle elektronik imza ve el yazısı ile imza fiziki olarak aynı değildir.

Elektronik imza ile uygulamada “ıslak imza” olarak nitelendirilen el yazısı ile imzanın hukuki anlamda eşdeğer sayılabilmesi için elektronik imzanın el yazısı imzanın sağladığı fonksiyonları aynı şekilde sağlaması gereklidir. Islak imzanın işlevlerini genel

olarak “sonuçlandırma, devamlılık, kimlik tespit etme, gerçeklik, tasdik, ispat, uyarı ve teklik” işlevleri olarak sıralayabiliriz⁹⁶. Bu durumda elektronik imzanın da bu işlevleri yerine getirmesi icap etmektedir. Aşağıda görüleceği gibi elektronik imza, ıslak imza ile fonksiyonel anlamda eşit olup, elektronik imza ıslak imzanın tüm fonksiyonlarını yerine getirebilmektedir. Bu anlamda elektronik imza ile ıslak imza hukuki sonuçları anlamında eşdeğerdir. Hatta elektronik imzanın “gizlilik” ve “veri bütünlüğü” gibi ekstra fonksiyonları da mevcut bulunmaktadır. Söz konusu fonksiyonları ve bu fonksiyonlardaki eşitliği aşağıda açıklamaya çalışacağız.

1.7.2.1- Sonuçlandırma İşlevi

El yazısı ile atılan imza, bir metnin içerik itibarıyla sona erdirilmesidir. Elektronik imzada ise, öncelikle elektronik ortamda hazırlanan metnin tümünün, gizli imza anahtarı ile imzalanacak olan hash değerinin çıkarılması gerektiği için, dijital imzalama süreci belgenin tümüne ilişkindir. Bu şekilde hazırlanan belgeye ilişkin olan imza, ancak metnin hazırlanmasından sonra oluşturulabilecektir. İmzalanan metin ve imza arasındaki bu mantıki bağlantı, sonuçlandırma işlevini yerine getirmektedir.⁹⁷

1.7.2.2- Devamlılık İşlevi

Yazılı şekil zorunluluğu, imzanın ve imzalanacak olan metnin okunabilir bir şekilde bir belgede yer almasını ve sürekli bir kontrole elverişli olmasını gerektirir. Bu sayede yapılan beyan hakkındaki bilginin bir belgede tespit edilerek kalıcı olması sağlanmış olur. Elektronik olarak imzalanan bir belgede de, bu elektronik metnin istenildiği zaman okunabilmesi ve kontrol edilebilmesini mümkündür⁹⁸. Zira, bilgisayarın hafızasına, ayrı bir diskete veya CD’ye kopyalanan elektronik imzalı bir metnin her zaman için okunabilmesi mümkün olmaktadır. Yine sertifika hizmet sağlayıcılarının herhangi bir uyumsuzluk durumunda kullanılabilmesi için elektronik imzalı verilerin saklanması yönünde işlevleri de bulunmaktadır.

⁹⁶ Keser Berber (Şekil), s.6; Erturgut, s.104; Altınışık, s.92

⁹⁷ Erturgut, s.106; Keser Berber (Şekil), s.39; Altınışık, s.93; Sağiroğlu-Alkan, s.29

⁹⁸ Keser Berber (Şekil), s.39; Caron, s.1; Erturgut, s.118

1.7.2.3- Kimlik Tespit Etme İşlevi

İmzanın el yazısı ile atılması sayesinde belgeyi düzenleyen kişinin kimliği şüpheye yer vermeyecek şekilde tespit edilebilmektedir. Aynı şekilde elektronik imzada da kimlik tespit etme işlevi, sertifika hizmet sağlayıcıları tarafından elektronik imza sahibine verilen ve elektronik imzalama işlemi esnasında imza verisine eklenen elektronik sertifika bilgisi ile sağlanmaktadır⁹⁹. Anahtar sahibinin açık anahtarını bilen alıcı, herkes tarafından ulaşılabilen imza anahtarı sertifikasının kontrolü sayesinde, tanzim eden kişinin kimliği hakkında bilgi sahibi olabilecektir.

1.7.2.4-Gerçeklik İşlevi

İrade beyanının yapıldığı belgede yer alan imzanın, bu belge ile olan lokal ilişkisi, belge ve imza arasında bir bağlantı meydana getirecektir. Bu suretle beyanın içerik olarak imza sahibi tarafından kabul edildiği garanti edilmiş olacaktır. Elektronik imzada da metin ve imza arasındaki matematiksel ve mantıki bağlantı nedeniyle, beyan ve imzalama arasında da sıkı bir bağlantı ortaya çıkmaktadır. Bu suretle beyanın içerik olarak imzalayan tarafından hazırlandığı ve sonradan değiştirilmediği garanti edilmektedir¹⁰⁰.

1.7.2.5- Tasdik İşlevi

Tasdik işlevi, gerçeklik ve kimlik tespiti fonksiyonları ile yakından bağlantılıdır. Tasdik işlevi sayesinde belgenin alıcısı, imza karşılaştırması yapmak suretiyle, imzanın gerçek olup olmadığını kontrol etmek olanağına sahiptir. Elektronik belgede de güvenilir ve sağlam bir elektronik imza tekniği sayesinde alıcı, imzanın, imza anahtarı sahibi tarafından atılıp atılmadığını ve imzalanan metnin sonradan değiştirilip değiştirilmediği kolay bir şekilde kontrol etmek edebilmektedir¹⁰¹.

⁹⁹ Acır, s.25; Keser Berber (Şekil), s.39; Altınışık, s.93

¹⁰⁰ Acır, s.27; Keser Berber (Şekil), s.39;Erturgut, s.112;Altınışık, s.93; Caron, s.1;Erdoğan-Karagül-Elitaş, s.191

¹⁰¹ Keser Berber (Şekil), s.39; Altınışık, s.93; Karakoçak ve diğerleri, s.6;

1.7.2.6- İspat İşlevi

Bir metnin altına el yazısı ile atılan imza, delil ikamesine ve hukuki işlemin içeriğinin açıklanmasına ve bu sayede taraflar arasındaki işlem bakımından sürekli bir şeffaflığa hizmet etmektedir. Yazılı şekil, ispatla yükümlü olan tarafın delil ileri sürmesini kolaylaştıracaktır. Yasanın aradığı özellikleri taşıyan bir elektronik imza, bu imza ile imzalanan elektronik belgeye kesin delil olan “senet” niteliği kazandırmaktadır. Böylece elektronik şekilde yapılan bir irade beyanı, alıcısı bakımından, klasik yazılı şekilde hazırlanmış bir belgeye verilen delil değerine sahip olacaktır¹⁰².

1.7.2.7- Uyarı İşlevi

İmza sayesinde beyanda bulunan kişi, imzalanan beyanın hukuki bağlayıcılığını ve sonuçlarını hesaba katmak zorundadır. Böylece kişiler, hukuki işlemler bakımından aceleci davranmaktan, düşüncesizce hareket etmekten korunmuş olacaklardır. Elektronik belgede de, imza atacak olan kişinin öncelikle ilgili metni bilgisayarda hazırlaması gerekmektedir. Daha sonra elektronik imza oluşturma aracını bilgisayara takması ve PIN kodunu girmesi gerekecektir. Sadece bu prosedür bile, işin ne kadar bağlayıcı olduğu konusunda imza atacak olan kişinin dikkatini çekecek düzeydedir¹⁰³.

1.7.2.8- Teklik İşlevi

El yazısı düşüncesinin grafik ifadesi olması nedeniyle, kişinin duygularının ve karakterinin izlerini taşır. Bu nedenle her insanın imzası kendine özgüdür ve benzersizdir. Benzer şekilde elektronik imzada da her bir kişinin elektronik imzası (elektronik sertifikası) ve hatta atılan her bir elektronik imza benzersizdir¹⁰⁴.

Görüldüğü gibi elektronik imza el yazısı ile atılan imza ile işlevsel eşitliğe sahiptir. Bunların yanında elektronik imzanın başkaca avantajları da vardır. Bunları aşağıdaki, şekilde sıralayabiliriz¹⁰⁵.

¹⁰² Acır, s.27; Erturgut, s.119; Caron, s.1; Rüssmann, s.41; Erdoğan-Karagül-Elitaş, s.190

¹⁰³ Keser Berber (Şekil), s.40; Altınışık, s.93; Erturgut, 115

¹⁰⁴ Erdoğan-Karagül-Elitaş, s.190; Erturgut, s.80; Caron, s.1

¹⁰⁵ Keser Berber (Şekil), s.17; Altınışık, s.94; Orta, s.59; Ahi, s.2-3; Caron, s.1; Erturgut, s.104 vd.; Bensghir, s. 79 vd.; Karakoçak ve diğerleri, s.6

1- Elektronik imza, bir kullanıcı tarafından gönderilen bilgilerin veya verilerin kesinlikle o kişi tarafından gönderildiği teyit eder. Kısacası, başkası tarafından gönderilmediğini garanti eder. Dolayısıyla, klasik imzadaki gibi taklit edilme olasılığı da ortadan kalkar. Gönderici göndermediğini, alıcı da almadığını iddia edemez.

2- Elektronik imzada şifreleme sayesinde gizlilik sağlanabilir. Bu sayede bir kullanıcı tarafından gönderilen bilgilerin veya verilerin bir başkasının eline geçmesi veya değiştirilmesi engellenir.

3- Elektronik imzalı olarak gönderilen bilgi ve verilerin içeriği, gönderici tarafından veya alıcı tarafından inkar edilemez. Çünkü, değil başkası, kendileri dahi gönderimden sonra içeriğini değiştiremez. Kaldı ki, bir uyumsuzluk halinde elektronik belgenin bir kopyası da sertifika hizmet sağlayıcısındadır.

4- Elektronik imza ile gönderilen verilerin tarih açısından damgalanması sağlanabildiği gibi, arşivleme kolaylığı sağlar.

5- Elektronik imzalama ve muhataba gönderme elektronik ortamda gerçekleştiği için, gönderilen verilerin çabuk ulaşması sağlanır, baskı, kağıt, posta ve arşivleme maliyetleri en aza indirgenir.

6- Elektronik imzanın oluşturulması ve kullanımı kolaydır,

7- Her yeni mesajda elektronik imzanın farklı bir “ bit “ örneği ortaya çıktığı için, taklit edilmesi son derece güçtür ve gizli anahtara imza üzerinden ulaşılması mümkün olmadığı için, bilgi ağı üzerinden dijital imzanın elde edilmesi zordur,

8- Elektronik imza ile fikri haklar ve telif hakları da imzalanabilir. (Örneğin; dijital resimler, besteler, yazılımlar gibi). Bu sayede diğer imza türlerinde olmayan verinin korunması ve izinsiz kullanılamaması güvencesi sağlanmış olur.

1.8- Elektronik İmza Hakkındaki Uluslararası Düzenlemeler ve Bu Düzenlemelerin Türkiye'ye Yansıması

Bilişim teknolojilerindeki akıl almaz ilerleme ve iletişim güvenliğinin sağlanması arayışları neticesinde ulaşılan teknik çözümler, tüm kanun koyucu ve

uygulayıcılarını, bir hukuk politikası belirleyerek, bu teknolojiyi sıkı disiplin altına alıp, teknolojik gelişmeleri engelleyici bir rol oynamadan ve ulaşılan teknik çözümleri hukuki korumadan yoksun bırakmadan, söz konusu teknik çözümleri hukuken koruyucu yasal düzenlemeleri gecikmeksizin yerine getirmek konusunda harekete geçirmiştir. 1997 yılından beri bir çok ülkede sayısal imzanın hukuki çerçevesi hakkında çalışmalar yapılmıştır. Yine çoğu ülkenin sayısal imza düzenlemelerinde UNCITRAL¹⁰⁶ model yasaları ve Avrupa Birliği direktifleri rol oynamıştır¹⁰⁷. AB üyesi ülkelerin yanı sıra, ABD, Kanada, Arjantin, Brezilya, Japonya, Singapur, Hindistan, Rusya, Çin, Tayvan, İsrail ve Avustralya'da sayısal imza kanunlaşmıştır ve elektronik ticarete hız ve güvenilirlik kazandırılmıştır.

Ülkemizde de bu konuda çalışmalar Dış Ticaret Müsteşarlığı'na bağlı Elektronik Ticaret Koordinasyon Kurulu ve Adalet Bakanlığı tarafından başlatılmış, hazırlanan yasa tasarısı tartışmaya açılmış ve 5070 sayılı Elektronik İmza Kanunu 23.01.2004 tarihinde resmi gazete yayınlanarak 23.07.2004 tarihi itibarıyla yürürlüğe girmiştir. Kanun hazırlanırken yabancı mevzuattaki benzer düzenlemeler ve Avrupa Komisyonu'nun 99/93/EC sayılı elektronik imzalara ilişkin direktifi baz alınmıştır¹⁰⁸. Bu düzenlemenin yapılmasında Adalet Bakanlığı ve bağlı kuruluşların bünyesinde yürütülen faaliyetlerin ve yargı sistemi ile ilgili işlevlerin bilgisayar yardımı ile tam entegre bir şekilde otomasyona geçirilmesi için çalışmaları devam eden Ulusal Yargı Ağı Projesi çalışmasının etkisi büyük olmuştur¹⁰⁹.

Elektronik imzanın elektronik ortamda kimlik tespiti, veri bütünlüğü ve gizlilik gibi işlevleri nasıl gerçekleştirdiği ve bunun için gerekli teknik altyapı ilerde ayrıntılı olarak açıklanacaktır. Ancak, elektronik imzanın yaygın olarak kullanılabilmesi, her türlü sözleşme ve resmi işlemin yapılabilmesi ve dahi e-ticaretin gelişip yaygınlaşmasının sağlanabilmesi için, tarafların (kullanıcı-onay kurumu-üçüncü kişi) hak ve sorumlulukları ile risklerin tahsisini belirleyen, elektronik imza ile imzalanan kayıtların hukuki geçerliliğini ve ispat değerini düzenleyen bir hukuki altyapının da kurulması gereklidir.

¹⁰⁶ UNCITRAL: Birleşmiş Milletler Uluslararası Ticaret Komisyonu

¹⁰⁷ 13 Aralık 1999 tarihli Avrupa Konseyi Elektronik İmza Direktifi ile Birleşmiş Milletlerin 14 Haziran 1996 tarihli Elektronik Ticarete İlişkin Model Kanunu

¹⁰⁸ Sevim, s.1

¹⁰⁹ Biçkin, s.351

Diğer yandan elektronik iletişimin, özellikle e-ticaretin, açık ağlar üzerinden yapılan ve uluslararası yönü de olan bir yapısının olduğu dikkate alındığında, kurulacak hukuksal altyapının, bu husustaki dünya düzenlemeleriyle uyumlu olması da gerekecektir. Daha açık bir ifadeyle, farklı ülkelerde, farklı düzenlemelere tabi olan sertifika hizmet sağlayıcılarınca çıkarılan sertifikaların ve onaylanan elektronik imzaların ülke dışında geçerli olup olmayacağı ve geçerliliğin tabi olduğu kuralların, diğer ülke düzenlemeleriyle işbirliği içinde ve/veya UNCITRAL, OECD, AB gibi uluslararası kuruluşlarca hazırlanan Standartlar, Yeknesak Kurallar, Rehberler ve Direktifler dikkate alınarak belirlenmesi gerekmektedir¹¹⁰.

Elektronik imza ve elektronik ticaret konusunda dünyada çeşitli çalışmalar yapılmış, özellikle uluslar arası düzeyde yapılan çalışmalar ile diğer ülkelerin bu yöndeki ulusal düzenlemelerine yol gösterecek genel kurallar ve standartlar belirlenmiştir. Bu çalışmalardan en önemlileri Birleşmiş Milletler Uluslararası Ticaret Yasası Komisyonu (UNCITRAL) çalışmaları olan, UNCITRAL Elektronik Ticaret Model Kanunu, UNCITRAL Elektronik İmza Model Taslağı ve UNCITRAL Elektronik İmza Yeknesak Kurallar Taslağı ile Avrupa Birliği'nin 2000/31 ve 1999/93 sayılı direktifleridir. Aşağıda bu yöndeki uluslar arası çalışmalar incelenecek ve yabancı ülkelerdeki hukuki altyapıdan kısaca bahsedilecektir. Daha sonra ise ülkemizdeki bu düzenlemelere paralel hukuki altyapı incelenecektir.

1.8.1- UNCITRAL Elektronik Ticaret Model Kanunu

Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu'nun (UNCITRAL) hazırlanmış olduğu Elektronik Ticaret Model Kanunu Tasarısı, ülkelere örnek alabilecekleri kuralları sunmakta olup, 16 Aralık 1996 tarihinde Birleşmiş Milletler Genel Kurulu'nda kabul edilmiştir. Kanun, ticari faaliyetler kapsamında kullanılan elektronik mesaj şeklindeki her türlü bilginin kanunların yazılı olma ve orijinal nüsha olma şartlarını yerine getirebileceği, saklanması, ispat güçleri, taraflarca tanınması, alındığının teyidi gibi sadece elektronik veri ile ilgili ayrıntılı bilgi vermektedir. Bu kanunun amacı, modern iletişim araçlarının kullanımının artması ile birlikte hukuken önem arz eden bilgilerin elektronik olarak iletilmesinin hukuki etki ve geçerliliklerindeki belirsizlikleri ve hukuki engelleri ortadan kaldırmak, elektronik

¹¹⁰ Acır, s.33

ticaret alanını hukuki güvence altına almaktır¹¹¹. Model Kanun her ülke tarafından aynen veya değiştirilerek ulusal hukuka aktarılabilecektir.

Model Kanun'un öngördüğü temel prensiplerden birisi, beşinci maddede zikredilmiştir. Buna göre, irade beyanlarının, sadece elektronik ortamda ifade edilmeleri sebebiyle hukukî etkisi, geçerliliği ve icra edilebilirliği engellenemez. Yine 11 inci maddeye göre, taraflar aksini kararlaştırmadığı sürece, elektronik yolla, sözleşmenin kurulmasına ilişkin icap ve kabul beyanında bulunabilir. Bu yolla kurulan bir sözleşme, sırf elektronik ortamda kuruldu diye geçersiz sayılamaz ve yerine getirilmesinden kaçınılamaz. Kanunun 6 ncı maddesine göre ise ulusal hukukun bir beyan için yazılı şekli şart koştuğu durumlarda, bu şekil şartı bu beyan daha sonra erişilebilir olduğu sürece, elektronik yolla da yerine getirilebilir. Buradaki "erişilebilirlik" sözcüğü, bilgisayar verisi şeklindeki bilginin, okunabilir ve yorumlanabilir olması, bu bilginin okunabilmesi için gerekli olan yazılımin muhafaza edilmesi anlamındadır¹¹². Madde 7 nci maddesinde de elektronik imzanın, güvenilir bir şifreleme yöntemi kullanılması şartıyla el yazısıyla imzaya eşdeğer olduğu ifade edilmiştir. Bu maddeye göre ulusal hukukun kişinin imzasını şart koştuğu durumlarda, göndericinin kimliğini tespit eden ve bu kişinin veri mesajının muhtevasını kabul ettiğini gösteren bir yöntemin kullanılması halinde imza şartı yerine getirilmiş sayılacaktır.

1.8.2- UNCITRAL Elektronik İmza Model Kanun Tasarısı

UNCITRAL Elektronik ticaret çalışma grubu tarafından Elektronik Ticaret Model Kanunu'nda benimsenen yaklaşımları esas alan Elektronik İmza Yeknesak Kuralları çalışması yapılmış ve grubun 31-37'inci oturumlarında, bir Elektronik İmza Model Kanunu Tasarısı hazırlanarak 30 Ocak 2001 tarihinde yayımlanmıştır. Söz konusu tasarı ile, ülkelerin çıkaracakları elektronik imza kanunları için model olunarak, elektronik imzanın temel kurallarını oluşturarak çeşitli ülkelerin farklı mevzuatlar geliştirme riskini önlemek hedeflenmiştir. Bu şekilde çerçeve bir yasa hazırlanarak elektronik imzalarla ilgili genel esasların belirlenmesi amaçlanmıştır¹¹³.

¹¹¹ Şenocak, s.105; Topaloğlu, s.122; Orta, s.71; Demirel, s.2; Falcıoğlu, s.64

¹¹² Şenocak, s.106

¹¹³ Şenocak, s.107; Topaloğlu, s.123; Orta, s.71; Falcıoğlu, s.65; İnalöz, s.59

Tasarının 1 inci maddesinde, Elektronik Ticaret Model Kanunu'nda olduğu gibi, bu Tasarının, elektronik imzanın ticari faaliyetlerde kullanılması durumunda uygulanacağı belirtilmiş ve Tasarı hükümlerinin tüketicinin korunmasıyla ilgili kuralları yürürlükten kaldırmadığı hususu ifade edilmiştir.

Elektronik Ticaret Model Kanunu'nun elektronik imzanın güvenilir bir şifreleme yöntemi kullanılması şartıyla el yazısıyla imzaya eşdeğer olduğuna dair 7 nci maddesi hükmü tasarının 6 ncı maddesine aynen alınmış ve ayrıca bu güvenilirliğin kabul edilme şartları sayılmıştır. Bu şartlar, elektronik imzayı yaratan verinin (özel anahtarın), imzanın atılması anında, sadece imza sahibinin kontrolü altında bulunması, imzalamadan sonra da elektronik imzadaki herhangi bir değişikliğin tespit edilebilirliği ve bilginin muhtevasının bütünlüğünün, imzadan sonra bu muhtevada yapılacak değişikliğin tespitini mümkün kılacak derecede sağlanması olarak belirtilmiştir (m.6/3). Yine, sözü edilen şartların, kişilerin, elektronik imzanın güvenilirliğini başka bir şekilde gerçekleştirme veya elektronik imzanın güvenilir olmadığını ispat etme imkanını ortadan kaldırmayacağı da hüküm altına alınmıştır(m.6/4). Tasarı'da ayrıca, imza sahibinin, üçüncü kişilerin ve sertifika hizmet sağlayıcılarının sorumluluklarına ilişkin hükümlere de yer verilmiştir(m.8, 9, 11).

1.8.3- 2000/31 Sayılı ve 8 Haziran 2000 Tarihli, Avrupa Birliği Elektronik Ticaret Direktifi

Avrupa Birliği üyesi ülkelerin 16.01.2002 tarihine kadar iç hukuka uyarlamak zorunda olduğu Elektronik Ticaret Yönergesi'yle, bilgi toplumu hizmetlerinin üye ülkeler arasında serbest dolaşımını sağlamak amaçlanmış ve Avrupa iç pazarında elektronik ticaret için önem arz eden iktisadi ve özel hukuka ilişkin çerçeve şartlar belirlenerek, elektronik sözleşmeler ile bunların hukuki neticelerine ilişkin hususlar düzenlenmiştir¹¹⁴. Yönerge'nin 9'uncu maddesi, üye ülkeleri sözleşmelerin elektronik yolla kurulmasına ilişkin hukuki engelleri ortadan kaldırma yükümlülüğü altına sokmaktadır. Söz konusu hükme göre, üye ülkelerin sözleşmelerin kurulmasına ilişkin hukuki düzenlemelerinin, sözleşmelerin elektronik yolla kurulmasına ve bu sözleşmelerin elektronik yolla kurulmuş olmaları nedeniyle hukuki geçerlilik ve etki

¹¹⁴ Orta,72; Demirel, s.3; Şenocak, s.109

kazanmasına engel teşkil etmemesi gerekir¹¹⁵. Ancak, aile hukuku ve miras hukuku sözleşmeleri başta olmak üzere, mahkemelerin ve kamu yetkisi icra edenlerin iştiraki gereken sözleşmeler dahil bir kısım sözleşmeler bu hüküm kapsamı dışında bırakılmıştır.

1.8.4- 1999/93/EC Sayılı ve 13 Aralık 1999 Tarihli, Avrupa Birliği Elektronik İmza Direktifi

Avrupa Birliğine üye ülkeler bakımından, Avrupa Topluluğu Telekomünikasyon Bakanlığı Kurulu 30 Kasım 1999 tarihinde, üye ülkelerde elektronik imzanın kabulünü gerçekleştirmeyi hedefleyen bir Direktif kabul etmiştir. Söz konusu Direktif, elektronik imza ile ilgili her konuyu ayrıntılı olarak düzenlemeyip, imza işlemleri ve güvenlik standartları konusunda alınması gerekli asgari tedbirleri belirtmekte olup, Avrupa Birliği çerçevesinde elektronik ticaretin gelişmesi bakımından son derece önemli bir adım niteliğindedir. Direktifin amacı elektronik imza konusunda temel yasal çerçeveyi ve bu yasal çerçevenin en önemli bileşenleri olan sertifika hizmet sağlayıcılarının statüsünü düzenlemek, elektronik imzanın kullanılmasını kolaylaştırmak ve hukuken tanınmalarına katkıda bulunmaktır¹¹⁶. Direktif ile üye devletlere, iç hukuklarında bu Direktif doğrultusunda, gerekli yasa, düzenleme ve idari hükümleri yürürlüğe koymaları için, 19 Temmuz 2001 tarihine kadar süre verilmiştir(m.13/1).

Direktifin 2. maddesine elektronik imza ve gelişmiş elektronik imza tanımlanmış ve elektronik imza olarak gelişmiş elektronik imza esas alınmıştır¹¹⁷. Buna göre, gelişmiş elektronik imzanın; a) *Sadece imza sahibine özgülenmesi*, b) *İmzalayanın kimliğinin tespitine imkan vermesi* c) *Sadece imza sahibinin kontrolü altındaki araçlarla yaratılması* ve d) *İlişkili olduğu verilerde sonradan yapılan tüm değişiklikleri tespiti imkan sağlaması* gereklidir(m.2/2). Direktifin 5 inci maddesi üye ülkelere, nitelikli bir sertifikaya dayanan ve güvenli bir imza oluşturma aracı ile oluşturulan gelişmiş elektronik imzaların, el yazısı ile imzaya eşdeğer tutulmasını ve yargılamada ispat aracı olarak tanınmasının sağlamaları gerekmektedir.

¹¹⁵ Şenocak, s.109; Falcıoğlu, s.66; Orta, s.72

¹¹⁶ UKK Hukuk Çalışma Gurubu Raporu, s.18; Topaloğlu, 123; Şenocak, s.109; İnalöz, s.76; Orta, s.73

¹¹⁷ Şenocak, s.109; Orta, s.73

Direktife göre, elektronik imzaların tedarik edileceği, imzaları kaydeden ve gelişmiş imzaları geçerli kılan sertifika hizmet sağlayıcılarının bulunması gerekir. Yönerge'nin 3'üncü maddesinin ilk fıkrasında, üye ülkelerin, sertifika hizmetlerinin sunumunu önceden verilecek bir izne tabi tutamayacağı belirtilmiştir. Bununla birlikte, üye ülkelerin, sertifika hizmetlerinin standardını yükseltmek amacıyla isteğe bağlı bir akreditasyon sistemi getirilebilecekleri ifade edilmiştir(m.3/2). Avrupa Birliği üyesi olmayan bir ülkede faaliyet gösteren sertifika hizmet sağlayıcılarının düzenlemiş olduğu nitelikli elektronik sertifikaların tanınmasına ilişkin hususlar ise Direktifin 7 nci maddesinde düzenlenmiştir.

1.8.5- Dünyada Elektronik İmza

Yukarıda belirtilen uluslararası düzenlemeler esas alınarak başta ABD olmak üzere birçok ülkede elektronik ticaret ve elektronik imza alanında düzenlemeler yapılmıştır. Aşağıda bu ülkelerdeki düzenlemeler ve uygulama süreçleri liste halinde belirtilmiştir¹¹⁸.

ABD: 1 Ekim 2000 tarihinde yürürlüğe giren Küresel ve Ulusal Ticarete Elektronik İmzalar yasası ile çeşitli eyalet yasaları bulunmaktadır.

İngiltere: Elektronik imza hakkında 1998 yılından beri süregelen bazı düzenlemeler mevcut olmakla birlikte e-imza Kanunu 25 Mayıs 2000'de İngiliz parlamentosunda kabul edilmiş ve 2002 yılında yürürlüğe girmiştir. En fazla gerçekleştirilen ticari elektronik işlem tipi bireysel elektronik bankacılıktır ve bu alanda şifreleme teknikleri kullanılmaktadır. İşlemlerin sertifika tabanlı kimlik doğrulama yöntemleri ya da güvenli elektronik imza oluşturma aracı ile güvenli şekilde yapılmasına çok az ihtiyaç duyulmaktadır. Elektronik imzaların yaygınlaşmasını engelleyen başlıca sebep talep eksikliğidir. Potansiyel kullanıcıların neye ihtiyaçları olduğu konusunda kafaları karışıktır. Sertifikalar kazanılacak olan faydaya göre çok pahalı olarak algılanmaktadır ve tüketiciler şu an için gerçek bir fayda görememektedirler¹¹⁹.

¹¹⁸ Yeşil-Alkan-Acarer, s.1-8; Orta, s.74 vd., Sağıroğlu-Alkan, s.54; Bensghir, s.90 vd.; Demirel s.5 vd.

¹¹⁹ Bkz. Yeşil-Alkan-Acarer, s.3

Danimarka: Elektronik İmza Kanunu, 1 Ekim 2000'de yürürlüğe girmiştir. Danimarka Bilgi Teknolojileri ve Telekom Otoritesi tarafından yapılan açıklamaya göre Mayıs 2005 itibariyle, 350,000 adetten fazla sayısal imza dağıtılmış durumdadır ve 5,5 milyonluk bir nüfusa sahip olan ülkede hedef 2007 yılı itibariyle 1.3 milyon sayısal imzaya ulaşmaktır. Ancak, ülkede ticari alandaki yasal çerçevenin iyi çalışmasından dolayı e-imzaya yatırım yapma isteğinin düşük olması ve mahkemelerin e-imza ile imzalanmış olan ticari sözleşmelerin geçerli olup olmadığını sorgulamakta serbest olması nedenleriyle iş dünyasında e-imza kullanımı çok kısıtlıdır. Buna karşılık e-imza, kimlik tanımlama mekanizması olarak e-devlet hizmetlerinde sıklıkla kullanılmaktadır¹²⁰.

Fransa: 2 ayrı yasa mevcuttur. Mart 2000 tarihli, 2000-230 sayılı yasada, elektronik imza ve belgelere, ispat konusunda kağıda dayalı belgelere benzer esaslar getirmektedir. 2001 tarihli, 2001-272 sayılı yasa ile AB Direktifinde yer alan hususların çoğu tanınmaktadır. Yasa ile ilgili yönetmelik 31 Mart 2001 tarihinde yayınlanmıştır. Danimarka'da olduğu gibi ticari alanda delil hukukunun etkin bir şekilde işliyor olması ve mahkemelerin e-imza ile imzalanmış olan ticari sözleşmelerin geçerli olup olmadığını sorgulamakta serbest olması gibi nedenlerin iş dünyasının e-imza teknolojisine yatırım eğilimini ve e-imza kullanma isteğini azaltması nedeniyle e-imza çok kısıtlı kullanılmaktadır¹²¹.

Almanya: AB Direktifinden önce, 1997 tarihinde hazırlanıp 1998 de yürürlüğe giren Alman Sayısal İmza Yasası Avrupa Birliği direktifiyle uyumsuz hükümler içerdiği için, AB Direktifi ilkelerine göre hazırlanan yeni Alman Elektronik İmza Yasası 22 Mayıs 2001'de yürürlüğe girmiştir. Bu yasa ile ilgili Yönetmelik de 22 Kasım 2001 tarihinde yayımlanmıştır. Almanya Telekomünikasyon ve Posta Regülasyon Kurumu, kök sertifikasyon makamı olarak faaliyet göstermektedir. Ancak, vatandaşların kendi arasındaki, vatandaş ile şirketler arasındaki ve şirketlerin kendi arasındaki bir çok işlemin kanunlara göre ıslak imza gerektirmemesi nedeniyle e-imzaya talep düşük olup, e-imzadan daha kolay ve ucuz olan çözümler kullanılmaktadır¹²².

¹²⁰ Bkz. Yeşil-Alkan-Acarer, s.3

¹²¹ Bkz. Yeşil-Alkan-Acarer, s.3

¹²² Bkz. Yeşil-Alkan-Acarer, s.3

Hollanda: Elektronik imza, elektronik kayıtların tanınması, sözleşmelerin geçerliliğini koruması ile veri ve tüketici korumasını Elektronik imza kanunu 2003 yılında yürürlüğe girmiştir. Hollanda’da e-imza kanununa göre, ESHS (Elektronik Sertifika Hizmet Sağlayıcı) tarafından sertifika verilecek olan kişi, kimlik tespiti esnasında bizzat hazır bulunmak zorundadır. Ticari iş ilişkilerinde e-imza kullanımının çok az olmasına karşın, e-devlet hizmetlerinde kimlik tanımlama mekanizması olarak kullanımı gittikçe artmaktadır¹²³.

İtalya: Mart 1997 tarihli, 59 sayılı Yasa ve 1997 tarihli Kararname ile Açık Anahtar Altyapısı (PKI) esasına dayanan, sayısal imzalarla ilgili esasları tanımlamıştır. Bunlar AB Direktifinden önemli konularda ayrılık göstermektedir.

Finlandiya: AB Direktifi ile uyumlu olan Elektronik İmza Yasası 24 Ocak 2003 tarihinde yayınlanmış yasa ile ilgili yönetmeliklerse 29 Ocak 2003 tarihinde yayınlanmışlardır. Ayrıca 1998 yılında, Fin Hükümeti elektronik kimlik tanımlama, veri transferinde şifreleme ve elektronik işlemler için sayısal imza kullanımına imkan tanıyan bir sistem yaratmaya karar vermiş ve Nüfus Kayıt Merkezince PKI tabanlı sertifikasyon hizmetleri sunulmaya başlanmıştır¹²⁴. Vatandaşlar bu merkezden, üzerinde gizli anahtar ve sertifikaların yüklü olduğu bir EID kartı satın alabilmektedirler.

İspanya: AB Direktifi 17 Eylül 1999 tarihli ilk Elektronik İmza Yasası şeklinde yürürlüğe konmuştur. İkinci yasa ise 26 Temmuz 2002 tarihinde yayınlanmıştır. 21 Şubat 2001’ tarihinde de Elektronik İmza Yönetmeliği yürürlüğe girmiştir. Kamu sektöründe e-imza kullanımını teşvik etmek için vergi iade işlemlerinde olduğu gibi bazı başarılı girişimler olduysa da, e-imza diğer sektörlerde yaygınlaşmamıştır¹²⁵.

Ayrıca İsveç, Belçika, Portekiz, Yunanistan, İrlanda, Avusturya, Çek Cumhuriyeti, Macaristan, Polonya, Bulgaristan, Estonya, Latviya, Litvanya, Malta, Romanya, Slovak Cumhuriyeti, Lüksemburg, Slovenya, İzlanda, Norveç, Ukrayna, Kanada, Arjantin, Bermuda, Brezilya, Kolombiya, Ekvator, Meksika, Japonya, Singapur, Hindistan, Hong Kong, Çin Cumhuriyeti, Rusya, Malezya, Güney Kore,

¹²³ Bkz. Yeşil-Alkan-Acarer, s.3

¹²⁴ Bkz. Yeşil-Alkan-Acarer, s.3

¹²⁵ Bkz. Yeşil-Alkan-Acarer, s.4

Tayvan, Tayland, İsrail, Avustralya, Yeni Zelanda, Gibralta gibi ülkelerin de elektronik imza ile ilgili düzenlemeleri bulunmaktadır.

1.8.6- Türkiye'deki Düzenlemeler

Ülkemizde elektronik imzanın kullanımı için gerekli yasal çalışmalar, ilk kez Sermaye Piyasası Kanunu Yönetmeliğinde "kendisine bağlı çalışan kurum ve e-imza dahil elektronik işlem usul ve esasları belirlenir" hükmüdür. Bu hükümden hareketle SPK, e-ticaret için pilot bir proje hazırlamıştır¹²⁶. Daha sonra 29 Haziran 2001 tarihinde Hazine Dış Ticaret Müsteşarlığı koordinasyonunda oluşturulan Hukuk Alt Çalışma Grubu oluşturulmuştur¹²⁷. Adalet Bakanlığı, 14 Ocak 2002 tarihli yazısı ile yeni bir çalışma komisyonu kurarak kısa sürede "Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı" taslağını hazırlamış, söz konusu tasarı taslağı, 10 Eylül 2002 tarihli yazı ile kurumların görüşüne sunulmuş ve 19 Şubat 2003 tarihinde başbakanlığa gönderilmiştir.

Elektronik İmza Kanun Tasarısı, 15 Ocak 2004 tarihinde TBMM Genel Kurulu'nda görüşülerek kabul edilmiş, Kanun, 23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete'de yayımlanmıştır. Yasanın gerekçesinde, "*Günümüzde geleneksel ve alışılmış iletişim yöntemlerinden elektronik iletişim yöntemine doğru hızlı bir değişim ve gelişim yaşanmaktadır. Bilgi ve iletişim teknolojilerinin bu değişimi ve hızlı gelişimi, ekonomik faaliyet alanlarında ve sosyal yaşamda yeni olanaklar yaratmaktadır. Bilgisayar ve internetin sosyal ve ekonomik yaşama girmesi, bu alandaki gelişim ve değişimi hızlandırmıştır. Özellikle elektronik imzanın çeşitli alanlarda kullanılır olması sonucu bazı düzenlemelerin yapılması ihtiyacı ortaya çıkmıştır*" denilmiştir.

İkincil düzenleme çalışmaları Telekomünikasyon Kurumu'na verildiğinden Kanunun verdiği 6 aylık zamandan önce ikincil mevzuat çalışmaları tamamlanarak yürürlüğe girmiştir. Mevzuat çalışmalarının ardından elektronik imzanın uygulamaya girmesi için gerekli çalışmalar başlamıştır.

Elektronik imzanın kullanımı konusunda hâlihazırda geçerli bulunan mevzuat aşağıda sıralanmıştır.

¹²⁶ Topaloğlu, s.126

¹²⁷ Çamurdan, s.1; Orta, s.79

- 5070 Sayılı Elektronik İmza Kanunu (23 Ocak 2004)
- Elektronik İmza Kanununun Uygulanmasına İlişkin Usul Ve Esaslar Hakkında Yönetmelik (6 Ocak 2005 R.G. 25692)
- Kamu Sertifikasyon Merkezi Oluşturulması Hakkında Genelge
- Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26 Ağustos 2004 R.G. 25565)
- Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı (27.01.2005 R.G.25709)
- Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları (27.01.2005, R.G. 25709)
- Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ (06 Ocak 2005 ve R.G. 25692)
- Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ’de Değişiklik Yapılmasına Dair Tebliğ

Yukarıda da görüldüğü gibi ülkemizde elektronik imza hakkındaki temel düzenleme 5070 sayılı Elektronik İmza Kanunudur. Diğer mevzuat bu kanuna paralel olarak hazırlanmıştır. Kanun güvenli elektronik imzanın hukuki sonucu ve uygulama alanını 5 inci maddede belirtmiştir. Buna göre “*güvenli elektronik imza, elle atılan imza ile aynı hukukî sonucu doğurur*”. Bu hüküm Avrupa Birliği Direktifi ile uyumludur. Zira Direktife göre nitelikli sertifikaya dayanan ve güvenli imza oluşturma aracı ile oluşturulan imzaların hukuki etkisi kâğıda elle atılmış imza ile aynı olmalıdır ve bu imzanın delil niteliği inkâr edilmemelidir(m.5/1).

Kanunla birlikte elektronik imza, el yazısı imza ile eşdeğerde görüldüğünden el yazısı imza hakkında mevcut düzenlemenin yapıldığı 818 sayılı Borçlar Kanununda değişiklik yapılmış ve 14 üncü maddesinin birinci fıkrasına. “*Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir*” cümlesi eklenmiştir. Bu şekilde, el ürünü imza ile ilgili düzenleme yapan mevcut yasal düzenleme gelişen teknolojinin doğurduğu ihtiyaçlara cevap verebilecek hale getirilmiştir. Bu durum elektronik imzanın kullanımını yaygınlaştıracak ve güvenilirliğini artıracaktır. Ancak yukarıda da

belirtildiđi gibi teminat sözleşmeleri ve özel merasim gerektiren işlemlerde elektronik imza kullanılamayacak, kullanılması durumunda işlem geçersiz olacaktır¹²⁸.

Kanunun 24 üncü maddesi ile de, 2813 sayılı Telsiz Kanunu'nun 7 nci maddesinde Telsiz İşleri Genel Müdürlüğü'nün 16 bent halinde sayılan görevlerine, bir görev daha eklenmiş ve "Elektronik İmza Kanunu ile verilen görevleri yapmak" hükmüne yer verilmiştir.

¹²⁸ Erturgut, s.118; Biçkin, s.352

İKİNCİ BÖLÜM

ELEKTRONİK İMZANIN KULLANIM ALANLARI, ELEKTRONİK SÖZLEŞMELER VE ELEKTRONİK İMZANIN HUKUKİ SONUÇLARI

2.1- Genel Olarak

Sayısal imzalar daha önce de açıklandığı üzere el yazısı ile imzanın elektronik ortamdaki karşılığıdır. Dolayısıyla yasal engel olmadığı mühletçe, gerçek ortamda el yazısı ile imzanın kullanıldığı her muamelenin elektronik ortamda gerçekleştirilmesinde elektronik imza (nitelikli elektronik imza) kullanılacaktır. Diğer bir ifade ile elektronik ortamda kimlik tespitinin gerekli olduğu her durum elektronik imzanın uygulama alanına girmektedir¹²⁹. Bu itibarla elektronik imzanın kullanım alanı oldukça geniştir.

Bilindiği üzere genel anlamda imzanın ana kullanım alanı sözleşmelerdir. Zira sözleşmeler borç ilişkisinin en temel kaynağı olup yaşantımızın odak noktasında yer alır ve sözleşmelerin şekil şartlarının yerine getirilmesi veya ispatı imza ile gerçekleştirilir. Hukuk sistemimizin irade özerkliği ilkesini kabul etmesi ve bunun yanında elektronik

¹²⁹ Erdem-Kırımlı, s.1

ortamın sağladığı hız ve iletişim imkanları neticesinde elektronik ortamda sözleşme kurulumu yaygın hale gelmiştir. Elektronik iletişim vasıtaları aracılığıyla kurulan ve doktrinde elektronik sözleşme olarak nitelendirilen bu tür sözleşmeler elektronik imzaların anlam kazandığı en önemli kullanım alanlarıdır. Ancak bu nitelikteki sözleşmeler klasik sözleşmelerden bazı yönleri itibariyle ayrılıp, bu durum doktrinde görüş ayrılıklarına neden olduğundan özel bir öneme sahiptir. Bu nedenle elektronik sözleşmelerin hukuki yönleriyle detaylı olarak ele alınması uygun olacaktır.

Öte yandan elektronik imza, el yazısı imza ile aynı hukuki sonucu doğurmanın yanında eşdeğer ispat gücüne de sahiptir. Ancak elektronik imzanın yasal olarak kabul edilmediği bazı istisnai durumlarda söz konusu olabilmektedir. Nitekim hukukumuzda bazı istisnai hukuki işlemlerin güvenli elektronik imza ile kurulmasının mümkün olamayacağı hükme bağlanmıştır¹³⁰. Bunun yanında elektronik imza kullanımı elektronik imza sahibine ve elektronik sertifika hizmet sağlayıcısına bazı hukuki sorumluluklar yüklemektedir.

Bu bölümde öncelikle elektronik imzanın kullanım alanlarından ve yasal olarak kullanılamayacağı işlemlerden bahsedilecek, daha sonra elektronik sözleşmeler detaylı olarak incelenecektir. Son olarak ise elektronik imzanın hukuki sonuçlarından olan ispat gücü ile hukuki sorumluluk konularına değinilecektir.

