TÜRKİYE BİLİŞİM DERNEĞİ

Kamu Bilişim Merkezleri Yöneticileri Birliği

Kamu Bilişim Platformu 17

E-Ticaret Güvenlik Sertifikasyonu ve Hukuksal Düzenlemeler

Nihai Rapor

Sürüm 1.0

http://www.tbd.org.tr

5 EKİM 2015

TBD Kamu-BİB

Kamu Bilişim Platformu 17

2. ÇALIŞMA GRUBU

Bu rapor, TBD Kamu Bilişim Merkezleri Yöneticileri Birliği (TBD Kamu-BİB)'nin **onyedinci dönem** çalışmaları kapsamında, **2. Çalışma Grubu (ÇG2)** tarafından hazırlanmıştır.

Hedef Kitle

Elektronik ticaret, bilgi toplumu hizmetlerinin ve malı temsil eden ticari, resmi, taşıma, sigorta ve finans belgelerinin (poliçe, bono, rehin senedi) iletişim şebekesine erişim olanağı veren veya hizmet alanlar tarafından sağlanan bilgileri tutan bir iletişim ağı yoluyla ilgili tarafa (alıcıya) iletilmesi ve ilgili tarafın semeni (mal bedelini) yine aynı elektronik ortamı kullanarak satıcıya ulaştırması hizmetidir.

Elektronik ticaret işlerinin güvenliği ise son derece önemlidir ve e-Ticaret işlemlerinin güvenli ve özel olmasını sağlamak için esasın belirlenmesini sağlamak, makbuz, ve gelen bilginin bütünlüğünün oluşturulması için ise hem altyapısal hem de hukuksal bazı düzenlemeler gerekmektedir.

Bu noktada Türkiye Bilişim Derneği Kamu-BİB bünyesinde oluşturulan 2. çalışma grubu e-Ticaret sitelerine yönelik güvenlik sertifikasyonu mekanizması ve e-Ticaret Kanunu çerçevesinde ihtiyaç duyulan ikincil düzenlemeler hakkında hazırlanan bu raporu 15-18 Ekim 2015'de düzenlenecek olan Kamu Bilişim Platformunda kamu ve özel sektörün bilgi ve ilgilerine sunacaktır.

Yayını Hazırlayanlar

Başkan

Ayşe Gül İBRİŞİM (Türk Standardları Enstitüsü)

Kamu-BİB YK Temsilcileri

Furkan CİVELEK (Kalkınma Bakanlığı)

Grup Üyeleri

Ayşenur AKINCI (Kalkınma Bakanlığı)

Lütfi ÖZBİLEN (Focus Akademi)

Belge No	:	TBD/Kamu-BIB/2015-ÇG2
Tarihi	:	5 Ekim 2015
Durumu	:	Nihai Rapor – S 1.0

İÇİNDEKİLER

TANIMLAR VE KISALTMALAR

AB	Avrupa Birliği
PKI	Açık Anahtar Altyapısı
SSL	Güvenli Giriş Katmanı
SET	Güvenli Elektronik Transfer
3D SECURE	3 Boyutlu Güvenlik

TABLOLAR

ÖNSÖZ

Elektronik ticaret, 20. yüzyılın son döneminde bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ve gelişmelere paralel bir şekilde ve giderek artan ölçüde dünya genelinde tartışılan bir kavram olarak karşımıza çıkmaya başlamıştır.

Elektronik ticaret, bilgi toplumu hizmetlerinin ve malı temsil eden ticari, resmi, taşıma, sigorta ve finans belgelerinin (poliçe, bono, rehin senedi) iletişim şebekesine erişim olanağı veren veya hizmet alanlar tarafından sağlanan bilgileri tutan bir iletişim ağı yoluyla ilgili tarafa (alıcıya) iletilmesi ve ilgili tarafın semeni (mal bedelini) yine aynı elektronik ortamı kullanarak satıcıya ulaştırmasıdır.

Bu noktada elektronik ticaret işlerinin güvenliği son derece önem kazanmaktadır. e-Ticaret işlemlerinin güvenli ve özel olmasını sağlamak için esasın belirlenmesini sağlamak, makbuz ve gelen bilginin bütünlüğünün oluşturulması için teknik ve özellikle kişisel verilerin korunması huşunda hukuksal bazı düzenlemeler gerekmektedir.

Ayrıca; elektronik çevrede ödeme mekanizmalarının bir parçası olarak kimlik ve hakların tesis edilmesi için resmi onaylamaya ihtiyaç bulunmaktadır. (Örneğin akıllı kart ya da şifreleme yoluyla biyometrik tekniklerin paylaşılması).

Küresel olarak tanınan resmi onay ve sertifikasyon teknolojileri/mekanizmaları/enstitüleri gereksinimleri karşılamada ve elektronik işlemlere olan güvenin tesisinde önemli bir rol oynamaktadır. Bu Sertifikasyon mekanizması, elektronik çevredeki organizasyonun ve bilginin güvenilirliğini sertifikalar yoluyla sağlayarak sistemler ve taraflar arasındaki işlemlerin belirsizliklerini azaltır.

BÖLÜM 1

GİRİŞ

Bu çalışma; güvenli e-ticaret için uygulanması gereken standartların belirlenerek e-ticaret yapan firmaların yetkilendirilmiş kuruluşlarca bu standartlara uygunluk açısından denetlenmesini esas alan bir sertifikasyon mekanizmasının kurulması ve İnternet üzerinden yapılan alışverişin güvenli ve güvenilir olması için uygun ortam oluşturulması ve yakın zamanda yürürlüğe girmiş olan e-Ticaret Kanunu'nu tamamlamak üzere hazırlık çalışmaları devam eden ikincil düzenlemeler kapsamında odaklanılması gereken temel sorunlara ve ihtiyaçlara yönelik önerilerin geliştirilmesi için yapılmıştır.

1.1. Amaç ve Kapsam

Söz konusu çalışma için kamu ve özel sektör uzmanlarından alınan bilgi alışverişleri çerçevesinde;

a. **E-Ticaret kapsamının tanımlanması**
b. **E-Ticaret taraflarının tanımlanması**
c. **Aracı tarafların tanımlanması**
d. **Tarafların birbirlerini doğrulayacakları yöntem ve teknolojiler**
e. **Ödeme araçlarının en ideal kullanım yönteminin belirlenmesi**
f. **Alıcı bilgilerinin satıcı nezdindeki muhafaza şekli**
g. **E-Ticaret Kanunu ve İkincil Mevzuatlar**
h. **Dünyada kabul edilmiş Kanun ve Mevzuatlar**

konuları görüşülmüş, ülkemizde e-Ticaret yapacak kuruluşların işin güvenliği adına asgari düzeyde uygunluk/uyumluluk göstermeleri gereken güvenlik gereklerine karar verilmiştir. Bu rapor, ilgili kapsamda yetki, sorumluluk, esas, prensip, yöntem ve güvenlik gereklerini belirlemek adına bir ön çalışma olması ve Bu çalışma kapsamında kavramsal tartışmalara girilmeksizin, iç hukuk mevzuatımız bakımından kaynak teşkil etmesi dolayısıyla AB'nin ilgili mevzuatı da değerlendirilerek ülkemizdeki elektronik ticaret mevzuatının gelişimi ve mevcut durumu ele almak amacıyla hazırlanmıştır.

Rapor; 4 bölümden oluşmaktadır. Birinci Bölümde Giriş Kısmına, İkinci Bölümde; Güvenlik ve Sertifikasyon Konularına, Üçüncü Bölümde; Dünyada ve ülkemizde Hukuksal Düzenlemelere, Dördüncü Bölümde ise önümüzdeki dönemde yürütülecek tamamlayıcı nitelikteki çalışma ihtiyaçlarına ilişkin önerilere (SONUÇ) yer verilmektedir.

BÖLÜM 2

GÜVENLİK

2.1 Tanımlar

E-Ticaret: e-ticaret, işletme faaliyetlerinin elektronik olarak yapılmasıdır. Bu faaliyet metin, ses ve video verilerinin elektronik olarak işlenmesi ve aktarımına dayanmaktadır. E-ticaret bu boyutuyla mal hizmet alımı ödemelerinin dijital olarak yapılmasını kapsamaktadır. Bu faaliyetler hem mamulleri (tüketici malları, özel ekipmanları) ve hizmetleri (bilgi hizmeti, finansal ve yasal hizmetler) hem de geleneksel faaliyetleri (sağlık, bakım, eğitim) kapsamaktadır.