2.2- Elektronik İmzanın Genel Kullanım Alanları

Elektronik imzanın kullanım alanlarının başında elektronik sözleşmeler gelir. Elektronik ortamda kurulan sözleşmelerde şekil şartının sağlanması, tarafların kimliklerinin ve sözleşmenin içeriğinin belirlenmesi, zamanın tayini ve sözleşme şartlarında sonradan yapılan değişikliklerin ispatı gibi durumlarda elektronik imzanın hayati bir fonksiyonu vardır.

Öte yandan, hukuki anlamda elektronik sözleşmelerden oluşan elektronik ticarete güvenliği sağlamak amacıyla elektronik imza çok rahat bir şekilde kullanılabilir. Genel olarak e-ticaret, taraflarca bir malın, semen karşılığında alışverişinden ibaret olan ve işlemlerin tamamının sanal ortamda gerçekleştirildiği bir

¹³⁰ EİK, m.5/II

işlemdir. İşte tamamen sanal ortamda gerçekleştirilen bu işlemlerde taraflardan birinin zarar görmesi veya satın alınan üründe bir ayıbın olması veya ürünün beğenilmemesi durumlarında ortaya çıkan olumsuzluğun giderilmesinde, tarafların kimliklerinin net biçimde bilinmesi ve paranın ödeneceği durumlarda, güvenliğin sağlanması açısından elektronik imza bir kurtarıcıdır. Çünkü niteliği gereği elektronik imzada, e-imza sahiplerinin kimlikleri ve alışverişe onay verip vermediği şüpheye yer bırakmayacak biçimde belirlenebilmektedir.

Elektronik imzanın rahatlıkla kullanılabilmesi bir diğer alan ise elektronik bankacılıktır. Günümüzde neredeyse her banka kuruluşunun elektronik bankacılık hizmeti bulunmaktadır. Hesap sahipleri bu sayede banka şubesine bizzat giderek yapabilecekleri neredeyse tüm işlemleri internet bankacılığı aracılığıyla yapabilmektedirler. Ancak basından da takip edildiği üzere bu hesaplara erişim için kullanılan şifrelerin ve diğer güvenlik altyapılarının zaman zaman kırıldığı ve illegal işlemler yapıldığı görülmektedir. İşte bu tür risklerin önüne geçilmesi ve yeterli güvenliğin sağlanmasında kanımızca en iyi çözüm yine elektronik imzadır. Zira işlemlerin elektronik imza ile yapılması söz konusu olduğunda imza sahibinin gizli anahtarı sadece kendisinde daha doğrusu kendisinde bulunan elektronik imza oluşturma aracında bulunduğundan bu araç kullanılmadan hesaba erişim şuan için imkansızdır.

Elektronik imzanın kullanılabilmesi diğer önemli bir alan ise E-Devlet'tir. Zira klasik devlet-birey ilişkilerinde kırtasiyecilik diye ifade edilebilen bürokrasi, gerek zaman kaybı gerekse ekonomik israfa yol açmaktadır. Bu iki taraf için de söz konusudur. Oysa E-Devlet projesinin hayata geçirilmesi halinde, devlet daha az sayıda eleman ve daha az masraf ile hizmet sunabilecek, vatandaş ise devlet dairelerinde büyük zaman ve emek harcayarak yaptırdığı tüm işlemleri çok daha kısa bir zaman içerisinde ve hızlı bir biçimde elektronik ortamda gerçekleştirme imkanına kavuşacaktır. Örneğin, kendi evinden bilgisayar vasıtasıyla her türlü resmi başvuruyu yapabilecek, tüm vergi vs. ödemelerini yapabilecek, çocuğunu okula kaydettirip okuldaki durumunu takip edebilecek ve daha aklımıza gelebilecek pek çok şeyi yapabilecektir. Üstelik elektronik ortam mesai kavramından bağımsız olduğundan bu işlemleri mesai saatleri dışında ve tatil günlerinde de yapabilecektir. İşte bu alanda bireyin kendi kimliğinin devlete tam ve güvenilir bir şekilde kabul ettirilebilmesi elektronik imza ile mümkün olacaktır. Diğer bir ifadeyle devlet ile ilgili her tür işlemde dijital imza güvenli bir biçimde

kullanılabilecektir. Hatta, seçimlerde sandık başına gidip parmakları boyatıp oy kullanmak demokrasinin gereği olmasına rağmen birçok kimse için sıkıcı bir durumdur. Bu nedenle, medeni dünyada örneklerine yeni yeni rastladığımız e-seçim, e-referandum, e-kamuoyu gibi uygulamaların genel ve yerel seçimlerde uygulanması düşünülürse elektronik imza bu projenin temelini oluşturacaktır.

Ülkemizdeki e-devlet çalışmaları son yıllarda büyük hız kazanmış ve pek çok kurumun resmi dairelerde gerçekleştirdiği işlemler elektronik ortamda yapılabilir veya erişilebilir hale gelmiştir. E-devlet uygulamalarının en önemlilerinden biri de, E-adliye'dir. Bu uygulamanın tamamen hayata geçmesi halinde adliyede gerçekleştirilebilecek neredeyse tüm işlemler elektronik ortamda gerçekleştirilebilecek yada takip edilebilecektir. Ülkemizde, Ulusal Yargı Ağı Projesi (UYAP) olarak da adlandırılan bu proje büyük ölçüde hayata geçmiştir. Şuan için, avukatların elektronik ortamda dava açıp takip etmesi de dahil olmak üzere, vatandaşların, duruşma gün ve saatleri ile sonuçlanma durumlarını internet üzerinden takip etmeleri, adli sicil kayıtlarını adli sicil bürosu olmayan adliyelerden dahi çıkartabilmeleri mümkün hale gelmiştir. Öte yandan, başvuru dilekçesinden başlamak üzere tüm yazışma ve işlemlerin elektronik ortamda gerçekleşmesi, nüfus, adli sicil, GBT, ehliyet vs. pek çok bilginin anında öğrenilmesinin mümkün olması düşünüldüğünde, mevcut yargılama hızı ciddi ölçüde kısılacaktır. Zira mevcut uygulamada ciddi zaman kaybına yol açan, resmi kayıtların ilgili kurumlardan istenmesi, mahal dışından taleplerde bulunulması ve dava dosyalarının üst derece mahkemesine gönderilmesi ve dönüşünün beklenmesi gibi işlemler elektronik iletişime bağlı olarak çok kısa sürede gerçekleşmektedir. Bunun yanında bu proje kapsamında gerekli tüm adli personele elektronik imza dağıtılması ve dava dosyasına dışarıdan girecek tüm belgelerin de elektronik ortama aktarılması ile tozlu dosyalar sanal dünya ya taşınacak, kararlar elektronik ortamda verilecek ve dava dosyası, üst derece mahkemesi veya Yargıtay'a elektronik ortamda gidecektir. Duruşmalar ise şimdilik yüz yüze gerçekleşmekte ancak ileriki yıllarda belki bu da tamamen elektronik ortamda gerçekleşebilecektir. Bu proje hakkında yapılan resmi açıklamaya göre, adalet görevlileri odalarında, evlerinde, keşifte, duruşma salonunda ya da istedikleri herhangi bir noktada, anında sisteme katılacaklar. Savcılar iddianamelerini İnternet üzerinde hazırlayacaklar. Birimler arası yazışmalar, istatistikler, iddianameler, temyiz işlemleri, talimatlar ve müzekkereler maille yollanacak. Böylece dava süresi çok

kısalacak. Şu an için davaların büyük çoğunluğu 6 hafta içinde bitecektir¹³¹. Tabii bu projenin tam anlamıyla hayata geçmesi ve tüm adli işlemlerin elektronik ortamda gerçekleştirilebilmesi için elektronik imza kullanımı gerekecektir.

Yukarıda anlatılan temel kullanım alanlarını da dahil etmek suretiyle elektronik imzanın kullanım alanlarını aşağıdaki şekilde listeleyebiliriz.

Kamusal Alanda

- E-Devlet uygulamalarında
- E-Belediye (yerel yönetim) uygulamalarında
- Her türlü başvurular (ÖSS, KPSS, LES, pasaport, vb.)
- Kurumlararası iletişimde (emniyet müdürlükleri, nüfus müdürlükleri, adliyeler, vb)
- Sosyal güvenlik uygulamalarında (e-bildirge, vb.)
- Sağlık uygulamalarında (sağlık personeli - hastaneler - eczaneler)
- Sermaye piyasası işlemlerinde
- Vergi dairesi ve maliye işlemlerinde (e-beyanname, vs.)
- Gümrük işlemlerinde
- Dış ticaret işlemlerinde
- Elektronik oy verme işlemlerinde
- Dava ve takip açma
- Dilekçe verme

Özel Sektörde

- Elektronik Sözleşmelerde
- Bireysel-kurumsal bankacılık işlemleri ve finansal uygulamalar
- Sigortacılık işlemlerinde
- E-İş uygulamalarında
- E-Ticaret uygulamalarında
- Ticaret sicili işlemlerinde

¹³¹ Adalet Bakanlığı Bilgi İşlem Dairesi başkanı Ali KAYA'nın beyanı
<http://www.imedya.com/asp/haberdetay.asp?a=122992&z=58>

- Kağıtsız ofis uygulamalarında
- E-Siparişlerde
- Elektronik fatura ve elektronik muhasebe uygulamalarında
- Güvenli bağlantı uygulamalarında
- Fikri hakların korunmasında (Copyright)
- Yazılımlardaki manipülasyonların kontrolünde
- Elektronik postalarda
- Kimlik veya yetki tanımlanması (bir bilgisayar sistemine girebilme yetkisi veya bir web sunucunun kendini tanımlaması gibi) işlemlerinde
- Uzaktan erişim kontrolünde

Ve bunlara benzer sayısız uygulamalarda elektronik imza kullanılabilmekte ve bu uygulamaların sayısı giderek artmaktadır.

2.3- Güvenli Elektronik İmza İle Yapılamayacak Hukuki İşlemler

Daha önce de ifade edildiği gibi güvenli elektronik imza yasal bir engel olmadığı sürece ıslak imza yerine elektronik ortamda kullanılabilir ve aynı hukuki sonucu doğuracaktır. Ancak, 5070 sayılı Elektronik İmza Kanunu güvenli elektronik imzanın el yazısı imza ile aynı hukuki sonucu doğuracağı genel hükmüne bazı istisnalar da getirmiştir. Buna göre “*Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez (EİK m.5/2)*”. Bu düzenleme ile teminat sözleşmeleri kapsam dışı bırakılarak, elektronik imzanın kullanımının çabukluğu dolayısıyla doğması muhtemel zararların önlenmesi amaçlanmıştır¹³². Benzer şekilde noterlerin yapacağı işlemler, noterlerin huzurunda yapılan işlemler, tescil zorunluluğu olan işlemler (gayrimenkul, motorlu araç alım satımı), evlenme gibi resmi memur önünde yapılması zorunlu olan işlemlerin elektronik imza ile yapılamayacağı anlaşılmaktadır. Dolayısıyla kanunların resmi şekle bağladığı, örneğin, araç satışları, mal rejimi sözleşmeleri, evlilik akdi, tapuda yapılan taşınmaz tescilleri, resmi vasiyetname, kefalet sözleşmeleri vb. hukuksal işlemler de güvenli elektronik imza kullanılamayacak, kullanılsa da geçersiz olacaktır.

¹³² TBMM Adalet Komisyon Raporları,22. Dönem, 2.Yasama Yılı,(1/613)

Öte yandan elektronik imza teknolojisinin yaygınlaşmasına bağlı olarak elektronik noterlik ve buna benzer kavramlar ortaya çıkmış ve bu yönde çalışmalara girişilmiştir. Kanımızca elektronik noterlik müessesesi gerçekleşecek olursa az önce bahsedilen elektronik imza ile gerçekleştirilemeyecek işlemlerde E-Noter aracılığı ile elektronik imza kullanılarak gerçekleştirilebilecektir. Yine elektronik ortamda gönderilen belgelerin E-Noter tarafından doğruluğu sınanıp kendi elektronik imzası ile imzalanması suretiyle "noter tasdikli" hale gelmesi sağlanacaktır¹³³.

Sonuç olarak, elektronik imza bilişim çağının gereği olarak, yaşantımızın sanal âleme uyarlandığı bir süreçte ve her alanında elektronik ortamdaki güvenliğimizi sağlama aracı olarak kullanılabilir orijinal bir yöntemdir.

2.4- Elektronik Sözleşmeler

Sözleşme (Akit) kavramı Borçlar Hukuku'nun odak noktasında yer alır. Günlük hayatımızda mutlak ihtiyaçlarımızın karşılanmasında dahi hukuki araç olarak sözleşme yer alır. Belki çoğu zaman bunun farkında bile olmayız. Sözleşmeler borç ilişkisinin en başta gelen kaynağıdır. Bu husus Borçlar Kanunu'nun lafzına da sirayet etmiş ve kanun "Akitten Doğan Borçlar" ana başlığı ile başlamış ve yine ilk maddesinde de akdin kurulmasına yer verilmiştir.

Türk Borçlar Hukuku'na hâkim olan temel ilke, irade özerkliği ilkesidir. İrade özerkliği, hukuk düzeninin bireylere kişisel ilişkilerini hür iradelerine göre diledikleri gibi düzenleme hususunda tanımış genel yetki olup¹³⁴, bu ilkeye göre kişi, hür bir varlık olarak istediği biçimde hukuki ilişkiler kurmak, değiştirmek ve ortadan kaldırmak, başka bir ifade ile, hukuki açıdan kendi kaderini bizzat tayin etmek yetkisine sahiptir.

İrade özerkliğine işlerliğini kazandıran hukuki işlem ve özellikle sözleşmedir. İrade özerkliği, sözleşme özgürlüğünün temelini oluşturur ve iki ana ilkeyi barındırır; bunlardan birincisi "*Akit serbestisi*", ikincisi ise "*Şekil serbestisi*"dir

Sözleşme (Akit) serbestisi, dayanağını Anayasa'dan alır. Anayasamızın 48 inci maddesi "*Herkes dilediği alanda çalışma ve sözleşme hürriyetlerine sahiptir*" diyerek

¹³³ <http://www.hostingturk.com/haber.php>

¹³⁴ Eren, s.16

akit serbestisini güvence altına almış ve madde gerekçesinde kanunun bu hürriyetleri ancak kamu yararı amacıyla sınırlayabileceği belirtilmiştir¹³⁵. Bu gerekçe de nazara alınarak Borçlar Kanunu'nun 19 uncu maddesinde, akdin konusunun, kanunun gösterdiği sınırlara bağlı kalınarak, serbestçe tayin edilebileceği belirtilmiştir.

Akit serbestisi ile hukuk düzeni, fertlere, kanunun gösterdiği sınırlar dahilinde, kişisel ilişkilerini diledikleri gibi düzenlemek, aralarında geçerli olacak bir hukuk düzeni yaratmak yetkisini vermektedir.

Akit serbestisi, genellikle dört anlamda kullanılmaktadır. Bunlar; her hangi bir sözleşmeyi yapıp yapmama, sözleşmenin muhtevasını diledikleri gibi düzenleme, sözleşmeyi dilediği kimseyle yapma, sonuncusu ise kurulmuş olan sözleşmeyi değiştirme ve ortadan kaldırma serbestisidir¹³⁶.

Şekil serbestisi ise, sözleşmelerin geçerli olması için özel bir şekil şartına tabi olmamasını ifade eder. Bu husus Borçlar Kanunu'nun 11 inci maddesinde “*Akdin sıhhati, kanunda sarahat olmadıkça hiç bir şekle tabi değildir*” hükmü ile açıklanmıştır. Bu hükümden de anlaşılacağı üzere asıl olan şekil serbestisidir. Şekil mecburiyeti ise istisnadır.

2.4.1- Sözleşme ve Elektronik Sözleşme Kavramı

En genel tanımı ile sözleşme; iki tarafın bir hukuki sonucu elde etmek üzere iradelerini karşılıklı ve birbirine uygun surette açıklamalarıyla oluşan bir hukuki işlemdir¹³⁷. Bu tanım hemen hemen tüm Kara Avrupa hukuk düzeninde kabul edilmektedir¹³⁸.

Elektronik sözleşme ise, Borçlar Hukuku kapsamında ayrı bir sözleşme türü olmayıp, sadece sözleşmenin kurulması ve/veya ifasının elektronik vasıtalarla yapılmasını ifade eder¹³⁹. Hal böyle olunca bu sözleşmelerle ilgili kendine özgü kurallar oluşturulmasına gerek olmayıp, Borçlar Hukuku'nun sözleşmenin kuruluşuna,

¹³⁵ Başyiğit, s.1

¹³⁶ Eren, s.17; Velidedeoğlu-Özdemir, s.49; Başyiğit, s.1

¹³⁷ Eren, s.191; Akıntürk, s.21; Akıncı, s.75; Uygur, s.450

¹³⁸ Özsunay, s.126

¹³⁹ İnal, s.93; Acır, s.11; Özdemir Kocasakal, s.11

geçerliliğine ve ifasına ilişkin genel hükümlerinin bu niteliği taşıyan sözleşmeler için de aynen uygulanması söz konusudur. Bu durum klasik sözleşme ile elektronik araçlar vasıtası ile kurulan sözleşmeler arasındaki fonksiyon eşitliğinden kaynaklanmaktadır. Nitekim Avrupa Parlamentosu ve Konseyi'nin 8.6.2000 tarih ve 2000/31/EC sayılı Elektronik Ticaret Direktifinde e-sözleşmelerin, kağıda dayanan, geleneksel usul ve araçlarla yapılan sözleşmelerle eşit hukuki statüde olması amaçlanmış ve bu nedenle sözleşmelere ilişkin 9 uncu maddenin 1 inci bendinde “*Üye Devletler, kendi hukuk sistemlerinin, sözleşmelerin elektronik vasıtalarla akdedilmesini temin edeceklerdir. Üye devletler, özellikle sözleşme sürecine uygulanan şartların elektronik sözleşmelerin kullanılmasına engel oluşturacak ya da bu çeşit sözleşmelerin elektronik vasıtalarla yapılmış olması nedeniyle hukuki etkiden ve geçerlilikten mahrum kalmalarına neden olacak şekilde uygulanmamasını temin edeceklerdir*” hükmüne yer verilmiştir.

Yukarıdaki açıklamalar doğrultusunda, elektronik sözleşmeyi, elektronik araçlarla kurulmuş ve/veya elektronik araçlarla tamamlanan sözleşmeler olarak tanımlayabiliriz¹⁴⁰. Doktrinde elektronik sözleşmeler, elektronik veri değişimi (EDI), elektronik posta (e-mail), web sayfası ve usenet kullanılarak yapılan sözleşmeler olarak tanımlanmaktadır¹⁴¹.

Bazı yazarlar ise elektronik sözleşme kavramını dar yorumlamakta ve yalnızca internet ortamında web sayfası üzerinden kurulan sözleşmeleri bu kapsama almakta, stok ikmali ve bankacılık uygulamaları gibi birçok alanda kullanılan ve e-ticaretin temel araçlarından biri olarak kabul edilen; kapalı özel ağlar üzerinden bilgisayardan bilgisayara belge ve bilgi değişimini sağlayan sistem olarak nitelendirilebilecek EDI uygulamasının, bir sözleşme olmayıp, kurulmuş sözleşmenin ifa aşamasında uygulanan bir yöntem olması nedeniyle elektronik sözleşme kapsamında kabul etmemektedirler¹⁴². Yine e-mail kullanımının, telefon ve teleks gibi klasik iletişim yöntemlerinden tek farkının dijital ortamda gerçekleştirilmiş olması olduğu ve yine Usenet kullanıcıları arasındaki iletişimin e-mail yolu ile yapılması nedeniyle bu yöntemler kullanılarak yapılan sözleşmelerin elektronik sözleşme sayılamayacağı ifade edilmektedir¹⁴³.

¹⁴⁰ Acır, s.11; Özdemir Kocasakal, s.37; Altınışık, s.33

¹⁴¹ Acır, s.11

¹⁴² Sözer, s.92; Topaloğlu, s.105

¹⁴³ Sözer, s.92

Tarafımızca bu görüşlere katılmak mümkün değildir. Zira yukarıda açıkladığımız üzere, elektronik sözleşme kavramındaki “Elektronik” tabiri kendine özgü kuralları olan ayrı bir sözleşme kategorisi olmayıp, sözleşmelerin kurulması ve/veya ifası esnasında kullanılan yöntemi göstermektedir. Aksi halde e-mail yolu kurulan sözleşmelerin veya intranet olarak adlandırılan ve bir ülke sınırları içerisinde veya uluslar arası alanda iletişim imkanı veren, ağ yapılanmalarında¹⁴⁴ kullanıcıların yapmış oldukları sözleşmelerin, geçerliliği ve ispatı ile ilgili sorunlar yaşanacaktır. Oysa UNCITRAL¹⁴⁵ tarafından hazırlanan *Elektronik Ticaret Model Kanunu*’nun 11 inci maddesi ve *Veri Mesajları Aracılığıyla Kurulan veya Tespit Edilen Sözleşmelere İlişkin Konvansiyon Ön Tasarısı*’nın 8/3 üncü maddesinde, bir sözleşmenin veri mesajları aracılığı ile kurulmuş olmasının, sırf bu nedenle geçerlilikten veya icra edilebilirlikten yoksun bırakılmasına yol açmayacağı öngörülmüştür. Ayrıca elektronik sözleşmelerin geçerliliği ve ispatı için son derece önemli olan ve ileride ayrıntılı olarak değineceğimiz, elektronik imzanın çoğunlukla e-maillerde kullanılıyor olması da bu yolla kurulan sözleşmelere ayrı bir önem kazandırmaktadır.

Sonuç olarak, kanımızca elektronik araçlarla kurulan veya ifa edilen tüm sözleşmeleri, geçerlilik, hüküm doğurma ve ispat kuralları açısından elektronik sözleşme kapsamında saymak gerekecektir. Zaten ABD hukukunda faks ile yapılan sözleşmelerin dahi elektronik sözleşme kapsamında kabulü yönünde eğilim olduğu bilinmektedir¹⁴⁶.

2.4.2- Elektronik Sözleşmelerin Konusu

Elektronik sözleşmeleri konusuna göre, fiziki mal satışına yönelik sözleşmeler, dijital ürün satışına yönelik sözleşmeler, hizmet sunumuna yönelik sözleşmeler ve bilgi teminine yönelik sözleşmeler olmak üzere dört grupta incelememiz mümkündür.

¹⁴⁴ Bankalar, E-devlet kapsamında bir veya daha fazla kamu kurumunun tüm birimlerini birbirine bağlayan ağlar, gibi

¹⁴⁵ Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu

¹⁴⁶ Topaloğlu, s.105, dn.496

2.4.2.1- Fiziki Mal Satışına Yönelik Sözleşmeler

Elektronik ticaretin temelini oluşturan elektronik sözleşmelerin büyük bir bölümünü fiziki mal satışına ilişkin sözleşmeler oluşturur. Günlük hayatta çarşı, pazar, mağaza gibi yerlerde görüp satın alabileceğimiz hemen hemen her şeyi elektronik ortamda almamız mümkündür. Burada satıcı ifa edimini posta, kurye ve kargo gibi fiziki yollarla yapmakta; alıcı ise ödemeyi, kredi kartı, havale veya hediye çeki ile yapabileceği gibi, kapıdan ödeme sureti ile dahi yapabilmektedir. Şu anki uygulamada sadece taşınır mallar bu sözleşmelerin konusunu oluşturmaktadır. Ancak bu durum taşınmaz malların bu sözleşmelerin konusunu oluşturmayacağı anlamına gelmez. Kanımızca taşınmaz mallar da bu sözleşmelere konu edilebilir. Sözleşmenin kurulması elektronik ortamda yapılıp, tescil işlemleri klasik usulde yapılabileceği gibi, özellikle elektronik imzanın da kullanılıyor olması ve ileride uygulamaya konulabilecek elektronik noter müessesesi ile gayrimenkul devir sözleşmelerinin kurulum ve ifası elektronik ortamda yapılabilecektir.

2.4.2.2- Dijital Ürün Satışına Yönelik Sözleşmeler

Bu tür sözleşmelerde, sözleşmenin kurulması ve ifası tamamen elektronik ortamda gerçekleşmekte olup, son derece yaygın olarak kullanılmaktadır. Uygulamada internet veri bankası sözleşmesi olarak da nitelendirilmektedir¹⁴⁷. Burada satıcı ürününü elektronik ortamda satışa sunmakta veya karşılıksız olarak bağışta bulunmakta,¹⁴⁸ alıcı ise usulüne uygun kabul beyanı ve edimini ifa ile, ilgili ürünü (yazılım, kitap, resim, film, müzik v.s.) bilgisayarına doğrudan indirmektedir (Download).

2.4.2.3- Hizmet Sunumuna Yönelik Sözleşmeler

Bu tür sözleşmelerde elektronik ortamda kullanıcıya hizmet sunma taahhüdü altına girme söz konusudur¹⁴⁹. Hizmet edimine ilişkin ifa da tamamen elektronik ortamda gerçekleşir. İnternet bankacılığı hizmetleri, sinema, uçak, konser bileti rezervasyon ve satış hizmeti, üniversitelerin veya çeşitli kamu veya özel kuruluşların uzaktan eğitim çalışmaları bu tür sözleşmelerden bazılarıdır.

¹⁴⁷ Kırcı, s.100

¹⁴⁸ Kırcı, s.100

¹⁴⁹ Özdilek, s.29; Kırcı, s.101; Altınışık, s.34

2.4.2.4- Bilgi Teminine Yönelik Sözleşmeler

Burada sadece bilgi iletimi söz konusudur. Bazı yazarlar bu gruptaki sözleşmeleri de hizmet sunumu kapsamında saymışlardır¹⁵⁰. Ücretli veya ücretsiz olarak döviz, borsa bilgileri, hava raporları ve buna benzer pek çok faaliyeti içine alan sözleşmeleri bu kapsama alabiliriz.¹⁵¹

2.4.3- Sözleşmelerin Kurulması

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 gerekmektedir¹⁵². Diğer bir ifade ile sözleşmenin kurulabilmesi için tarafların sözleşmenin hükümleri ile bağlı oldukları hususunda anlaşıklarını göstermelidirler. Bu da ancak irade unsuru ile gerçekleşir. Sözleşmelerin elektronik ortamda, örneğin ağ veya internet ortamında yapılması bu ilkede yeni bir değişiklik veya ekleme yapmayacaktır¹⁵³. 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)¹⁵⁴, bu öneriyi uygun gördüğünü bildiren karşı irade beyanına da *kabul* adı verilir¹⁵⁵.

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 muhabata 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

¹⁵⁰ Özdilek, s.29; Kırca, 101

¹⁵¹ Altınışık, s.34

¹⁵² Oğuzman-Öz, s. 48; Renda-Onursan, s.4; Özsunay, s.126

¹⁵³ Gezder, s.81

¹⁵⁴ Tunçomağ, s.183, Oğuzman-Öz s.49

¹⁵⁵ Tunçomağ, s.184, Oğuzman-Öz, s.60

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 veremez¹⁵⁶. 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 edilmektedir¹⁵⁷.

2.4.3.1- İcâp ve İcâba Davet

İcâp, sözleşmenin yapılması teklifini içeren ve zaman itibari ile önce yapılan, muhataba varması gerekli, tek taraflı, kesin ve bağlayıcı nitelik taşıyan, muhatabın kabulü ile sözleşmenin kurulması sonucunu doğuran irade açıklamasıdır¹⁵⁸. İcâp sözleşme yapılması için gerekli irade beyanlarından ilki olması nedeniyle, sözleşme yapma çağrısı niteliğindedir ve bu nedenle sözleşmenin taraflarından herhangi biri tarafından yapılabilir. Niteliği itibari ile tek taraflı bir hukuki işlem olup¹⁵⁹, icâp sahibinin belirli bir süre icabı ile bağlı ve istekli olduğunu, ayrıca teklif ettiği sözleşmenin kurulması hususunda muhataba yetki verdiğini ifade eder¹⁶⁰.

İcâp, kural olarak herhangi bir özel şekle tabi değildir. Zira, Borçlar Kanunu 11 inci maddesi, sözleşmelerin kurulması için kural olarak şekil serbestisi ilkesini kabul etmiştir. Buna göre sözleşmenin kurulumu için gerekli irade beyanları olan icâp ve kabulün, genel kurala göre, herhangi bir şekli ihtiva etmesi gerekmemektedir. Ancak, şekil serbestisinin istisnaları olan, taraf iradesi veya kanun hükmü ile bu kural geçersiz hale getirilebilir¹⁶¹. Şöyle ki, yasa hükmü ile herhangi bir sözleşmenin geçerliliği belli bir şekil şartına bağlanmış ise, icabın da bu şekil şartına göre yapılması gerekir. Yine icapta bulunan sözleşmenin geçerliliğini belli bir şekil şartına tabi tutmuş ise, icabın da bu şekil şartına uygun yapılması gerekir.

¹⁵⁶ Gezder, s.84

¹⁵⁷ Gezder, s.85; Büyükay, s.5

¹⁵⁸ Eren, s.226; Oğuzman, s.49; Uygur, s.451

¹⁵⁹ Uygur, s.451; Eren, s.226

¹⁶⁰ Eren, s.226

¹⁶¹ Uygur, s.452; Eren, s.228; Altınışık, s.41

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

İcabin hüküm ve sonuçlarını doğurabilmesi için muhataba varması gereklidir. Varma tabirinden muhatabın hâkimiyet alanına ulaşması anlaşılmaktadır¹⁶². Doktrinde kabul edilen görüşe göre, icabın, uygun bir zamanda muhatabın posta kutusuna, ev veya işyerine varması yada yetkili personel veya aile bireylerince kabul edilmesi halinde hakimiyet alanına ulaşmış sayılır¹⁶³. Bu çerçeveden bakıldığında icabın muhatabın elektronik posta adresine ulaşması, online olarak kullanıcının bilgisayarına ulaşması veya telesekreterine mesaj olarak bırakılması hallerinde de hakimiyet alanına ulaştığı kabul edilmelidir.

İcap ciddi olmalı, icabı yapan icabı ile bağlanma niyetinde olmalıdır. İcapta sözleşme yapma niyeti açık ve kesin olmalıdır. İrade beyanı bağlanma niyeti ile yapılmamışsa, mesela espri veya şaka ile yapılmış ise icap sayılmaz. Ancak bazen şartları var ise icaba davet olarak telakki edilebilir.

İcap, sözleşmenin objektif ve sübjektif yönden tüm esaslı noktalarını kapsamalıdır. Dolayısı ile icap öyle olmalıdır ki muhatabın peki, evet, kabul gibi bir söz söylemesi veya elektronik ortamda bir tuşa basması, fareyi tıklaması ile¹⁶⁴ sözleşmenin kurulmasını sağlayacak nitelikte olmalıdır. Sözleşmenin hangi noktalarının esaslı hangi noktalarının ikinci derecede olduğunu ayırmak için kesin bir ölçü yoktur. Bu husus her sözleşmenin niteliğine, tarafların maksatlarına ve teamüllere göre tayin edilir¹⁶⁵.

Sözleşme yapma çağrısı yukarıda belirtilen özelliklere sahip değilse, sözleşme yapılmasına yönelik teklif, icap olmayıp, icaba davet niteliğinde kabul edilecektir¹⁶⁶. Gerçekten icap, sözleşme yapılması için gerekli bütün esaslı noktaları ihtiva ettiğinden, muhatabın kabulü ile sözleşme kurulmuş olur. İcaba davette ise beyan sahibi nihai ve kesin işlem iradesini açıklamamakta muhataba sözleşme yapmaya hazır olduğunu

¹⁶² Uygur, s.452; Eren, s.226

¹⁶³ Uygur, s.452; Eren, s.226

¹⁶⁴ Fare (mouse) kıklemesi ile sözleşme kurulmasının hukuki bağlayıcılığı hakkında bkz. Gezder, s.131

¹⁶⁵ Uygur, s. 452

¹⁶⁶ Reisoglu, s.58; Eren, s.228

açıklamakta ve muhatabı icapta bulunmaya veya sözleşme şartlarını müzakere etmeye davet etmektedir¹⁶⁷.

Bir irade beyanının icap mı yoksa icaba davet mi olduğunu ayırt etmek her zaman kolay olmayabilir. Bu durumda beyanın icap olup olmadığı genel hükümler çerçevesinde yorumlanması ve beyanda bulunanın maksadının ve durumunun tespiti ile anlaşılabilir¹⁶⁸. Bu sebeple Borçlar Kanunu bazı hükümlerinde irade beyanının icap mı yoksa icaba davet mi kabul edileceği hususunda yorumlayıcı kurallar koymuştur. Buna göre reklam broşürü, tarife, katalog, fiyat listesi v.s. göndermek veya yayımlamak icap olmayıp, icaba davettir(BK m. 7/2). Yine üzerinde fiyatı gösterilmek suretiyle herkesin görebileceği çarşı, pazar, mağaza gibi yerlerde mal sergilenmesi icap sayılır(BK m. 7/3)¹⁶⁹. Ancak bu hükme göre malın bizzat kendisinin fiyatı ile sergilenmesi gerekir. Malın resminin veya maketinin sergilenmesi ya da fiyat konulmadan malın sergilenmesi icap sayılmaz. Keza araç veya ev satışı gibi geçerliliği şekil şartına bağlanmış sözleşmelerde, malın üzerine fiyatı konularak teşhir edilmesi icap sayılmamaktadır¹⁷⁰.

Borçlar Kanunu, fiyatı gösterilmek suretiyle eşya teşhirini kural olarak icap saymış ise de, bu durum yasa gereği kesin bir hüküm olmayıp karine teşkil etmektedir. Dolayısı ile bir malın üzerine fiyatı konularak sergilenmesinin icapta bulunmak niyetini taşımadığı iddia ve ispat olunabilir. Yine doktrinde kabul edilen görüşe göre bu şekilde yapılan icap teşhir edilen mal ile sınırlıdır¹⁷¹. Bununla beraber kanun koyucu bazı istisnai durumlarda fiyatı gösterilmese de mal sergilenmesi halinde sözleşme yapma zorunluluğu, hatta alıcıya, satıcının elinde bulunduğu sürece dilediği miktarda alma hakkı tanımaktadır. Gerçekten de Tüketicinin Korunması Hakkında Kanun'un 5 inci maddesi gereğince; Üzerinde "numunedir" veya "satılık değildir" gibi bir ibaresi bulunmadığı sürece bir malın; ticari bir kuruluşun vitrininde, rafında veya açıkça görülebilir herhangi bir yerinde teşhir edilmesi halinde satıcı bu malların satışından kaçınamaz(m. 5/1). Yine aynı madde gereğince aksine bir teamül yada ticari adet yoksa alıcı, satıcının elinde var olduğu sürece bir mal veya hizmetten dilediği kadar

¹⁶⁷ Onursan, s.185; Eren, s.228; Reisoğlu, s.58

¹⁶⁸ Tunçomağ, s.186; Reisoğlu, s.58; Eren, s.229

¹⁶⁹ Oğuzman-Öz, s.51; Eren, s.230

¹⁷⁰ Oğuzman-Öz, s.51; Eren, s. 230; Altınışik, s.43

¹⁷¹ Eren, s.230

alabilir(m.5/3). Burada fiyat belirtme zorunluluğu olmaması, icabın sözleşmenin bütün esaslı unsurları içermesi gerektiği ve icabın teşhir edilen mal ile sınırlı olduğu kuralına ters düşmektedir. Dolayısı ile bu şekilde ürün teşhiri bir icap olmayıp, sözleşme yapma ya da yapılacak icabı kabul etme zorunluluğu olarak anlaşılmalıdır¹⁷².

Web sitelerinde mal veya hizmet sunumuna ilişkin bilgilerin yayımlanmasının, yine elektronik posta kullanılarak muhatabın e-mail adresine teklif gönderilmesinin, icap mı yoksa icaba davet mi sayılacağıın tespiti özellik arz etmektedir. Öncelikle, bireysel elektronik posta kullanılarak muhatabın e-mail adresine teklif gönderilmesinin, fonksiyonları itibari ile mektupla yapılan tekliften pek farkı yoktur¹⁷³. Bu nedenle normal posta ile olduğu gibi, elektronik posta ile de icapta bulunulabilir. Ancak, web sitesinde yer alan ürün sunumları, nitelik itibari ile umuma yapılmış olması nedeniyle, uygulamada ve öğretilerde farklı değerlendirmektedir. Bu husustaki görüş ve düzenlemeleri aşağıda inceleyeceğiz.

2.4.3.1.1- Web Sitesindeki Sunumun Hukuki Niteliği

Yukarıda açıklandığı üzere elektronik sözleşmelerin konusunu, fiziki mal satım sözleşmeleri ile *internet veri tabanı sözleşmeleri*¹⁷⁴ olarak adlandırılan, dijital mal satımı, hizmet sunumu ve bilgi temini oluşturmaktadır. Fiziki mal satımına ilişkin sözleşmeler dışındaki sözleşmelerin kurulumu ve ifası doğrudan elektronik ortamda gerçekleşmektedir. Fiziki mal satımına ilişkin sözleşmeler ise elektronik ortamda kurulmakla beraber, tarafların ifası klasik yöntemlerle gerçekleşmektedir. Bu nedenle internet sitesindeki sunumun hukuki niteliği sözleşmelerin konusuna göre ayrı ayrı değerlendirilmektedir.

Web sitesi üzerinden fiziki mal sunumu yapılan hallerde, bu sunumun icap mı yoksa icaba davet mi olduğu hususunda doktrinde görüş ayrılıkları bulunmaktadır. Doktrinde çoğunluğun kabul ettiği görüş, bu bilgilerin, icap olmayıp, icaba davet olarak kabul edilmesi yönündedir. Bu görüşü savunanlar, web sayfasında sunumu yapanın, bağlanma iradesi ile hareket etmediğini kabul etmektedirler¹⁷⁵. Buna göre bu bilgileri

¹⁷² Oğuzman-Öz, s.51, dn.50b; Altınışık, s.43

¹⁷³ Özdemir Kocasakal, s.70; Sözer, s.92

¹⁷⁴ Gezder, s.106; Kırca, s.104

¹⁷⁵ Özsunay, s.129; Özdemir Kocasakal, s.58; Kırca, s.103

sunanların, muhatabın ödeme gücü, kredi durumu hakkında bilgi sahibi olmaları ve talep edilen ürünün stoklarında bulunup bulunmadığını, teslim hazır olup olmadığını kontrol edip ona göre öneriyi kabul veya ret etmeleri mümkün olacaktır¹⁷⁶. Web sitesinde yer alan bilgilerin icap olarak kabul edilmesi halinde, satıcı veya sağlayıcı, bu sayfanın ulaştığı her yerden, dolayısıyla potansiyel olarak dünyanın her yerinden gelen kabul cevabı ile sözleşmeyi kurmak zorunda kalacaktır. Böylece bir yandan, stoklarında kalmamış ürünleri satmak ve teslim etmek yükümlülüğü altına girecek, diğer yandan, muhatabın kimliği ve özellikle onun ödeme gücü hakkında araştırma yapma imkânı bulamayacaktır. Bu nedenle, bu görüşü savunanlar, web sitelerinde satışa sunulan fiziki mallarla ilgili sözleşmeler açısından, bu yöndeki sunumun icaba davet, muhatabın web sayfasındaki sipariş formunu doldurarak göndermesinin ise icap olduğunu kabul etmektedirler¹⁷⁷. Türk ve İsviçre Hukukunda, bu görüşü savunan bazı yazarlar ise, web sitelerinde yer alan mal ve hizmetlere yönelik açıklamaları, BK m.7/2 (İsviçre BK m. 7/2) anlamında, tarife, katalog ve fiyat listesi gönderilmesine benzetmekte ve bu nedenle icaba davet niteliği taşıdığını kabul etmektedirler¹⁷⁸.

Bir diğer görüş ise, aksine bir açıklama olmadığı takdirde web sitesinde fiziki mal satımına ilişkin yer alan bilgilerin icap olarak kabul edilmesi gerektiği yönündedir¹⁷⁹. Bu fikri savunan yazarlar, web sayfasında fiziki mal sunumu yapan sunucunun, bu irade beyanı ile bağlı olmadığını açıkça belirtmesi, örneğin ürünlerin stoklardaki miktarı hakkında kesin bilgisi olmaması halinde, “bağlayıcı değildir, stoklarla sınırlıdır” gibi bir ifade ile teklifi ile bağlı olmadığı hususunda açıklamada bulunmasının zorunlu olduğunu savunmaktadırlar. Buna göre böyle bir açıklama olmadığı sürece, web sayfasında yer alan sunumun icap olarak kabulü gerekir¹⁸⁰. Diğer bir iddia ise, BK. m. 7/3 gereğince, bir malın fiyatının da gösterilmek suretiyle teşhir edilmesinin icap sayılacağı karinesinden hareketle, aksine bir nitelendirmeyi gerektirecek somut bir kayıt olmadığı sürece, web sayfasında ürünün fiyatı da dâhil tüm

¹⁷⁶ Özsunay, s.129; İnal, s.128

¹⁷⁷ Özsunay, s.129; Özdemir Kocasakal, s.58; Kırca, s.104; Topaloğlu, s.110; İnal s.129

¹⁷⁸ Kırca, s.103; Topaloğlu, s.109; Özdilek, s.29; Altınıış, s.43

¹⁷⁹ Sözer, s.96; Özdilek, s.31; Altınıışık s.45; Büyükay, s.5; Gezder, s.99

¹⁸⁰ Özdemir Kocasakal, s.58; Kırca, s.103

bilgilerinin, özellikle ödeme ve teslim şartlarının yer almasının icap sayılması gerektiğidir¹⁸¹.

Konusunu internet veri tabanı sözleşmelerinin oluşturduğu sözleşmelerde ise, mal veya hizmetin web sitesinde sunulması, icap olarak kabul edilmektedir¹⁸². Bu hususta fiziki malların web sitelerinde ki sunumlarının hukuki niteliğine dair görüş ayrılıklarının aksine herhangi bir ihtilaf bulunmamaktadır. Fiziki mallara ilişkin sunumu icaba davet kabul eden yazarlar, internet veri tabanı sözleşmelerine ilişkin sunumu, sözleşmelerin kurulum ve ifasının¹⁸³ elektronik ortamda gerçekleşmesi ve bu tür ürünlerin stok probleminin olmayıp, sınırsız kopyasının yapılmasının mümkün olması ve dilenen miktarda yüklemesinin (download) yapılabilmesi nedenleriyle icap sayılması gerektiğini ifade etmektedirler¹⁸⁴. Yine bu tür bir mal veya hizmeti sunan kişinin irade beyanı ile bağlılık niyetinin olduğu, muhatap veya üçüncü tarafından anlaşılabilir kabul edilmektedir¹⁸⁵.

Halen yürürlükte bulunan Borçlar Kanununda, web sayfasındaki bilgilerin icap mı yoksa icaba davet olarak kabul edileceği hususunda bir hükme yer verilmemiştir. Ancak henüz yasalaşmamış olan Türk Borçlar Kanunu tasarısında, mevcut düzenlemeden farklı olarak, “*fiyatını göstererek mal sergilenmesi veya tarife, fiyat listesi ya da benzerlerinin gönderilmesi, aksi açıkça ve kolaylıkla anlaşılmadıkça öneri sayılır*”(m. 8/2) hükmüne yer verilmiştir. Tasarı bu hali ile yasalaşır ise, web sayfasında yer alan sunumlar icap olarak kabul edilmekle kalmayıp, tarife, fiyat listesi, katalog v.s. gönderilmesi de kural olarak icap kabul edilecektir.

UNCITRAL tarafından hazırlanan *Veri Mesajları Aracılığıyla Kurulan veya Tespit Edilen Sözleşmelere İlişkin Konvansiyon Ön Tasarısı*, web sayfasında olduğu gibi, belirli bir ya da birkaç kişiye değil de umuma teklif yapılması halinde, teklifi yapanların bu teklifleri ile bağlı olduklarına dair düşüncelerini ortaya koymadıkları sürece, teklifin icaba davet olarak kabul edileceğini belirtmektedir(m. 9/1)¹⁸⁶. Buna göre

¹⁸¹ Sözer, s.96

¹⁸² Özsunay, s.130; Kırca, s.104; Özdemir Kocasakal, s.59; Acır, s.14; Gezder, s.108; İnal, s.128; Topaloğlu, s.110

¹⁸³ Elektronik ortamda satıcının (sunucu) ifası, ürünü alıcının (kullanıcı) bilgisayarına yüklemeye imkân tanınması, alıcının ifası ise ücretsiz veya elektronik (kredi kartı, v.s) ödeme yapması şeklinde gerçekleşir.

¹⁸⁴ Özsunay, s.130; Kırca, s.104; İnal, s.129; Topaloğlu, s.110

¹⁸⁵ Kırca, s.104

¹⁸⁶ Özdemir Kocasakal, s.61

aksine bir hüküm yoksa web sitelerinde yer alan bilgiler icaba davet olarak değerlendirilecektir.

Avrupa Birliğince kabul edilen Elektronik Ticaret Yönergesi'nin sipariş verilmesi başlıklı 11 inci maddesine göre web sitesi üzerinden hizmet sunumuna ilişkin yapılan irade açıklamalarında, alıcının sipariş vermesi ile sözleşme kurulmuş olur. Buna göre sunucunun bu yöndeki irade beyanı icap, alıcının sipariş vermesi ise kabul sayılmaktadır¹⁸⁷. Ancak madde metninden anlaşıldığı üzere bu düzenleme hizmet sunumunu ele almaktadır. Dolayısıyla fiziki mal sunumuna ilişkin bilgilerin hukuki niteliğine ilişkin bir düzenlemeye yer vermemektedir.

Yine 20.05.1997 tarihli Mesafeli Sözleşmelere İlişkin AB Direktifi'nin 7/1 inci maddesi, aksi kararlaştırılmadığı sürece, tüketicinin siparişini satıcıya ulaştırdığı tarihi takip eden günden itibaren 30 gün içerisinde satıcının edimini ifa etmesi gerektiği hükmüne yer verilmiştir¹⁸⁸. Bu hükümde satıcının sunumu veya teklifi icap, tüketicinin siparişi ise kabul olarak değerlendirilmiştir.

Kanımızca, herhangi bir sözleşme yapılmasına ilişkin teklifi içerir irade beyanının, sırf web sitesinde yer alması nedeniyle bunun icap veya icaba davet olarak değerlendirilmesi gerektiği düşüncesi yanlıştır. Zira bu her şeyden önce irade özerkliği prensibine aykırıdır. Ayrıca bazı yazarlarca gerekçe olarak ileri sürülen, stok kontrolü yapılması ve stok durumunun web sayfasında gösterilmesi son derece kolaydır. Yine alıcının ekonomik durumu da, günümüzde elektronik sipariş ödemelerinin büyük bölümünün kredi kartı ile yapılıyor olması da nazara alındığında, tek başına kıstas alınacak bir gerekçe olarak kabul edilemez. Öte yandan web sitesindeki sunumun BK. m.7/2 kapsamında, tarife veya fiyat listesi olarak değerlendirilebileceği iddiası da kanımızca yerinde değildir. Çünkü tarife ve fiyat listesinden farklı olarak, web sitesinde ürün teşhirinde, ürünün çarşı, pazar gibi yerlerde olduğu gibi hatta bazen daha da ayrıntılı olarak, inceleme, özelliklerini öğrenme imkânı bulunmakta, bunun da ötesinde ürünü direkt satın alma imkânı tanınmaktadır. Bu hali ile söz konusu sunum BK. m.7/3 kapsamında “*semenini göstererek emtia teşhiri*” olarak da değerlendirilebilir¹⁸⁹. Zaten yukarıda da arz ettiğimiz üzere, yeni Türk Borçlar Kanunu yasa tasarısında, fiyatını

¹⁸⁷ Kırcı, s.105; Topaloğlu, s.110

¹⁸⁸ Altınışık, s.45; İnal, s.128

¹⁸⁹ İnal, s.130; Sözer, s.96

göstererek mal teşhiri ile fiyat listesi ya da tarife gönderilmesi arasında bir ayrıma gidilmemiş ve aynı hükme bağlanmıştır.

Sonuç olarak, biz de bir kısım yazarlar gibi, web sitesindeki sunumun niteliğinin, genel hükümlere göre yorum yapılarak tespiti gerektiği düşüncesindeyiz¹⁹⁰. Zira web sitelerindeki sunumu genel ve kesin bir yargı ile icap veya icaba davet olarak kabul etmek yanlıştır. Bu nedenle web sitesinde yapılan açıklamalar ve sunumun niteliği, sunucunun iradesi ile bağlanma niyetinin olup olmadığı ve açıklamaların, sözleşmenin objektif yönden tüm esaslı noktalarını kapsayıp kapsamadığı tespit edilerek nitelendirme yapılmalıdır¹⁹¹. Eğer ki sunucunun teklifi ile bağlanma iradesinin varlığı kabul ediliyor, teklif de sözleşmenin objektif yönden tüm esaslı noktalarını kapsıyorsa, sunum icap olarak kabul edilecek, aksi takdirde icaba davet sayılacaktır.

2.4.3.1.2- İcabın Bağlayıcılığı

İcabın bağlayıcılığı hususunda ülkelerin hukuk sistemlerinde bazı farklılıklar bulunmaktadır. Örneğin, Türk-İsviçre hukuku ile Alman hukukunda icap bağlayıcı olmakla birlikte, İtalyan ve İngiliz hukuk sistemlerinde icap bağlayıcı kabul edilmemektedir¹⁹².

Hukuk sistemimizde icap, kural olarak icapta bulunana bağlar. Yani icap muhataba sözleşmeyi kurma imkânı verir ve icapta bulunan buna engel olamaz. Yine icapta bulunan kural olarak icabından dönemez¹⁹³. İcabın geri alınması ancak, hazır olmayan kimseye yapılması halinde ve icap beyanından önce icabın geri alınması beyanının muhataba ulaşması veya icaptan sonra ulaşmakla beraber icap beyanından önce öğrenilmesi halinde geçerli olur¹⁹⁴ (BK. m.9). Borçlar Kanunumuz iki durumda, icapta bulunana icabı ile bağlı olmaktan muaf tutmuştur. Buna göre icapta bulunan, icabı ile bağlı olmadığını açıkça belirmiş ise yada işin mahiyetinden veya durumun

¹⁹⁰ Özdemir Kocasakal, s.62-63; İnal, s.131; Büyükay, s.5

¹⁹¹ İnal, s.130; Özdemir Kocasakal, s.63

¹⁹² Tunçomağ, s.189; Özdemir Kocasakal, s.70; İnal, s.122

¹⁹³ Oğuzman-Öz, s.53; Eren, s.231; Reisoğlu, s.59; Sözer, s.37; Tunçomağ, s.187

¹⁹⁴ Oğuzman-Öz, s.55; İnal, s.123; Reisoğlu, s.60; Akıntürk, s.27

gereğinden bu anlaşılıyorsa, icapta bulunan icabı ile bağlı olmaktan kurtulur¹⁹⁵(BK. m.7/1).

İcabın bağlayıcılık süresinin tespitinde öncelikle icapta bulunanın bir süre belirleyip belirlemediğine bakılmalıdır. Zira icapta bulunan, kabul beyanında bulunulması için muhataba dilediği miktarda süre verebilir. Bu durumda icapta bulunan öngördüğü sürenin sonuna kadar icabı ile bağlıdır¹⁹⁶. Bu süre içerisinde kabul beyanının icapçıya ulaşmaması halinde icabın bağlayıcılığı sona erer. Söz konusu süre bittikten sonra icapçıya ulaşan kabul beyanı yeni bir icap sayılır¹⁹⁷. Burada icabın hangi araçla yapıldığının bir ehemmiyeti yoktur. Klasik yöntemlerde olduğu gibi web siteleri veya elektronik posta yolu ile yapılan icaplarda da pekâlâ kabul süresi öngörülebilir.

İcapta bulunanın kabul için bir süre belirtmemiş olduğu hallerde ise, icabı ikiye ayırarak incelemek durumundayız. İcabın hazırlar arasında, yani icapta bulunan ile bir arada bulunan ya da doğrudan iletişim halinde olan kişi veya kişilere yapılması halinde, kabul beyanının derhal yapılması gerekir. Aksi halde icap bağlayıcılığını yitirir¹⁹⁸. İcabın hazırlar arasında kabul edilmesi için tarafların bir arada ve aynı yerde olmaları gerekmez. Taraflar farklı yerlerde olsalar da doğrudan iletişim kurabiliyor ve irade beyanlarını anında öğrenip, cevap verebiliyorlar ise hazırlar arasındaki icap kuralları geçerlidir. Bu iletişim Borçlar Kanunu 3 üncü maddesi anlamında telefonla olabileceği gibi, doktrinde kabul edildiği ve yeni Türk Borçlar Kanunu tasarısı 4 üncü maddesinde zikredildiği üzere, bilgisayar vasıtasıyla doğrudan sesli, görüntülü veya anlık yazışma (chat) gibi yöntemlerle de olabilir¹⁹⁹. Yine, tarafların bizzat kendilerinin değil de temsilci ya da vekillerinin teklifte bulunması da durumu değiştirmez²⁰⁰. Bu hallerde de icap derhal kabul edilmez ise bağlayıcılığı sona erer.

Hazır olmayanlar arasında yapılan ve süre belirtilmeyen icapta ise, icapta bulunan, normal bir kabul beyanının kendisine ulaşacağı ana kadar icabı ile bağlıdır. Bu sürenin hesabında, önerinin muhataba ulaşması için gereken süre, muhatabın icapçı ile ilişkisi, icabın niteliği ve içeriğine göre teklifi düşünmesi için gereken süre ve

¹⁹⁵ Oğuzman-Öz, s.55; Akıntürk, s.25; Özsunay, s.126

¹⁹⁶ Oğuzman-Öz, s.54; Eren, s.232

¹⁹⁷ Reisoğlu, s.59; Özdemir Kocasakal, s.71; Akıntürk, s.60

¹⁹⁸ Tunçomağ, s.192; Özsunay, s.126; Eren, s.233

¹⁹⁹ Özdemir Kocasakal, s.23; Reisoğlu, s.60; Akıntürk, s.26; Kırca, s.107

²⁰⁰ Eren, s.233; Akıntürk, s.26

muhatapın kabul beyanının icapçıya ulaşması için gereken sürelerin toplamı esas alınmalıdır²⁰¹. İcabın muhataba ulaşmasının gecikmesi icapçıya bir külfet yüklememektedir. Zira icapta bulunanın icabın muhataba makul sürede vardığını kabul etme ve ona göre hareket etme hakkı bulunmaktadır(BK. m.5/2). Ancak, muhatapın makul sürede gönderdiği kabul beyanının icapçıya geç ulaşması halinde, icapta bulunanın icabı ile bağlı olmaktan kurtulabilmesi için bu yöndeki beyanını derhal muhataba bildirmesi gerekir. Aksi halde sözleşme kurulmuş olur²⁰².

Elektronik ortamda yapılan irade beyanlarının hazırlar arasında olup olmadığının tespitinde iletişimin niteliği önem arz etmektedir. Söz konusu iletişimde taraflar, aynı anda diyalog kurarak, belirsiz konuları karşılıklı sorularla çözebilecek konumda değil iseler, hazır olmayanlar arasında irade beyanından söz edilecektir²⁰³. Bunun en çarpıcı örneği elektronik postadır. Zira e-postada tarafların doğrudan iletişim söz konusu olmayıp, klasik posta kutusunda olduğu gibi gönderilen beyanı geri almak mümkün olmadığı gibi, bu beyanın irade beyanının okunup okunmayacağı ya da ne zaman okunacağı tamamen alıcının iradesindedir²⁰⁴. Web sitelerinde yer alan sunumlar vasıtası ile sözleşme kurulmasında da doğrudan diyalog ve müzakere imkânı mümkün olmayıp, genelde sitede yer alan formun doldurulması veya ilgili butonun kliklenmesi ile sözleşme kurulduğundan, burada da hazır olmayanlar arasında iletişim söz konusudur. Aynı şekilde EDI yöntemi ile kurulan sözleşmeler de taraflar yüz yüze olmayıp diyalog imkânı olmadığından hazır olmayanlar arasında cereyan etmektedir²⁰⁵. Bu nedenle elektronik ortamda, hazır olmayanlar arasında icabın varlığı kabul edilen hallerde muhataba kabul için uygun bir düşünme süresi tanınmalı ve icabın bu sürenin sonuna kadar bağlayıcı olduğu kabul edilmelidir²⁰⁶.

Tarafların elektronik ortamda, doğrudan diyalog kurarak ve karşılıklı etkileşime girerek, gerektiğinde sorular sorup, anında cevaplandırabilme yani müzakere etme imkânlarının var olduğu iletişim durumlarında ise, hazırlar arasında iletişimin varlığı kabul edilmektedir²⁰⁷. İnternette, chat, sesli veya görüntülü internet telefonu, video

²⁰¹ Eren, s.233; Tunçomağ, s.192; Reisoğlu, s.60; Akıntürk, s.26; Onursan, s.8

²⁰² Tunçomağ, s.193; Eren, s.233; Reisoğlu, s.60

²⁰³ Kırca, s.108; İnal, s.107; Özdemir Kocasakal, s.74

²⁰⁴ Özsunay, s.131; İnal, s.108

²⁰⁵ Altınışık, s.52; Kırca, s.108

²⁰⁶ Özsunay, s.131; İnal, s.115; Özdemir Kocasakal, s.74

²⁰⁷ Kırca, s.108; İnal, s.118; Özdemir Kocasakal, s.73; Acır, s.15; Gezder, s.112

konferans gibi iletişim yöntemleri, bu kategoride kabul edilmektedir. Dolayısı ile bu tür iletişimde yapılan icap, hazırlar arasında gerçekleştiğinden, derhal kabul edilmemesi halinde bağlayıcılığını kaybedecektir²⁰⁸.

2.4.3.2- Kabul

Kabul, icapçı tarafından yapılan icaba karşılık, muhatap tarafından icapçıya yöneltilen ve icaba uygun olarak sözleşmenin kurulmasına imkân sağlayan, tek taraflı irade beyanıdır²⁰⁹. Kabul, sözleşmenin kurulması için gerekli olan irade beyanlarından zaman itibari ile ikincisidir²¹⁰. Kabul beyanının içeriği icaba uygun olmalı, icabın içerdiği esaslı noktalarda değişiklik, daraltma ya da genişletme yapmamalıdır. Aksi halde bu, duruma göre icabın reddi veya yeni bir icap sayılır²¹¹. Mesela muhatap, yapılan icaba karşı icapta bulunana bir ısıım şartlar ileri sürer ise, bu yöndeki beyan yeni bir icap sayılır. Ancak, icap muhataba tercih hakkı tanıyor ve muhatap bu hakka dayanarak miktar, renk vs. yönden bir tercihte bulunuyorsa, bu yöndeki beyan yeni bir icap olmayıp, kabul sayılır²¹².

İcapta olduğu gibi, kabul için de kural olarak şekil serbestisi geçerlidir. Kanun, sözleşmenin geçerliliği için bir şekil şartı öngörmemiş ya da icapta bulunan kabul için bir şekil şartı koymamış ise, kabul beyanı, sözlü yada yazılı olabileceği gibi, muhatapın kabul iradesini gösteren bir hareketi, bir davranışı ile de olabilir. Yine kabul her zaman açık bir irade beyanı ile yapılmak zorunda değildir. Zımni olarak da yapılabilir²¹³. Örneğin, icapta bulunan tarafından gönderilen mal veya hizmet, muhatapça kullanılmaya, tüketilmeye başlanırsa, icap kabul edilmiş olur. Yine yapılan icap üzerine karşı bir beyanda bulunulmadan, muhatapça icabın gereği ifa edilir ise, söz konusu ifa kabul anlamına gelir²¹⁴. Örneğin, yapılan sipariş üzerine sipariş edilen malın gönderilmesi, tamir için bırakılan bir eşyanın muhatapça bir beyanda bulunulmadan tamir edilmesi, durumlarında zımni kabul söz konusudur.

²⁰⁸ Özsunay, s.131; Gezder, s.114

²⁰⁹ Oğuzman-Öz, s.60; Uygur, s.452; Eren, s.235; Akıntürk, s.27

²¹⁰ Eren, s.235; Uygur, s.453

²¹¹ Eren, s.235; Akıntürk, s.28; Oğuzman-Öz, s.60

²¹² Oğuzman-Öz, s.60; Sözer, s.40

²¹³ Oğuzman-Öz, s.61; Eren, 236; Tunçomağ, s.195; Onursan, s.8

²¹⁴ Tunçomağ, s.195-196; Akıntürk, s.28; Eren, s.237; Reisoğlu, s.62

Elektronik sözleşme kurulum araçları vasıtası ile kurulan sözleşmelerde de kabul beyanı çeşitli şekillerde iletilebilmektedir. Sohbet (chat) ve e-posta da yazılı olarak, sesli ve görüntülü internet telefonu aracılığı ile sesli olarak ve nihayet internet sitelerinde sözleşmeye ilişkin formu doldurarak yada sözleşmeyi kabule ilişkin butonu tıklayarak kabul beyanında bulunulabilmektedir²¹⁵.

Kural olarak, susma bir irade beyanı değildir. Dolayısıyla icaba karşı susan muhatap, icabı kabul etmiş sayılmaz²¹⁶. Hatta icapta bulunan, susma halinde icabın kabul etmiş sayılacağına dair kayıt bile koysa sonuç değişmez. Zira hiç kimse kendi sebep olmadığı bir beyanı cevaplamak zorunda değildir²¹⁷. Ancak bazı istisnai durumlarda muhatapın icapta bulunana cevap verme yükümlülüğü vardır. Bu gibi hallerde susma, kabul sayılır²¹⁸. Gerçekten, Borçlar Kanunu 6 ncı maddesi gereğince, icapta bulunan, kanun veya işin özelliği ya da durumun gereği, açık bir kabulü beklemek zorunda değilse, öneri uygun bir sürede reddedilmediği takdirde, sözleşme kurulmuş sayılır. Örneğin, bir kişiye yapılan bağışlama teklifi, durumun özelliği gereği, muhatap tarafından uygun sürede reddedilmez ise, susma kabul anlamına gelir ve sözleşme kurulmuş olur.

Kabul, yenilik doğuran bir işlemdir. Kabul beyanı ile sözleşme kurulmuş olur²¹⁹. Bu nedenle kural olarak kabul geri alınamaz. Ancak, Borçlar Kanunu 9 uncu maddesinde zikredilen istisnai durum burada da geçerlidir. Buna göre, hazır olmayanlar arasındaki işlemlerde, kabul beyanından önce kabulün geri alınması beyanının icapta bulunana ulaşması veya kabulden sonra ulaşmakla beraber, icapta bulunana kabul beyanından önce kabulden dönme beyanının öğrenilmesi halinde, kabul geçersiz olur²²⁰. Hiç yapılmamış sayılır²²¹.

²¹⁵ Özdemir Kocasakal, s.74; Özsunay, s.133; Zammit-Galant, s.942

²¹⁶ Oğuzman-Öz, s.61; Özsunay, s.132; Eren, s.237; Uygur, s.454; Akıntürk, s.28

²¹⁷ Uygur, s.454; Eren, s.237; Oğuzman-Öz, s.61, dn.78; Tunçomağ, s.196

²¹⁸ Eren, s.237; Oğuzman-Öz, s.62; Reisoğlu, s.62; Özsunay, s.132; Akıntürk, s.28

²¹⁹ Tunçomağ, s.200; Akıntürk, s.28; Uygur, s.453; Oğuzman-Öz, s.62; Eren, s.239

²²⁰ Tunçomağ, s.200; Eren, s.239; Oğuzman-Öz, s.63; Reisoğlu, s.63; Akıntürk, s.29

²²¹ Akıntürk, s.29; Eren, s.239

2.4.3.3- Sözleşmenin Kurulduğu, Hüküm ve Sonuçlarını Doğurduğu An

Sözleşmenin meydana geldiği anın tespiti ile ilgili olarak doktrinde dört farklı görüş bulunmaktadır. Açıklama teorisine göre, sözleşme muhatabın kabul beyanını açıklaması ile kurulur. Dolayısıyla kabul haberinin icapta bulunana gönderilmesine gerek yoktur. Gönderme teorisine göre sözleşme, muhatabın kabul beyanını icap sahibine gönderdiği anda kurulmuş olur. Varma teorisine göre sözleşme, kabul beyanının icapta bulunanın hâkimiyet alanına ulaştığı, vardığı anda kurulmuş olur. Öğrenme teorisinde ise sözleşmenin kurulabilmesi için icap sahibinin kabul beyanını öğrenmesi gerekir. Buna göre icap sahibinin kabul beyanını öğrendiği anda sözleşme kurulmuş olur²²².

Hukuk sistemimizde sözleşmenin meydana geldiği anın tespitinde, sözleşmenin hazırlar arasında olup olmadığına göre ayrıma gidilmiştir. Hazırlar arası sözleşmelerde, iradenin açıklanması, ulaşması ve öğrenme aynı anda gerçekleştiği için sözleşmenin kurulum anının tespitinde bir problem bulunmamaktadır. Hazırlar arasındaki icapın derhal kabulü gerektiği için, muhatabın kabul beyanında bulunduğu anda sözleşme kurulmuş olur²²³. Sözleşme yazılı olarak yapılıyorsa muhatap sözleşmeyi imzaladığı anda sözleşme kurulmuş olacaktır. Elektronik sözleşme kurulum araçlarından olan, chat ve internet telefonu benzeri iletişim hazırlar arasında kabul edildiğinden kabul beyanında bulunulduğu an sözleşme kurulmuş olur²²⁴.

Hazırlar arasında meydana gelen sözleşmelerde sözleşmenin kurulduğu an ile hüküm ve sonuçlarını doğurduğu an aynıdır. Bu itibarla sözleşme, kabul beyanının açıklandığı anda kurulmuş ve de hüküm ve sonuçlarını doğurmaya başlamıştır²²⁵.

Hazır olmayanlar arasında kurulan sözleşmelerde hukukumuz, kurulum anı olarak, varma teorisini kabul etmiştir. Bilindiği gibi İsviçre-Türk hukukunda, varma anı olarak irade beyanının muhatabın hâkimiyet alanına girdiği an kabul edilmektedir. Buna göre, kabul beyanının icap sahibinin hâkimiyet alanına ulaştığı anda sözleşme kurulmuş

²²² Eren, s.241-242; Akıncı, s.85; Altınışık, s.49

²²³ Tunçomağ, s.204; Akıntürk, s.29; Eren, s.242; Reisoğlu, s.62; Onursan, s.9

²²⁴ Gezder, s.121; İnal, s.103; Özdemir Kocasakal, s.81; Büyükay, s.6; Acır, s.15;Altınışık, s.50

²²⁵ Tunçomağ, s.207; Eren, s.242; Akıncı, s.87; Reisoğlu, s.62

olur²²⁶. Açık bir kabule ihtiyaç bulunmayan hallerde ise uygun bir bekleme süresinin sonunda sözleşme kurulmuş olur²²⁷. Görüldüğü üzere varma teorisi, icapta bulunanın kabul beyanını öğrenip öğrenmemesine değer vermemektedir. Buna göre kabul beyanı icapta bulunanın hâkimiyet alanına ulaştıktan sonra icapta bulununca öğrenilmeden, kayıp veya zayi olsa da sözleşme kurulacaktır. Bu sonuç bazı yazarlarca ağır bulunmakla eleştirilmiş ve bu kuralın tüm sözleşmelerde uygulanamayacağı, varma teorisinin sadece tarafların menfaatleri arasında denge olan sözleşmelerde uygulanacağı, somut olaya göre icapta bulunandan muhatabın beyanını öğrenmesi beklenmiyorsa ve kabul beyanı kayıp ya da zayi olmuş ise ulaşmamış sayılması gerektiği savunulmaktadır²²⁸.

Hazır olmayanlar arasında gerçekleşen sözleşmelerin hüküm ve sonuçlarını doğurmasında ise hukukumuz, gönderme teorisini benimsemiştir. Buna göre sözleşme, kabul haberinin icapta bulunana gönderildiği andan itibaren hüküm ve sonuçlarını doğurmaya başlayacaktır²²⁹(BK. m.10/2). Açık bir kabule ihtiyaç bulunmadığı durumlarda ise sözleşme, icabın muhataba ulaştığı andan itibaren hükümlerini doğuracaktır²³⁰.

Web sitesi ve elektronik posta kullanılarak irade beyanı gönderiminin, kural olarak hazır olmayanlar arasında iletişim kategorisinde bulunduğunu, daha önce ifade etmiştik. Dolayısıyla, bu hallerde sözleşme, kabul beyanının icapta bulunanın hâkimiyet alanına girdiği anda kurulmuş olacaktır. Ancak, internet üzerinden gönderilen irade beyanları genel itibari ile, tarafların sahibi olmadığı internet servis sağlayıcısı yada elektronik posta hizmet sunucusu aracılığı ile muhataba ulaşmaktadır. Söz konusu hizmet sağlayıcıları tarafların hâkimiyet alanı kabul edilemez²³¹. Hizmet sağlayıcısının taraflara tahsis ettiği e-posta kutusu ise hâkimiyet alanı dâhilindedir²³². O halde, irade beyanı ne zaman hâkimiyet alanında kabul edilecektir.

²²⁶ Oğuzman-Öz, s.66; Eren, s.242; Reisoğlu, s.62; Akıncı, s.30

²²⁷ Tunçomağ, s.204; Eren, s.242

²²⁸ Oğuzman-Öz, s.66-68; Özdemir Kocasakal, s.82, dn.232; Akıncı, s.86, dn.217

²²⁹ Tunçomağ, s.205; Eren, s.243; Altınışık, s.54; Reisoğlu, s.63; Akıntürk, s.30

²³⁰ Tunçomağ, s.206; İnal, s.125; Eren, s.243; Akıntürk, s.30

²³¹ Acır, s.15; İnal, s.109; Özdemir Kocasakal, s.83; Sözer, s.101; Kırca, s.110

²³² İnal, s.110; Gezder, s.122; Özdemir Kocasakal, s.83

E-posta kullanımında, gönderilen mesaj önce hizmet sağlayıcı vasıtası ile mail sunucusu (server) bünyesinde bulunan muhataba ait posta kutusuna kaydedilir ve muhatap bu sunucuya bağlanarak gelen mesajı öğrenir. Şu halde ulaşma anı, mesajın muhatabın e-posta kutusuna ulaştığı an mı, yoksa muhatabın sunucuya bağlanarak mesajı öğrendiği, yani bilgisayarına indirdiği an mıdır? Doktrinde her iki durumu da savunanlar vardır. Ancak hâkim olan görüş, beyanı içeren mesajın muhatap tarafından erişilmek üzere, muhatabın e-posta kutusuna kaydedildiği anda mesaj muhatabın hâkimiyet alanına ulaşmıştır²³³. Yine beyanın muhatabın hâkimiyet alanına varması yeterli olmayıp, muhatabın bunu öğrenme imkânının da olması aranmaktadır²³⁴. Buna göre muhatap, başka kişilerin yardımı veya müdahalesi olmadan kendi elektronik posta kutusuna girerek, beyanı içeren mesajı öğrenebiliyor ise mesaj muhatabın hâkimiyet alanına ulaşmıştır. Ancak günümüzde, elektronik posta adresi olduğu halde bunu hiç kullanmayan, kontrol dahi etmeyen kişiler olduğu gibi, birden çok elektronik posta adresi kullanan ve bunlardan bazısını özel işlerinde, bazılarını ise ticari ve hukuki işlerinde kullananlar da bulunmaktadır. Yine elektronik posta adresi kullanımına rağmen, posta kutusunun boşaltılmamasından veya posta kutusuna spamming yolu ile çok sayıda mail gelmesinden dolayı posta kutusunun kapasitesinin dolması nedeniyle, gelen mesajın kaydedilemediği durumlarda olmaktadır. O halde posta kutusuna kaydedilemeyen veya muhatabın haberi olmadan posta kutusuna kaydedilen ama muhatabın öğrenmediği maillerin durumu ne olacaktır?

Doktrinde e-mail ile iletişimin klasik iletişim yolları ile aynı hukuki sonucu doğurabilmesi için elektronik posta adresi sahibinin, bu yönde bir kullanıma izin vermesinin aranması gerektiği ifade edilmektedir²³⁵. Buna göre e-posta adresi ticari bir işletmeye veya ticari bir kullanıcıya ait ise, e-posta adresinin evrak, web sitesi, reklâm broşürü gibi herhangi bir yolla açığa vurulması halinde bu yönde kullanıma izin verilmiş demektir. Buna paralel olarak da ticari işlerde tacirlerin e-posta adreslerini günlük bir veya birden çok kez kontrol etmeleri gerektiği kabul edilmektedir²³⁶. E-postanın mesai kavramından bağımsız olarak, günün 24 saati gönderilebildiği nazara alındığında, tacirler açısından e-posta mesajı muhatabın e-posta kutusuna kaydedildiği

²³³ Özdemir Kocasakal, s.183; Altınışık, s. ; Gezder, s.123; İnal,s.110; Kırca, s.110

²³⁴ Kırca, s.111; Özdemir Kocasakal, s.84; Altınışık, s.52

²³⁵ Gezder, s.122; Kırca, s.112; İnal, s.111

²³⁶ Kırca, s.112; Gezder, s.124; İnal, s.111; Özdemir Kocasakal, s.83; Altınışık, s.52

anda muhataba ulaşmıştır. Bu an muhatabın posta kutusunu kontrol yükümlülüğü olmadığı bir zaman, örneğin gece ise, en geç gönderildiği günü takip eden günün sabahı muhataba ulaşmış kabul edilecektir²³⁷.

Elektronik posta adresinin bir tüketiciye ait olması durumunda ise, mesajın e-posta kutusuna ulaşmasının, kullanıcının hâkimiyet alanında kabul edilebilmesi için, tüketicinin, bu adresini hukuki işlemlerinde kullandığını muhatabına bildirmesi gerekmektedir²³⁸. Bu bildirim, tüketici tarafından sözleşme kurulmasına yönelik girişimin e-mail aracılığı ile başlatılması şeklinde olabileceği gibi, web sitesine kayıt yapılırken e-posta adresinin belirtilmesi şeklinde de olabilecektir. Bu şekilde bir bildirimde bulunulmuş ise, kullanıcının e-posta adresini günlük kontrol etmesi gerektiği kabul edilecek ve irade beyanı posta kutusuna kayıt anında veya en geç gönderilen günü takip eden gün tüketiciye ulaşmış sayılacaktır²³⁹. Kullanıcı tarafından böyle bir bildirimde bulunulmamış ise irade beyanı ancak, kullanıcı tarafından mesajın içeriğinin öğrenildiği an ulaşmış kabul edilecektir²⁴⁰.

Elektronik posta adresi sahibinin, posta kutusunu kontrol yükümlülüğünün olduğu kabul edilen hallerde, irade beyanının gönderilmesine rağmen, ulaşma engelleri nedeniyle posta kutusuna kaydedilememesi durumlarında ise, bizim de katıldığımız görüşe göre, ulaşma engelinin kaynağına göre değerlendirme yapılacaktır. Söz konusu engel, muhatabın etki alanında bulunmayan harici bir sebepten kaynaklanıyor ise, örneğin, virüs, hacker saldırısı veya hizmet sağlayıcısının sisteminin çökmesi yada spamming tarzı bir saldırı ile e-posta kutusunun dolması gibi nedenlerle, mesajın posta kutusuna kaydedilememesi halinde, riziko göndericiye yüklenerek mesaj ulaşmamış kabul edilecektir²⁴¹. Buna karşılık, alıcının etki alanındaki bir sebepten; örneğin, posta kutusunu düzenli kontrol ve gerektiğinde boşaltma yükümlülüğü olduğu halde, posta kutusunun boşaltılmaması nedeniyle, kapasitesinin dolması ve bu nedenle mesajın kaydedilememesi veya mesaj posta kutusuna kaydedilmekle beraber, alıcının

²³⁷ Gezder, s.124; Kırca, s.111; Özdemir Kocasakal, s.84 İnal, s.111

²³⁸ İnal, s.112; Kırca, s.111; Özdemir Kocasakal, s.85; (UNCITRAL tarafından hazırlanan tasarımlarda, bu bildirim gerekliliğine yer verildiğine dair, bkz. s.27 vd.)

²³⁹ Gezder, s.124; Kırca, s.111, İnal, s.112

²⁴⁰ Özdemir Kocasakal, s.85, 87; İnal, s.112; Gezder, s.124

²⁴¹ Gezder, s.123; İnal, s.113; Büyükay, s.6

bilgisayarındaki arıza yada başka nedenle silinmesi halinde, riziko alıcıya ait olacak ve mesaj muhataba yani alıcıya ulaşmış olacaktır²⁴².

Web sayfaları üzerinden gönderilen irade beyanlarında ise, tarafların doğrudan diyalogu olmamakla beraber, elektronik posta iletişiminden farklı olarak irade beyanı, genelde üçüncü bir bilgisayara (mail server) kaydedilmeyip doğrudan muhatabın bilgisayarına gönderilmektedir²⁴³. Yani bir nevi doğrudan iletişim söz konusudur. Bu nedenle irade beyanının gönderilmesi ile muhataba ulaşması neredeyse aynı anda olur. Ancak ulaşma engelleri ve iletişim kopukluğu gibi sebepler dikkate alınarak diyebiliriz ki, web sayfaları üzerinden gönderilen irade beyanları, muhatabın bilgisayarına kaydedildiği anda ulaşmış sayılmalıdır²⁴⁴. Şu halde sözleşmenin kuruluş anı da, web sayfasındaki sunumun icap veya icaba davet olarak nitelendirilmesine göre değişecektir. Web sayfasındaki sunumun icap kabul edildiği hallerde, muhatabın kabul beyanının icapta bulunana ulaşma anında sözleşme kurulmuş olacaktır²⁴⁵. Web sayfasında ki sunumun icaba davet kabul edildiği durumlarda ise, sunumu yapanın kabul beyanının icapta bulunana ulaştığı anda sözleşme kurulacaktır. Yine bu halde sunumu yapanın sözleşme yapmaya hazır olduğunu belirtmesi nedeniyle, açık kabule ihtiyaç bulunmayan hallerde sunumu yapan kabul beyanında bulunmayıp susarsa uygun bir bekleme süresi sonunda sözleşme kurulmuş olacaktır²⁴⁶.

UNCITRAL tarafından hazırlanan, Elektronik Ticaret Model Kanunu(m.15) ve Veri Mesajları Aracılığıyla Kurulan veya Tespit Edilen Sözleşmelere İlişkin Konvansiyon Ön Tasarısı(m.8,11), mesajların muhataba ulaşma anını, muhatabın haberleşme sistemi bildirip bildirmemesine göre, iki şekilde düzenlemiştir. Buna göre, muhatap elektronik haberleşme adresini bildirmiş ise mesajların bu adrese ulaştığı an muhataba ulaşma anıdır. Aksi halde, yani adres bildirilmemesi veya bildirilen adresten başka bir adrese mesaj gönderilmesi durumunda ise ulaşma anı, muhatabın mesajı öğrendiği andır²⁴⁷.

²⁴² İnal, s.115; Gezder, s.123; Büyükay, s.6

²⁴³ İnal, s.116; Özdemir Kocasakal, s.85

²⁴⁴ İnal, s.117; Özdemir Kocasakal, s.85; Kırca, s.110

²⁴⁵ Özdemir Kocasakal, s.88; Sözer, s.102; Kırca, s.113; Topaloğlu, s.112

²⁴⁶ Kırca, s.113; Özdemir Kocasakal, s.85; Altınışık, s.53

²⁴⁷ Özdemir Kocasakal, s.87; Topaloğlu, s.112

Elektronik Ticaret Model Kanununa göre, elektronik sözleşme kuruluşu araçları ile yapılan irade beyanları, onu gönderenin kontrolü dışında olan bir elektronik ortama girdiği anda gönderilmiş sayılır(m.15/1). Bu doktrinde de benimsenmiştir. Bu ilkedan hareketle denebilir ki, elektronik sözleşme kuruluşu araçları ile kurulan sözleşmeler, açık bir kabule ihtiyaç olan hallerde, kabul beyanının gönderenin kontrolü dışındaki bir elektronik ortama girdiği andan, açık bir kabule ihtiyaç olmayan durumlarda ise, icabın muhataba ulaştığı andan itibaren hüküm ve sonuçlarını doğurmaya başlar²⁴⁸. Ancak, elektronik ortamda kabul beyanının icapta bulunana gönderilme anı ile ulaşma anı arasında çok kısa bir zaman geçmektedir. Bu nedenle genel olarak elektronik ortamda yapılan bir sözleşmenin kurulma anı ile hüküm ve sonuçlarını doğurmaya başladığı an aynı olmaktadır²⁴⁹.

AB Elektronik Ticaret Yönergesi ise, web sayfasında hizmet edimi sunan kişinin bu davranışının icap olduğundan hareketle, hizmet sunucusuna, hizmet alıcısının kabul beyanını (siparişini) aldığını derhal ve elektronik yoldan teyit etme zorunluluğu getirmektedir(m.11/1). Kanaatimizce bu hüküm tüketicinin korunmasına yönelik bir hüküm olup, sözleşmenin kuruluşu anını etkilememektedir²⁵⁰. Yine şurası da unutulmamalıdır ki, bu hüküm yalnızca hizmet sunumuna ilişkin olup, diğer sözleşmeler bu hüküm kapsamı dışında bulunmaktadır.

2.4.3.4- Sözleşmenin Kurulduğu Yer

Sözleşmenin kurulduğu yerin tayini, milli hukukta yetkili mahkemenin tespiti, milletlerarası hukukta ise sözleşmeye uygulanacak hukukun tespitinde önem arz etmektedir. Zira sözleşmenin doğumu, kurulduğu yerin (ülkenin) hukukuna tabidir²⁵¹.

Hukukumuzda sözleşmenin kurulduğu yerin tespitine ilişkin açık bir hüküm bulunmamaktadır. Bu nedenle sözleşmenin kuruluşuna ilişkin genel hükümlerin yorumlanması ile bu hususun tespiti cihetine gidilmektedir. Bilindiği üzere sözleşme, hazırlar arasında, kabul beyanında bulunulduğu an; hazır olmayanlar arasında ise kabul beyanının icapta bulunana ulaştığı anda kurulmuştur. Ancak sözleşmenin hüküm

²⁴⁸ Sözer, s.100; Özdemir Kocasakal, s.88; Topaloğlu, s.112; Kırcı, s.113; Acır, s.16

²⁴⁹ Sevinç, s.31; Özdemir Kocasakal, s.85; ETKK, Hukuk Çalışma Grubu Raporu, s.8

²⁵⁰ Benzer görüş, Sözer, s.95, Özdemir Kocasakal, s.86, dn.246; Karşı görüş, Kırcı, s.114, Topaloğlu, s.112 (Sözleşme kabul haberinin onaylandığına ilişkin beyanın kullanana ulaştığı anda kurulur.)

²⁵¹ Velidedeoğlu-Özdemir, s.27; Birsen, s.72; Onursan, s.9; Topaloğlu, 113; Sözer, s.104

doğurmaya başladığı an her iki halde de kabul beyanının yöneltildiği(gönderildiği) andır. Bu itibarla doktrinde hâkim olan görüş, kabul beyanının yapıldığı yerin sözleşmenin yapıldığı yer olduğu yönündedir²⁵².

İnternetin global bir dünya oluşu ve kullanıcıların dünyanın herhangi bir yerinden, herhangi bir bilgisayar vasıtası ile bu ortama erişmesinin mümkün olması karşısında; elektronik ortamda kurulan sözleşmelerin kurulma anında tarafların işyeri veya ikametgahları dışında bulunmaları da mümkündür. Yine klasik yöntemler olan, telefon ve postada da bu durum söz konusu olabilir. Bu durumda sözleşmenin kurulduğu yerin kabul beyanının yapıldığı anda bulunulan yer kabul edilmesi, hayatın olağan akışına ters olmakta ve bazı sorunlara yol açabilmektedir. Bu nedenlerle, sözleşmenin kurulduğu yer olarak, taraflarca aksi kararlaştırılmamış ise, kabul beyanında bulunanın, tacirler açısından işyerinin, tacir olmayanlar için ise ikametgâhının bulunduğu yerin esas alınması gerektiği görüşü ağır basmaktadır²⁵³.

Nitekim, Elektronik Ticaret Model Kanunu(m.15/4) ve Veri Mesajları Aracılığıyla Kurulan veya Tespit Edilen Sözleşmelere İlişkin Konvansiyon Ön Tasarısında (m.11/5) tarafların aksini kararlaştırdığı haller dışında, mesajın göndericinin işyerinin bulunduğu yerde gönderilmiş ve yine muhatabın işyerinin bulunduğu yerde alınmış sayılacağı belirtilmiştir²⁵⁴.

2.4.3.5- Sözleşmelere Uygulanacak Hukukun Tespiti

Sözleşmelerin kurulum aşamasında tarafların aynı ülke sınırları içerisinde bulunmalarında, sözleşmeye uygulanacak hukukun tespitinde kural olarak bir sorun bulunmamaktadır. Ancak yabancılık unsuru içeren sözleşmelerde, örneğin taraflardan birinin yabancı ülke vatandaşı olması veya sözleşmenin kurulum yeri ile ifa yerinin farklı ülkeler olması durumunda, sözleşmeye hangi ülkenin hukukunun uygulanacağı hususunda kanunlar ihtilafı ortaya çıkmaktadır. Bu durum elektronik ortamda kurulan sözleşmelerde de karşımıza çıkmaktadır.

²⁵² Birsen, 72; Sözer, s.104; Topaloğlu, s.103; Karşı görüş: Özdemir Kocasakal, s.89 (Sözleşme kabul cevabının icabı yapana ulaştığı anda kurulduğuna göre, kuruluş yeri bu anda icabı yapanın bulunduğu yerdir.)

²⁵³ Velidedeoğlu- Özdemir, s.27; Onursan, s.9; Özdemir Kocasakal, s.89; Topaloğlu, s.113

²⁵⁴ Özdemir Kocasakal, s.89; Topaloğlu, s.113

Hukukumuzda, yabancılık unsuru içeren sözleşmelere uygulanacak hukukun tespitine ilişkin yasal düzenleme Milletlerarası Özel Hukuk ve Usul Hukuku Hakkında Kanun'un (MÖHUK) 24 üncü maddesinde bulunmaktadır. Buna göre öncelikle taraflar, akit serbestisi kapsamında sözleşmeye uygulanacak hukuku da kendileri bizzat seçebilirler. Tarafların hukuk seçimi açık, belirgin şekilde olmalıdır(MÖHUK. m.24/1).

Ancak sözleşmeye uygulanacak hukukun taraflarca seçimine ilişkin hükmün taraflardan birinin tüketici olması halinde mutlak olarak uygulanamayacağı ifade edilmektedir. Özellikle elektronik sözleşmelerde, hukuk seçiminin genelde mümkün olmaması veya sipariş formunda hukuk seçimi şartı bulunsa dahi, tüketicinin esas iradesinin hukuk seçimi şartını da kapsamayacağı düşüncesi ile bu şartın varlığı ve geçerliliği tartışmalı görülmekte ve bu nedenle hükmün tüketicinin taraf olduğu sözleşmelerde uygulanamayacağı kabul edilmektedir²⁵⁵.