E-Ticaret Verileri: E-Ticaretin gerçekleşmesi için/sırasında kullanılan veriler:

- Müşteri Adı
- Müşteri Posta Adresi
- Müşteri Fatura Adresi
- Diğer Bilgiler

Hassas e-Ticaret Verileri: Aşağıdaki veri tipleri hassas olarak değerlendirilmeli ve kurum içinde dahi farklı bölümlere (pazarlama, satış, vb) aktarılmamalı ya da depolanmamalıdır:

- Kredi Kartı Numarası
- Kredi Kartı Şirketi (Kartı üreten banka)
- Kredi Kartı doğrulama numarası (cvc2)
- Kredi Kartı Son Kullanım Tarihi
- Havale Gönderen Hesap Numarası
- Havale Gönderen Banka/Şube Bilgileri
- TC Kimlik No
- Müşteri Parola/Kimlik Doğrulama Bilgileri

2.2 Güvenlik Dinamikleri

Geleneksel ticarette var olan güven sağlayıcı yöntemler aslında e-ticarettekilerle aynıdır. Aradaki fark sadece e-ticaretin güvenlik sistemlerinin sayısal (dijital) bir sisteme dayalı olmasıdır. Sayısal (Dijital) imza ve sayısal (dijital) sertifikalar aracılığı ile ticari işlemlerin muhatabı olan taraflar bilgilerini elektronik güvenlik ortamında kolayca aktarabilmektedirler.

Açık bilgi iletişim ağlarında, örneğin Internet'te bu tür ticari faaliyetlerin olası güvenlik açıklarını önceden önlemek için kriptoloji bilimi (Bilgileri şifreleme bilimi) kullanılır.

E-ticaret uygulamalarına geçmeyi planlayan bir firma öncelikle ticari yapısına uygun bir güvenlik politikası belirlemeli, ardından bu politikayı destekleyecek etkin bir güvenlik sistemi kurmalıdır.
Sistem 4 güvenlik özelliğini kapsamalıdır:

- Gizlilik
- Bütünlük (integrity)
- Doğruluk/Geçerlilik (authentication)
- İnkar Edememe (non-reputation)

2.2.1 Açık Anahtar Yapısı (PKI)

Gönderilen ve alınan verinin değişik şifreleme algoritmaları kullanılarak gönderici tarafından şifrelenmesi ve alıcı tarafından şifrelenmiş verinin, şifresinin açılması temeli üzerine kurulmuş yazılımsal ve yordamsal bütünlük

2.2.2 Dijital imza

Gelen bir mesajin(verinin) gerçekten gönderen kişiden geldiğinin doğrulunu ispatlama (authentication) mekanizması.

2.2.3 Dijital Sertifikalar

Sertifika, açık anahtar sahibinin kimliğini doğrulayan bilgidir. Ehliyet, nüfus cüzdanı gibi sertifika da sahibinin kimliğini ispatlar.
Sertifikalar,
- Sertifika otoritesinin kimliğini
- Sahibinin kimliğini

- Sahibinin açık anahtarını
- Sertifikanın kullanımının bitiş zamanını
- Sertifika sunucusunun, bu sertifikayı onaylayan imzasını ve diğer bir takım bilgileri tutar.

Sertifika sayesinde, herhangi bir bilgi alan kişi, bu bilgiyi gönderen kişinin kimliğini, kullandığı sertifikanın geçerli olup olmadığını, sertifikanın güvenilir bir sertifika otoritesi tarafından onaylanıp onaylanmadığını anlayabilir.

2.2.4 SSL (Güvenli Giriş Katmanı)-secure sockets layer

Bu sistemde sunucu (server) bilgisayar ile bilgi alan bilgisayarlar arasında, dijital bir doğrulama amacıyla şifreli bilgiler içeren sertifikalar gönderilir. Bu sayede bilgilerin doğru bilgisayarlar dolayısı ile doğru kişiler/kurumlar arasında gidip gelmesi, kötü niyetli üçüncü şahıs ya da kurumlarca ele geçirilmemesi sağlanır. Gönderilen şifrelerin doğruluğu bu katmanda teyit edildikten sonra güvenli olarak veri değişimi ve aktarımına geçilir.