Sözleşmeye uygulanacak hukuk taraflarca açık olarak seçilmemiş ise yada taraflarca seçim ilkesinin uygulanamayacağı durumlarda, sırasıyla borcun ifa yeri hukuku, borcun ifa yerinin birden fazla olması halinde borç ilişkisinin ağırlığını teşkil eden edimin ifa yeri hukuku, bu yerin de tespit edilemediği hallerde ise, sözleşmenin en yakın irtibat halinde bulunduğu yer hukuku uygulanacaktır(MÖHUK m.24/2).

Bu hükümden de anlaşılacağı üzere hukukumuzda, sözleşmelere uygulanacak hukukun tespitinde objektif kriter olarak, sözleşmenin ifa yeri esas alınmaktadır. Her iki tarafa borç yükleyen sözleşmelerde ise ifa yeri birden fazla olduğundan, borç ilişkisinin ağırlığını teşkil eden yani sözleşmeye özelliğini veren karakteristik edimin ifa edileceği yer hukuku uygulanacaktır. Örneği satış sözleşmelerinde borç ilişkisinin ağırlığını teşkil eden edim satıcının edimidir²⁵⁶. Yani malı teslim borcudur.

Yine taraflardan birinin tüketici olduğu ve milletlerarası özel hukukun tüketicinin korunması amacını taşıdığı sözleşmelerde tüketicinin mutlak meskeni hukukunun uygulanacağı kabul edilmektedir. Ancak tüketicinin bu korumadan faydalanabilmesi için, ya sözleşmeye mutlak meskeninin bulunduğu ülkede taraf olacak ve kendisinin tamamlaması gereken hukuki safhaları burada tamamlayacak yada

²⁵⁵ Acır, s.18; İnal, s.163

²⁵⁶ Sözer, s.108

tüketici mutad meskeninde karşı tarafın e-mail, reklam ve benzer şekillerde bilerek ve ticari olarak kendisine yönelmesi üzerine sözleşmeye taraf olacaktır²⁵⁷.

2.4.4- Mesafeli Sözleşme ve Elektronik Sözleşme

2.4.4.1- Genel Olarak

Teknolojinin günden güne gelişmesi ve bu gelişmeye paralel olarak insanlar arasındaki iletişim imkânlarının artması; işletmelerin araya aracı firma veya başka işletmeci sokmadan tüketiciye doğrudan ulaşarak mal veya hizmet sunumuna yönelmeleri ve sözleşmelerin kuruluşunda geleneksel yöntemlerden uzaklaşarak modern iletişim araçlarının kullanılması sonucunu doğurmuştur.

Bu şekilde yapılan iletişim ve doğrudan pazarlama neticesinde kurulan sözleşmelerde tarafların fiziksel olarak karşı karşıya gelmesi söz konusu olmadığından, tüketicilerin sözleşme konusu mal ve hizmetin niteliği ve kalitesi hususunda aldatılması, tüketicinin söz konusu mal ve hizmeti kontrol imkânı olmadığından mal ve hizmet hakkında yeteri kadar bilgi sahibi olamayışı ve dolayısıyla taraf iradesinin sağlıklı bir şekilde oluşmaması gibi sorunlar ortaya çıkabilmektedir²⁵⁸. Bu gibi durumlarda sağlayıcı karşısında tüketicinin güçsüz konumda olduğu görülmektedir. Modern iletişim araçları kullanılarak akdedilen sözleşmelerde bu ve benzeri sorunları ortadan kaldırmak ve tüketiciyi korumak amacı ile uluslar arası hukukta ve iç hukukta birtakım yeni kurallar koyma zorunluluğu ortaya çıkmıştır.

Tüketicinin korunması amacına yönelik bu yeni normların en önemlilerinden biri de mesafeli sözleşmelerle ilgili bulunmaktadır. Bu konudaki düzenlemelere Avrupa Birliğince, 20 Mayıs 1997’de kabul edilen 97/7/AT sayılı “Mesafeli Sözleşmelerde Tüketicinin Korunmasına İlişkin Yönerge” öncülük etmiştir. Yönergenin hükümleri bağlayıcılığı olmamakla birlikte, üye ülkelerin iç mevzuatlarını 4 Haziran 2000 tarihine kadar yönerge ile uyumlu hale getirmeleri öngörülmüştür(m.15). Yönerge ile sağlanan koruma üye ülkeler açısından nazara alınması gereken asgari düzeydeki korumadır.

²⁵⁷ Acır, s.20; İnal, s.164

²⁵⁸ Yıldırım, s.136; Bozbel-Atalı (Cayma), s.452; Demir, s.69; Büyükay, s.2; Bülter, s.5

Dolayısı ile üye ülkeler iç hukuklarında bu düzenlemelerden daha üst seviye koruma öngören bir düzenleme kabul edebileceklerdir²⁵⁹.

Bununla birlikte, niteliği itibari ile mesafeli sözleşme olmalarına rağmen bir kısım sözleşmeler de yönerge kapsamı dışında bırakılmışlardır. Bunlar; Finansal hizmet edimlerinin ifasını içerecek şekilde, banka ve diğer finansal kuruluşlarla kurulan sözleşmeler²⁶⁰, Taşınmaz yapımı ve satımını konu alan yada kira dışında taşınmazlar üzerindeki aynı haklarla ilgili sözleşmeler, Halka açık telefonlar vasıtasıyla akdedilen sözleşmeler, Açık artırma yolu ile kurulan sözleşmeler, Gıda maddeleri ve günlük ihtiyaçlarla ilgili sözleşmeler, Konaklama, taşıma ve yemek teslimi ile ilgili sözleşmeler ve son olarak Otomatik makineler vasıtasıyla yapılan sözleşmeler ve konusu telekomünikasyon hizmetleri olan sözleşmelerdir²⁶¹.

Yönerge ile mesafeli sözleşmelerde öngörülen en önemli düzenlemeler, tüketiciyi açık, kapsamlı ve yazılı bir şekilde bilgilendirme yükümlülüğü(m.4-5) yüklenmesi ve tüketicilere belirli bir zaman dilimi içerisinde cayma hakkının tanınmasıdır(m.6). Bunların yanında saldırgan satış yöntemleri, mesafeli sözleşmelerin ifası ve kredi kartı ile ödeme hususunda önemli düzenlemeler yapılmıştır²⁶².

Ülkemizde mesafeli sözleşme kavramı yeni bir kavramdır. Önceleri “mesafeli satış” kavramı yer almakta ve bu kavram, Kapıdan Satışlara İlişkin Uygulama Usul ve Esaslarına Dair Yönetmelik’in 2 nci maddesine göre “kapıdan satış” kavramı içerisinde değerlendirilmekte ve 4077 sayılı Tüketicinin Korunması Hakkında Kanun’un ve 8 ve 9 uncu maddesi hükümleri kapsamında yer almakta idi²⁶³. Ancak “mesafeli sözleşme” kavramı ve bu husustaki düzenleme Avrupa Birliği’ne uyum yasaları çerçevesinde kabul edilen 06.03.2003 tarihli 4822 Sayılı Tüketicinin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun ile 4077 sayılı TKHK’a eklenen 9/A maddesi ile mevzuatımıza girmiştir. Bu madde “mesafeli sözleşmeler” başlığını taşımakta ve mesafeli sözleşmelere ilişkin AB yönergesine paralel düzenlemeler içermektedir.

²⁵⁹ Yıldırım, s.139; Demir, s.70;

²⁶⁰ Bu konu 23.09.2002 tarihli “Mesafeli Satış Yoluyla Tüketicie Sunulan Finansal Hizmetlere İlişkin Yönerge” ile özel olarak düzenlenmiştir

²⁶¹ Demir, s.71; Büyükay, s.7; Yıldırım, s.139; Bülter, s.18; Bozbel (Yönerge), s.18

²⁶² Yıldırım, s.138; Demir, s.71; Bozbel(Yönerge), s.18.vd; Bozbel-Atalı(Cayma), s.452

²⁶³ Sözer, s.117

2.4.4.2- Tanım

Hukukumuzda mesafeli sözleşmenin tanımı TKHK'un 9/a ve Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmelik'in 4 üncü maddesinde tanımlanmıştır. Buna göre mesafeli sözleşme; *“Yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmelerdir.”*

Mesafeli Sözleşmelerde Tüketicinin Korunmasına İlişkin 97/7/AT sayılı AB Yönergesinde ise, mesafeli sözleşme; *“tüketici ile sağlayıcı arasında kurulan ve sağlayıcının mesafeli sürüme özgü olarak organize ettiği bir satış veya hizmet ağı çerçevesinde, bir mal veya hizmet edimi ile ilgili olarak, sözleşmenin kurulması anına kadarki süreç de dahil olmak üzere münhasıran bir veya birden çok mesafeli iletişim aracı yardımı ile kurulan sözleşme”* olarak tanımlanmıştır(m.2/1).

Bu tanımlardan da anlaşılacağı üzere mesafeli sözleşme, satım, kira, vs. gibi ayrı bir sözleşme tipi olmayıp, sözleşmelerin akdedilme şeklini gösteren bir kavramdır. Yine elektronik sözleşmelerle karşılaştırıldığında, mesafeli sözleşme bir üst kavram olup elektronik sözleşmeleri de kapsamaktadır. Bu anlamda tüm elektronik sözleşmeler aynı zamanda birer mesafeli sözleşmedir. Ancak mesafeli sözleşmeler elektronik sözleşme kurulum araçları haricindeki vasıtalar ile de kurulabileceğinden, her mesafeli sözleşme elektronik sözleşme değildir.

2.4.4.3- Unsurları

Mesafeli sözleşme ile ilgili tanımlardan da yola çıkarak, bir sözleşmenin mesafeli sözleşme sayılabilmesi için gereken unsurları aşağıdaki gibi sıralayabiliriz.

2.4.4.3.1- Tarafların Fiziksel Olarak Karşı Karşıya Gelmemesi

Mesafeli sözleşmenin varlığı için aranacak ilk unsur, tarafların sözleşmenin kurulum aşamasında fiziksel olarak karşı karşıya gelmemesidir. TKHK'un 9/A maddesinde yer alan *“karşı karşıya gelinmeksizin”* ibaresinden, tarafların fiziksel olarak

karşı karşıya gelmemesi anlaşılmalıdır. Zira telekonferans, chat gibi mesafeli iletişim araçları ile kurulan sözleşmelerde taraflar, fiziksel olarak olmamakla birlikte zaman itibarıyla karşı karşıya bulunmaktadır. Şu halde bu şekilde kurulan sözleşmeleri yasanın amacına aykırı olacaktır²⁶⁴.

Buradaki taraf kavramı, satıcı/sağlayıcı ve tüketiciden başka, bunların temsilcileri ve malların tanıtımını yaparak siparişlerin yapılmasını sağlayan araçları da kapsamaktadır²⁶⁵. Yine 97/7/AT sayılı AB yönergesinin tanımlar kısmında tüketici tanımı içerisinde sadece gerçek kişiler yer almış iken(m.2/2), hukukumuzda tüketici tanımı içerisinde gerçek kişilerin yanında tüzel kişilere de yer verilmiştir(TKHK m.3/e).

2.4.4.3.2- Sözleşmenin Kurulmasında Mesafeli İletişim Araçları Kullanılması

Mesafeli sözleşmeleri diğer sözleşmelerden ayıran ve ayrıcalıklı kılan ikinci unsur ise, fiziksel olarak karşı karşıya bulunmayan tarafların, sözleşmenin kurulmasında münhasıran bir veya birden fazla mesafeli iletişim aracından faydalanmalarıdır.

Mesafeli iletişim aracı, 97/7/AT sayılı AB yönergesinde “*sağlayıcı ve tüketicinin aynı anda fiziksel olarak bir arada bulunmaları gerekmeksizin, sözleşmenin taraflar arasında kurulmasına imkan tanıyan her türlü araç*” olarak tanımlanmıştır. Görüldüğü üzere mesafeli sözleşmenin kurulması açısından, elektronik sözleşmelerden farklı olarak, sözleşmenin kurulumunda modern iletişim araçlarının kullanılması ile geleneksel yöntemlerin kullanılması arasında bir fark ön görülmemiştir. TKHK’da da benzer düzenleme yapılmış, hatta “diğer iletişim araçları” tabiri ile de gelecekte ortaya çıkabilecek iletişim araçları da kapsama alınmıştır.

Yine mesafeli sözleşmenin kurulması için, tek iletişim aracının kullanılmasına da gerek yoktur. Sözleşmenin kurulması aşamasında birden fazla iletişim aracı da kullanılabilir. Örneğin, internet ortamında yapılan bir icaba karşılık, kabul beyanı telefonla veya başka bir iletişim aracı ile gönderilebilir. Yeter ki sözleşmenin kurulmasına imkan sağlasın.

²⁶⁴ Yıldırım, s.144

²⁶⁵ Yıldırım, s.144

2.4.4.3.3- Organize Bir Mesafeli Sürüm Sisteminin Varlığı

TKHK ve Yönetmelikte yer alan tanımda böyle bir şart açıkça öngörülmemiştir. Ancak 97/7/AT sayılı AB yönergesinde mesafeli sözleşme tanımı içerisinde, sağlayıcının mesafeli sürüme özgü olarak organize ettiği bir satış veya hizmet ağı olması gerektiği açıkça belirtilmiştir. Hukukumuzda da bu kuralın kabulü yasanın amacına ters düşmemektedir²⁶⁶.

Buna göre, mesafeli sözleşmelere ilişkin tüketiciyi koruyucu hükümlerin uygulanabilmesi için, satıcı/sağlayıcının mal satımı veya hizmet sunumuna ilişkin faaliyetlerinin tamamı veya bir kısmını mesafeli sürüme özgülemiş olarak, sistemli bir satış veya sunum ağı içerisinde yürütüyor olmalıdır. Bu anlamda satıcı ve tüketici arasında tesadüfen iletişim araçları kullanılarak kurulan sözleşmeler bu hükümlerin koruma alanı içerisinde bulunmayacaktır. Yine sağlayıcının pazarlama yöntemi olarak, sadece mesafeli sürümü kullanması zorunlu değildir²⁶⁷. Günümüzde de yaygın olarak kullanıldığı üzere, satıcı/sağlayıcı bir yandan geleneksel yöntemlerle satış yapmaya devam ederken, bir yandan da çeşitli iletişim araçlarını mesafeli sürüme özgüleyerek mesafeli sürüm yöntemi ile de pazarlama yapabilecektir. Önemli olan mesafeli sürüme ilişkin organize bir sistem kullanıyor olunmasıdır. Satıcı/sağlayıcının mesafeli satış yapmak amacıyla, personel istihdam etmesi, web sitesi oluşturması, web sitesine veya gazeteye ilan vermesi gibi haller, organize bir sistemin var olduğu anlamına gelecektir²⁶⁸.

2.5- Elektronik İmzanın Türk İspat Hukukundaki Yeri

Türk İspat Hukuku sisteminde, “*Kanuni Delil sistemi*” mevcuttur. Bu sisteme göre hâkim, Hukuk Usulü Muhakemeleri Kanunu’nda sayılan ve “*Kesin Delil*” olarak da adlandırılan, ikrar (HUMK m. 236), kesin hüküm (HUMK m. 237), senet (HUMK m. 286 vd.) ve yemin (HUMK m. 377 vd.) delillerinden biri ile ispat edilen bir vakıayı,

²⁶⁶ Büyükay, s.4; Yıldırım, s.146

²⁶⁷ Büyükay, s.4; Yıldırım, s.147

²⁶⁸ Büyükay, s.4

dođru olarak kabul etmek zorundadır. Yani hakim, bu delillerle bađlıdır ve bu delilleri takdir yetkisi yoktur²⁶⁹.

Hukuk Usulü Muhakemeleri Kanunumuz, kesin deliller kategorisi yanında, ayrıca “*Takdiri Delilleri*” de düzenlemektedir. Takdiri deliller ile hâkim, kesin delillerin aksine bađlı deđildir. Bu delillerle ispatlanan bir vakıanın dođru olup olmadığını serbestçe takdir eder. Bunlar; tanık (HUMK m. 245 vd.), bilirkiři (HUMK m. 275 vd.), keřif (HUMK m. 363 vd.) ve özel hüküm sebepleridir (HUMK m. 367)²⁷⁰.

Hukuk Usulü Muhakemeleri Kanununun 288/1 inci maddesi hükmüne göre; “*Bir hakkın doğumu, düşürülmesi, devri, deđiřtirilmesi, yenilenmesi, ertelenmesi, ikrar ve itfası amacıyla yapılan hukuki işlemlerin, yapıldıkları zamanki miktar veya deđeri 400 YTL’ ni geçtiđi takdirde senetle ispat olunması gerekir.*” Senetle (veya kesin delille) ispat zorunluluđu olarak adlandırılan bu kurala göre, yapıldıkları zamanki miktar veya deđeri 400 YTL’ ni geçen hukuki işlemlerin kanunda sayılan istisnalar saklı kalmak koşuluyla, kesin delillerden biri ile ispatlanması zorunludur. Bu hukuki işlemler, kural olarak tanıkla ispat edilemez. Senetle (veya kesin delille) ispat zorunluluđu hakkındaki ikinci ana kural ise, “*senede karřı senetle ispat zorunluluđudur.*” Bu kurala göre ise senede bađlı olan her çeřit iddiaya karřı savunma olarak ileri sürülen ve senedin hüküm ve kuvvetini ortadan kaldıracak veya azaltacak nitelikte bulunan hukuki işlemler, 400 YTL’ dan az miktara iliřkin olsa bile, tanıkla ispat olunamaz.

5070 sayılı Elektronik İmza Kanunundan önce mevzuatımızda bu yönde bir düzenleme olmadığından, elektronik ortamda yapılan işlemlerin güvenliđi ve hukuki bađlayıcılıđı sorunu ile karřılařılmakta idi. Zira, elektronik ortamda bulunan kayıt ve belgelerin ispat hukuku açısından senet niteliđinde kabul edilmemesi ve yazılılık işlevini de yerine getirmediđi kabul edilmekle yazılı delil bařlangıcı dahi kabul edilmemesi söz konusu olmaktaydı. Bu tür bir kayıt ve belgeler hakkında taraflar delil sözleşmesi yapmamıř iseler, bu belgeler ancak, ses bandı ya da manyetik bantlar gibi kanunda sayılmayan ve özel hüküm sebepleri olarak belirtilen takdiri delil kabul

²⁶⁹ Kuru, s. 1398

²⁷⁰ Kuru, s. 1399

edilmektedir²⁷¹. HUMK'nun 288 ve 290. maddeleri de dikkate alındığında bu nitelikteki belgelerle ispat işlevini gerçekleştirmek neredeyse imkânsız bulunmaktaydı.

Elektronik İmza Kanunu ile birlikte el ürünü imza ile güvenli elektronik imza eşdeğerde kabul edilmiş ve elektronik imza ile tanzim edilen belgelerin senet hükmünde olacağı açıkça belirtilmiştir. 5070 sayılı Kanun bu eşitliği güvenli elektronik imza için kabul etmiş ve bunu da açıkça ifade etmiştir(EİK. m.5). Kanunda güvenli elektronik imzanın yapılacak hukuki işlemler açısından geçerlilik ve ispat şartını sağlayacağını belirtmesi, elektronik imzaların güvenli elektronik imza kavramı ile sınırlandırılması sonucunu beraberinde getirecektir²⁷². Bu itibarla her elektronik imza, klasik imza ile eş değerde tutulmamaktadır²⁷³. Yani, e-mail kullanırken kendimize göre, oluşturduğumuz imzalar veya ilgili sitenin oluşturulmasına imkan verdiği imzalar veya bazı sitelerin güvenilirliği artırmak için kendilerine göre oluşturdukları imza niteliğindeki şekiller, rakamlar, şifreler vs. bütün bunlar elektronik imza kanununun kapsamı dışındaki uygulamalardır ve bu tür imzalar hukuksal koruma altında olmayıp, klasik imza ile elbette eş tutulamaz. Kanunun bir elektronik imzayı, klasik imzayla eş değerde tutabilmesi için, öncelikle elektronik imzanın kanunda tanımlanan nitelikte olması gerekir. Yani kanunda belirtilen sertifika vermeye yetkili kurumlar tarafından verilmiş güvenli elektronik imza olması gerekir.

Elektronik imza ile imzalanmış belgelerin uygulamada ispat vasıtası olarak kullanılması durumunda hangi delil kategorisinde olacağı konusunda doktrinde çok tartışmalar yapılmıştır. Kimi zaman özel hüküm sebeplerinde takdiri delil olarak değerlendirilebileceği söylenmiş, kimi zamanda el ürünü imza ile aynı hukuki güvenceyi sağlayabilmesi nedeniyle kesin delil olarak değerlendirilebileceği belirtilmiştir²⁷⁴. Bu tartışmalar üzerine 5070 sayılı Kanunda 1086 sayılı Kanunun 295 maddesine ek olarak bir madde getirilmiştir. Elektronik İmza Kanunu'nun 23 üncü maddesinin 2 nci fıkrasında Hukuk Usulü Muhakemeleri Kanunu'nun 295 inci maddesine ek olmak üzere 295/A maddesi eklenmiş ve bu maddeye göre, “*Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar* ” denilmiştir (EİK. m.23).

²⁷¹ Pekcanitez, s.425

²⁷² Falcioğlu, s.96

²⁷³ Ergün, s.63

²⁷⁴ Değişik görüşler için bkz. Pekcanitez, s.390; Arıkan, s.134-135; Acır, s.47

Yukarıdaki açıklamalar da göz önüne alındığında; senetle ispat zorunluluğu olan, 400 YTL’ni aşan her türlü hukuki işlemin ispatında, elektronik olarak imzalanmış belgeler kullanılabilir. Yine bu miktarın altında dahi olsa, senede veya bu niteliği haiz elektronik belgeye dayanan hukuki işlemlerin aksi ancak bu nitelikteki başka bir belge ile ispatlanabilecektir²⁷⁵.

Yeni Hukuk Usulü Muhakemeleri Kanunu tasarısının “Adî senetlerin ispat gücü” başlıklı 209 uncu maddesi “*Mahkeme huzurunda ikrar olunan veya mahkemece inkâr edenden sadır olduğu kabul edilen adî senetler, aksi ispat edilmedikçe kesin delil sayılırlar.*

“Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir.

Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını re’sen inceler”. Şeklinde düzenlenmiştir.

Bu hükme göre de güvenli elektronik imza ile oluşturulan elektronik ortamdaki veriler doğrudan senet olmamakla birlikte, senet kuvvetinde kabul edilmiştir. Ayrıca, belgenin üst kavram olarak kabul edilmiş olması, ilerde meydana gelecek teknik gelişmelere daha kolay ayak uydurulmasını ve bu yönde düzenleme yapılmasını mümkün kılacak niteliktedir. Zira herhangi bir veri taşıyıcısı, bugün anladığımız anlamda senet ya da güvenli elektronik imza ile imzalanmış elektronik verilerden daha kuvvetli bir ikna gücüne ve güvenliğe sahipse, onun kesin delil olarak kabulü de kolaylaşacak, bunun için kanunun sisteminin bozulması da gerekmeyecektir. İkinci fıkra ile güvenli elektronik imzalı belgeler, adi senet niteliğinde kabul edilmiştir. 1086 sayılı Kanunda 5070 sayılı Kanunla yapılan değişiklikle medeni yargılama hukukumuzda giren elektronik imzalı belgelerin, delil gücü konusundaki tereddüdün, bu düzenlemeyle ortadan kaldırılması amaçlanmıştır. Ancak, elektronik imzalı belgelerden sadece, güvenli elektronik imza ile oluşturulanlar adi senet kuvvetinde sayılmış, diğer elektronik belgeler ya da güvenli elektronik imza dışında imzalanarak oluşturulmuş elektronik belgeler adi senet olarak kabul edilmemiştir.

²⁷⁵ İnal, s.155; Keser Berber (Şekil), s.12; Sevinç, s.1; Pekcanitez, s. 398; Orta, s.33; Rüssmann, s.346

Kanımızca, güvenli elektronik imza ile oluşturulan belgeler için doğrudan adi senettir ifadesi yerine, adi senet hükmündedir ifadesinin tercih edilmesi doğrudur. Zira, güvenli elektronik imza, dar ve teknik anlamda adi senet değildir. Bu tür belgelerin oluşturulması ve ibrazı adi senetlerden farklılık gösterdiği gibi, inkârı halinde uygulanacak hükümler de farklıdır. Bu sebeple, adi senetle aynı ispat gücüne sahip olmakla birlikte, doğrudan adi senet olarak kabulü doğru görülmemiştir. Nitekim adi senetlerin inkârı ile elektronik belgelerin inkârı hâlinde uygulanacak usul ayrı maddelerde düzenlenmiştir.

Üçüncü fıkrada, hâkime bir yetki verilmiştir. Elektronik imzalı belgelerin güvenli elektronik imza ile oluşturulup oluşturulmadığını hâkim kendiliğinden inceleyecektir. Zira bir elektronik belge, ancak güvenli elektronik imza ile oluşturulması halinde adi senet kuvvetinde delil olma niteliğine sahiptir. Bu fıkra, ispat ve delillere ilişkin genel hükümler içinde yer alan, bir delilin geçerli ve caiz bir delil olup olmadığını inceleme yetkisinin mahkemede olmasının bir sonucu olarak yer verilmiştir. HUMK tasarısının “Güvenli elektronik imzalı belgenin inkârı” başlıklı 214 üncü maddesi ise “*Güvenli elektronik imzayla oluşturulmuş verinin inkârı hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılmamışsa, bilirkişi incelemesine başvurulur*” şeklindedir. Bu hüküm elektronik imzanın inkârı halinde mevcut düzenlemedeki izlenecek yöntemi belirtmesi açısından yerindedir. Mevcut düzenlemedeki HUMK 308 inci maddesinin kıyasen uygulanacağı hükmü kanımızca yetersizdir. Çünkü maddenin gerekçesinde de bahsedildiği üzere, güvenli elektronik imzayla oluşturulan verinin inkârı hâlinde, bu iddianın incelenmesi, diğer belgelerdeki sahtelik incelemesinden farklılık gösterecektir. Zira güvenli elektronik imzayla oluşturulan verinin doğruluğu konusundaki tereddüdün giderilmesi, ancak teknik bir incelemeyle mümkündür. Bu sebeple, güvenli elektronik imzalar konusundaki iddialar, konunun uzmanı bilirkişilerin yapacağı inceleme ile açıklığa kavuşturulabilir. Bilirkişi incelemesi yapılmasına karar verilmeden önce, inkârda bulunan tarafın dinlenmesi ve inkâr eden tarafın yapacağı açıklamanın mahkemede bir kanaat uyandırması halinde bilirkişi incelemesine yaptırılmayacak, tarafın dinlenmesinden sonra da kanaat oluşmazsa, bu takdirde bilirkişi incelemesi yaptırılacaktır. Elektronik imzalama işleminin teknik yönü ve imza oluşturma verisini yetkili veya yetkisiz elinde

bulunduran kişinin imza sahibi adına imza atmasının mümkün oluşu düşünüldüğünde bu hükmünde yerinde olduğu görülmektedir.

2.5.1- Güvenli Elektronik İmza İle İmzalanmış Verilerin Delil Değeri

Bilindiği üzere, bir hukuk normunun uygulanması, o normla düzenlenen, yani kendisine hukuksal sonuç bağlanan, olumlu veya olumsuz vakıaların somut olarak gerçekleşmiş bulunmasına bağlıdır. Bir başka ifade ile hukuk normunun soyut olarak düzenlediği ve kendilerine hukuksal sonuç bağladığı vakıalar, somut olarak gerçekleşmiş bulunmadıkça, o norm uygulanamaz. Dava konusu hakkın ve buna karşı yapılan savunmanın dayandığı vakıaların var olup olmadıkları hakkında mahkemeye kanaat verilmesi işlemi ise “ispat” olarak adlandırılır.

Hukukumuz bakımından kanuni ve takdiri ispata birlikte yer veren karma bir sistemin geçerli olduğu söylenebilir. Zira, her ne kadar hukuki işlemler alanında kesin delillerle ispat geçerli ise de, bu düzenleme kamu düzenine ilişkin değildir ve ayrıca kanuni ispat sistemine, gene kanun tarafından geniş ölçüde istisnalar tanınmıştır (HUMK m. 289, 293 ve 294).

Hukuk Usulü Muhakemeleri Kanunu m. 288 vd. hükümleri ile hukuki işlemler bakımından senetle (kesin delille) ispat zorunluluğu kabul edilmiştir. Bu hükümlerde açıkça düzenlenen kanuni ispat halleri dışında delil serbestisi esası geçerlidir.

Delil, Hukuk Usulü Muhakemeleri Kanunumuzda, “*davanın halline tesir edebilecek münazaalı hususların ispatı için başvuru olan vakıalar*” şeklinde tarif edilmiştir (m. 238/I).

Kanun bir yandan güvenli elektronik imzanın elle atılan imza ile aynı hukuki sonucu doğuracağını düzenlemişken (m. 5/1), diğer yandan m. 22 ve m. 23’te konuya ilişkin açık düzenleme getirmiştir.

Hukuk Usulü Muhakemeleri Kanununun 295/A maddesine göre, güvenli elektronik imza ile imzalanmış verilerin senet hükmünde olduğu belirtilmiştir. Buna göre, yargılamada taraflarca, güvenli elektronik imzalı bir belge ibraz edildiği takdirde,

bu belge “kesin delil” olarak hâkimi bağlayacaktır. Bu belgelere, resmi senetlere yaklaşır bir nitelik verildiği belirtilmelidir. Nitekim bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.

Hâkimin, yargılamada ibraz edilen elektronik belgenin, güvenli elektronik imza ile imzalanıp imzalanmadığı hususunun kendiliğinden araştırması gerekir. Aksi halde sadece tarafın beyanı üzerine, ibraz edilen herhangi bir elektronik belgeye senet niteliği atfedilmiş olacaktır. Hâkim keşif ve bilirkişi incelemesine re’sen karar verebileceği için, ibraz edilen elektronik belgedeki imzanın güvenli elektronik imza olup olmadığı bu suretle incelenecektir²⁷⁶.

Hâkimin kağıda dayalı senetlerde bu şekilde bir inceleme yapmasına gerek yoktur. Çünkü, senedin, senet niteliği gözle görülebilir. İbrahim edilen senet, ispat edilmek istenen hukuki işlem hakkında tam bir bilgiyi içeriyorsa ve kendisine karşı senet ileri süren tarafından imzalanmış ise hâkim, bu belgeyi senet olarak kabul edecektir. Böylece iddianın ispatı konusunda ibraz edilen kesin delil sebebiyle kanaate varacaktır.

Buna karşılık, elektronik belgelerde durum farklıdır. İbrahim edilen bir elektronik belgenin, kanunun saydığı şartları haiz bir belge ve dolayısıyla senet olup olmadığı hâkim tarafından gözle görülebilir ve değerlendirilebilir durumda değildir. Bundan başka, hâkimin bu konudaki teknik bilgi eksikliği de söz konusudur.

Doktrinde Konuralp, HUMK m. 295/A hükmünün dolaylı olarak elektronik senedi düzenlediğini, elektronik senedin tanımının ise yapılmadığını, ancak elektronik senedin tanımının “bir kimsenin kendi güvenli elektronik imzası ile meydana getirdiği ve aleyhine delil olarak kullanılma amacı taşıyan ve bilgisayar ortamında varlığını sürdürebilen elektronik veriler” şeklinde yapılabileceği görüşündedir²⁷⁷.

Kanımızca, kanun koyucu elektronik senet tabirini bilinçli olarak kullanmaktan kaçınmış ve sadece, elektronik verilerin senet hükmünde olduğunu kabul etmekle yetinmiştir. Kanun koyucunun böyle bir kabulündeki sebep, elektronik imzanın, senetteki imza kadar müşahhas olmamasıdır²⁷⁸. Buradaki müşahhaslıktan kastedilen

²⁷⁶ Erturgut, s.257

²⁷⁷ Konuralp, s.5

²⁷⁸ Deliduman, s.8

imzanın kişiye aidiyeti ve gerçekliği konusundaki ihtimal derecesi olmayıp, imzanın somut olarak algılanabilir olmasıdır.

Kanımızca, burada asıl tartışılması gereken husus elektronik imzalı olduğu için senet hükmünde sayılan belgelerin adi senetlerin mi yoksa resmi senetlerin mi hüküm ve sonuçlarını doğuracağıdır.

Resmi senetler, resmi bir makamın katılımı ile düzenlenen senetlerdir. Resmi makamların katılımı düzenleme biçiminde olabileceği gibi onaylama biçiminde de olabilir. O halde resmi makamın katılımı yalnızca imza ve tarih onaylaması suretiyle de olsa, senet ispat hukuku anlamında resmi bir senettir²⁷⁹.

Kanımızca elektronik imzalı verilerin adi senet mi yoksa resmi senet mi sayılacağı büyük oranda elektronik sertifika hizmet sağlayıcılarına atfedilecek niteliğe göre belirlenecektir. Bizce elektronik imza ile imzalanmış verilerin senet hükmünde sayılmasının, onaylama biçiminde düzenlenmiş resmi senetler olarak kabul edilmesi ve elektronik imza ile imzalanmış verilerin içeriğinin aksinin, elektronik imzanın ve tarihin ise sahteliğinin ispat edilebilmesi gerekir.

2.5.2- Elektronik İmza İle İmzalanmamış Verilerin Delil Değeri

Elektronik İmza Kanunu sadece güvenli elektronik imzanın unsurlarını ve hukuki sonuçlarını düzenlemiş olup güvenli olmayan, başka bir ifade ile, güvenli elektronik imzanın dışında kalan elektronik imzanın hukuki niteliğini düzenlememiştir.

Kanunun güvenli olmayan elektronik imzayı ve hukuki sonuçlarını düzenlememiş, olması bilinçli olarak bırakılmış bir boşluktur. Çünkü Avrupa Birliğinin 93 sayılı Direktifinin 5 inci maddesinin 2 nci bendine göre, üye ülkeler her türlü elektronik imzanın delil olarak kullanılabilmesine olanak sağlamayı üstlenmişlerdir. Buna göre, güvenli olmayan elektronik imzaya da, güvenli elektronik imza kadar olmasa bile, bir ölçüde caiz delil sayılma özelliği tanınmak istenmiştir²⁸⁰. Bundan çıkan sonuç güvenli elektronik imza dışında kalan, başka bir ifade ile güvenli olmayan

²⁷⁹ Ulukapı, s.2; Deliduman, s.8

²⁸⁰ Konuralp, s. 4.

elektronik imzalarla imzalanmış veya hiç imzalanmamış elektronik veriler de delil olarak kullanılabilir.

Mevcut hukuki düzenlememiz açısından, Pekcanitez, Konuralp ve Deliduman'a göre, güvenli olmayan elektronik imzalar kanuni (kesin) delil olmayacağından takdiri delil olarak değerlendirilebilir ve güvenli olmayan elektronik imza ile imzalanmış veya elektronik imza ile imzalanmamış elektronik veriler kanunda düzenlenmemiş deliller kategorisine girerler²⁸¹.

Güvenli elektronik imza ile imzalanmamış elektronik veriler takdiri delil olarak kabul edilebileceğine göre, bu konudaki usul kuralı dayanağımız hangisi olacaktır. İlk akla gelen HUMK m. 367'de düzenlenmiş olan "özel hüküm sebepleri"dir. HUMK m. 367 hükmü, "*Tahkikat hakimi senetsiz ispatı caiz olan davalarda re'sen veya talep üzerine bu kanunda düzenlenmemiş olan diğer hüküm sebeplerinin istima ve tetkikatına karar verebilir ve bu husus hakkında iki tarafı istima ettikten sonra tebeyyün edecek hale göre iktiza eden tedbirleri ittihaz eder*" şeklindedir. O halde açıkça görülmektedir ki, güvenli elektronik imza ile imzalanmamış elektronik verilerin HUMK m. 367 kapsamında değerlendirilmesi mümkündür.

Sorunun çözümünde bir diğer çıkış yolu olarak da Hukuk Usulü Muhakemeleri Kanunu m. 287/II ve m. 289 hükümlerinde düzenlenmiş olan delil sözleşmesine ilişkin düzenleme görülebilir. Zira hukukumuzda geçerli olan kanuni delil sisteminin sonucu olarak, kanunun belli bir delille ispatı aradığı vakıaların ispatı için başka delillerin kullanılması mümkün değildir. Bu nedenle kanun, taraflara, belli vakıaların belli delillerle ispatı konusunda anlaşma yapabilme imkânı vermiştir. Bu durumda taraflar arasındaki delil sözleşmesine göre sözleşme konusu vakıanın ispatında başka delillerin kullanılmayacağı hükme bağlanmıştır (HUMK m. 287/II). Delil sözleşmesi belli bir vakıanın, belli bir delil veya diğer deliller yanında kararlaştırılan türdeki deliller ile ispat edilebileceği konusunda taraflar arasında davadan önce veya dava sırasında yapılan usulü bir sözleşmedir²⁸². Ancak hemen belirtelim ki, tarafların elektronik verilerin delil olarak kullanılabilmesine ilişkin olarak yaptıkları delil sözleşmesi de çoğunlukla elektronik ortamda gerçekleşeceğine göre, burada artık elektronik imza ile imzalanmış

²⁸¹ Pekcanitez, s. 424; Deliduman, s.9; İnal'a göre ise bu belgeler yazılı delil başlangıcı sayılmalıdır. Bkz. İnal, s.155

²⁸² Kuru, C.III, s.2881; Pekcanitez, s. 420

elektronik verilerdeki elektronik imzanın güvenli elektronik imza olup olmasına göre getirilecek çözüm de farklı olacaktır.

Galiba bu konuda en kolay çözüm sunan husus, güvenli olmayan elektronik imza ile imzalanmış olan verilerin delil olarak kullanılmasına karşı tarafça muvafakat edilmesidir.

Hukuk Muhakemeleri Usulü Kanunu tasarısının kabulü halinde ise durum değişecektir. Zira, tasarı ile senet kavramından ayrı ve kapsamlı olan belge kavramı ispat sistemine dahil olmakta ve belgenin delil başlangıcı olma özelliği bulunmaktadır. Tasarının 203 üncü maddesine göre “*uyuşmazlık konusu vakıaları ispata elverişli, yazılı veya basılı metin, senet, çizim, plân, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları*” belge kapsamında değerlendirilmektedir. 206 ncı maddeye göre ise, “*söz konusu hukukî işlemi muhtemel gösteren ve kendisine karşı ileri sürülen kimse veya temsilcisi tarafından verilmiş veya gönderilmiş*” belge delil başlangıcı sayılmakta ve bu konuda tanık dinlenmesi mümkün olmaktadır. Öyleyse tasarının kabulü halinde güvenli elektronik imza ile imzalanmamış elektronik belgeler delil sözleşmesine veya karşı tarafın muvafakatine lüzum olmaksızın takdiri delil olan delil başlangıcı (mevcut düzenlemede yazılı delil başlangıcı) olarak kabul edilecektir.

5070 sayılı Elektronik İmza Kanunu’nun 23 üncü maddesi ile düzenlenen HUMK 295/a hükmü gereğince, güvenli elektronik imza ile oluşturulmuş veriyi imzaladığı iddia edilen taraf, imza inkârında bulunursa, HUMK’nun 308 inci maddesi kıyas yoluyla uygulanacaktır. Bu maddenin kıyas yoluyla uygulanması için, yine öncelikle elektronik belgenin güvenli elektronik imza ile imzalanmış olup olmadığının tespiti gerekir. Zira güvenli elektronik imza dışında kalan imzalar bakımından, bu belgeler senet sayılmadığı için, imza incelemesine ilişkin kanunun 308 inci maddesinin uygulanması mümkün olmayacaktır. İmza kontrolünde hem belgenin değiştirilip değiştirilmediğinin hem de imzaladığı iddia edilen kişiden sadır olup olmadığının incelenmesi gerekir. Bu sebeple hem imzanın kontrolü hem de sertifikanın kontrolü gerekecektir.

Yine, Hukuk Muhakemeleri Usulü Kanunu tasarısının “Tarafların belgeleri ibrazı zorunluluğu” başlığını taşıyan 223 üncü maddesi, (1) *Taraflar, kendilerinin veya karşı tarafın delil olarak dayandıkları ve ellerinde bulunan tüm belgeleri mahkemeye ibraz etmek zorundadırlar. Elektronik belgeler ise, belgenin çıktısı alınarak ve talep edildiğinde incelemeye elverişli şekilde elektronik ortama kaydedilerek mahkemeye ibraz edilir.*

(2) *Ticari defterler gibi devamlı kullanılan belgelerin sadece ilgili kısımlarının onaylı örnekleri mahkemeye ibraz edilebilir.* Şeklinde düzenlenmiştir.

Bu maddede elektronik belgelerin nasıl ibraz edileceği ayrıca belirtilmiştir. Zira elektronik belgelerin ibrazı diğer belgelerin ibrazından farklıdır. Bu sebeple, elektronik belgenin kâğıt üzerine çıktısı alınarak ve talep edildiğinde de incelemeye elverişli şekilde elektronik ortama kaydı yapılmak suretiyle mahkemeye ibrazı gereklidir. İncelemeye elverişli şeklin ne olduğu, o günkü teknik imkânlarla uygun olarak tespit edilecektir. Burada ibraz edilecek elektronik belgenin, güvenli veya basit elektronik imza ile imzalanmış olup olmaması önemsizdir. Güvenli elektronik imza ile imzalanmamış ya da hiç elektronik imza taşımayan bir elektronik belgenin de delil olarak ibrazı gerekebilir. Belgenin ibrazı ile onun delil değeri ayrı değerlendirildiğinden böyle bir ayrıma gidilmemiştir²⁸³.

2.6- Elektronik İmza ve Hukuki Sorumluluk

Sorumluluk, uyulması gereken hukuk kurallarına aykırı davranışın hesabını verme durumudur. Kişi, kural olarak, başkalarına verdiği zararlardan hukuken sorumludur. Hukukumuzda sorumluluğun sözleşme ve kanun olmak üzere iki kaynağı bulunmaktadır. Taraflar arasında sözleşme ilişkisinin bulunduğu veya bir başkası ile mevcut sözleşme ilişkisinden bir biçimde yararlanıldığı yada sözleşme olmamasına rağmen somut olayın özelliklerinin sözleşme var imiş gibi tarafların korunması amacıyla uygulandığı hallerde, sorumluluğun kaynağı sözleşmedir. Diğer hallerde ise sorumluluğun kaynağı kanundur ve bu kaynak da kendi içerisinde “haksız fiil, sebepsiz zenginleşme ve fedakârlığın denkleştirilmesinden doğan sorumluluk” olmak üzere üçe

²⁸³ HUMK tasarısı gerekçesi, m.223

ayrılmaktadır. Haksız fiil sorumluluğu ise kendi arasında kusur sorumluluğu, sebep sorumluluğu ve tehlike sorumluluğu olarak ayrılmaktadır²⁸⁴.

İmza ise, yukarıda da açıklandığı üzere, her türlü resmi veya özel belgenin geçerlilik kazanması ve bu itibarla kişilere hak kazandırıp, sorumluluk yüklemesi bakımından zorunlu olan en önemli unsurlar arasındadır. İmza ile imzalayanın kimliği ve imzalı belgenin içeriğinin imzalayanca kabul edildiği başta olmak üzere pek çok fonksiyon gerçekleştirilir. İmzasız bir belge kural olarak sahibine hak veya yükümlülük getirmediği gibi imzalı bir belge de sahibine belge içeriğine göre hak kazandırır ve sorumluluk yükler. Elektronik imza ve el yazısı ile imza hukuki açıdan aynı niteliğe sahip olduklarından ait oldukları belgeler açısından da aynı sonucu doğururlar. Bu bakımdan ıslak imza ve elektronik imza kişilere hak sağlayıp, sorumluluk yükleyen birer olgudur. Bununla birlikte elektronik imzanın ıslak imzadan farklı olarak imza oluşturma aracı olarak nitelendirilen bir cihaz aracılığı ile atılması nedeniyle elektronik imzanın sahibi yanında, imza sahibi adına bu cihazı hazırlayan ve bir sertifika ile ilişkilendiren sertifika hizmet sağlayıcılarının sorumluluğu söz konusu olmaktadır. Aşağıda bu sorumluluklardan bahsedilecektir.

2.6.1- Elektronik İmza Sahibinin Sorumluluğu

Daha önce de ifade edildiği gibi kişinin el yazısı ile imzası kendine özgü olup genellikle benzersizdir ve insanın el yazısı düşüncesinin grafik ifadesi olması nedeniyle kişiliği ve karakteri ile bütünlük gösterir. Ancak elektronik imzada durum farklıdır. Gerçekten elektronik imzanın oluşturulmasına yarayan ve imza oluşturma verisi olarak tanımlanan veriler, bir yazılım veya donanımdan ibaret olan "imza oluşturma aracı" ile oluşturulmaktadır. Bu imza oluşturma aracı ise genelde akıllı kart olarak nitelendirilen çipli kart veya akıllı çubuk olarak nitelendirilen ve içerisinde çip bulunan USB aracı (e-token) olarak karşımıza çıkmaktadır. Dolayısıyla bu aracın ve aracı kullanmak için gerekli şifrenin, bir başka kişi tarafından ele geçirilmesi ve kullanılarak elektronik bir belgenin bu kişi tarafından sanki imza sahibi tarafından imzalanıyormuş gibi imzalanması mümkündür. İşte, imzalayanın gerçek imza sahibi, yani belgeyi imzalamış olarak görünen kişi olmaması durumunda elektronik imza sahibinin hukuki sorumluluğu ne olacaktır?

²⁸⁴ Uygur, s.71; Karahasan, s.61; Yıldırım, s.264; Orta, s.127

Bir imza oluřturma aracının, imza sahibinden bařka bir kiřinin elinde bulunması hukuken iki řekilde gerekleřebilir. Bu durum ya imza sahibinin iradesi ile gerekleřir, ya da uüncü kiři imza oluřturma aracını imza sahibinin iradesi dıřındaki bir řekilde ele geirmiř olabilir.

İmza oluřturma verisinin uüncü bir kiři tarafından kullanılarak imza sahibiyymiř gibi imza atılması durumunda, bu uüncü kiřinin hibir řekilde sözleřmenin tarafı olamayacađı aıktır. Bununla beraber imza sahibinin imza oluřturma aracının kullanımı nedeniyle hukuken sorumlu olup olmayacađını, temsil kurallarının kıyasen uygulanması ve kusur sorumluluđu hükümleri yönünden deđerlendirilmek gerekecektir.

Öncelikle imza sahibi, imza oluřturma aracını belli bir iřlemin yapılması amacıyla diđer bir kiřiye vermiř ve bu kiři de o iřlemi yapmıř ise böyle bir durumda, bu kiři temsil yetkisi ile hareket etmektedir. Dolayısıyla bu iřlemden dođan haklar ve borlar, imza sahibine ait olacaktır (BK. m. 32/1).

Öte yandan, imza oluřturma aracı, imza sahibi tarafından diđer bir kiřiye verilmekle birlikte bu kiři temsil yetkisinin sınırlarını ařmıř veya hi yetkili olmadıđı bir konuda iřlem yapmıř olabilir. Bu durumda yetkisiz temsil durumu söz konusudur. Yetkisiz temsil durumunda kural olarak temsil olunan sözleřme ile bađlı deđildir. Fakat sözleřmeye icazet vererek sözleřmenin geerli olarak kendisi bakımından hüküm ifade etmesini sađlayabilir(BK. m.38). Burada imza sahibi yetkisiz temsilcinin yaptıđı bu iřleme icazet vererek sözleřmenin geerli olarak kurulmasını sađlayabilir. Fakat icazeti bulunmasa bile, bu durumda güven prensibi geređince imza sahibinin hukuki görünüř sorumluluđu bulunmaktadır²⁸⁵. Gerekten BK. m. 38 hükmüne rađmen, güven prensibinin haklı gösterdiđi istisnai hallerde yetkisiz temsilci tarafından yapılan hukuki iřlemler, adına hareket edilen kimse için de bađlayıcı olabilmektedir²⁸⁶.

Burada imza sahibi, imza oluřturma aracını vermekle imzayı atan kiřinin uüncü kiřiler nezdinde sanki imza sahibinin kendisi veya yetkili temsilcisiymiř gibi görünüřüne bilinli olarak sebep olmaktadır. İřte bu durumu kendisi yaratmıř olan

²⁸⁵ İnal, s.152

²⁸⁶ Tekinay-Akman-Burođlu-Alttop, s.207; Eren, s.406; İnal,s.152

imza sahibinin, (icazeti bulunmasa bile) sözleşme ile bağı olduğunu kabul etmek gerekecektir.

Diğer durum ise imza oluşturma aracının imza sahibinin iradesi dışında üçüncü bir kişinin eline geçmesi durumudur. Bu durum değişik şekillerde ortaya çıkabilmektedir. Örneğin imza sahibi, şifresini üzerine yazdığı imza oluşturma aracını kaybetmiş veya gelişi güzel bırakmış ve üçüncü kişi de bunları kolayca ele geçirmiş olabilir veya imza oluşturma aracını çalan kişi daha öncesinde imza sahibini gözetleyerek şifreyi öğrenmiş ya da araştırma yaparak şifreyi bulmuş veya çözmüş olabilir. Öyleyse imza oluşturma aracının imza sahibinin elinden rızası dışında çıkmış olması durumunda da acaba bir hukuki görünüş sorumluluğundan bahsedilebilecek ve imza sahibinin sözleşme ile bağı olduğu sonucuna varılabilecek midir?

Bu konuda ağırlıklı görüş, isteyerek olmasa bile hukuki görünüşe ihmali ile sebebiyet veren kişinin, bu ihmali sebebiyle yarattığı izlenimin sonuçlarına katlanması gereğini savunmaktadır²⁸⁷. Buna göre, imza sahibinin ihmali bir davranışı ile başka bir kimsenin kendi imza oluşturma aracını kullanmasına imkan sağlaması ve bu şekilde elektronik irade beyanının kendisinden kaynaklandığı izlenimini doğurması halinde imza sahibi sözleşme ile bağı olmalıdır.

Gerçekten internetin erişim ve kullanım alanının genişliği, hızı ve sağladığı doğallık karşısında, elektronik imzaların kötüye kullanımında muhatabın, geleneksel hukuki işlemlere göre çok daha belirgin bir korunma ihtiyacı karşısında bulunduğunu kabul etmek gerekmektedir.

Bu görüşün uluslararası hukukta ve bir kısım yabancı mevzuatta da kabul edildiği söylenebilir. Zira, UNCITRAL Elektronik İmza Model Kanunu'nun 8 inci maddesinde imzalayanın yükümlülükleri düzenlenmiş ve bu yükümlülükleri yerine getirmemesinin sonuçlarına imzalayanın katlanacağı belirtilmiştir. Buna göre imzalayan, (a) imza oluşturma verisinin yetkisiz kullanımını önlemek için makul özeni gösterecek (b) imza oluşturma verisinin (yetkisiz kullanıma yol açabilecek şekilde) tehlikede olması durumunda, makul olarak elektronik imzaya güvenmesi veya elektronik imzayı desteklemek üzere hizmet sağlaması beklenebilecek kişileri

²⁸⁷ İnal, s 152; Sertifika İlkeleri, s.13; Acır, s.37

gecikmeksizin durumdan haberdar edecek ve (c) sertifikaya dahil edilmek üzere veya sertifikanın geçerliliği süresince sertifikaya ilişkin olarak imzalayan tarafından yapılan tüm gerekli bildirimlerin doğru ve eksiksiz olduğunu sağlamak için makul özeni gösterecektir.

Benzer şekilde, İsviçre kanun koyucusu, bu konuyu bir hükümle düzenlemiş bulunmaktadır. Elektronik imza kanunu ile İsviçre Borçlar Kanunu'na elektronik imza sahibinin üçüncü kişilere karşı sorumluluğunu düzenleyen "OR. Art. 59a" hükmü eklenmiştir. Bu hükümde, tanınmış bir sertifika hizmet sağlayıcısı tarafından düzenlenmiş geçerli bir nitelikli sertifikaya güvenmelerinden dolayı üçüncü kişilerin uğradığı zararlardan, imza sahibinin sorumlu olduğu öngörülmüştür. Ancak maddenin ikinci fıkrasında, imza sahibine bir kurtuluş beyinnesi getirme imkanı tanınmıştır. Buna göre, imza sahibi, imza anahtarlarının (imza oluşturma araçlarının) korunması için halin icabına göre, gereken ve beklenen güvenlik önlemlerini aldığını inandırıcı şekilde ispatlarsa sorumluluktan kurtulacaktır²⁸⁸.

Hukukumuzda imza sahibinin yüklenmek zorunda olduğu sorumluluklarla ilgili açık bir düzenlemeye gidilmemiştir. Ancak EİK'nun uygulanmasına ilişkin yönetmeliğin 15 inci maddesinde, elektronik imza sahibinin özel hukuk sorumluluğundan bahsedilmese de, yukarıdaki düzenlemelerdeki yükümlülüklerle paralel olarak, nitelikli elektronik sertifika dolayısıyla elektronik imza sahibine, elektronik imza oluşturma aracının başkalarınca kullanılmaması için makul özeni gösterme ve gerekli önlemleri alma yükümlüğü ile elektronik imza oluşturma aracı, verisi veya şifresinin kaybolması, çalınması yada güvenliğinden, gizliliğinden şüphe edilmesi gibi durumlarda elektronik sertifika hizmet sağlayıcısını derhal bilgilendirme yükümlülükleri yüklenmiştir. Dolayısıyla bu yükümlülükler uymama nedeniyle ortaya çıkacak zararlardan elektronik imza sahibi sorumlu olacaktır. Bu itibarla elektronik irade beyanının kendisinden kaynaklandığı izlenimine ihmali ile sebebiyet veren elektronik imza sahibinin bu beyanla bağlı olduğu kabul edilmelidir. Buna karşılık her türlü makul özeni göstermesine ve önlemi almasına rağmen yetkisiz kullanıma engel olamayan elektronik imza sahibinin sorumluluğu reddedilmelidir. Örneğin, imza oluşturma aracını gereği gibi korumayıp, şifresi üzerinde yazılı imza oluşturma aracını

²⁸⁸ İnal, s. 153

kaybeden veya ortalıkta bırakan bir elektronik imza sahibinin sorumluluğu kabul edilmelidir. Buna karşılık elektronik imza oluşturma aracının iyi bir şekilde korunmasına rağmen hırsız tarafından çalınması ve hırsızın daha önce imza sahibini gözetleyerek şifreyi öğrenmiş olması veya şifreyi araştırarak yada çözümlenerek bulması durumlarında, imza sahibinin sorumluluğu ve elektronik imza ile bağılılığı reddedilmelidir. Benzer şekilde, imza oluşturma aracını saklama konusunda makul özeni gösteren ve kural olarak sorumluluğu bulunmayan imza sahibinin, imza oluşturma aracının tüm önlemlere rağmen yine de yetkisiz kullanıma yol açabilecek şekilde tehlikede olduğunu fark etmesi durumunda, durumu gecikmeksizin sertifika hizmet sağlayıcısına ve varsa elektronik imzaya muhatap olabileceğini düşündüğü kişilere bildirmesi gerektiğinden, bu konuda ihmal göstermesi halinde de yine sorumluluğu doğacaktır²⁸⁹.

2.6.2- Elektronik Sertifika Hizmet Sağlayıcısının Sorumluluğu

İnternet ortamında hukuki işlemleri güvenli bir biçimde yapmak isteyen gerçek kişilerin, kendilerine bu imkânı sağlayacak yetkili bir elektronik sertifika hizmet sağlayıcısı ile bir sözleşme akdetmesi gerekmektedir. Bu sözleşme uyarınca sertifika hizmet sağlayıcısının, kullanıcıya, biri gizli diğeri açık olmak üzere bir çift anahtar (şifre) tahsis etmek, bunun yönetimini ve gizliliğini sağlamak, yine kamuya açık şifreyi kamuya duyuracak rehberi hazırlamak yükümlülüğü bulunmaktadır. Bunun karşılığında ise sertifika sahibinin ücret ödeme yükümlülüğü bulunmaktadır.

Öncelikle belirtmek gerekir ki, Elektronik İmza Kanunumuzda elektronik sertifika hizmet sağlayıcısı ile elektronik sertifika sahibi arasındaki ilişkinin hukuki niteliğine dair kesin bir belirleme yapılmamıştır. Taraflar irade özgürlüğü çerçevesinde kanuni sınırlamalara riayet etmek suretiyle aralarındaki ilişkiyi serbestçe düzenleyebilirler. Bununla birlikte bu sözleşmenin hukuki niteliğini belirlerken göze batan ilk husus, bu ilişkinin sürekli bir borç ilişkisi niteliği arz ettiğidir. Zira sertifikanın tanzim edilmesiyle ilişki sona ermemektedir. Gerektiğinde sertifikada değişiklikler yapmak şeklinde veya kamuoyuna duyurulan şifrelerle ilgili içerik hizmetleri sunmak

²⁸⁹ İnal, s.153; Acır, s.37; Çomaklı, s.1

şeklinde ilişki devam etmektedir. Doktrinde bu sözleşmenin hukuki niteliği konusunda çeşitli görüşler ileri sürülmüştür. Bu görüşleri eser sözleşmesi görüşü, eser teslimi sözleşmesi görüşü, hizmet sözleşmesi görüşü, karma sözleşme görüşü ve kendine özgü sözleşme görüşü şeklinde gruplandırmak mümkündür²⁹⁰.

Bu sözleşmenin satım ve benzerleri olamayacağı, zira sözleşmenin kuruluşu esnasında hali hazırda bir satım konusunun, yani katılımcı sertifikasının bulunmadığı, sertifikanın başvuruyu müteakiben hazırlandığı ifade edilmektedir²⁹¹.

Bir diğer düşünce tarzı, sözleşmenin eser veya eser teslimi olabileceği yolundadır. Eser sözleşmesi ve eser teslimi sözleşmesi arasında temel farklılık, müteahhidin imal edeceği eserin malzemesini de kendisinin sağlaması noktasındadır²⁹². Türk-İsviçre hukukunda da ise eser teslimi sözleşmeleri ismi altında bir sözleşme tipi düzenlenmemiş olmakla birlikte malzemenin müteahhit tarafından sağlandığı hallerde, sağlanan malzemenin orta kalitede olmasından müteahhidi satıcı gibi sorumlu tutan BK. m.357/1 hükmü, eser teslimi sözleşmelerinin dogmatik temeli olarak görülmektedir. Buna göre sertifika, imali üstlenilen bir eserdir ve böyle bir sözleşme vekalet sözleşmesinden belirli bir iş sonucunun üstlenilmesi sebebiyle ayrılmaktadır. Acaba gerçekten sertifika sağlayıcısının üstlendiği yükümlülük bir iş sonucu mudur, dolayısıyla sorumluluğu sonuç sorumluluğu mu olacaktır, yoksa belirli bir amaca uygun faaliyet mi borçlanılmaktadır?

Sertifika tanzimi ve bu sertifikanın akreditasyonu bir faaliyet olarak değerlendirildiğinde sözleşmeye vekalet hükümleri, bir iş sonucu olarak kabul edildiğinde ise eser sözleşmesine ilişkin hükümler uygulama alanı bulmaktadır. Doktrinde bir görüş AB yönergesinde ve buna dayalı olarak Alman elektronik imza yasasında sertifikanın akreditasyonuna göre sözleşmenin hukuki niteliklerinin değişebileceğine ilişkin bir emare bulunmadığından hareketle her iki durumda da, eser sözleşmesine dair hükümlerin uygulanmasını gerektirebilecek bir iş sonucunun üstlenildiğini ileri sürmektedir²⁹³.

²⁹⁰ Yıldırım, s.267

²⁹¹ Yıldırım, s.267

²⁹² Yıldırım, s.267

²⁹³ Yıldırım, s.269

Bu görüşe karşı çıkan bir başka görüş ise, şifrelerin ve dolayısıyla şifreyi taşıyıcı araçların kullanıcıya devri gerçekleştirilmede elektronik imzadan yararlanmanın imkânsız olduğundan hareketle, ilişkide eser teslimi sözleşmesi niteliği görmekte ve dolayısıyla satım sözleşmesine ilişkin hükümlerin kıyasen uygulama alanı bulması gerektiğini ileri sürmektedir²⁹⁴.

Bizim de katıldığımız görüş ise, nitelikli elektronik imza sertifika sağlama sözleşmesinin, bünyesinde çeşitli sözleşmelere ait unsurlarla birlikte, kanunda düzenlenmeyen sözleşmelere ait unsurları²⁹⁵ içeren kendine özgü bir sözleşme (sui generis) olarak değerlendirilmesi gerekir. Zira sertifika sağlayıcısının yükümlülüğü imzayı imal etme ve bunu içeren veri taşıyıcısını iş sahibine devretmekle sona ermemekte, örneğin sertifika içerik hizmetleri sertifikanın geçerliliği süresince veya geri alınıncaya kadar devam etmektedir. Bu itibarla taraflar arasındaki hukuki ilişkinin akdi niteliği, sözleşmelere ait diğer hüküm ve kuralların da uygulama alanı bulmasına imkan vermektedir. Özellikle ayıba karşı tekeffülden sorumluluk, temerrüt, kötü ifaya ilişkin hükümler olayda uygulanabilecektir. Yine sözleşmenin tüketici sözleşmesi sayıldığı hallerde Tüketicinin Korunması Hakkındaki Kanun hükümleri de Borçlar Kanunu'na nazaran özel nitelikli olmaları sebebiyle öncelikle uygulanacaktır.

Elektronik sertifika hizmet sağlayıcısının hukuki sorumluluğu Kanun'un 13 üncü maddesinde düzenlenmiştir. Buna göre, elektronik sertifika hizmet sağlayıcısının elektronik sertifika sahibine karşı sorumluluğu genel hükümlere tabi olup, Elektronik İmza Kanunu veya bu kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlali suretiyle üçüncü kişilere verdiği zararları da, herhangi bir kusuru bulunmadığını ispat edemediği sürece, tazminle yükümlüdür(EİK m13/I-II).

Görüldüğü gibi buradaki sorumluluk, ispat külfeti yer değiştirmiş bir kusur sorumluluğudur²⁹⁶. Ayrıca elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlalinin istihdam ettiği kişilerin davranışına dayanması halinde de zarardan sorumlu olup, bu sorumluluğundan, BK. m. 55 gereğince bir kurtuluş beyinnesi getirerek kurtulamayacaktır (EİK. m. 13/3). Nihayet, elektronik sertifika hizmet

²⁹⁴ Yıldırım, s.269

²⁹⁵ Şifreleme yönteminin bilgisayar programı şeklinde imza sahibinin kullanımına sunulduğu hallerde, bilgisayar program devir sözleşmesini de içermesi ve taraflar arasında sürekli bir borç ilişkisi tesis etmesi

²⁹⁶ İnal, s.153; Yıldırım, s.265; Orta, s.128

sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersiz kabul edilmiştir (EİK. m.4).

Bu hükümlerden de anlaşılacağı üzere, kanunda sertifika hizmet sağlayıcısının nitelikli sertifika düzenleyip düzenlememesi ayırımına gidilmemiş, aksine bu hükümlerin nitelikli sertifika düzenlesin veya düzenlemesin tüm sertifika hizmet sağlayıcıları bakımından geçerli olduğu anlamına gelen genel ifadeler kullanılmıştır. Bu düzenleme tarzı kanımızca isabetli değildir. Zira uygulamayı zaman gösterecek olmakla birlikte, bu düzenleme tarzı tüm sertifika hizmet sağlayıcılarını aynı hukuki rejime tabi tutmakla, nitelikli sertifika düzenlemek istemeyecek sağlayıcıları faaliyet göstermekten caydırıcı veya tüm sertifika hizmet sağlayıcılarını nitelikli sertifika düzenlemeye zorlayıcı bir etkiye sahip bulunmaktadır. Kanunun 5 inci maddesine göre sadece güvenli elektronik imzaların elle atılan imza ile aynı hukuki sonucu doğuracağı ve güvenli elektronik imzanın nitelikli sertifikaya dayanması zorunlu olduğuna göre, nitelikli sertifika düzenlemeyen sağlayıcıların ağır hukuki yükümlülüklere tabi tutulması anlamsızdır. Çünkü sertifika nitelikli değilse ve nitelikli olduğu iddiasını da taşıyorsa ilişkili olduğu elektronik imza da güvenli elektronik imza olmayacak ve el yazısı ile imza ile aynı hukuki sonucu doğurmayacaktır. Bu durumda bu nitelikteki bir sertifikaya muhatap olan kimse sertifikanın nitelikli olmadığını görmesine rağmen buna güvenir ve zarara uğrarsa, bu zarardan sertifika hizmet sağlayıcısını sorumlu tutmak ne kadar doğrudur? Zira sertifika nitelikli olmadığı için sertifika hizmet sağlayıcısı Kanun'un 9 uncu maddesindeki bilgilerin doğruluğunu taahhüt etmemektedir. Bu durumda bu bilgilerin doğruluğunu taahhüt eden ve dolayısıyla nitelikli sertifika düzenleyen bir sağlayıcı ile aynı hukuki yükümlülüklere ve özellikle Kanun'un 18 inci maddesinde belirtilen idari para cezasına muhatap olması düşünülemez.

Kanımızca kanunda bu yönde bir açıklık bulunmasa da sertifika hizmet sağlayıcılarına ilişkin yükümlülüklerin ve sorumlulukların sadece nitelikli sertifika düzenleyen sağlayıcılar bakımından geçerli olduğu kabul edilmelidir.

Öte yandan, sertifika hizmet sağlayıcısının sertifika sahibine karşı sorumluluğunun genel hükümlere tabi olduğunun belirtilmiş olması "üçüncü kişilere karşı sorumlulukla sertifika sahibine karşı sorumluluğun farklı esaslara tabi olduğu izlenimini yaratmaktadır. Halbuki maddenin devam eden fıkralarının düzenlemesi

karşısında, sertifika hizmet sağlayıcılarının üçüncü kişilere karşı sorumluluğu ile sertifika sahibine karşı sorumluluğu arasında önemli bir fark bulunmadığı görülmektedir. Zira sertifika sahibi ile sertifika hizmet sağlayıcısı arasında bir sözleşme ilişkisi bulunmaktadır ve sertifika sahibinin zarara uğraması durumunda BK.m.96 ve devamı hükümleri uygulanacaktır. Bu durumda pratik olarak, gerek ispat külfeti gerekse yardımcı şahısların kusurundan sorumluluk konusunda, sertifika hizmet sağlayıcısının üçüncü kişilere karşı sorumluluğu ile sertifika sahibine karşı sorumluluğu aynı esaslara tabi olmaktadır. Şu halde aradaki tek fark zamanaşımı sürelerinde olmaktadır. Sertifika sahibinin talep hakkı BK. m. 125 gereğince on yıllık zamanaşımına tabi iken, buna karşılık üçüncü kişilerin talep hakkı BK. m. 60 gereğince zararı ve sorumluyu öğrenmelerinden itibaren bir ve her halde on yıllık zamanaşımına tabi olacaktır²⁹⁷.

²⁹⁷ İnal, s.144

ÜÇÜNCÜ BÖLÜM

ELEKTRONİK İMZANIN UNSURLARI

3.1- Genel Olarak

Yakın tarihe bakıldığında, teknolojinin baş döndürücü şekilde geliştiği ve buna paralel olarak kâğıda dayalı geleneksel iletişimin, dijital iletişim olarak da nitelendirilen modern iletişim yöntemlerine doğru hızlı bir gelişim ve değişim gösterdiği gözlemlenmektedir. Özellikle internetin kullanıma açılmasıyla veri alış verişi ve iktisadi faaliyetler alanlarında yeni imkânlar doğmuş, iletişim ve ticari eğilimler değişmiş ve gelişmiştir. Bilgisayarların birbirine bağlı olduğu ağlar dünyanın tüm coğrafi bölgelerine açılmış, bilişim ağında bilgi transferinin ötesinde, sözleşmeler akdedilebilecek, eş zamanlı ve online(çevrimiçi) ödemeler yapılabilecek teknolojiler geliştirilmiştir. Bilişim teknolojilerindeki bu gelişmeler nedeniyle içinde bulunduğumuz yüz yıl “bilişim ve teknoloji” çağı olarak adlandırılmaya başlanmıştır.

Bilgi ve iletişim teknolojilerinin bu hızlı gelişimi neticesine internet kullanımı çok yaygınlaşmış ve artık günlük yaşamımızın ayrılmaz bir parçası haline gelmiştir. Mal ve hizmet siparişlerinden, sanal kütüphanelere, bankacılık işlemlerinden tıp alanındaki bilgilerin paylaşımına kadar pek çok özel sektör işlemi internet üzerinden

yapılabilmektedir. Özellikle, ülke sınırlarını aşan mal ve hizmet edimlerini içeren hukuki ilişkiler de dâhil olmak üzere, birbirlerini hiç tanımayan ve aralarında hiç bir güven unsuru bulunmayan şirketler veya kişiler arasında ticari sözleşmeler veya anlaşmalar bu yolla yapılabilmektedir. Yine sağlıktan adalete, eğitimden emniyete ve diğer devlet kurumlarına kadar, yapılacak pek çok resmi başvuru ve işlem, günümüzde dünyada ve ülkemizde büyük ölçüde elektronik yolla yapılabilir hale gelmiştir. Ancak internet üzerinde yapılan işlemlerde, özellikle elektronik ticaret uygulamalarında, en çok ihtiyaç duyulan şeylerin başında güvenlik gelmektedir. Zira söz konusu teknolojik gelişmelere paralel olarak modern bilgi ve iletişim tekniklerinin artan kullanımı ile bir yandan hız, rekabet ve gelişmişlik adına sevindirici faydalar sağlanmış ise de, bir diğer yandan, kötü niyetli kişilerin bu teknolojileri kullanarak, her türlü yolsuzluğu, aldatma ve hileyi çok daha kolay ve inandırıcı yapabilmeleri de mümkün hale gelmiştir. Örneğin, elektronik olarak iletilen ya da kaydedilen verilerin, üçüncü kişiler tarafından, gönderici veya alıcı fark etmeksizin ve herhangi bir iz bırakmaksızın iletişim esnasında ya da sonradan değiştirilebilmesi söz konusu olabilmektedir. Bu yönde bir değişiklik yapıldığının ispatlanması ise şuan için neredeyse imkansız görülmektedir. Öte yandan muhatabın, internet üzerinden kendisine gelen bir bilgi ya da veri dosyasının gerçekten gönderici olarak gözüken kişi tarafından gönderilmiş olup olmadığını da kesin olarak tespit etmesi teknik olarak mümkün görülmemektedir. Herkese açık global bir haberleşme ağı olan internetin, özellikle elektronik ticarete yaygın olarak kullanılmaya başlanması ve resmi işlerde de kullanılmasına ilişkin altyapı çalışmalarına gidilmesiyle birlikte, bu risklerin karşılanması ihtiyacı da kendisini fazlasıyla hissettirmeye başlamış ve internet üzerinde yapılan iletişimin güvenliği, güvenilirliği ve bağlayıcılığı konusunda teknik ve hukuki tedbirler alınması zorunluluğu doğmuştur.

Söz konusu güvenliği sağlayıp, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğunu, garanti edebilmek amacıyla, özellikle bankalar tarafından yoğun çalışmalar yapılarak internet bankacılığı benzeri uygulamalarda kullanılacak sistemler geliştirilmiştir. Ancak bu tür sistemlere girişte kullanılan bilgiler de kullanıcı tarafından fare veya klavye kullanılarak girildiğinden bu bilgilerin üçüncü kişiler tarafından ele geçirilebildiği görülmüştür. Bu nedenle geleneksel usulde ıslak (el yazısı ile) imza ile sağlanan kimlik tespiti, bütünlük ve güvenlik işlevine karşılık, elektronik ortamda kimlik tespitinin güvenli bir şekilde

yapılmasını sağlayıp, el yazısı ile imza yerine geçebilecek kadar güvenilir bir mekanizma ile belgenin değiştirilmediğinin garanti edilmesini sağlayacak arayışlara gidilmiştir. İşte bu ihtiyaca çözüm bulmak ve elektronik ortamda bulunan veya gönderilen veri, bilgi ve belgelerin güvenliğinin ve güvenilirliğinin sağlanması, bütünlüğünün korunarak, güvenli ve değişmeden iletilmesinin temini ve en önemlisi gönderenin ve alanın kimliğini tespit etmek, aynı zamanda da el yazısı ile imza ile aynı hukuki korumayı sağlayacak bir teknik yöntem olarak “*elektronik imza*” daha dar ifade ile “*nitelikli elektronik imza*” ortaya çıkmıştır.

Ancak, elektronik ortamda veri güvenliği ve bütünlüğü, kimlik tespiti ve inkar edememe gibi fonksiyonlar dahil olmak üzere el yazısı ile imzanın tüm fonksiyonlarını karşılamak üzere bir zorunluluk olarak ortaya çıkan Elektronik İmza, teknik ve sayısal yönü itibariyle toplumumuzda henüz tam olarak anlaşılammış ve yakın zamanda da anlaşılacak gibi gözükmemektedir. Bununla birlikte, kısmen özel sektörde kısmen de kamu sektöründe²⁹⁸ kullanılmaya başlanan Elektronik İmza'nın yakın bir zamanda, başta kamu ve finans sektörü olmak üzere her alanda günlük yaşamımıza gireceği ve yaşamımızın ayrılmaz bir parçası olacağı konusunda başta uzmanlar olmak üzere toplumun pek çok kesiminin görüş birliği söz konusudur. Zira, güvenli bir imza yöntemi olmadan güvenli bir elektronik haberleşmeden ve hukuki korumadan söz etmek mümkün değildir. Başta şirketler ile kamu kurum ve kuruluşları olmak üzere, teknolojinin sağlamış olduğu hızlı, doğru ve güvenli iletişimden faydalanmak ve hukuken bağlayıcı işlemler yapmak isteyen herkesin, elektronik ortamda kullanabilecekleri güvenli bir imza yöntemine yani Elektronik İmza'ya gereksinimleri bulunmaktadır.

Öte yandan, internet veya yerel ağlar üzerinde yapılan işlemlerde, özellikle elektronik ticaret alanında, en çok ihtiyaç duyulan olguların başında güvenlik gelmektedir. E-yaşamın geliştirilebilmesi ve tarafların birbirleri ile doğru olarak haberleşebilmesi ve bilgi alışverişinin sorunsuz bir şekilde yapılabilmesi elektronik ortama ve açık ağ sistemine güvenin sağlanmasına bağlıdır.

Genel olarak elektronik ortamda bilgi güvenliğinden bahsedebilmek için üç işlevin birlikte gerçekleşmesi gerekir. Bunlar, **gizlilik** yani bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olması, diğer bir ifade ile alıcıya varana kadar başkalarının

²⁹⁸ Uyap kapsamında personele dağıtılan elektronik imzalar

bu bilgiye vakıf olamaması, **bütünlük** yani bilginin bozulmadan, başkaları tarafından değiştirilmeden, üzerine eklemeler veya silintiler yapılmadan (tahrif edilmeden) alıcıya ulaşması ve **gerçeklik** yani bilginin görünürde onu göndermiş olarak gözükene kişiden gelmiş olup olmadığının tespitinin, garanti edilmesidir²⁹⁹. Bu unsurların aynı anda gerçekleşmesi, verilerin şifrelenmesine, verilere karşı yapılacak “hacker” saldırılarının ve tahriplerin önlenmesine, şayet böyle bir saldırı söz konusu ise metnin bütünlüğünün bozulduğunun kolaylıkla anlaşılmasına ve nasıl ki el yazısı ile imzanın kimin tarafından atıldığına tespiti hususunda zorluk çekilmiyorsa, aynı şekilde elektronik ortamda bilgiyi gönderen kişinin kimliğinin de kolaylıkla tespit edilmesine imkan veren bir teknik sistemin, altyapının varlığına bağlıdır.

Bu sistem şu an için “Açık Anahtar Altyapısı” olarak adlandırılan ve kısaca “AAA” olarak nitelendirilen ve asıl adı İngilizce PKI (Public Key Infrastructure) olan bir teknoloji ile sağlanmaktadır. Bu teknoloji elektronik imzanın da temelini oluşturmaktadır.

Açık anahtar altyapısı (AAA), asimetrik şifreleme temeline dayanan kriptografik bir sistem olup, temel görevi elektronik ortamda haberleşen, işlem gören ve çalışan kişiler, kurumlar veya cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır³⁰⁰. Bu sistem veriler için gizlilik, bütünlük, inkâr edememe, kimlik doğrulama veya onaylama ve elektronik belgenin düzenlendiği zamanın tespiti işlevlerini yerine getiren hizmetleri sağlar.

Bu hususların sağlanması için şifreleme yöntemine başvurulmaktadır. Şifreleme, yetkisi olmayan kişilerin gönderilen verileri elde etmesini, okumasını önleyecektir³⁰¹. Şifreleme anahtar vasıtasıyla yapılır. Anahtar, verilerin işleme tabi tutularak anlaşılmaz hale getirildiği sonrada yine anlaşılabilir hale sokulduğu yani deşifre edildiği algoritmaya dayanan formüldür. Şifreleme için tek bir anahtar kullanılabilirdiği gibi çift anahtarda kullanılabilir.

Elektronik imzanın teknik altyapısı, kimlik tespiti, bütünlük kontrolü ve inkâr edilemezlik gibi ıslak imza ile sağlanan fonksiyonları elektronik ortamda temin etmeye

²⁹⁹ Özgül, s.3; Sağiroğlu-Alkan, s.2; Sözer, s.123

³⁰⁰ Sağiroğlu-Alkan, s.75; Yükseliyor, s.1; Babür, s.1; Önel, s.2; Orta, s.51; Kılıçlı, s.1

³⁰¹ Rüssmann, s.341

imkân tanımakta ve bunun yanında elektronik belgenin şifrelenmesini ve birden çok kişi ile mesajın şifrelendiği anahtarın öğrenilmesine gerek kalmadan iletişime imkân sağlayarak güveli bir ortam ihtiyacını karşılamaktadır. Bu bölümde elektronik imza ile ilgili bazı teknik terimler açıklanacak ve devamında elektronik imzanın teknik altyapısını ve unsurlarını oluşturan yapılar ayrıntılı olarak incelenecektir.

3.2- Elektronik İmza Kanununda Yer Alan Teknik Terimler

Elektronik İmza Kanunu ile birlikte genelde bilim ve teknoloji alanında kullanılan, mevzuatımızda pek yer bulmayan ve hukuken yabancı olduğumuz bazı terimler de mevzuatımızda yerini almıştır. Elektronik imza kavramını ayırık tutar isek, elektronik veri, elektronik belge, imza oluşturma verisi ve aracı, imza doğrulama verisi ve aracı, elektronik sertifika, anahtar ve zaman damgası gibi bu terimlerden bazılarıdır. Bu terimlerin bir kısmı kanunda tanımlanmaya çalışılmıştır. Ancak ileride de görüleceği üzere çalışmamızda bu terimlerin birçoğundan sıklıkla söz edilecektir. Bu nedenle öncelikle bu terimlerin ne anlama geldiği ve neyi ifade ettikleri hususlarını kanun ve uygulamadan faydalanarak izah etmeye çalışacağız.

Elektronik Veri: Sayısal veya mantıksal her türlü değer bir veridir. Verinin bir anlam ifade eden haline ise bilgi denir³⁰². Verinin sözlük anlamı, 1- Bilgi; 2- Bir araştırma, tartışma, muhakemenin ana ögesi; 3- Bir esere temel olan ana ilke, 4- Matematikte bilinmeyi bulmaya yarayan şey; 5- Bilişim alanında, olgu, kavram veya komutların işlem için elverişli gösterimi olarak tanımlanmaktadır³⁰³. Elektronik veri ise 5070 sayılı yasada tanımlanmıştır. Buna göre “Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar” elektronik veridir (m.3-a). Bu tanımdan da anlaşılacağı gibi kağıt ve benzeri fiziki ortamda bulunmayan, bilgisayar, cep telefonu, televizyon gibi elektronik cihazlar ile fotoğraf makinesi, tarayıcı, kamera, cd/dvd okuyucu-yazıcı gibi optik cihazlar tarafından üretilen, taşınan veya saklanan her türlü kayıt bir elektronik veridir. Yine kanun benzeri yollarla tabirini de ekleyerek henüz bilmediğimiz ama ileride ortaya çıkabilecek farklı cihaz ve yöntemlerle üretilecek, saklanacak veya taşınacak kayıtları da elektronik veri kapsamına dahil etmiştir.

³⁰² Sungur s.2

³⁰³ TDK, Güncel Türkçe Sözlük

Elektronik Belge: Belge sözlük anlamı olarak “*bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika, doküman*” şeklinde tanımlanmaktadır. Bu tanıma benzer şekilde Hukuk Muhakemeleri Usulü Kanun tasarısında da belge “Uyuşmazlık konusu vakıaları ispata elverişli, yazılı veya basılı metin, senet, çizim, plân, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları” olarak tanımlanmıştır(m.203).

Elektronik belge ise en basit ifadeyle belge tanımı kapsamında bulunan verilerin, sayısal ortamda bulundurulmasıdır³⁰⁴. Yani elektronik belge elektronik ortamda sayısal olarak kodlanmış³⁰⁵ şekilde bulunan elektronik verilerdir. Kodlanmış şekilde bulunan bu veri bilgisayarda veya benzer nitelikteki cihazlarda işlenerek yazı, şekil, hareketli/hareketsiz görüntü, ses veya başka bir biçime büründürülerek anlamlı hale dönüştürülür. Bu açıklamalara göre elektronik belgeyi, sayısal olarak kodlanmak suretiyle elektronik formata dönüştürülen ve metin, hesap tablosu, grafik, görüntü, multimedya dokümanı veya bunların kombinasyonu biçiminde, elektronik cihaz, manyetik disk, manyetik teyp, optik disk kompakt disk veya benzeri ortamlarda saklanabilen belgeler olarak tanımlayabiliriz.

Elektronik belgeler genelde, bilgisayar hafızasında veya başka bir veri taşıyıcısında kayıtlı veriler olarak ya da mail adresinde veya web sayfasında bulunup bilgisayar veya benzeri bir ekranda görülebilir olarak karşımıza çıkmaktadır. Bilgisayar çıktısı ise elektronik ortamdaki belgenin kâğıtta vücut bulmuş kopyası niteliğindedir³⁰⁶.

İmza Oluşturma Verisi (Gizli Anahtar): Adından da anlaşılacağı üzere elektronik imza oluşturmak yani elektronik belgeleri imzalamak ve kendisine gelen şifreli mesajları çözmek için kullanılan veridir. Yasada “*imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler*” olarak tanımlanmıştır. İmza oluşturma verisi gizlidir ve Elektronik Sertifika Hizmet Sağlayıcısı (ESHS) tarafından sadece imza sahibine verilir. Yasa kapsamında güvenli elektronik imza atmada

³⁰⁴ Yaşar-Atabağ-Dalan, s.4

³⁰⁵ Yani bilginin “1” ve “0” (bit) halinde sayısal formda üretilmesi, işlenmesi ve saklanması ile elektronik belge oluşur. Bu sayısal kodların bilgisayar ve benzeri cihazlarda anlamlı bir görüntü haline getirilmesi için bazı alfabeler kullanılır. Bunların en yaygın olanları ASCII (American Standart Code Information Interchange) ve EBCDIC (Extenden Binary Coded Decimal Intenchange) dir.

³⁰⁶ Erturgut, s.29

kullanılabilmesi için de imza oluşturma aracı içerisinde bulunmalıdır. Dolayısıyla bazı ESHS ler tarafından deneme sertifikası adı altında internet üzerinden dağıtılan sertifika ve bunun içerdiği imza oluşturma verisi yasanın aradığı şartları taşımadığı için elektronik imza kapsamında yer alsa da, güvenli kabul edilmediğinden BK. 14 üncü madde gereğince el yazısı ile imzaya eşdeğer kabul edilmemektedir.

İmza Oluşturma Aracı: İmza oluşturma aracı kanuni tanımıyla “*elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracıdır.*” Bu tanım kapsamında pek çok yazılım veya donanım elektronik imza oluşturmak için kullanılabilir. Ancak bu şekilde oluşturulacak imzanın güvenli olması ve daha da önemli yasa kapsamında ıslak imza ile aynı fonksiyonu eda edebilmesi için imza oluşturma aracının bazı nitelikleri taşıması gerekmektedir. Buna göre imza oluşturma aracının, ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiç bir biçimde çıkarılamamasını ve gizliliğini, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesi, kullanılamaması ve elektronik imzanın sahteciliğe karşı korunmasını ve son olarak da imzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini temin edecek nitelikte olmalıdır(m.6). Aksi takdirde oluşturulan elektronik imza güvenli elektronik imza olarak kabul edilemeyecektir. Şu an için ülkemizde güvenli elektronik imza oluşturma aracı olarak, uluslararası standartlar ölçüsünde, en az EAL4 sertifikalı akıllı kart ve kart okuyucu veya USB token kullanımı öngörülmektedir³⁰⁷. Bunun yanında bilgisayarlar veya veri işleme kapasitesi olan el terminalleri (PDA, cep telefonları, Pocket Pc’ler v.b.) ile kullanımı da söz konusu olabilmektedir. Özellikle cep telefonları ile elektronik imza kullanımına yönelik çalışmalar günümüzde oldukça yaygınlaşmıştır.

İmza Doğrulama Verisi (Açık Anahtar): Açık anahtar yani imza doğrulama verisi de imza oluşturma verisi gibi imza sahibine aittir ve bir eşi daha yoktur. Yasa da “*Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler*” olarak tanımlanmıştır. İmza sahibinin elektronik sertifikası içerisinde bulunur. Ancak gizli tutulması gerekmediğinden, kural olarak kamuya açıktır ve

³⁰⁷ Beceni s.4; Sağiroğlu-Alkan (söyleşiler), s.1

sahibince yada ESHS tarafından yayımlanmasında bir engel yoktur. Açık anahtar başka bir elektronik imza sahibince atılmış imzayı doğrulamak veya başka bir elektronik imza sahibine gönderilecek mesajı şifrelemede kullanılır.

İmza Doğrulama Aracı: İmza doğrulama aracı, istemci veya sunucu bilgisayarları üzerlerinde çalışan ve elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracıdır. Şu an için imza doğrulama aracı olarak genel itibari ile yazılım kullanılmaktadır. Yine imza doğrulama aracının, 5070 sayılı yasa kapsamında güvenli elektronik imza doğrulama aracı olarak kabul edilebilmesi için bazı standartları sağlaması gerekmektedir. Buna göre bu yazılım veya donanımın; doğrulama işlemini güvenilir ve kesin bir şekilde çalıştıracak, imza sahibinin kimliğini, doğrulama için kullanılan verileri ve doğrulama sonuçlarını değiştirmeksizin gösterecek, doğrulama ile ilgili şartlara etki edebilecek değişiklikleri tespit edebilecek ve doğrulamada kullanılacak sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit edecek nitelikte olmalıdır(m.7). Bu nedenle Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ gereğince imza doğrulama aracının CWA 14171 güvenlik standartlarına sahip olması gerekmektedir.

Elektronik Sertifika: Elektronik sertifika yasada “İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıt” olarak tanımlanmıştır (EİK m.3). Bu tanıma göre kamuya açık bir anahtarın yani imza doğrulama verisinin, bir gerçek veya tüzel kişiye yada kuruma bağlanmasını mümkün kılan ve bu sertifikayı veren elektronik sertifika hizmet sağlayıcısının elektronik imzasının doğrulanmasını sağlayan veriler bütünüdür. Elektronik sertifika gerçek hayattaki ehliyet, pasaport veya üyelik kartlarının elektronik ortamdaki benzerleridir ve bunların gerçek hayattaki işlevlerini elektronik ortamda gerçekleştirirler. Elektronik sertifikanın elektronik olarak gösterilmesiyle kimlik ispat edilebilir, online bilgi yada hizmetlere erişme izni sağlanabilir. Elektronik sertifikalar nitelikleri ve ait olduğu imza sahibinin özelliklerine göre farklı türlere ayrılmaktadır. Elektronik sertifikanın özellikleri ve çeşitlerini ileride ayrı bir başlık altında inceleyeceğiz.

3.3- Kriptografi (Şifreleme)

Kriptografi, matematik, elektronik, optik, bilgisayar, sosyal mühendislik bilimleri gibi çok sayıda disiplini içeren ve bilgi ve belgelerin şifrlenmesi ve şifrelerinin çözülmesi yöntemlerini kapsayan özelleşmiş bir bilim dalıdır³⁰⁸. Kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve bunları çözme bilimi ise “kriptoanaliz” olarak nitelendirilmektedir. Şifreleme (kriptografi) ve şifre analizi (kriptoanaliz) bilimlerinin tek çatı altında değerlendirilmesi ise bilgi güvenliği bilimi yani “kriptoloji” olarak tanımlanmaktadır³⁰⁹.

Kriptoloji günümüzde, internet ve intranet olarak adlandırılan ağ teknolojileri yanında, mobil ve sabit telefonlar, bilgisayarlar, televizyonlar, ev aletleri, araçlar, ileri teknoloji uydular, uçaklar ve füze sistemleri gibi pek çok alanda kullanılmaktadır. Bunun nedeni ise temelde, iyi niyetli meraklıların yanında, saldırganlar, korsanlar, casuslar gibi kötü niyetli kişi veya oluşumların, haberleşme sistemlerini dinleme, elektronik bilgi depolarına erişme ve mevcut bilgileri elde etme istekleridir. Bu isteklerin nedeni merak, kendini tatmin etme, eğlenme gibi basit şeyler olabileceği gibi, zarar verme, etkisiz hale getirme, haksız para kazanma, kişisel mahremiyete saldırı, politik çıkar elde etme, kişisel, kurumsal veya ulusal çıkarları zedeleme gibi ciddi konular da olabilmektedir. Bilgi güvenliği teknolojilerindeki ciddi ilerlemelere rağmen, saldırıların arttığı ve halen 20.000’den fazla saldırı türünün olduğu kaydedilmektedir³¹⁰.

Şifreleme, anlaşılır bir bilginin anlaşılmaz yapılarak, istenmeyen şahıslar tarafından algılanamaz veya öğrenilemez bir forma dönüştürülmesi işlemidir. Bu işlemde temel amaç bilgi güvenliğini sağlamaktır. Şifrelenen bilgi uygun bir anahtar bilgisine sahip olunmadan okunamaz veya anlaşılmaz.

Şifre biliminde bilinen ilk şifreleme yaklaşımlarının MÖ. 1900’lü yıllarda Mısırlılarca hiyeroglif yazıları üzerinde yapıldığı tespit edilmiştir. Yine MÖ. 100-44’lü yıllarda ortaya çıkan “Sezar” yaklaşımı ilk şifreleme yaklaşımlarındandır. Zaman içerisinde kriptografi alanında farklı yaklaşımlar ve teknikler geliştirilmiştir. Bunlar arasında 1623 yılında Francis Bacon’un, 5-bit ikili kodlamayla karakter tipi

³⁰⁸ Sağıroğlu-Alkan, s.21; Orta, s.61

³⁰⁹ Sağıroğlu-Alkan, s.21; Orta, s.61;

³¹⁰ Sağıroğlu-Alkan, s.7

değişikliğine dayanan yaklaşımı, 1790 yılında Thomas Jefferson tarafından “strip cipher” makinesinin icat edilmesi ve 1917’de Joseph Mauborgne ve Gilbert Vernam tarafından “one time pad” algoritmasının geliştirilmesi en önemlilerinden kabul edilmektedir³¹¹.

Yakın tarihte, teknolojik gelişmeler neticesinde elektronik cihazların ve bilgisayarların da hayatımıza girmesiyle birlikte, mekanik kriptografi yerini yazılım ve donanım teknolojilerine dayalı elektronik kriptografiye bırakmıştır. Özellikle II. Dünya Savaşı sonrasında kriptolojideki gelişmeler hız kazanmış ve 1970’li yılların başında, çok güvenli olmadığı kabul edilse de bankacılık ve e-ticaret alanında halen dahi kullanılmaya devam edilen, simetrik şifreleme tabanlı DES (Data Encryption Standard) standardı benimsenmiştir³¹².

Açık Anahtar Altyapısına dayalı elektronik imzanın temelini teşkil eden asimetrik şifreleme sistemi ise, ilk olarak 1976 yılında Whitfield Diffie ve Martin Hellman tarafından teorik olarak ortaya atılmıştır. Bundan iki yıl sonra yani 1978’de Ronald Rivest, Adi Shamir ve Len Adelman adlı üç bilim adamı, büyük asal tamsayı çarpanlarının etkileşmesi temeline dayanan ilk açık anahtarlı şifreleme yaklaşımını pratik olarak gerçekleştirdiler. Bu şifreleme metoduna bilim adamlarının baş harflerinden oluşan RSA şifreleme metodu adı verilmektedir. Daha sonraları da bu alanda pek çok yeni gelişmeler olmuş, ancak bunlardan hiçbirisi RSA sisteminin güvenilirliğini bozamamıştır. RSA sistemi halen açık anahtarlı kriptolama teknolojisinde yaygın olarak kullanılmaktadır³¹³.

Kriptografi genel olarak şu ana konularla ilgilenir:

Gizlilik: Bilgi istenmeyen kişiler tarafından anlaşılmalıdır.

Bütünlük: Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine yanlış bir ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememeli.

³¹¹ Sağıroğlu-Alkan, s.22

³¹² Winn, s.34; Orta, s.63; Sağıroğlu-Alkan, s.23

³¹³ Winn, s.35; Sağıroğlu-Alkan, s.23; Orta, s.63; Yükseliyor, s.1; Önel, s.1;

Reddedilemezlik: Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememeli. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.

Kimlik belirleme: Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. davetsiz bir misafir başkasının kimliğine bürünme şansına erişmemelidir.

3.3.1- Kriptografide Kullanılan Teknikler

Kriptografinin temel taşları anahtarlardır. Anahtar, verileri şifrelemek veya deşifre etmek için kullanılan sayısal karakterler dizisidir³¹⁴. “48-bit”, “128-bit” kodlama ifadeleri anahtarın uzunluğunu gösterir. Şifreleme algoritmalarında güvenlik, anahtarın uzunluğu ile doğru orantılıdır. Şu an için anahtarların en az 128 bit uzunluğunda olması gerektiği kabul edilmektedir. Günümüzde 48 bitlik kodlamanın kolaylıkla kırılabilirdiği, hatta PC hızlarındaki artış nedeniyle, yakın gelecekte 256-bit kodlamanın bile kırılabilirdiği ifade edilmektedir³¹⁵.

Verileri şifreleme ve şifreli verileri çözmeye kullanılan çok sayıda yaklaşım, teknik ve algoritma bulunmaktadır. Bunlar kendi aralarında kategorize edilmek istendiğinde, şifreleme ve şifre çözmeye kullanılan anahtar yapılarına göre kapalı anahtarlı (simetrik) ve açık anahtarlı (asimetrik) şifreleme sistemi olarak ikiye ayrıldığı görülmektedir. Simetrik algoritmalarda veriyi şifrelemek ve çözmek için tek anahtar kullanılırken, asimetrik algoritmalarda ise birbiri ile mantıksal bağı bulunan iki ayrı anahtar kullanılır. Simetrik algoritmalar hızlı şifreleme yapmalarına karşın güvenlik riskleri taşımakta, asimetrik yöntemler ise tüm güvenlik unsurlarını desteklemekle beraber şifreleme hızları bakımından yavaşlardır. Bu nedenle her iki sistemin birlikte kullanıldığı “hybrid” yaklaşımlarda bulunmaktadır. Bu teknikler aşağıda ayrı ayrı incelenmiştir.

³¹⁴ Sağiroğlu-Alkan, s.34; Altınışık, s.82-83; Özgül, s.4; Orta, s.42

³¹⁵ Sağiroğlu-Alkan, s.35; Winn, s.28

3.3.1.1- Simetrik Anahtar Şifrelemesi

Simetrik algoritmalar, tek anahtarlı algoritmalar olup, verilerin şifrenmesi veya deşifre edilmesi için aynı anahtar kullanılır. Güvenli iletişimde bulunabilmek için tarafların bir anahtar üzerinde uzlaşmaları ve bu anahtarı paylaşmaları gerekir³¹⁶. Bu anahtar ile açık veriler şifrenir veya şifrenmiş veriler deşifre edilebilir. Bu anahtarın başkaları tarafından öğrenilmesi, bu kişilerin şifreli verileri çözebileceği anlamına gelir. Bu nedenle iki tarafın iletişimde gizli anahtarın yani şifrenin sadece taraflarca bilinmesi ve diğer kişilere karşı mutlak surette korunması gerekmektedir. Aksi halde güvenli bir iletişimden söz edilemeyecektir.

Simetrik şifreleme genellikle bankalar gibi güvenli bir temele sahip, iyi kurulmuş elektronik servis ağlarında kullanılmaktadır³¹⁷. Özellikle banka ATM'lerinde kullanılan PIN kodları yani hesaba erişim şifresi, simetrik yani tek anahtarlı bir yapıdır. Kişi ve banka bu anahtarı paylaşır ve ancak bu anahtarın kullanımı ile verilere erişim sağlanabilir. Simetrik anahtar sisteminde öncelikli problem, dolaşımda güvenlikten ödün vermeden ona ihtiyaç duyan kimselere bu anahtarları ulaştıracak bir yolun bulunmasıdır. Bunun bir merkezi anahtar dağıtım sistemi ile çözülebileceği düşünülse de anahtar dağıtım sisteminde çalışan kimselerin, olmaları gerektiği kadar güvenilir olmama ihtimali ile karşılaşılabilir. Simetrik anahtar sisteminin diğer bir eksikliği ise, taraflar arasında anahtar paylaşımı zorunlu olduğundan, daha önceden aralarında bir ilişki bulunmayan taraflar arasında kullanılamamasıdır. Simetrik anahtar şifrelemenin sebep olduğu anahtar paylaşımı ve yönetimi problemlerinin çözümü ancak dijital imzaların kalbi olan asimetrik diğer adıyla açık anahtar şifreleme sisteminin kullanılması ile mümkün olabilir.

Günümüzde en yaygın kullanılan simetrik şifreleme algoritmaları, DES ve 3DES'tir. Bununla birlikte RC2, RC4, RC5, IDEA, AES ve Blowfish algoritmaları da simetrik şifreleme algoritmalarıdır.

³¹⁶ Sağiroğlu-Alkan, s.33; Orta, s.64; Altınışık, s.81; İnalöz, s.30; Kodaz, s.3; Özgül, s.4; Kılıçlı, s.1

³¹⁷ Winn, s.33; İnalöz, s.30

3.3.1.2- Asimetrik Anahtar Şifrelemesi

Asimetrik anahtar şifrelemesi yöntemi, açık anahtar şifrelemesi olarak da bilinir. Güvenli elektronik imzanın temelini bu sistem oluşturur. Bu şifreleme algoritmalarında verileri şifreleme veya deşifre etmek için farklı anahtar çiftleri kullanılır. Bu anahtarlardan veri şifreleme ve imza doğrulamada kullanılan ve kamuya açık olanına “açık anahtar(Public Key)³¹⁸”, kişiye özel ve gizli olup, verileri deşifre etme ve imza oluşturmada kullanılanına ise “özel anahtar (private key)³¹⁹” adı verilir. Açık anahtar, kamunun erişimine açık olmakla, liste halinde yayımlanabileceği gibi muhataba e-posta ve benzer yollarla iletilebilir. Özel anahtar ise kişiye özeldir ve gizli tutulur. Başkalarının bu anahtara erişmesi, verileri deşifre etmek veya özel anahtar sahibi adına imza atabilmek anlamına gelir. Dolayısıyla özel anahtarın güvenli bir ortamda tutulması ve özenle saklanması icap eder. Bu anahtarlar çift olarak üretilir ve tek yönlü çalışırlar. Yani bu anahtar çiftleri birbirlerine mantıksal ve matematiksel bir bağla bağlıdırlar. Ancak birinden hareketle diğerini elde etmek imkânsız kabul edilmektedir³²⁰.

Asimetrik yani açık anahtarlı şifreleme yönteminde veriler, şifrelendiği anahtarla değil bu anahtarla mantıksal bağı bulunan diğer anahtarla deşifre edilebilir. Yani açık anahtar kullanılarak şifrelenen bir veri buna karşılık gelen özel (gizli) anahtarla, özel anahtar ile şifrelenen bir veri ise genel (açık) anahtarla deşifre edilebilir³²¹. Bu şifreleme tekniğinin açık anahtarlı şifreleme olarak adlandırılmasının sebebi açık anahtarın herkesin erişimine açık olmasıdır. Özel anahtar ise yalnızca ait olduğu kişide bulunur. Dolayısıyla bir kişi başka birisine şifreli bir veri göndermek istediğinde o kişinin özel anahtarına sahip olması söz konusu olmadığı için o kişinin açık anahtarını kullanarak şifreleme yapabilecektir. Bu durumda bu şifreli veriyi ancak özel anahtar sahibi kişi deşifre edebilecektir. En çok tercih edilen açık anahtarlı şifreleme yaklaşımı RSA’dır. Bunun yanında Sayısal İmza Algoritması (DSA), Eliptik Eğri Şifreleme Sistemi ve Diffie-Hellman Anahtar Anlaşması Protokolü, popüler açık anahtarlı şifreleme yaklaşımlarıdır.

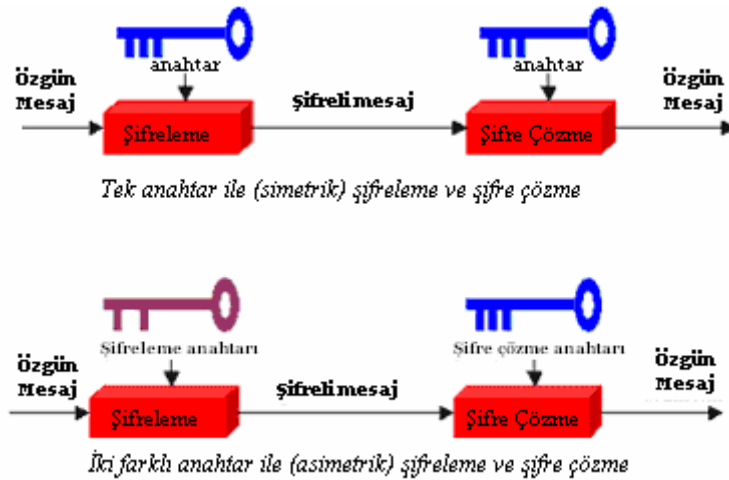
³¹⁸ 5070 sayılı yasada “imza doğrulama verisi” şeklinde tanımlanmıştır.

³¹⁹ 5070 sayılı yasada “imza oluşturma verisi” şeklinde tanımlanmıştır.

³²⁰ Sağiroğlu-Alkan, s.32; Winn, s.33; Orta, s.43,64; Babür, s.2; Altınışık, s.82

³²¹ İnalöz, s.31; Sağiroğlu-Alkan, s.33; Orta, s.64 Altınışık, s.82; Erturgut, s.67; Keser Berber (Şekil), s.25

Asimetrik kriptolojinin çalışma şeklini herkes tarafından anlaşılması bakımından bir örnekle açıklayalım; diyelim ki ben arkadaşım Mehmet'e başkalarının öğrenmesini ve değiştirmesini istemediğim bir mesaj veya belge göndereceğim; bunun için öncelikle göndereceğim metni bilgisayarda hazırladım. Şimdi bu metni şifreleyeceğim. Yukarıda izah ettiğimiz gibi bu metin ancak bana özel ve kimsenin bilmediği "özel anahtar" ile şifrelenecektir. Ben metni özel anahtarım ile şifreledim diyelim. Şimdi benim genel anahtarım kamuya açık olduğundan isteyen herkes tarafından mesajın deşifre edilmesi söz konusudur. Ancak ben bu mesajın yalnızca Mehmet tarafından deşifre edilebilmesini istiyordum. İşte bu nedenle çapraz şifreleme yapılması gerekmektedir. Yani ben hazırladığım metni önce Mehmet'in kamuya açık olan genel anahtarı ile şifreledikten sonra bu hali ile kendi özel anahtarım ile de şifreliyorum ve Mehmet'e gönderiyorum. Mehmet kendisine mesaj ulaştığında, mesajı açabilmek için benim özel anahtarım ile şifrelememe karşı kamuya açık genel anahtarımı, Kendisinin genel anahtarı ile şifrelememe karşın da kendi özel anahtarını kullanarak mesajı deşifre edecektir. Yani ne ben, ne de Mehmet birbirimizin özel anahtarını öğrenemeyecek ve bu mesajı üçüncü kişiler açamayacaktır. Bu örneği sadeleştirirsek; mesajı gönderen, alıcının genel, kendisinin özel anahtarını kullanarak şifreleme yapacak; alıcı da gönderenin genel, kendisinin özel anahtarı ile mesajı deşifre edecektir. İşte bu çapraz şifreleme yöntemidir. Yani özel anahtarla yapılan şifrelemeyi genel anahtar, genel anahtarla yapılan şifrelemeyi ancak özel anahtar açabilir. Şu anki uygulamada üçüncü kişilerin mesajı deşifre etmeleri imkansız kabul edilmektedir.



Şekil-1: Simetrik ve Asimetrik Kriptolama

3.3.1.3- Hybrid Şifreleme Yöntemi

Yukarıda da açıklandığı üzere simetrik şifreleme yöntemi hızlı olmasına karşın güvenlik riskleri taşımakta, asimetrik şifreleme ise güvenli olmasına karşın yavaş olmaktadır. Bu durum *hybrid kriptosistem* olarak adlandırılan yapıyı ortaya çıkarmıştır. Bu yöntemde gönderilecek asıl veri öncelikle simetrik şifreleme yöntemi ile şifrelenir. Dolayısıyla bu verinin deşifre edilebilmesi için şifrelemede kullanılan anahtarın alıcıya ulaştırılması gerekir. İşte bu aşamada şifrelemede kullanılan anahtar asimetrik şifreleme yöntemi kullanılarak alıcının genel anahtarı ile şifrelenir ve mesaj alıcıya gönderilir. Alıcı önce özel anahtarını kullanarak simetrik anahtarı deşifre eder. Bilahare bu anahtarla da mesajı deşifre ederek açar³²².

Bu sistemde simetrik ve asimetrik şifreleme yöntemleri birlikte kullanıldığından haberleşme, simetrik yöntem nedeniyle hızlı ve asimetrik yöntem nedeniyle güvenli olmaktadır. Dolayısıyla hız ve güvenlik bir arada olduğundan verimliliği artırmaktadır. Bu nedenle bu ve buna benzer yaklaşımlar pek çok işlemde kullanılmakta ve geliştirilmektedir.

3.4- Açık Anahtar Altyapısı

Günümüzde internet kullanımının yaygınlaşması, özellikle elektronik bankacılık ve elektronik ticaret sistemleri ile elektronik haberleşme ve elektronik eğitim platformlarının kullanıma alınmasını beraberinde getirmiştir. İnsanların evden veya işyerlerinden tüm ihtiyaçlarını elektronik platform ve uygulamalar ile yürütmesi kullanım açısından çok büyük kolaylık sağlıyor olsa da beraberinde çeşitli güvenlik açıkları doğurmaktadır. Özellikle elektronik bankacılık ve elektronik ticaret alanlarındaki güvenlik açıkları neticesinde ortaya çıkan kayıplar (ticari casusluk, para aktarımı, yetkisiz erişim vs.) milyon dolarlar mertebesine ulaşmıştır. Alınan önlemler her defasında yine hem insana hem de teknolojiye bağımlı olarak kırılabilir olmuştur. Özellikle bu uygulamalarda kullanılan statik şifreler ile buna benzer statik kişi tanıma yöntemleri gerçek bir kimlik tanıma işlevi sağlamamaktadırlar. Bu nedenle elektronik işlemlerin tam ve güvenli olarak yapılabilmesi için, onay ve yetki güvenliğinin sağlanmasına ihtiyaç bulunmaktadır. Özellikle ülkemizde ve Birçok Avrupa ülkesinde

³²² Orta, s.64; Sağıroğlu-Alkan, s.34

hayata geçirilmeye başlanan e-devlet modelleri ve buna bağlı uygulamalarda gerçek bir kişisel kimlik tanıma sisteminin oluşturulması kaçınılmazdır. İşte yukarıda da belirtildiği üzere elektronik ortamda yapılan ve yapılacak işlemlerde, güvenliğin sağlanması, işlem gerçekleştiren kişinin kimliğinin belirlenmesi, bu işlemlerin ve belgelerin yasalar önünde delil niteliği taşıması gibi pek çok ihtiyacı teknik olarak karşılamak amacıyla Açık Anahtar Altyapısı olarak adlandırılan sistemler oluşturulmuştur.

Bugün için yasal anlamda bağlayıcılığı olan ve yasada güvenli elektronik imza olarak tanımlanan elektronik imzanın temelini de Açık Anahtar Altyapısı oluşturur.

Açık Anahtar Altyapısı, güvenli bilgi iletişimini gerçekleştirmek için açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlayan ve birbirleriyle eşgüdüm içinde çalışan organizasyonların, sistemlerin (yazılım-donanım), süreçlerin ve politikaların toplamına verilen ad olup, makamlar, sertifikalar, depolama ve arşivleme birimleri ve güvenlik prensiplerini kapsamaktadır³²³. Bir AAA içerisinde, sertifikaların oluşturulması, yönetimi, saklanması, yayımlanması ve kaldırılması için gereken prosedürler ile kişiler, yazılımlar ve donanımlar yer almaktadır.

AAA (Açık Anahtar Altyapısı “*Public Key Infrastructure*”), 1978 yılında 3 bilim adamı Rivest, Shamir ve Adleman’ın baş harflerinden oluşan RSA matematik algoritmasının onaylanması ile başlar³²⁴. Açık anahtar altyapısının (AAA) temel görevi, elektronik ortamda haberleşen, işlem gören ve çalışan kişiler, kurumlar veya cihazlar arasında güvenilir bir haberleşme ortamı oluşturmaktır. Bu altyapı içerisinde, gizlilik, bütünlük, inkâr edememe, kimlik doğrulama veya onaylama, yetkilendirme ve imzalama, süreklilik ve zaman damgası gibi hizmetler verilerek sanal ortam güvenli hale getirilir. Bu altyapılar, kullanıcıların sahip oldukları açık ve gizli anahtarlara göre hizmet vermektedirler. Bu hizmetler, anahtarların oluşturulması, yetkili bir kurum tarafından onaylanması, sertifikaların saklanması ve dağıtılması, gerektiği durumlarda onayın geri alınması, geçici olarak durdurulması ve sonlandırılması gibi işlemlerden oluşmaktadır.

³²³ Sağiroğlu-Alkan, s.75; Gökalp, s.1; İnalöz, s.35; Gülaçtı, s.1; Babür.s.1; Genç, s.2; Önel, s.2

³²⁴ Orta, s.51; Yükseliyor, s.1; Levi, s.1; Önel, s.1

AAA'yı iyi anlamak için, simetrik (tek anahtarlı) ve asimetrik şifreleme (iki anahtarlı) yaklaşımları iyi anlamak gereklidir. Yukarıda detaylı anlatıldığı üzere, tek anahtarlı simetrik şifreleme sistemlerinde şifreleme ve deşifreleme işlemleri için aynı anahtar kullanılmaktadır. Birbiriyle şifreli olarak haberleşmek isteyen taraflar, bu anahtara sahip olmak zorundadırlar. Asimetrik şifreleme Açık Anahtar Altyapısı çözümlerinde kullanılan önemli bir kriptolama tekniği olup, bu teknikte birbiriyle matematiksel açıdan ilişkili iki adet anahtar bulunmaktadır. Bu anahtarlardan biri bilindiğinde diğesinin bulunması mümkün değildir. Gizli anahtar (private key), diğes kullanıcılarla paylaşılmayan, gizli kalması gereken, kişiye özel olan, sadece sahibince bilinip, kullanılan anahtardır. Bu nedenle gizli anahtarların, güvenliği yüksek ortamlarda üretilmesi ve korunmaları gereklidir. Bunun için uygulamada, akıllı çubuklar (e-token) veya akıllı kartlar gibi donanımlar kullanılmaktadır. Açık anahtar (public key) ise gizlenmesi gerekmeyen ve tüm kullanıcılar tarafından bilinebilen anahtardır. Açık anahtarın herhangi bir şekilde kamunun erişimine açılması, web sitesi veya e-posta aracılığıyla duyurulması, sahibince veya yetkili makamca yayımlanması mümkündür. Açık anahtarlı kriptolama tekniğine göre, açık anahtarla kriptolanan bir veri ancak o açık anahtarın çifti olan gizli anahtar kullanılarak açılabilir. Yine aynı şekilde, gizli anahtarla kriptolanan bir veri ancak o gizli anahtarın çifti olan açık anahtar kullanılarak açılabilir.

Elektronik ortamda işlemlerin sağlıklı ve güvenilir olarak yapılabilmesi için, hizmetlerden faydalanan kullanıcıların kendilerini, hem karşı tarafa güvenli olarak tanıtmaları, hem de karşı tarafın kendilerine güvenmelerini sağlayacak, elektronik olarak oluşturulmuş bir güven ortamı olmalıdır. İşte bu güvenlik AAA yapısı ve bu yapı içerisinde yer alan sertifika otoritelerince yerine getirilmektedir³²⁵. Güvenli üçüncü taraf olarak nitelendirilen sertifika otoriteleri her kullanıcıya kullanıcıların kimlikleriyle ilişkilendirilmiş sertifikalar dağıtmaktadır. Kullanıcın açık anahtarı, ismi, e-posta adresi gibi kimlik bilgilerini içeren bu sertifikalar, sertifika otoriteleri tarafından imzalanarak oluşturulur ve her an ulaşılabilir şekilde depolanırlar. Sertifika otoriteleri bu sertifikaları gerektiğinde iptal ederek bunlara ilişkin bilgileri de saklarlar. Sertifika otoriteleri, tüm ülkelerde kimlik üreten makamlar konumundadır. Böylece, AAA yapısı kullanıcılara, internet üzerinde yapılan tüm elektronik işlemlerin ve gönderilen her türlü

³²⁵ Orta, s.35; Önel, s.1; Sağırođlu-Alkan, s.78 vd.

bilginin iletimi esnasında, alınan ve gönderilen bilginin kesinliği, bilginin kaynağı ve gideceği yerin kesinliği, zamanlama güvencesi, bilginin gizliliği güvencesi, bilginin mahkeme veya yasal makamlarca delil olarak sunulabilme güvencesi gibi faydalar sağlar.

3.4.1- AAA'nın Görevleri

Yukarıda da izah edildiği üzere açık anahtar altyapısı, birçok hizmet ve teknolojinin birleşimiyle oluşmuş bir sistem olup, bir ağ ortamında açık anahtarlı şifreleme sisteminin kullanımına izin veren servislerden oluşur. Açık anahtar altyapısının başlıca görevi, açık anahtarların sahipleri olan varlıklar için dijital sertifikaların üretilmesi, dağıtılması, yayınlanması ve iptalini sağlamaktır. Buna kısaca sertifika yönetimi adı verilmektedir. Bu altyapı içerisinde sertifika yönetimi ile birlikte pek çok başka hizmetin de yerine getirilmesi gerekmektedir. Bunları aşağıdaki şekilde sınıflandırarak kısaca belirtmeye çalışacağız.

Kayıt İşlemi: Bir AAA ortamına kullanıcıların katılıp kullanmaları için AAA sistemine ait güvenilir üçüncü şahıs servisine kayıt olmaları gerekir. Bu sayede sertifika içerisine konulacak bilgilerin doğruluğu kontrol edilir ve onaylanır³²⁶.

Dijital İmzalar: Mesajların doğrulanması, bütünlüğü ve inkar edemezlik gibi ihtiyaçları karşılayan AAA hizmetidir. Bu hizmet içerisinde mesajların özetinin çıkarılması, özet şifreleme/deşifreleme gibi fonksiyonlar bulunur.

Şifreleme: Bir ağ ortamında iletilerin güvenliğini ve gizliliğini sağlayan algoritmalar ve kriptofonksiyonlarından oluşur.

Zaman Damgası: Veri ve dokümanlara eklenen zaman damgası ile güvenli bir zaman bilgisi kullanılması sağlanır ve bu veri ve dokümanların geçerli olduğu zaman aralığı belirlenir. Bu fonksiyonları içeren hizmet içinde, zaman damgası istekleri, zaman damgası sertifikalarının doğrulanması, depolanması ve üretilmesi gibi fonksiyonlar bulunur³²⁷. Zaman damgası ileride ayrıca açıklanacaktır³²⁸.

³²⁶ Genç, s.2; Sağiroğlu-Alkan, s.83

³²⁷ Genç, s.2; Sağiroğlu-Alkan, s.83

İnkâr Edemezlik: Verilerin işlenmesi, toplanması, tekrar elde edilmesi ve doğruluğunun onaylanması gibi işlemleri içerir.

Anahtar Yönetimi: AAA'nın en önemli servislerindedir. Bu hizmet anahtarlarının güvenli ve ölçeklenebilir olarak tutulmasından sorumludur. Bu hizmet içinde anahtarların üretimi, anahtarların ilişkilendirilmesi, dağıtılması, depolanması, geri alınması, yedeklenmesi, güncellenmesi, anahtar erişim isteklerinin doğrulanması ve yönetim fonksiyonlarından oluşur³²⁹.

Dizin Servisleri: AAA'daki kullanıcılarının diğer kullanıcılar hakkında bilgi almak için kullandığı fonksiyonları içerir. Bunun içinde yeni sertifikaların ilanı, mevcut sertifikaların güncellenmesi, sertifika iptal listelerinin yayımlanması ve güncellenmesi, dağıtım, yedekleme, arama, sertifika isteklerinin karşılanması gibi fonksiyonlar bulunur.

Yetkilendirme: AAA'daki bir varlık, haklarının bir kısmını diğer bir varlığa vermek isteyebilir. Yani bir kaynağa erişen varlık diğer bir varlığında aynı kaynağa erişmesini isteyebilir. Bu hizmet içinde doğrulama, grup tanımlanması, hakların güncellenmesi, kullanıcıların gruba eklenmesi, hakların çözümlenmesi ve yönetim yetkilerinin belirlenmesi gibi fonksiyonlar bulunur³³⁰.

Bir AAA'da yukarıda belirtilen hizmetlerin birbiriyle uyumlu ve uluslararası standartlara uygun olması gerekir.

3.4.2- AAA'nın Bileşenleri

Bir AAA'da yukarıda belirtilen hizmetler sertifika otoriteleri olarak nitelendirilen güvenilir makamlar veya onlara hizmet veren birimlerce yerine getirilirler. AAA içerisinde bulunan bu makamlar Kayıt Makamı(KM), Sertifika Makamı(SM) ve Kök Sertifika Makamı(KSM) olarak adlandırılırlar. Bu makamlar dışında Sertifika Deposu ve Arşiv Modülü gibi hizmet birimleri de mevcuttur. Bu makam ve birimler AAA'yı meydana getiren bileşenler olup, birbirleriyle tam bir eşgüdüm ve işbirliği içerisinde çalışarak, sertifika yönetimi başta olmak üzere yukarıda açıklanan tüm

³²⁸ Bkz, s.110

³²⁹ Genç, s.2; Sağiroğlu-Alkan, s.83; Orta, s.51 vd.

³³⁰ Genç, s.3

hizmetleri yerine getirirler. Aşağıda bu makam ve birimlere ilişkin açıklamalara yer verilecektir.

3.4.2.1- Kayıt Makamı

Kayıt makamı bir sertifika makamına destek vermek ve yardımcı olmak için oluşturulmuş bir alt birim olup, AAA'ya giriş kapısı olarak nitelendirilebilir. Bu makam, sertifika makamı için sertifika başvurularını alır ve sertifika içine yerleştirilecek bilgilerin doğruluğunu kontrol ederek onaylar. Kişisel bilgilerin doğruluğunun sağlanması, başvuru sahibinin kimliğinin, pasaportunun veya ehliyetinin bir fotokopisinin alınması ile gerçekleştirilmektedir. Bu makamdan elde edilen bilgilerle bir sertifika isteği oluşturulur ve bu istek, sertifika makamına iletilir. Bu sayede sertifika makamı güvendiği bir makamdan doğrulanmış bilgileri alarak, kullanıcının güvenli olarak AAA'ya girişini sağlar³³¹. Sertifikalandırılan kullanıcılar, AAA içerisinde tanınmış, e-bireyler veya e-vatandaşlardır. Bu sertifikalar, bu ortam içerisinde bulunan e-vatandaşların güvenli olarak birbirleriyle haberleşmeleri için yayınlanırlar. Kayıt makamları, birden çok sertifika makamına hizmet verebilecek şekilde yapılandırılacakları gibi sadece bir sertifika makamının alt birimi olarak da hizmet verebilirler.

3.4.2.2- Sertifika Makamı(Elektronik Sertifika Hizmet Sağlayıcısı(ESHS))

Sertifika makamı, açık anahtar altyapısında yer alan sertifikaları ve sertifika iptal listelerini üretmekle görevli olan merkezi birime verilen addr³³². Sertifika makamı, donanım ve yazılım parçalarından ve sistemi işleten kişiler ve kurallardan oluşan bir yapıdır.

Sertifika makamının temel görevleri; sertifikaları ve sertifika iptal listelerini üretme, yayımlama ve güncel tutmanın yanında, kullanıcı kimlik bilgilerini doğru tespit etmek, özel anahtar bilgilerini, hem kullanım sırasında, hem de kullanımdan sonraki işlemlerde gizli tutmak, kendi özel anahtarını saklamak ve korumak için gerekli

³³¹ Sağiroğlu-Alkan, s.79; Yazıcı-Erdoğan, s.78

³³² Tubitak/UEKAE

önlemleri almak, kimlik ile, açık/gizli anahtar çifti arasında ilişki kuran sayısal sertifikaları oluşturmak, kullanıcılarının, güvenli olarak sertifika makamı ortamını kullanabilmeleri için yazılım, donanım, insan kaynakları ve oluşturulmuş üst düzey kurallar ve politikalar ile hizmet vermektir³³³. Bu makamın ciddiyeti ve almış olduğu güvenlik tedbirleri ne kadar yüksekse, sertifikaların güvenliği ve güvenilirliği de, o derece fazladır.

Sertifika makamlarının altında başka sertifika makamlarının oluşturulması da mümkündür. Bu durumda bir sertifika makamı altında hem kullanıcı, hem de başka sertifika makamları bulunabilecektir.

3.4.2.3- Kök Sertifikasyon Makamı

Kök sertifikasyon makamı, AAA hizmetlerinin güvenli verilebilmesi için, en önemli ve en üstteki makamdır. Sadece sertifika makamları için sertifika üretirler. Son kullanıcılara sertifika üretmezler. AAA'daki tüm bileşenler kök sertifikasyon makamının elektronik imzasına güvenirlirler. Bu nedenle bu makamın güvenilir olması ve herkes tarafından güven duyulacak bir makam olması şarttır³³⁴.

Sertifika makamları, sertifikalarını internet üzerinden bilgisayarlarına yüklerken, kök sertifikasyon makamının güvenilirliğini kabul ederek, işlem yapmaktadırlar. Sertifika ile birlikte gelen açık anahtar, öncelikle, sertifikasyon kurumunun kimliğini doğrulamakta kullanılır. Bu açık anahtar, sertifikasyon kurumunun dağıttığı sertifikaların da okunabilmesini ve böylece, bu sertifikaların, doğruluğunun kontrol edilebilmesini sağlar.

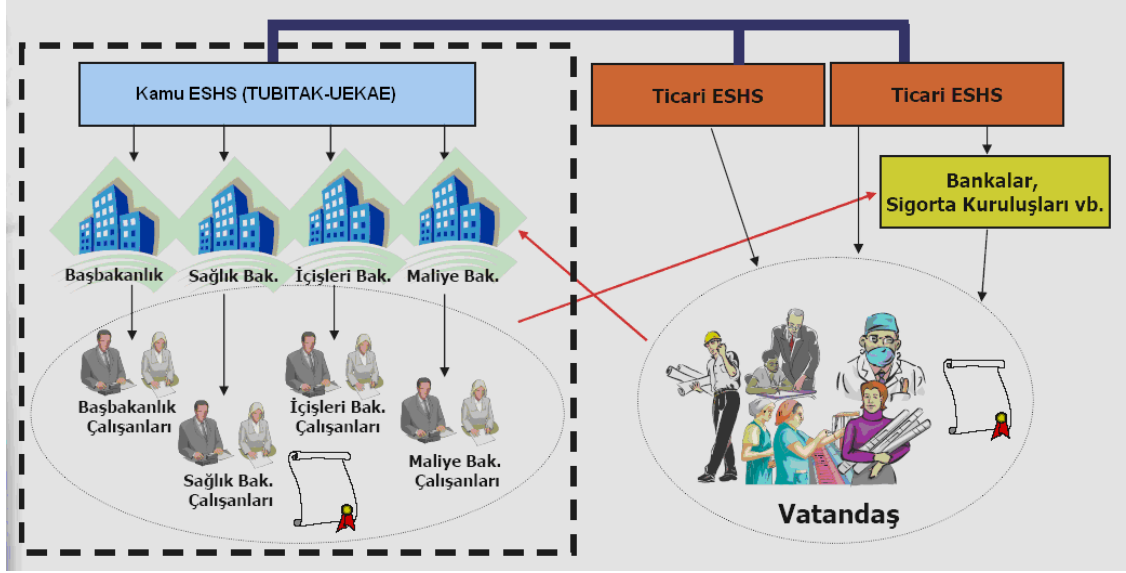
Kök sertifikasyon makamları, ülkelere göre farklı yapılanma şekilleri gösterebilmektedirler. Kök sertifikasyon makamları altında farklı sertifika makamları olabileceği gibi, sertifika makamlarının alt birimi olarak hizmet veren ve ona sertifika sağlayan farklı sertifika makamları da bulunabilir. Burada unutulmaması gereken husus kök sertifikasyon makamının bu yapılanmanın en tepesinde olmasıdır³³⁵. Ülkemizde

³³³ Tubitak/UEKAE, Sağırođlu-Alkan, s.80; Yazıcı-Erdoğan, s.4; Erol, s.45

³³⁴ Erol, s.44; Orta, s.59; Sağırođlu-Alkan, s.82; Önel, s.3

³³⁵ Tubitak UEKAE; Sağırođlu-Alkan, s.82; Erol, s.44

kök sertifikasyon makamı TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'dür.



Şekil-2: Başbakanlık Genelgesi İle Kabul Edilen Türkiye'nin Açık Anahtar Altyapısı Modeli

3.4.2.4- Sertifika Deposu

Sertifika deposu, açık anahtar altyapısında kullanılan sertifikaların ve sertifika iptal listelerinin (SİL) dağıtımını yapan birimlerdir. Bir sertifika deposu birden çok sertifika makamının sertifika ve SİL'lerini depolayabilir. Sertifika depoları olarak genellikle uygulamada X.500 standardı olarak bilinen erişim kuralları ile uyumlu olarak çalışan ve bilgilerin hiyerarşik bir yapıda saklanmasını sağlayan bilgisayar sistemleri ve yazılımlar kullanılır. Bunlar izin sistemleri olarak tanımlanırlar³³⁶.

Açık anahtar altyapısı açısından bir sertifika deposu tek başına güvenilir kabul edilmez. Sertifika deposu içindeki sertifikalara ve SİL'lere güvenilmesinin sebebi bunların sertifika makamı tarafından sayısal imza ile korunmuş olmalarıdır³³⁷.

3.4.2.5- Arşiv Modülü

Arşivleme bileşeni uzun dönemli veri saklama görevini sertifika makamı adına yapan modüldür. Arşivleme modülü bilginin kendisine ulaştığında doğru olduğunu ve

³³⁶ Tubitak UEKAE; Sağiroğlu-Alkan, s.84; Erol, s.47; Genç, s.3; Yazıcı-Erdoğan, s.4; İnalçz, s.37

³³⁷ Erol, s.47

geçen süre içinde değişmediğini garanti altına alır. Arşivlenecek bilgiler (sertifika ve SİL) sertifika makamı tarafından arşiv modülüne iletilir. Bu sayede ileride doğabilecek bir ihtilaf halinde geçmiş tarihli sertifikanın arşiv modülü tarafından isteyen taraflara veya makama verilebilmesi mümkün hale getirilmektedir³³⁸.

Bu açıklamalar ışığında genel bir AAA içerisinde, temel bileşenler arasındaki iletişim ve sistemin işleyişinin aşağıdaki şekilde gerçekleştiği söylenebilir.

1- Öncelikle sertifika makamı gerekli yasal prosedüre uygun olarak kök sertifikasyon makamından kök sertifikasını alır ve faaliyete başlar.

2- E-devlet, e-iş, e-ticaret veya e-bankacılık yapmak isteyen bir kullanıcı, sertifika diğer bir ifade ile elektronik imza talebi ile kayıt makamına müracaat eder ve kendisinden istenilen bilgi ve belgeleri, hazırlayarak kayıt makamına teslim eder.

3- Bilgi ve belgeler, kayıt makamı tarafından güvenli bir şekilde sertifika makamına ulaştırılır. Belgeler sertifika makamınca kontrol edilir.

4- Sertifika makamınca kullanıcıya açık ve gizli anahtar olmak üzere bir anahtar çifti üretilir.

5- Üretilen açık anahtar, bir sertifika ile ilişkilendirilir.

6- Gizli anahtar ise, kullanıcıya, bir akıllı çubuk veya akıllı kart içerisine aktarılarak sunulur. Kullanıcıya sunulan bu kart veya çubuğa, sertifika makamının prensibine göre, resen geçici veya sürekli bir erişim şifresi (PIN) verilebileceği gibi kullanıcıdan bu yönde bir PIN numarası belirlemesi de istenebilir. Bu uygulama cihazın çalınması veya kaybolması gibi durumlarda izinsiz erişimi zorlaştırır.

7- Sertifika makamı verilen sertifikanın açık anahtar ve sertifika bilgilerini sürekli olarak yayımlanmak üzere uygun bir sunucuya yani sertifika deposuna yönlendirir. Bu bilgiler kullanıcıların kendileri veya iş ve işlem yapabileceği diğer kullanıcılar tarafından erişilebilecek şekilde kullanıcılara sunulur.

³³⁸ Tubitak UEKAE; Erol, s.46; İnalöz, s.37

8- Benzer şekilde problemlı sertifikalar yani geçerliliđi bitmediđi halde kullanılması istenmeyen sertifikalar sertifika iptal listelerinde yayımlanır.

3.5- Elektronik Sertifika

Elektronik imza, verilerin elektronik ortamda, deđişikliğe uğramadan, gizli ve güvenli bir şekilde kullanılmasını ve paylaşılmasını yukarıda anlatıldığı şekilde gerçekleştirmektedir. Elektronik imza, sadece gizli anahtarla oluşturulur ve bu anahtara karşılık gelen açık anahtarla doğrulanabilir. Bu şekilde imzalı belgeyi alan taraf açık anahtarı kullanarak, belgedeki dijital imzanın gizli anahtar sahibi tarafından oluşturulduđunu tespit eder. Ancak dijital imza tek başına kişinin kimliğini tespit edici bir fonksiyona sahip değildir. Bu nedenle günlük yaşantımızda kendimizi, iş ve işlem yapmış olduğumuz kişi ve kurumlara tanıtabilmek için, nasıl nüfus cüzdanı veya ehliyet gibi, güvenilir makamlardan almış olduğumuz kimlikleri kullanıyorsak, elektronik ortamda da, bu iş ve işlemlerin güvenli olarak gerçekleştirilebilmesi için, elektronik bir kimliğe ihtiyacımız bulunmaktadır. Yine bu elektronik kimliđin gerçek sahibine ilişkin bilgiler taşıdığı ve bu bilgilerin diđer bir kişi yada tarafı tatmin edecek yeterlilikte olduğuna dair gerekli güvenin sağlanması için bu kimliđin güvenilir bir makam tarafından verilmiş olması gerekir. Zira ancak tarafsız bir üçüncü kişi tarafından kimlik belirlenmişse bu kimliğe güvenilebilir³³⁹.

Elektronik imzaya ve ait olduğü varlığın kimliğinin doğruluđuna güvenin sağlanması ve başkaca gereksinimlerin yerine getirilmesi için sertifika hizmet sağlayıcılarına ihtiyaç duyulur. Sertifika hizmet sağlayıcıları, “*sertifika otoriteleri*”, “*onay kurumları* “ yada “*güvenilir üçüncü kişiler*” olarak adlandırılan ve yukarıda AAA’nın bileşenleri içerisinde açıklanan sertifika makamları ve kök sertifikasyon makamlarıdır. Elektronik sertifika hizmet sağlayıcısının sertifika üzerindeki elektronik imzası, sertifikanın bütünlüğünü ve doğruluđunu garanti edecektir.

İşte, Elektronik Sertifika Hizmet Sağlayıcıları tarafından oluşturulan ve elektronik ortamda işlem yapan kişinin, nesnenin veya kurumun tanınması veya bilinmesi için kullanılan elektronik veya sayısal kimliğe yada dokümana, “*elektronik*

³³⁹ Erturgut, s. 82; Sağırođlu-Alkan, s.117; Orta, s.45

sertifika" denir³⁴⁰. Elektronik sertifika, kimlik sahibi hakkında detaylı bilgi vermenin yanında, bu bilgilerin doğruluğu, güvenilirliği, kullanıcıların ve sertifika hizmet sağlayıcıların zarar görmemeleri için nasıl kullanılması ve hangi kurallara uyulması gerektiği gibi detayları içerirler. Aynı zamanda, elektronik ortamda kişilerin gizliliğini ve kimlik doğrulamasını sağlamak amacıyla, kimlik sahibine ait olan açık ve gizli anahtar çiftleriyle, kimlik bilgileri arasında ilişki kurulmasını sağlarlar. Buna göre elektronik sertifika hizmet sağlayıcıları sertifikadaki kişinin gerçekten o şahıs olup olmadığını tescil ederler. Yani açık anahtar ve kimlik bilgilerini sertifikaya yerleştirip kendi özel anahtarlarını kullanarak tasdik ederler³⁴¹. Böylece imza anahtarı sahibi, sertifika hizmet sağlayıcısına başvurduktan sonra elde ettiği özel anahtarıyla elektronik belgeleri imzaladığında, imza anahtarı sahibinin sertifikası da imzalı elektronik belgelere eklenir³⁴².

Ekinde sertifika bulunan dijital imzalı bir elektronik belge alıcıya ulaştığında, alıcı kimlik tespiti yapmak için öncelikle, sertifika hizmet sağlayıcısının açık anahtarı ile sağlayıcının kimliğini kontrol edecektir. İkinci adım olarak sertifika sayesinde imza sahibinin açık anahtarı ile imza sahibinin kimliğini kontrol edecektir. İmza sahibinin kimliğinin tespiti ise sertifika hizmet sağlayıcısının her zaman ulaşılabilir izin hizmeti sayesinde mümkündür. Bu nedenle sertifikalar, elektronik ortamda herkese açık yapıdadırlar ve kullanıcılar tarafından kolaylıkla erişilebilecek yerlerde yayımlanırlar.

Aslında sertifikalar, erişimi yetkilendirmek, kimlikleri doğrulamak, inkâr edememeyi sağlamak, bilgileri şifrelemek ve şifrelenen bilgileri çözmek için kullanılan elektronik anahtar çiftleri ile ilişkilendirilmekle, açık anahtar taşıyıcısı görevi görürler. Ancak, açık anahtardan daha fazla belirleyici bilgiye sahip oldukları için daha çok işlevselliğe sahiptirler. Oluşturulan sayısal kimlik veya sertifika sayesinde kullanıcılar, bilgilerinin haberleşme esnasında, güvenli bir şekilde iletilmesini, alınmasını ve korunmasını sağlarlar.

Elektronik ortamda hizmet veren sertifikalar, sadece kişilerin veya kurumların kimliklerini belirlemede değil, aynı zamanda sunucuların ve internet üzerinde dağıtılan yazılımların kimliklerinin belirlenmesinde de kullanılmaktadırlar. Bu sayede sertifikalar

³⁴⁰ Sağıroğlu-Alkan, s.117

³⁴¹ Orta, s. 45; Altınışık, s. 85; Keser Berber (Şekil), s.27 ; Erturgut, s.83; Sevimli, s.1030

³⁴² Erturgut, s. 84; Sağıroğlu-Alkan, s.117

ile bilgisayar ağları üzerinde haberleşilirken yada iş yapılırken, güven, güvenlik ve güvenilirlik sağlamaktadır. Diğer bir ifade ile AAA içerisinde, kişiler, kurumlar, kuruluşlar, bilgisayarlar, yazılımlar veya ağ cihazları, elektronik olarak kimliklendirilir veya sertifikalandırılır. Bu sayede, on-line bilgi, sistem veya servislere, güven içerisinde erişebilme ve karşılıklı olarak güvenli haberleşme sağlanır³⁴³.

Bu açıklamalar ışığında denilebilir ki, elektronik sertifikalar, günlük hayatta kullanılan ehliyet, pasaport ya da kimlik kartlarının, elektronik ortamdaki karşılığdır. Diğer bir ifadeyle kimliğin sayısal ispatıdır³⁴⁴.

Bir sayısal sertifika; açık anahtar, sertifika sahibinin kişisel bilgileri, sertifikayı veren makam hakkında bilgi ve sertifikayı veren makamın imzası olmak üzere dört ana bileşenden oluşmaktadır. Bununla birlikte bu bileşenlerin tamamına yer verilmemesi veya ekstra bilgilere yer verilmesi teknik olarak mümkündür ve yasal mevzuat, sertifika makamı politikaları ve sair olgulara göre farklılık arz edebilir. Böyle bir eksikliğin veya farklılığın ortaya çıkarabileceği sorunları engellemek ve ideal bir sertifika tanımlaması yapmak isteyen uluslar arası kurumlar, halen yaygın olarak kullanılan X.509 standardını tanımlamışlardır³⁴⁵.

Elektronik imza hakkındaki genel açıklamalarımızda her elektronik imzanın yasal anlamda bağlayıcı nitelik taşımadığı bunun için bu elektronik imzanın güvenli elektronik imza niteliği taşıması gerektiğini belirtmiştik. Yine güvenli elektronik imza ile ilgili açıklamamızda da bir elektronik imzanın, güvenli elektronik imza sayılabilmesi için nitelikli elektronik sertifikaya dayanması gerektiğini vurgulamıştık. Bu vurgulamadan da anlaşılacağı üzere her elektronik sertifika, nitelikli elektronik sertifika kabul edilmemektedir. Nitelikli elektronik sertifikalar, kanunlar veya yönetmeliklerle nitelikleri belirlenmiş olan elektronik sertifikaların bu özelliklerine ek olarak bazı teknik gereksinimleri sağlayan ve sertifika sahibinin kişisel bilgilerini içeren elektronik sertifika türüdür. 5070 Elektronik İmza Kanununun 9 uncu maddesine göre, bir sertifikanın nitelikli elektronik sertifika kabul edilebilmesi için, sertifikada;

a) Sertifikanın “nitelikli elektronik sertifika” olduğuna dair bir ibarenin,

³⁴³ Orta, s. 45; Keser Berber (Şekil), s.27

³⁴⁴ Orta, s. 45; Sağiroğlu-Alkan, s.117

³⁴⁵ Orta, s.46; Tüfekçi (Elektronik İmza Niçin Yaygınlaşmıyor), s.5; Sağiroğlu-Alkan, s.118

- b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adının,
- c) İmza sahibinin teşhis edilebileceği kimlik bilgilerinin,
- d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisinin,
- e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin,
- f) Sertifikanın seri numarasının,
- g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin,
- h) Sertifika sahibi talep ederse mesleki veya diğer kişisel bilgilerinin,
- ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin,
- j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzasının,

Bulunması zorunludur.

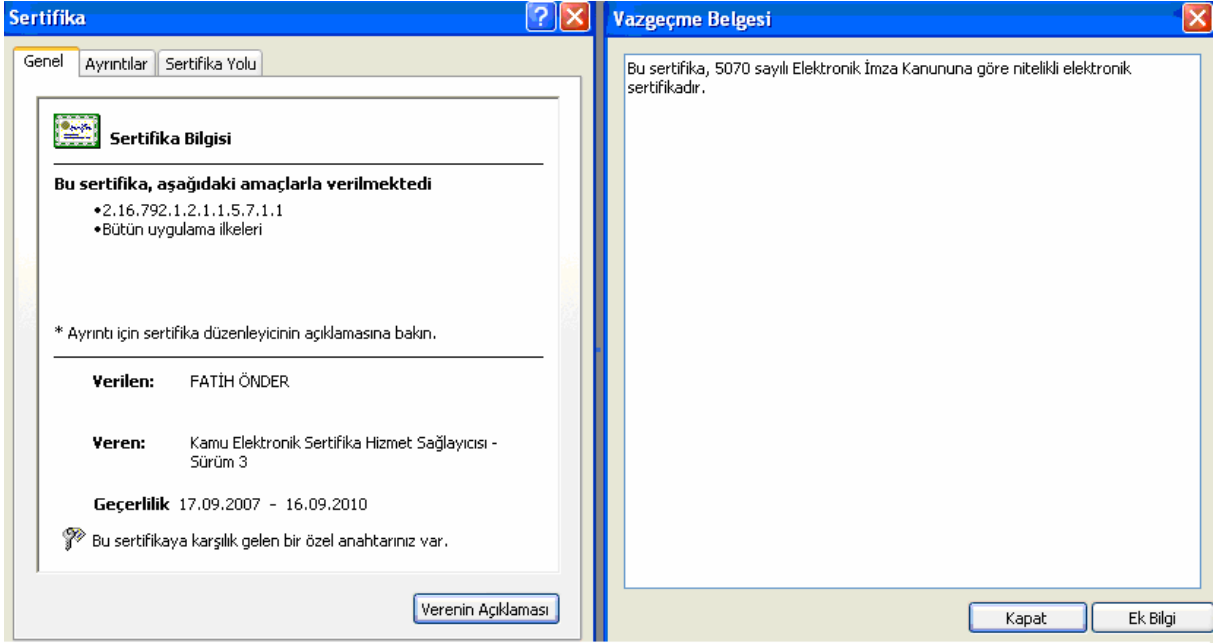
Elektronik sertifikalar ait oldukları varlıkların niteliğine göre aşağıda açıklandığı şekilde, bireysel sertifika, sunucu sertifikası, yazılım sertifikası ve kök sertifika olarak sınıflandırılmaya tabi tutulmaktadır.

3.5.1- Bireysel Sertifika

Adından da anlaşıldığı gibi, kişisel bazlı tanımlamalarda kullanılan sertifikalardır. Diğer bir ifadeyle şahısların kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyalardır³⁴⁶. Bu sertifikalar, günlük hayatımızda kullandığımız ehliyet pasaport ya da kimlik kartlarının elektronik karşılıklarıdır. Bu sertifikalar ile kimlik doğrulama, bütünlük, gizlilik ve inkâr edilememe gibi fonksiyonlar gerçekleştirilebilir. Bu itibarla bireylerin internet üzerindeki güvenli ve gizli iletişim yeteneklerinden

³⁴⁶ Sağıroğlu-Alkan, s.125;

faaydalanabilmeleri için öncelikle bir e-kimliğe yani sertifikaya sahip olmaları gerekmektedir.



Şekil-3: Bireysel Güvenli (Nitelikli) Elektronik Sertifika Örneği

Bireysel veya kişisel sertifikalar ile elektronik bankacılıktan alışverişe, online abonelik servislerinden ticari ve resmi yazışmalara kadar her türlü işlem güvenli bir şekilde yapılabilir. Gönderilen bilgilerin şifrelenebilir veya deşifre edilebilir olması nedeniyle gizlilik sağlanabilir ve belki de en önemlisi, sertifika sahibinin kendisini, diğer kişilere ya da web sitelerine güvenli olarak tanıtmaya veya başkalarını güvenle tanıyabilmesi mümkün olur. Diğer bir ifade ile elektronik ortamda güvenli şekilde haberleşme imkânı doğar.

3.5.2- Sunucu Sertifikası

Elektronik ortamda, web sitesinin kimlik bilgilerini ve açık anahtarını taşıyan ve web sitesine bağlanan kullanıcıların sunucu ile veya sunucuların birbirleriyle güvenli olarak haberleşmesi için oluşturulan elektronik belgelere, *sunucu sertifikası* denir³⁴⁷. Güvenli ve güvenilir bir ortamı sağlayan sunucu sertifikaları, sunucular arası kimlik tanımlama ve şifreleme gibi özelliklerin gerçekleştirilmesini, ziyaret edilen web

³⁴⁷ Sağırođlu-Alkan, s.125; Orta, s.48

sitelerinin kimliğinin doğrulanmasını ve karşılıklı olarak yapılan haberleşmeyi şifreleyerek gizliliği sağlarlar.

Örneğin bir internet tarayıcısı kullanıcısı bir web sunucuya gizli bir bilgi göndermek istediğinde, tarayıcı tarafından içerisinde web sunucusunun açık anahtarını bulunduran sunucu sertifikası alınır ve gönderilecek olan bilgi sunucu sertifikası içindeki açık anahtar ile şifrelenir. Bu şifreli bilgiyi çözecek gizli anahtar sadece sunucuda bulunduğundan başka birisinin şifreyi çözmesi mümkün değildir. Aynı şekilde sunucu sertifikası sayesinde web sunucunun kimliğinin doğrulanması da yapılır.

3.5.3- Yazılım Sertifikası

Sertifikalar, sadece bireysel kullanıcıların değil yazılımların kimliklerinin tespitinde de kullanılabilirler. İşte yazılım şirketleri veya kişisel yazılımcıların ürettikleri yazılımları dijital olarak imzalayabilmelerini sağlayan sertifikalar yazılım sertifikalarıdır³⁴⁸. Bilgisayar kullanıcıları olan müşteriler, yazılım geliştiricilerin kimliğinden, yükledikleri programın, gerçekten o kurum, firma, kuruluş veya kişi sunucusundan geldiğinden bu sertifikalar sayesinde emin olabilirler. Bu sertifikalarda, kuruluş ve ülke adresleri ile e-posta adresleri yer alabilmektedir. Dolayısıyla bu sertifikalar ile kimlik, e-posta adresi ve kuruluş belgeleri doğrulanmaktadır. Bu sertifikalar, SSL şifreleme gibi ek özellikler de sunulabilmektedir.

3.5.4- Kök Sertifika

Kök sertifika, sertifika hizmet sağlayıcısının kimlik bilgilerini ve açık anahtarını taşıyan elektronik dosyalardır. Kök sertifikayı diğer sertifikalardan ayıran tek özellik, üzerinde kendi imzasını taşıyor olmasıdır. Kök sertifika, elektronik sertifika hizmet sağlayıcısının sertifikasıdır. Kullanıcılar sertifika hizmet sağlayıcısının kök sertifikasını internet üzerinden bilgisayarlarına yüklerken, sertifika kurumunun güvenilirliğini kabul etmiş sayılırlar. Sertifika ile birlikte gelen açık anahtar öncelikle sertifikasyon kurumunun yani sertifika hizmet sağlayıcısının kimliğini doğrulamakta kullanılırlar. Bu

³⁴⁸ Sağıroğlu-Alkan, s.125;

sayede söz konusu sertifikanın o hizmet sağlayıcısı tarafından onaylanmış, gerçek ve doğru bir sertifika olduğu teyit edilmiş olur³⁴⁹.

Kök sertifikaların kullanım amacı sertifika kurumlarının yayınladıkları diğer sertifikalara güvenilirlik onayının verilip verilmeyeceğinin belirlenmesidir. Örneğin bir web sunucusunun sertifikasını alan tarayıcı bu kimliğe güvenip güvenmeyeceğine karar verebilmesi için sunucuya sertifika veren sertifika Hizmet Sağlayıcısının sertifikasına ihtiyaç duyar. Bazı sertifika hizmet sağlayıcıları Netscape ve Internet Explorer gibi popüler olan tarayıcılarda önceden tanımlanmıştır. Diğer bir ifade ile sertifika hizmet sağlayıcılarının kök sertifikaları tarayıcıya yüklenmiş durumdadır. Diğer sertifika Hizmet sağlayıcılarının da tarayıcıya tanımlanabilmesi için kök sertifikalarının tarayıcıya yüklenmesi gerekmektedir.

3.6- Hash Fonksiyonu

Bilgisayar terminolojisinde “*Hash*”, yazılan bir mesajın, kısaltılmış şeklidir. Daha önce izah edildiği üzere, elektronik imzalamada, her kullanıcının bir açık anahtarı bir de gizli anahtarının bulunduğu asimetrik sistemler kullanılır. Açık anahtardan gizli anahtara ulaşmanın matematiksel karmaşıklığı pratik bir saldırı veya atak düzenlenemeyecek derecede yüksektir. Açık anahtarla doğrulama işlemi ve gizli anahtarla imza atma işlemi yapılır. Diğer taraftan asimetrik sistemler simetrik sistemlere göre son derece yavaştır. Bu nedenle asimetrik sistemler ile bir veriye imza atılmadan önce, simetrik bir algoritma ile imzalanacak verinin boyutu küçültülerek özeti elde edilir. Sayısal imza da verinin bu özetine atılır. Kriptografide bu tekniğe “*hash fonksiyonu*” adı verilmektedir³⁵⁰. Günümüzde kullanılmakta olan Elektronik İmza şemalarının temel olarak iki kısımdan oluştuğunu düşünebiliriz. Bu kısımlardan ilki imzalanacak verinin boyunu küçülterek özetini çıkaran “hash fonksiyonu” ikincisi ise oluşturulan özetin kriptografik olarak imzalayan “imzalama algoritması”dır. Özet fonksiyonları genellikle simetrik algoritma tabanlı ve hızlı algoritmalarıdır. Ayrıca özetin uzunluğu, verinin uzunluğundan bağımsız ve sabittir. Özet uzunluğu mesajın uzunluğu ne olursa olsun oldukça kısadır. Hash fonksiyonu ile oluşturulan mesaj özeti

³⁴⁹ Orta, s.47; Sağıroğlu-Alkan, s.82;

³⁵⁰ Sağıroğlu-Alkan, s.46; Orta, s.53; Keser Berber (Şekil), s.24; Altınışık, s.83; Erturgut, s.75;

verilerin parmak izi olarak düşünülebilir³⁵¹. Teknik açıdan dijital imza, imzalanmış belgenin özünü (Hash) içerir³⁵². Buradaki algoritma genel olup aynı belgeye kim tarafından uygulanırsa uygulansın aynı hash değeri elde edilir. Çünkü mesaj özeti, metnin karakteristik özelliklerinin tümü dikkate alınarak oluşturulmaktadır. Yapılacak en küçük bir değişiklik mesaj özetinin değişmesine yol açacaktır³⁵³.

Burada bilinmesi gereken husus, sayısal imza denilen olgunun metnin içeriğinde değil mesaj özeti üzerinde uygulandığıdır. Metni imzalayan kişinin özel anahtarı ve asimetrik şifreleme sistemi vasıtasıyla mesaj özeti şifrelenir ve bu şekilde şifrelenen mesaj özeti elektronik metne eklenerek muhabata gönderilir. Şifrelenen mesaj özeti metinden ayrı olarak tutulur. Mesaj özetinden bir şekilde metne ulaşmak mümkün değildir.

Mesaj alındığında öncelikle tekrar mesaj özeti çıkarılır. Gelen mesaj ekinde yer alan şifreli mesaj özeti gönderenin açık anahtarıyla deşifre edilir. Bu işlemle gönderenin kimliği doğrulanmış olur. Gelen mesaj özeti ile yeni hesaplama sonucu bulunan mesaj özeti karşılaştırılır. İkisi de aynı ise mesaj orijinaldir, değişikliğe uğramamış demektir. Böylelikle bütünlük kontrolü gerçekleştirilmiş olmaktadır. Metinde yapılacak en küçük bir değişiklik, muhatap tarafında çıkarılacak mesaj özetinin gönderen tarafta oluşan mesaj özetinden farklı olacağından doğrulama işleminin başarısızlıkla sonuçlanmasına yol açacaktır.

3.7- Zaman Damgası

Elektronik bir belgenin ispat gücünü artırmak için, diğer koşulların yanı sıra belgenin düzenlendiği zamanın şüpheye yer bırakmayacak bir şekilde tespit edilmesi gerekir. Zira elektronik ortamda işlemlerin yapıldığı zamanın tayini, işlem güvenliği açısından önemli olup, imzanın doğrulanması ve mesaj bütünlüğünün denetlenmesi açısından vazgeçilmez bir unsurdur. Mesajı alan taraf mesajın geçerli olup olmadığını denetleyebilmek için imzanın atıldığı tarihe ihtiyaç duyar. İşte elektronik ortamda doküman, kayıt, sözleşme gibi elektronik verilerin, belirli bir zamandan önce var olduğunu kanıtlamak için zaman damgası kullanılır. Zaman damgası elektronik

³⁵¹ İnalöz, s.31; Orta, s. 53

³⁵² Topaloğlu, s.121

³⁵³ Sağiroğlu-Alkan, s.46; Şenocak, s.100; Keser Berber (Şekil), s.25; Orta, s. 54; Altınışık, s.84;

ortamdaki işlemlere güvenilir zaman bilgisi eklenebilmesini sağlar³⁵⁴ ve üzerinde zaman bilgisi olması gereken elektronik başvuru, tutanak, sözleşme ve benzeri her türlü elektronik veri üzerinde kullanılabilir.

5070 sayılı yasaya göre zaman damgası, “*Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve/veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kayıt*” tır(m.3-h). Buna göre eğer bir sertifika bloke edilmişse, mesajın veya metnin, bloke zamanından önce mi, yoksa sonra mı imzalandığı durumu, sadece zaman damgası sayesinde tespit edilebilir. Keza, sertifika ve elektronik imzanın geçerlilik süresi olduğu için bu sürenin geçip geçmediği, daha açık bir ifadeyle imzanın kullanıldığı zamanda geçerli bir sertifikaya dayanıp dayanmadığı ve böylece bağlayıcılığı da zaman damgasıyla belirlenebilir. Birbirinden farklı irade beyanları içeren, örneğin, biri icabın kabul edildiğine, diğeri icabın reddedildiğine ilişkin açıklamaların hangisinin önce oluşturulduğunun tespiti de yine zaman damgası sayesinde mümkündür.

Normal bilgisayarlarda ve işletme sistemlerinde, tarih ve saat ayarı, fazla bir zahmete gerek olmadan, kolaylıkla değiştirilebilmektedir. Dolayısıyla zaman damgası, kişinin kendi kullandığı bilgisayar sistemi içinde oluşturulduğu takdirde, bunun değiştirilmesi de kolay olacaktır. Normal belgelerdeki gibi, elektronik belgelerde de tarih ve saatin doğru bir şekilde tespit edilmesi gerektiğinden, bunu başarmak için güvenli bir yönteme ihtiyaç vardır. Bu sebeple zaman damgası görevinin yerine getirilmesi de güvenilir üçüncü kişiler olan sertifika hizmet sağlayıcılarına yüklenmiştir. Sertifika hizmet sağlayıcıları talep üzerine dijital tarihleri zaman damgası ile belirtir ve zaman damgasının sonradan değiştirilmesini engellemek için, zaman damgasına ilişkin veriyi de imzalı veriye ekleyerek kendi elektronik imzası ile imzalar. Bu yöntem sayesinde imza verisiyle zaman damgası birbirine bağlanır ve sonradan zaman damgasında yapılacak değişikliklerin tespiti mümkün kılınmış olur³⁵⁵.

³⁵⁴ Keser Berber (Şekil), s.26; Orta, s. 55; Sağiroğlu-Alkan, s.83

³⁵⁵ Samast, s.1; Altınışık, s. 88; Keser Berber (Şekil), s.26; Erturgut, s.125; KamuSM

3.8- Sistemin İşleyişi ve Örnek Uygulamalar

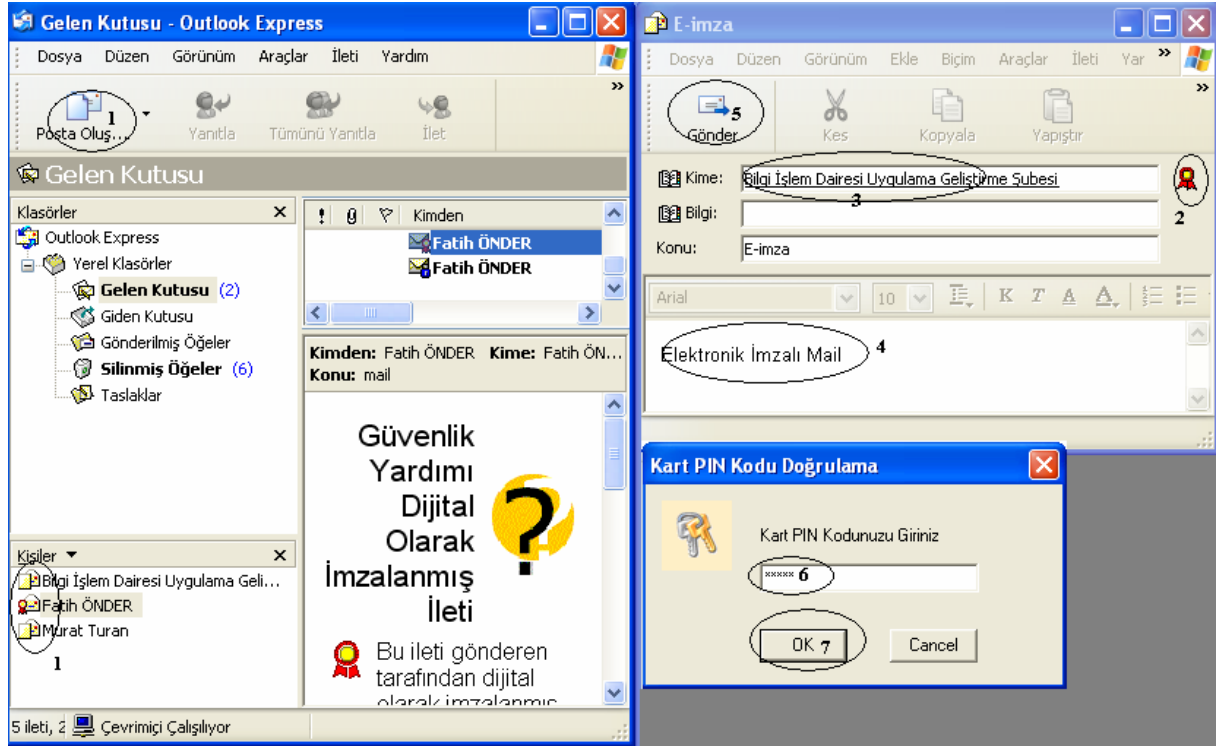
3.8.1- Sistemin İşleyişi


Elektronik ortamda dijital imzalı bir belge oluşturmak ve göndermek için öncelikle elektronik bir sertifika sahibi olunması gerektiğini yukarıda belirtmiştik. Yine bu sertifika ile daha doğrusu sertifikada yer alan açık anahtarla mantıksal bağı bulunan bir de özel anahtar sahibi olunması zorunludur. Zira gönderilecek belgenin imzalanabilmesi için bu özel anahtarın kullanılması gerekecektir. Özel anahtarın kullanımında yazılıma (software) dayalı olanlar ve donanıma dayalı olanlar olmak üzere iki yöntem bulunmaktadır. Yazılıma dayalı olanlarda bir program aracılığıyla özel anahtara ulaşılır. Bu yöntemde giriş kodu yazılarak sisteme girilir ve işlemler başlatılır. Donanım esaslı yöntemde ise, elektronik sertifika hizmet sağlayıcısının özel anahtarı kopyaladığı akıllı kart (smartcard) veya akıllı çubuk (e-token) bilgisayara takılarak ve bu cihazın giriş şifresi (PIN) girilerek özel anahtara ulaşılır³⁵⁶. Şuan için genel kullanım ve yasanın öngördüğü şartları taşıyan yöntem donanıma dayalı olan yöntemdir. Ancak her iki halde de elektronik imzayı kullanabilmek için öncelikle elektronik sertifika ve bu sertifikayı veren ESHS'nin kök sertifikasının bilgisayara yüklenmiş olması gerekmektedir.

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

³⁵⁶ Altınışık, s.91; Orta, s.44; Keser Berber (Şekil), s.18

mesaja eklenir³⁵⁷. Bu işlemde şifreleme özel anahtar ile yapılır 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.

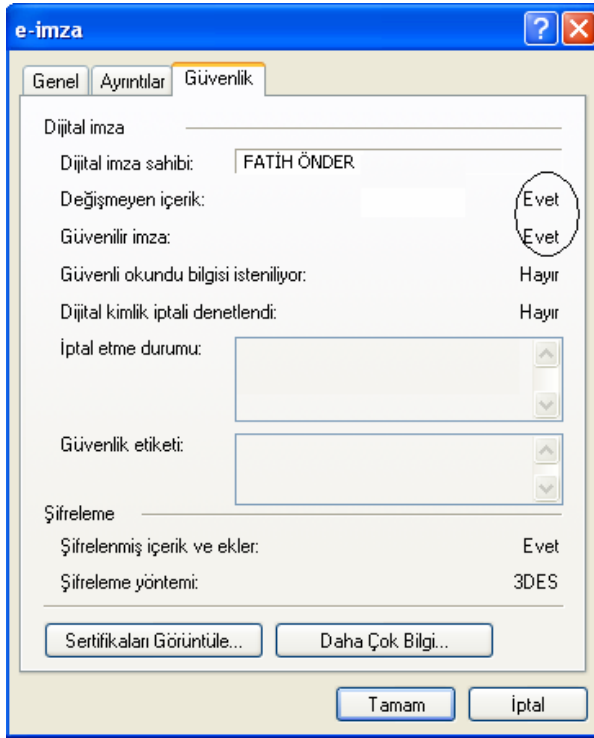



Şekil-4: Outlook Express'te elektronik imzalı mail gönderme prosedürü. Daire içerisinde alınmış  işareti gönderilecek mailin elektronik imzalı olacağını belirtmektedir.

Alıcı mesajı aldığı anda, 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

³⁵⁷ Sağiroğlu-Alkan, s.71; Orta, s.56; Altınışık, s.92;

hizmet sağlayıcısının ilan ettiği kişi olduğu anlaşılır.³⁵⁸ Bu şekilde mesajın bütünlük kontrolü ve kimlik tespiti fonksiyonları gerçekleştirilmiş olur. Ancak bu fonksiyonların yanında gizlilik de isteniyorsa bu durumda şifreleme metodu kullanılabilir.



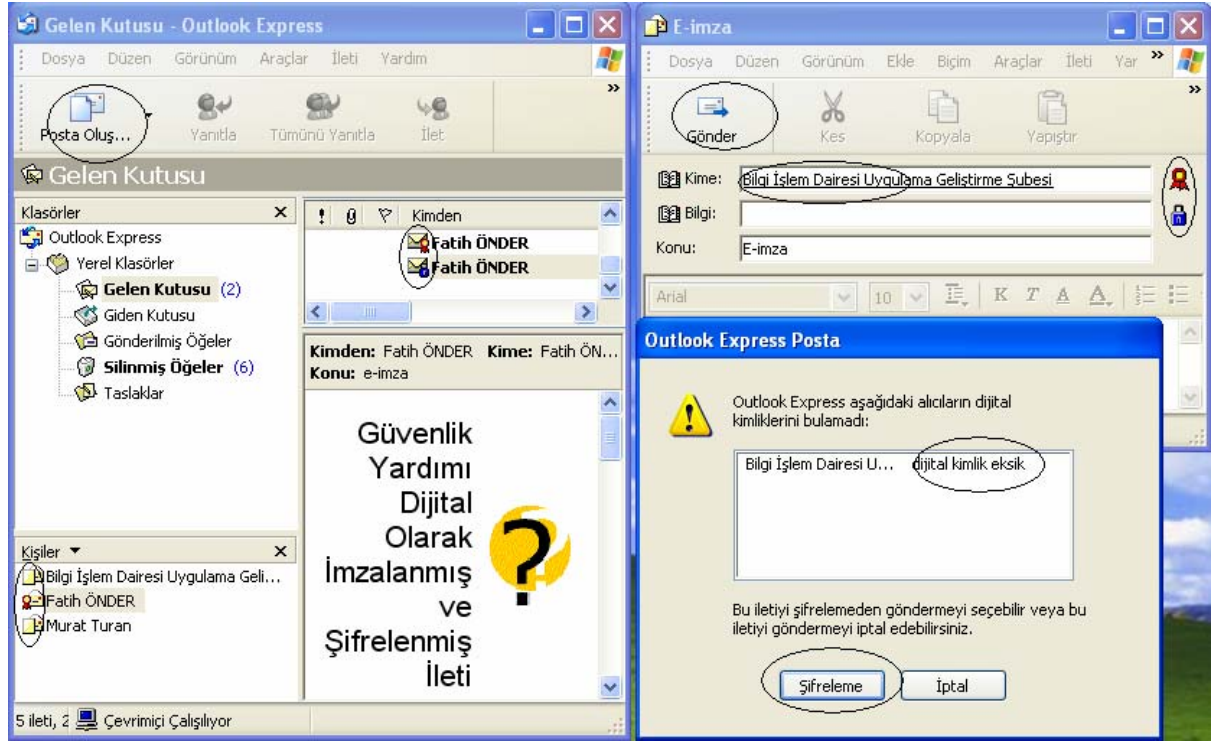
Şekil-5: Outlook Express'te elektronik imzalı olarak gelen maildeki  işareti üzerine kliklenmesi neticesinde yazılım tarafından otomatik olarak yapılan kimlik doğrulama ve bütünlük kontrolü.



Gönderici oluşturduğu mesajı alıcıya gizli olarak yani sadece alıcı tarafından açılacak şekilde göndermek isterse, öncelikle yine yukarıdaki metoda göre mesajın hash değerini elde ederek özel anahtarı ile şifreler ve mesaja ekler. İkinci aşamada ise, bu kez ekinde elektronik imza yani hash değeri de olduğu mesajın tamamını alıcının genel anahtarı ile şifreler ve alıcıya gönderir. Artık bu mesaj alıcının özel anahtarı dışında bir anahtar veya yöntemle açılmayacağından üçüncü şahıslar mesajı okuyamaz veya müdahale edemez (**gizlilik**)³⁵⁹. Alıcı mesajı aldığı anda önce kendi özel anahtarı ile mesajı deşifre eder. Daha sonra yukarıda anlatıldığı şekilde hash değeri kontrolü yaparak mesajın değişmediğini (**bütünlük**) ve gerçekten gönderen gözüken kişiden geldiğini (**kimlik tespiti**) tespit eder. Buradan da anlaşılacağı üzere, elektronik imzalı ve gizli (şifrelenmiş) mesaj veya belge oluşturmak yada gönderebilmek için alıcının da elektronik imzasının bulunması ve açık anahtarının gönderen tarafından bilinmesi daha

³⁵⁸ Sağiroğlu-Alkan, s.71; İnalöz, s.45-46;Altınışık, s.83-92; Keser Berber (Şekil), s.27; Şenocak, s.100; Özgül,s.8

³⁵⁹ Sağiroğlu-Alkan, s.65; Önel, s.4; Winn, s.35

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



Şekil-6: Outlook Express'te elektronik imzalı mail gönderme prosedürü. Daire içerisine alınmış  işareti gönderilecek mailin elektronik imzalı olacağını  işareti ise alıcının açık anahtarı ile şifreleneceğini belirtmektedir. Alıcı elektronik imza sahibi gözüküyor ise açık anahtarı sistem tarafından bilinemeyeceğinden şifreleme prosedürü çalışmaz.

Gönderilen mesajın imzalandığı tarihin de belirlenmesi istenirse, o halde sertifika hizmet sağlayıcısının sunduğu bir hizmet olan zaman damgası fonksiyonu çalıştırılır³⁶⁰. Yani gönderici tarafından talep edilmesi halinde mesajın alıcıya gönderilmesi aşamasında, sertifika hizmet sağlayıcısının imzasını taşıyan ve zamanı tayin zaman damgası da mesaja eklenir ve alıcıya gider. Bu sayede herhangi bir ihtilafa yer verilmeksizin zamanın tayini yapılmış olur. Yukarıda anlatmaya çalıştığımız imzalama prosedürü ilk bakışta karmaşık ve zor gibi görünse de durum zannedildiği kadar zor değildir. Bir metni dijital olarak imzalamak istediğimizde yukarıda bahsedilen kontrolleri ve işlemleri bilgisayar kendisi gerçekleştirmektedir. Aslında sayısal imzanın

³⁶⁰ Sağıroğlu-Alkan, s.73

oluşturulması ciddi bir matematiksel süreci gerektirir. Bu süreçte altyapısı çok karmaşık olan algoritmalar kullanılır. Ancak bu algoritmalar ve karmaşık işlemlerden kimsenin haberi olmaz. Biz kullanıcılara düşen görev, imzalama butonuna tıklamaktan ibarettir.

3.8.2- Örnek Elektronik İmza Uygulamaları

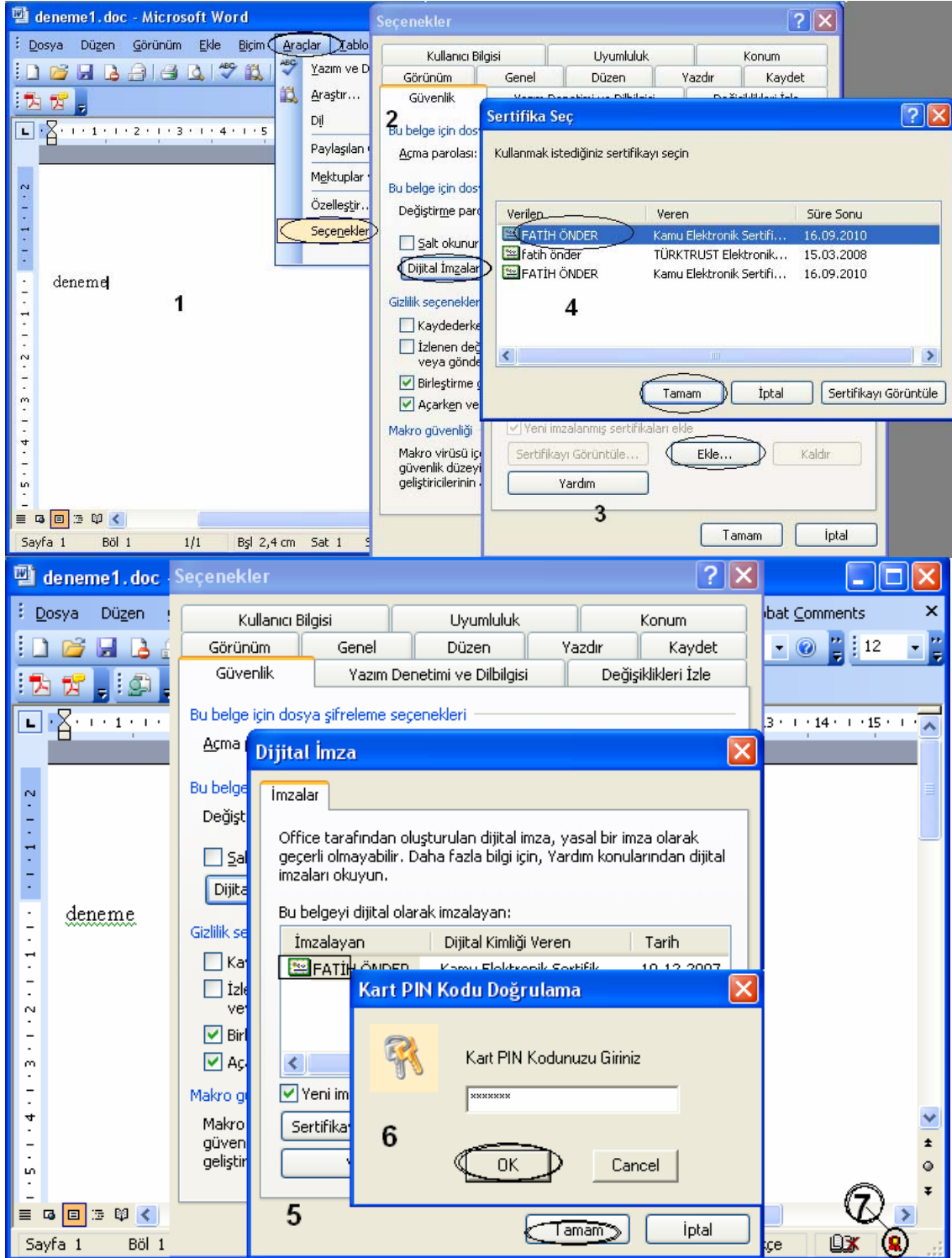
Elektronik imzanın gerek hukuki gerekse teknik yönlerini önceki bölümlerde açıklamaya çalıştık. Şimdi ise elektronik imzanın pratik olarak nasıl kullanıldığını birkaç genel uygulamada göstererek daha iyi ve kolay anlaşılmasını temin etmeye çalışacağız.

Öncelikle bir belgeyi elektronik olarak imzalayabilmek için bir elektronik kimliğe yani sertifikaya ve bu sertifika ve gizli anahtarı içerisinde barındıran bir imza oluşturma aracına gereksinim bulunmaktadır. Bunun haricinde ise unutulmaması gereken en önemli husus bu sertifikanın bilgisayarımıza kurulması ve bilgisayarın imzalama işlevi sırasında imza oluşturma aracına bağlanıp içerisinden gizli anahtarı okuması gerekeceğinden, imza oluşturma aracının bilgisayara tanıtılması ve içerisine erişilebilmesi için gerekli yazılım ve sürücünün bilgisayara kurulmuş olması gereklidir. Söz konusu yazılımlar nitelikli elektronik sertifika ve güvenli elektronik imzanın temin edildiği ESHS tarafından kullanıcıya verilmektedir. Bu saydıklarımızın tamamı elimizde var ise artık elektronik olarak imzalamaya hazırız demektir. Aşağıda Microsoft Word, Adobe Acrobat, Uyp Kelime İşlemci ve İmzager MİM uygulamalarındaki elektronik imza prosedürleri anlatılmıştır.

• **Microsoft Word:** Bu yazılım neredeyse tüm bilgisayarlarda kullanılmakta olan ve doküman hazırlamakta kullanılan ve elektronik imzayı destekleyen yaygın bir yazılımdır. Hazırlanan bir dokümanın imzalanması ise aşağıdaki şekilde imzalanır.

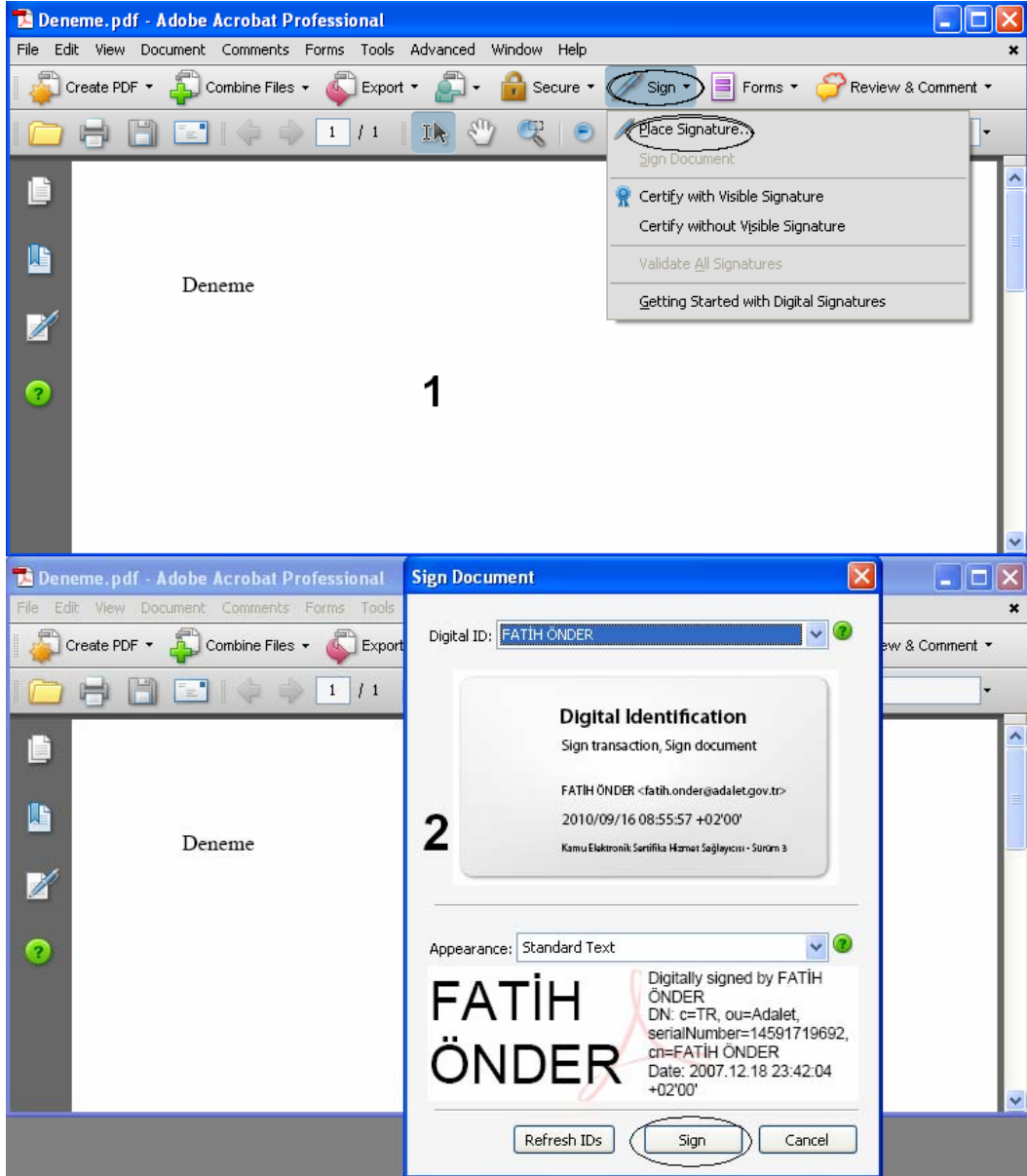
Aşağıda da görüldüğü gibi öncelikle bir belge oluşturulur ve kaydedilir. Daha sonra elektronik imza oluşturma aracı bilgisayara takılır ve sırasıyla “Araçlar” ve “Seçenekler” menüsü tıklanır. Seçenekler ekranı açılınca(2) “Dijital İmzalar” butonu tıklanır ve “Dijital İmza” menüsünden (3) “Ekle” butonuna tıklanır. “Sertifika Seç” (4) menüsünden sertifika seçilir ve seçilen sertifika “Dijital İmza” menüsünde(5) görüntülenir. Bu menüde “Tamam” butonu tıkladığında imza oluşturma aracının PIN

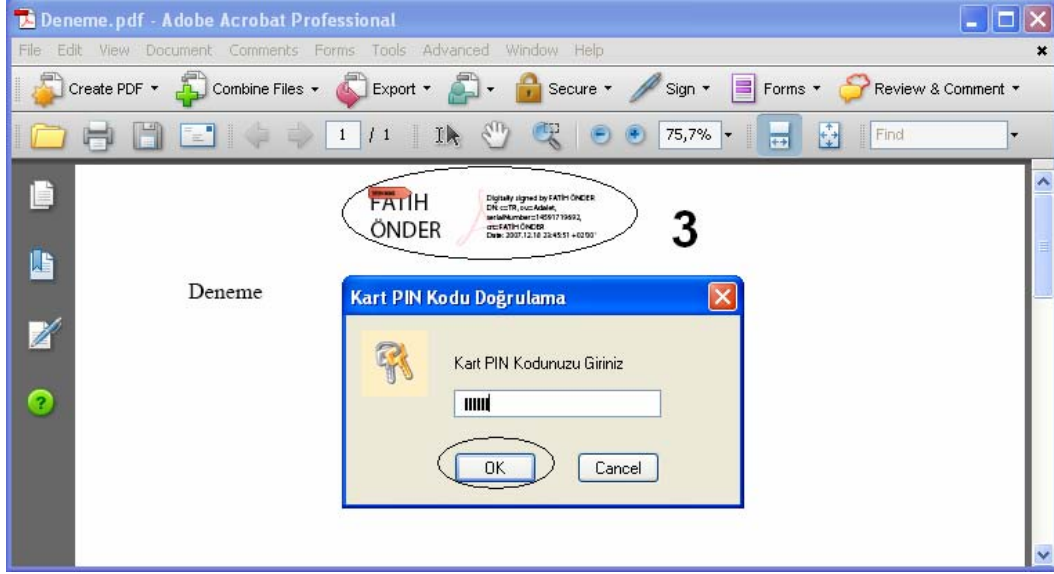
kodu istenir. PIN kodu girilip “OK” butonuna tıklanınca imzalama işlemi gerçekleşir ve yazılımın sağ alt köşesinde elektronik imzanın var olduğuna ilişkin işaret (7) belirir. Bu işaret üzerine tıklanarak imza sahibinin kimlik tespiti, vs. kontroller yapılabilir. Microsoft Excel ve Powerpoint gibi yazılımlarda da imzalama prosedürü aynıdır.



Şekil-7: Microsoft Word’da Elektronik İmzalama Prosedürü

• **Adobe Acrobat Professional:** Bu yazılım genelde Microsoft Word ve benzeri yazılımlarla oluşturulan dokümanları yada bilgisayara bağlı donanım yardımı ile gerçek ortamdan elektronik ortama aktarılan doküman ve resimleri sadece okunabilip üzerinde kolayca değişiklik yapılamayan “PDF” formatına çeviren bir yazılımdır. Dolayısıyla doküman üzerine atılan elektronik imza da kolaylıkla silinemez. Söz konusu yazılım ile elektronik imzalama işlemi ise aşağıdaki şekilde gerçekleştirilir.



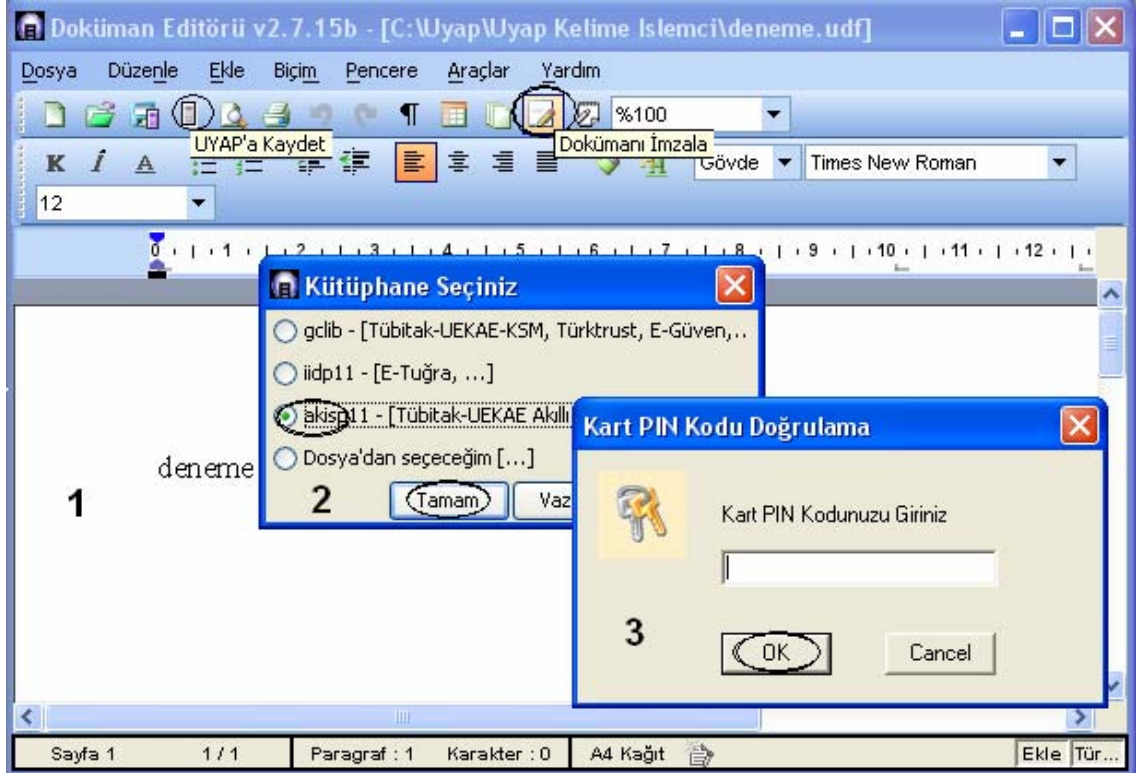


Şekil-8: Adobe Acrobat'ta Elektronik İmzalama Prosedürü

Öncelikle imzalanacak belge “PDF” formatında kaydedilir. Daha sonra imza oluşturma aracı bilgisayara takılarak, “Şekil-8” de gösterildiği şekilde sırasıyla ekrandaki “Sign” ve “Place Signature” seçenekleri tıklanıp (1) dokümanda imzanın ekleneceği yer seçildiğinde, “Sign Document” menüsü ekrana gelir(2). Bu menüde sertifika seçilerek “Sign” butonuna tıklanır. Kart PIN kodu girildiğinde imzalama gerçekleşir ve imzanın eklendiği yerde(3) elektronik imza sahibi ve imzalama zamanına ilişkin bilgiler gösterilir.

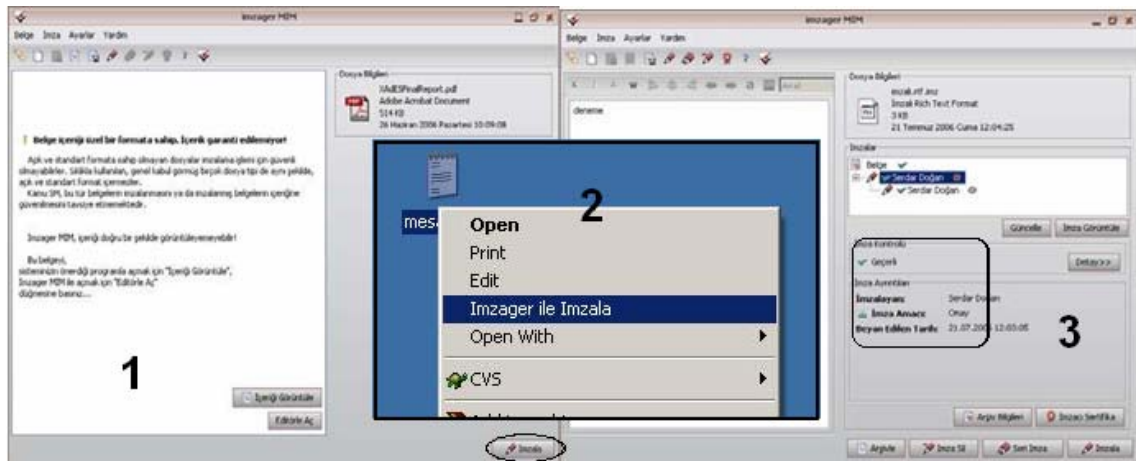
• **Uyap Kelime İşlemci:** Bu yazılım Adalet Bakanlığı tarafından geliştirilen ve Ulusal Yargı Ağı Projesi kapsamında tüm adliyelerde kullanılan yazılımdır. Bu yazılım ile hazırlanan ve sisteme kaydedilen tüm evraklar, daha sonradan erişilebilecek şekilde sistem tarafından saklanmakta ve üzerinde izinsiz değişiklik yapılamamaktadır. Dolayısıyla bu şekilde hazırlanan ve elektronik olarak imzalanan evrak resmi evrak olarak sisteme kaydedilmekte ve el yazısı imzalı sureti olmasa da yasal olarak geçerli olmaktadır.

Bu yazılım ile elektronik imzalama işlemi ise oldukça basittir. Yazılım ile oluşturulan belge açılıp “Şekil-9” da ki gibi ekrandaki “Dokümanı İmzala” ikonuna tıkladığında açılan pencereden (2) elektronik imza oluşturma aracının niteliğine uygun seçenek seçilip “Tamam” butonuna tıklanınca imza oluşturma aracının PIN kodu istenecektir. PIN kodu girilip “OK” butonuna basıldığında imzalama gerçekleşir. Son olarak ise “UYAP’a Kaydet” butonuna tıkladığında belge sisteme kaydedilecektir.



Şekil-9: Uyap Kelime İşlemci İle Elektronik İmzalama Prosedürü

• **İmzager-Mim Yazılımı:** Bu uygulama özel olarak geliştirilen elektronik imzalama yazılımlarından birisidir ve ülkemizde kök sertifikasyon makamı olarak görev yapan Tubitak-UEKAE tarafından geliştirilmiştir. Diğer ESHS kuruluşları da bu amaçla kullanıcılarına farklı yazılımlar sunmaktadırlar.



Şekil-10: İmzager-MİM Yazılımı İle Elektronik İmzalama Prosedürü

Şekilde İmzager yazılımının üç farklı kullanımı birlikte verilmiştir. Her üç ekranda da “İmzala” butonuna mouse ile tıklanarak ve imza oluşturma aracının PIN

kodu girilerek imzalama işlemi gerçekleştirilmektedir. Şekilden de anlaşılacağı üzere, bilgisayarda kayıtlı bir dosya yazılım ile açılarak veya yeni olarak hazırlanarak (1) veya kayıtlı dosya üzerine farenin sağ tuşu ile tıklanarak (2) imzalama gerçekleştirilebilmekte ve yine imzalı bir belge söz konusu yazılım ile açılarak mevcut elektronik imzanın kontrolü yapılabilmektedir(3).

Bu uygulamalar örnek nitelikte olup, sadece elektronik imzalama yapmak amacıyla geliştirilen veya daha farklı ve geniş amaçlarla geliştirilip elektronik imzayı da destekleyen çok sayıda yazılım mevcuttur ve her geçen gün bunlara yenileri eklenmektedir.

SONUÇ VE ÖNERİLER

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 ticarete sınırlar ortadan kalkacak, iş yapış ve sunuş metodolojileri değişecek, hizmetler hızlanacak, hizmet alış ve sunuş türleri farklılaşacak, karşılaşılabilecek problemler azalacak ve ticari yaşam boyut değiştirecektir.

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

Ayrıca bilgi ve belgeler, elektronik ortamda bir arşivde gizliliği sağlanarak tutulabilecek ve mevcut durumda kullanılan dosya ve arşivleme gibi uygulamalarda tasarruf sağlanabilecektir. Dolayısıyla kağıt ortamında zaman, para ve hizmet kalitesi kaybına sebep olan iş ve işlemler daha etkin, güvenli ve hızlı bir şekilde yapılarak, hizmet, zaman, mekan, kağıt ve kırtasiye tasarrufu sağlanmasıyla da verimlilik büyük oranda artacaktır.

Elektronik imza uygulamalarına tam anlamıyla geçildiğinde, hayatımız bütün yönleriyle etkilenecek ve ticari, hukuki ve sosyal yönlerden önemli bir değişim ve dönüşüm süreci yaşanacaktır. Özellikle, e-dönüşüm ve e-devlet sürecinde yaşanan bu

değişim, kendisini hissettirecektir. Devlet sektöründe gereksiz bürokrasi azaltılacak, kağıt ve zaman tasarrufu büyük ölçüde sağlanacak, kurum içi ve kurumlar arası işletilebilirlik sağlanacak, standart çözümler geliştirilebilecek, internet ortamında daha yüksek bilgi güvenliği sağlanacak, iş süreçleri iyileştirilebilecek, iş gücünün doğru kullanımı sağlanabilecek, önemli belgelerin güvenli olarak dağıtılması ve yönetimi gerçekleştirilebilecektir. Sosyal hayatta ise, vatandaşların veya sistem kullanıcılarının, hayatını kolaylaştıracak, beklentilerini arttıracak, yaptığı işlemleri hızlandıracak, verimliliği arttıracaktır. Ayrıca, elektronik imza sayesinde veri güvenliği, gizlilik, veri bütünlüğü, değiştirilemezlik ve inkar edilemezlik hususlarında önemli gelişmeler sağlanarak, elektronik işlemler daha güvenli bir ortamda yapılacaktır. Bu durum ülkemizde internet kullanımı başta olmak üzere, bilişim teknolojilerinin kullanımını önemli ölçüde arttıracak ve yaygınlaştıracaktır.

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

Sayısal devlet olma yolunda çabaladığımız, e-devlet, e-dönüşüm çalışmalarının çokça konuşulduğu ve icraata dönüştürülmeye çalışıldığı 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 karşılaştığı 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 artırılabilir, işlemler hızlandırılabilir, maliyetler düşürülebilir, müşteri memnuniyeti artırılabilir, zamandan ve mekandan tasarruf sağlanarak hayat daha yaşanılabilir bir hale gelebilecektir. Bunun sağlıklı olarak yapılabilmesinin tek yolu ise, bilgi güvenliği unsurlarını tamamıyla sağlayan ve hukuken de geçerli olan, elektronik imza ve açık anahtar altyapısının kullanılmasıdır.

Bu teknolojilerinin kullanımının ve üretiminin artması, bilinçli internet kullanımının yaygınlaştırılmasıyla olacaktır. Ülkemizin mevcut haberleşme altyapısının genel olarak değerlendirildiğinde çok iyi durumda olmadığı ve bilişim teknolojileri kullanımının yeterli düzeyde olmadığı bilinmektedir. Devlet İstatistik Enstitüsü'nün 2004 yılı raporunda, bu oranın %14 seviyelerinde olduğu açıklanmıştır. Bu itibarla yeni politikalar ve yaklaşımlar üretilerek, mevcut altyapının hızının artırılması, internet ve bilişim teknolojileri kullanımının yaygınlaştırılması için yeni stratejilerin geliştirilmesi gereklidir. Zira ancak haberleşme altyapısının geliştirilmesiyle, elektronik imza ve AAA yapıları, daha sağlıklı olarak kurulabilecek, işletilebilecek ve yaygınlaştırılacaktır. Yine bilişim teknolojileri kullanımının artırılması için toplumsal ve kamusal bilgilendirme ve bilinçlendirme faaliyetlerinin yapılması önem arz etmektedir.

Mevcut hukuki düzenlemeler değerlendirildiğinde, 5070 sayılı Elektronik imza Kanunu'nun bugünkü ihtiyaçları karşılayabilecek şekilde düzenlendiği ve özellikle

Borçlar Kanunu ve Hukuk Usulü Muhakemeleri Kanunu'nda yapılan deęişikliklerle Türkiye'de elektronik imzanın kullanımı için yasal altyapının hazır hale getirildięi söylenebilir. Ancak elektronik ortamdaki metinlerin yazılık işlevi ve nitelikli elektronik sertifikaya dayanmayan elektronik imzaların hukuki nitelięi ve deęeri hususlarında herhangi bir düzenlemenin mevcut olmayışı da önemli bir eksiklik olarak karşımıza çıkmaktadır. Oysa nitelikli bir elektronik sertifikaya dayanmayan elektronik imzaların da veri bütünlüğü dahil, el yazısı ile imzanın birçok işlevini yerine getirebildięi görülmektedir. Yine Elektronik İmza Direktifi'nin 5 inci maddesi gereęince elektronik imzaların nitelikli bir sertifikaya dayanmaması onun hukuki etki doğurmasına veya yargılamada delil olarak kullanılmasına engel teşkil etmemelidir. Bu itibarla güvenli elektronik imza dışındaki elektronik imza türlerine de hukuki deęer tanıyan yeni bir hukuki düzenleme yapılması veya mevcut düzenlemenin bu yönde genişletilmesi ya da en azından bu nitelikteki elektronik verilerin delil deęerini artıran ve yazılık işlevinin kapsamını deęiştiren “Türk Borçlar Hukuku” ve “Hukuk Muhakemeleri Usulü” kanun tasarılarının bir an önce yasalaşması gerektięi kanaatindeyiz.

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

Özetle diyebiliriz ki; yapılması gerekenler olmakla birlikte, mevcut elektronik imza ve AAA uygulamaları, toplumsal deęişim ve dönüşümde önemli bir rol oynayarak, ekonomik, teknik, hukuki ve sosyal gelişmeler açısından müspet sonuçlar doğuracak, ölkemize, ölkemiz insanına, bilişim sektörünün yapılanmasına ve yaygınlaşmasına büyük katkılar sağlayacaktır.

KAYNAKÇA

8 Mayıs 1998 tarihli Dış Ticaret Müsteşarlığı, Elektronik Ticaret Koordinasyon Kurulu, **Elektronik Ticaret Hukuk Çalışma Grubu Raporu**

<http://www.e-ticaret.gov.tr/Raporlar/hukuk.htm>

ACIR, Birsen; “Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi” Ankara, 2000

AHI, M. Gökhan, “Hukuki Bakımdan Dijital (Sayısal) İmza”

<http://www.hukukcu.com/bilimsel/kitaplar/sayisalimza.htm>

AKINCI, Şahin; “Borçlar Hukuku Bilgisi” Konya, 2006

AKINTÜRK, Turgut; “Borçlar Hukuku” İstanbul, 2006

ALTINIŞIK, Ulvi; “Elektronik Sözleşmeler”, Ankara, 2003

ALTUNDAĞ, Salahattin; “Dijital İmzanın Ticari Hayatta Kullanılması ve Düzenlenmesi” Gazi Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 10, Sayı: 1-2, Ankara, 2006

ARIKAN, Saadet; “Dünyada ve Türkiye’de Elektronik Ticaret Çalışmalarına Hukuki Bir Yaklaşım”, Ankara 1999

ATAMER, Yeşim M.; “İnternet ve Hukuk” İstanbul, 2004

AYDEMİR, İbrahim; “Elektronik Ticaret Alanındaki Rekabet Sorunları”
Ankara, 2004

BABÜR, Zafer; “Mühürden Elektronik İmzaya”
<http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=31&YazarNo=32>

BAŞYİĞİT, Özgür; “Sözleşme Serbestisi ve Sınırlanması”
http://www.hukukcu.com/bilimsel/kitaplar/sozlesme_serbestisi_ve_siniri.htm

BECENİ, Yasin; “Elektronik İmza ve Uygulamalar”
www.e-imza.gen.tr/templates/resimler/File/sunumlar/Eimza_21Ocak2006_Yasin_Beceni.ppt

BEKTAŞ, Atilla; “Bilgi Güvenliği ve Kriptografi”
http://www.pki.iam.metu.edu.tr/yazi-makale/abektas_01.pdf

BİÇKİN, İnci; “Elektronik İmza Kanunu ve Getirdiği Düzenlemeler”
[Yargıtay Dergisi, c.30, sy.3, Temmuz, 2004](http://www.yargitaydergisi.com.tr/c30/sy3/temmuz2004)

BİRSEN, Kemalettin; “Borçlar Hukuku Dersleri”, İstanbul, 1954

BOZBEL, Savaş; “İnternet Üzerinden Yapılan Hukuki İşlemler ve Bu Konudaki 97/7 Sayılı AB Yönergesi ile Alman ve İsviçredeki Düzenlemeler”
http://www.hukukcu.com/bilimsel/kitaplar/internet_uzerinden_hukuki_islem.htm

BOZBEL, Savaş; Murat ATALI; “Mesafeli Sözleşmelerde Cayma Hakkının Kullanılması ve Ortaya Çıkan Hukuki Sorunlar” Erzincan Hukuk Fakültesi Dergisi, C: 9, Sy: 1-2 Erzincan, 2005

BÜLTER, Ahmet; “Tüketicinin Korunması Hukukunda Mesafeli Sözleşme Kavramı” Gazi Üniversitesi Endüstriyel Sanatlar Eğitim Fakültesi Dergisi Y.11, S.13, Ankara, 2003

BÜYÜKAY, Yusuf; “İnternette Kurulan Mesafeli Sözleşmelerde Tüketicinin Korunması” <http://www.e-akademi.org/icerik.asp?kategori=Makale&kid=1&git=24>, E-Akademi Dergisi, Şubat 2004

CANPOLAT, Önder; “E-Ticaret ve Türkiye’deki Gelişmeler” Ankara, 2001

CARON, Nancy, “Elektronik İmza Yasal mı?”

<http://www.girisim.com.tr/bankatek/sayi11/kisa2.htm>

ÇAMURDAN, Çiğdem; “Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme” http://dergi.tbd.org.tr/yazarlar/26052003/cigdem_camurdan.htm

ÇANGA, Tarık Mete; “Elektronik İmza ve Elektronik İmza Yasa Çalışmaları” www.etkk.gov.tr/hukuk.htm

ÇOMAKLI, Şafak Ertan; “5070 Sayılı Elektronik İmza Kanunu Uygulaması ve Hukuki Sonuçları” http://www.muhasibetr.com/e_imza/06/

DELİDUMAN, Seyithan; “Elektronik Verilerin Delil Değeri”, <http://www.e-akademi.org/makaleler/sdeliduman-1.htm>

DEMİR, Mehmet; “Mesafeli Sözleşmelerle İlgili AB Yönergesine Göre Tüketicinin Geri Alma Hakkı”, Gazi Üniversitesi Hukuk Fakültesi Dergisi Cilt:VII, Sayı: 1-2, Ankara 2003

DEMİREL, İnci; “Hukuk Elektronik Yaşam ve Ticaretin Hizmetinde veya Siber Uzayda Hukukun Yükselişi” <http://www.dtm.gov.tr/dtmadmin/upload/EAD/TanitimKoordinasyonDb/inci.doc>

“**Elektronik İmza El Kitabı**”; Ankara Barosu-Türkiye Bilişim Derneği Ankara, 2006

“**Elektronik İmza Kanunu**” Genel Gerekçe ve Madde Gerekçeleri <http://www2.tbmm.gov.tr/d22/1/1-0613.pdf>

“**Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu**”, İstanbul, 2004

“**Elektronikteki Gelişmeler ve Hukuk**”, Noterlik Hukuku Araştırma Enstitüsü, Ankara, 2001

ENSARİ, Bedii; “Elektronik İmza Yasası Yürürlükte”

<http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=22&YazarNo=23>

ERDOĞAN, Melih; Aziz Arman KARAGÜL; Cemal ELİTAŞ; “Elektronik Veri Değişimi Güvenliği ve Elektronik İmza”, Prof. Dr. Yüksel Koç Yalkın’a Armağan, Ankara, 2003

EREN, Fikret; “Borçlar Hukuku Genel Hükümler”, C.I, İstanbul, 1998

ERGÜN, Ömer; “5070 Sayılı Elektronik İmza Kanunu ve Dijital İmza” Türkiye Noterler Birliği Hukuk Dergisi, Sy: 122, S. 63-73, Ankara, 2004

ERMİŞ, Kemal; “Sayısal İmza ve Elektronik Belge Yönetimi” Bilgi Dünyası, 2006

EROL, Hüseyin; “Sayısal (Elektronik) İmza ve Açık Anahtar Altyapısı”, Ankara, 2004 http://www.nvi.gov.tr/attached/NVI/sayisalimza/HuseyinEROL_BBG.pdf

ERTURGUT, Mine; “Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi”, Ankara, 2004,

“ETKK Hukuk Çalışma Grubu Raporu”

http://enoter_hukuk.tripod.com/icelnoterodasicjb/tic.htm

EVRİM, Semlin; Ali Arman OKAN; “Hukuk ve Psikoloji Açısından İmza ve Elyazısı” İstanbul, 1976

FALCIOĞLU, Mete Özgür; “Türk Hukukunda Elektronik Satım Sözleşmesi ve Kuruluşu” Ankara, 2004

GENÇ, Hasan; “Açık Anahtar Altyapısı ve Problemleri”

<http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/PKI-problems.pdf>

GEZDER, Ümit; “Mukayeseli Hukuk Açısından İnternette Akdedilen Sözleşmelerde Tüketicinin Korunması” İstanbul, 2004

GÖKALP, Ziya; “PKI (Public Key Infrastructure) Açık Anahtar Altyapısı”
http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=272

GÜLAÇTI, Ersin; “Bir Açık Anahtar Altyapısı Nasıl Planlanmalı” Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, s. 217-220, İstanbul, 2006

HMUK, Tasarısı ve gerekçesi, <http://www.kgm.adalet.gov.tr/gorus/hmk.htm>

İNAL, Emrehan; “E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması”, İstanbul, 2005

İNALÖZ, Ayşe; “Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi”, Ankara, 2003

KALPSÜZ, Turgut; “Noterlik Hukuku ile İlgili Bazı Sorunlar, Türk Hukuk Dili, Noterlik ve Tebligat Hukuku”, Noterlik Hukuku Sempozyumu, Ankara, 1999

KAPLAN, Yavuz; “İnternet Ortamında Fikri Hakların Korunmasına Uygulanacak Hukuk” Ankara, 2004

KARAHASAN, Mustafa Reşit; “Türk Borçlar Hukuku” Ankara, 2003

KARAKOÇAK Kemal; Osman SAKA; Ashhan TÜFEKÇİ; Neziha ÇARKIT; Aysim HANÇER; Mehmet EKİZ; Ufku KANDEMİR; Burçin ÖKSÜZ; Ahmet AYVALI; Çiğdem ÇAMURDAN; “E-İmza'nın Toplumsal Boyutu” Antalya, 2005

KAYA BENSGHİR, Türksel; “E-Dönüşüm ve E-İmza ve Uygulamaları” TODAİE Elektronik İmza Semineri, Ankara, 2006

KESER BERBER, Leyla; “Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi”
<http://turk.internet.com/haber/yazigoster.php3?yaziid=6212>

KESER BERBER, Leyla; “İmzalıyorum, O Halde Varım”, Türkiye Barolar Birliği Dergisi, 2000/2, s. 503-556

KESER BERBER, Leyla; “Şekil ve Dijital İmza” Ankara, 2001
http://www.hesy.de/sekil/SEKIL_VE_DIJITAL_IMZA.htm

KILIÇLI, Tolga; “Üniversitelerde Akıllı Kart Destekli PKI Uygulaması ve E-Kimlik” <http://www.inet-tr.org.tr/inetconf7/bildiriler/8.doc>

KIRCA, Çiğdem; “İnternette Sözleşme Kurulması”, Banka ve Ticaret Hukuku Dergisi, C:XX, Sy: 4, Ankara, 2000

KODAZ, Halife; “RSA Şifreleme Algoritmasının Uygulaması”
<http://ab.org.tr/ab03/sunum/90.doc>

KONURALP, Haluk; “Genel Hatlarıyla Elektronik İmza Kanunu”,
<http://www.tbb.org.tr/turkce/konferans.htm>

KURU, Baki; “Hukuk Muhakemeleri Usulü”, C: I-II-III, İstanbul, 2001

KÜÇÜKÖZYİĞİT, H.Galip; “Elektronik Ticaret, Elektronik İmza ve Hukuk”
www.geocities.com/ceteris_paribus_tr2/g_kucukozyigit2.doc

LEVİ, Albert; “Türkiye’nin PKI Altyapısı Nasıl Olmalı?”
<http://www.teknoturk.org/docking/yazilar/tt000043-yazi.htm>

NOMER, N. Füsün; “Borç Sözleşmelerinde Şekik Eksikliğinin Müeyyidesi ve Buna Dayalı Hükümsüzlüğün Dürüstlük Kuralı (MK. m. 2/II) Dışındaki Yollardan Giderilmesi” Prof.Dr.Kemal Oğuzman’ın Anısına Armağan, s.595-626, Ankara, 2000

OĞUZMAN, Kemal; M. Turgut ÖZ; “Borçlar Hukuku Genel Hükümler”, İstanbul, 2000

ORTA, Mesut; “Elektronik İmza ve Uygulaması”, Ankara, 2005

ÖNEL, Dinçer; “Açık Anahtar Altyapısı (AAA) Sistemindeki Sertifikasyon Problemleri ve Diğer Güvenlik Sorunları”
<http://www.bilmuh.gyte.edu.tr/~ispinar/BIL571/acik-anahtar.pdf>

ÖZDEMİR KOCASAKAL, Hatice; “Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti” İstanbul, 2003

ÖZDİLEK, Ali Osman; “İnternet ve Hukuk”, İstanbul, 2002

ÖZGÜL, Mehmet Emin; “İnternette Hukuki Güvenlik ve Dijital İmza”
<http://www.inet-tr.org.tr/inetconf8/bildiri/141.doc>

ÖZKAYA, Necla; Şeref SAĞIROĞLU; “Açık Anahtar Altyapısı ve Biyometrik Teknikler” Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, s.283-289, İstanbul, 2006

ÖZSUNAY, Ergun; “Uluslararası Çalışmaların ve Bazı Ulusal Düzenlemelerin Işığında Elektronik Ticaret ve E-Sözleşmelerin Temel Sorunları”, Uluslararası İnternet Hukuku Sempozyumu, s.121-141, İzmir, 2002

ÖZYILMAZ, Ayşe; “Elektronik İmza”
http://www.e-imza.gen.tr/templates/resimler/File/makaleler/Elektronik_imza_Ayşe_Ozyilmaz.doc

PEKCANITEZ, Hakan; “Elektronik Ticaretin Türk İspat Hukukuna Getirdiği Sorunlar ve Çözüm Önerileri” Uluslararası İnternet Hukuku Sempozyumu, s.389-427, İzmir, 2002

REİSOĞLU, Safa; “Borçlar Hukuku”, İstanbul, 2006

RENDİ, Nihat -ONURSAN, Galip “Borçlar Hukuku” Ankara, 1972

RÜSSMANN, Helmut; “İnternette Hukuki İşlemler: Hukuki Geçerliliği ve İspat (Alman Hukukuna Göre)”, Çev. Muhammet ÖZEKES Uluslararası İnternet Hukuku Sempozyumu, s. 325-353, İzmir, 2002

SAĞIROĞLU, Şeref ; Mustafa ALKAN; “Her Yönüyle E-İmza” Ankara, 2005

SAĞIROĞLU, Şeref; Demet KABASAKAL; Mustafa ALKAN; “Mobil Elektronik İmza, Altyapısı ve Türkiye” Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, s.91-97, İstanbul, 2006

SAMAST, Orhan; “Hoş geldin Zaman Damgası”,
<http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=30&YazarNo=31>

SEVİM, Tuğrul; “Elektronik İmzanın Hukuksal Boyutları”
Türkiye Bilişim Şurası Hukuk Çalışma Grubu, İstanbul, 2004

SEVİMLİ, K. Ahmet; “Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası”, Prof. Dr. Hayri DOMANIÇ’e 80. Yaş Günü Armağanı, C:II, S.1023-1041, İstanbul, 2001

SEVİNÇ, Eser; “Elektronik İmza”http://www.ymm.net/eser_sevinc.htm

SÖZER, Bülent; “Elektronik Sözleşmeler” İstanbul, 2002

“Söyleşiler” “Her Yönüyle E-İmza” Telekom Dünyası Dergisi, 2006 Şubat Sayısı, (Doç. Dr. Şeref Sağıroğlu ve Doç. Dr. Mustafa ALKAN ile söyleşi)

SUNGUR, Süleyman; “Bilgi Ağları”,
[http://www.hho.edu.tr/huten/2003-2004%20SEMINER%20INTERNET/SULEYMAN%20SUNGUR/SULEYMAN%20SUNGUR%20\[PW%20POINT\].pdf](http://www.hho.edu.tr/huten/2003-2004%20SEMINER%20INTERNET/SULEYMAN%20SUNGUR/SULEYMAN%20SUNGUR%20[PW%20POINT].pdf)

ŞENOCAK, Zarife; “Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması”, AÜHFD, C:50, Sy:2, Ankara, 2001

“SPK Sertifika İlkeleri”, SPK; TUBİTAK, 2004
http://www.spk.gov.tr/kap/kurul_kararlari/si.pdf

TBMM Adalet Komisyonu Raporları, 22.Dönem, 2.Yasama Yılı, (1/613)

TDK, Güncel Türkçe Sözlük,
<http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF05A79F75456518CA>

TEKİNAY, S. Sulhi; Sermet AKMAN; Haluk BURCUOĞLU; Atilla ALTOP; “Borçlar Hukuku Genel Hükümler”, İstanbul, 1993

TOPALOĞLU, Mustafa; “Bilişim Hukuku”, Adana, 2005

TUBİTAK/UEKAE, “Açık Anahtar Altyapısı Eğitim Kitabı”,
<http://www.kamusal.gov.tr/tr/Bilgideposu/Belgeler/teknik/aaa/index.html>

TUNÇOMAĞ, Kenan; “Türk Borçlar Hukuku” İstanbul, 1976

TURAN, Murat; “Elektronik İmza” Tezsiz Yüksek Lisans Projesi, Konya, 2006

TUTKUN, K. Yücel “İmza, Paraf, Kişisel Mühür, Parmak Basma” Ankara, 1993

TÜFEKÇİ, Tolga; “Elektronik İmza Niçin Yaygınlaşamıyor”,
www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar/Elektronik_imza_nicin_yayginlasamiyor-doc.pdf

TÜFEKÇİ, Tolga; “İki Yılın Sonrasında Elektronik İmzada Neredeyiz?”,
Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, S.10-15, İstanbul, 2006

TÜFEKÇİ, Tolga ; “Elektronik İmza Neler Getirecek”,
www.bilten.metu.edu.tr/Web_2002_v1/common/yayinlar/T_Tufekci_BIMY10_Copy.pdf

ULUKAPI, Ömer; “Noter İşlemlerinde Şekil”, TNB Hukuk Dergisi, Sy:98, Ankara, 1998

ULUSOY, Yasin; “Beyaza İmza”, AÜHFD C:VIII, Sy:3-4, Ankara, 2004

USLU, İzzet; “Sayısal İmza ve Türkiye”,
http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=469

UYGUR, Turgut; “Açıklamalı-İçtihatlı Borçlar Kanunu Sorumluluk ve Tazminat Hukuku” Ankara, 2003

UZUNAY, Yusuf; Kemal BIÇAKCI; “Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli”

UZUNAY, Yusuf; Mustafa KOÇAK; “Bilisim Suçları Kapsamında Dijital Deliller” Akademik Bilişim Konferansı, Gaziantep, Şubat 2005

ÜNEY, Tuncer; “Elektronik İmza ve Ağaçlar”
<http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=28&YazarNo=29>

VELİDEDEOĞLU, Hıfzı Veldet; Refet ÖZDEMİR; “Türk Borçlar Kanunu Şerhi”, Ankara, 1987

WİNN, Jane K.; “Bagajsız Kuryeler: Kıymetli Evrak ve Dijital İmzalar”, Çev. Hayri BOZGEYİK; Hüseyin ALTAY, Hukuk, Ekonomi ve Siyasal Bilimler Aylık İnternet Dergisi, Sy: 17, Temmuz 2003

YARDIM, Mehmet Ertan; “Güvenli Elektronik İmzanın İnkarı” Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, s.149-155, İstanbul, 2006

Yargıtay Kararları Dergisi, 1990-2000

YAŞAR, Cumali; Okan ATABAĞ; Türkay DALAN; “Evrak Yönetim Bilgi Sistemleri”, <http://www.ab.org.tr/ab06/bildiri/69.doc>

YAZICI, M.Ali; Hasan ERDOĞAN; “Açık Anahtar Altyapısı ve Milli E-Token Cihazı” Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, s.75-80, İstanbul, 2006

YEŞİL, Sezen; Mustafa ALKAN; Tayfun ACARER; “E-İmza Uygulamalarında AB ve Türkiye’de Mevcut Durum ve Öneriler”, Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, s.1-9, İstanbul, 2006

YILDIRIM, Mustafa Fadıl; “Nitelikli Elektronik Sertifika Hizmet Sağlayıcısının Hukuki Sorumluluğu” Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, C: VIII, Sayı: 3-4, Erzincan, 2004

YILDIRIM, Mustafa Fadıl; “Standart Bilgisayar Program Devir Sözleşmeleri”
İstanbul, 1999

YÜKSELİYOR, Turhan; “AAA Sayısal Sertifika Karmaşası”
<http://www.innova.com.tr/08Arsiv/makaleler01.htm>

ZAMMİT, Joseph P.; Felice B. GALANT; “Elektronik Sözleşme”, Çev.: İlyas
ÇELİKTAŞ, İstanbul Barosu Dergisi, C:73, Sy:1-2-3, İstanbul, 1999

ZİLAN, Ruken; Gülay YALÇIN; Abdullah BATTAL; “Gerçek Yaşamda
Açık Anahtar Altyapısı Riskleri ve E-imza”, <http://www.inet-tr.org.tr/inetconf11/bildiri/106.doc>

Yararlanılan Yazılımlar

AKİP, Açıklamalı Kanun ve İçtihat Programı

Meşe Yazılım, “İçtihat ve Mevzuat Bankası”

Corpus, Mevzuat ve İçtihat Programı

ÖZGEÇMİŞ

Fatih ÖNDER

1977 yılında Elbistan'da doğdu. İlk ve orta öğrenimini Elbistan'da tamamladı. Dokuz Eylül Üniversitesi Hukuk Fakültesinden 1998 yılında mezun olduktan sonra, 1999 yılında İzmir Hakim Adayı olarak göreve başladı. 2001 yılında stajını tamamlayan ÖNDER; aynı yıl ad çekme usulü ile Yatağan Hakimliğine atandı. Askerlik hizmetini Kuzey Deniz Saha Komutanlığı Askeri Mahkemesinde, Askeri Hakim olarak yaptı. Halen Dört Yol Hakimliği olarak görev yapan ÖNDER, evli ve iki çocuk babasıdır.