2.2.5 SET (secure electronic transaction)

Daha çok B2C pazarında müşteri-firma arasındaki kredi kartlı ödemelerde bilgi güvenliği sağlayan, çalışma prensibi SSL'e benzeyen elektronik güvenlik sistemleri.

2.2.6 Diğer Güvenlik Uygulamaları

- İşletim Sistemi Güvenliği
- Güvenlik Duvarı (Firewall) Sistemi
- Saldırı Tespit Sistemi
- Müşteri Bilgileri Veri tabanı güvenliği
- Web tabanlı dinamik içerik güvenliği
- VPOS(Sanal Ödeme Noktası) güvenliği
- Kart sahibi doğrulama metodu olarak VISA → 3-D Secure,

3D Secure (3 Boyutlu Güvenlik) Sistemi: VISA'nın uluslararası geçerliliği olan bu sistemi, internet alışveriş dünyasının 3 boyutu olan müşteri, kart sağlayıcısı banka ve işyeri arasındaki bilgi akışının (alışveriş esnasında özel şifre ve anahtarlar sayesinde) güvenliğini sağlayarak kart hamilinin ve işyerinin gerçekliğini doğrular. Kişisel güvenlik mesajı, ilgili banka tarafından alışveriş esnasında kart sahibine gösterilir.

Kart sahibi, kişisel güvenlik mesajı adı verilen kendine özel bilgiyi güvenli sitelerden yaptığı alışverişler esnasında görecek ve sitenin gerçek olduğunu anlayacaktır. Aynı şekilde kart sahibi sadece kendisinin bildiği 3 boyutlu güvenlik şifresini girerek işlemini onaylayacak, böylece alışveriş sitesine de kendini dolaylı olarak tanıtmış olacaktır. 3 boyutlu güvenlik sistemi kart sahibi-banka-işyeri arsındaki bilgi akışını şifreli olarak sağladığından kart sahibine özel bilgilerin kimse tarafından elde edilmemesi sağlanacaktır.

3 boyutlu güvenlik sistemi sayesinde kart sahibi bilgileri başkalarının eline geçse bile kişiye özel 3 boyutlu güvenlik sistemi şifresi ve kişisel güvenlik mesajı bilinemeyeceği için sisteme dahil üye işyerlerinden harcama yapılamayacaktır ve kart sahibi zarara uğratılamayacaktır

2.3 E-Ticaret Güvenlik Gereksinimleri

KURAL		NOT/ÖRNEK/REFERANS
BİLGİ GÜVENLİĞİ POLİTİKASI		
1	Bir politika belgesi, yönetim tarafından onaylanmalı, yayınlanmalı ve tüm çalışanlara bildirilmelidir. Yönetimin bağlılığını belirtmeli ve bilgi güvenliğini yönetmek için işletmenin yaklaşımını ortaya koymalıdır.	
2	Bu politika, tüm işletme içinde kullanıcılara, hedeflenen okuyucu için uygun, erişilebilir ve anlaşılır bir biçimde bildirilmelidir.	
AĞ GEREKLERİ		
3	Sunucu; ağ katmanındaki bir güvenlik duvarı vasıtası ile diğer bileşenlerden izole edilmelidir. Güvenlik duvarı sadece Internet'ten sunucuya değil, sunucudan diğer ağlara doğru da sadece tanımlanan ve beklenen verileri aktarmalıdır.	
4	Sunucu internete IDS veya IPS sistemi ile bağlanmalıdır	http://tr.wikipedia.org/wiki/%C4%B0ntrusion-detection_system
FİZİKSEL GÜVENLİK GEREKLERİ		
5	Sisteme fiziksel erişim yetkili kişilerle sınırlandırılmalı ve erişim 7x24 izlenmelidir. Sisteme yapılacak fiziksel atakları engelleyecek güvenlik önlemleri alınmalıdır (Çelik kapı, demir parmaklık, kilitli kabinet vb.)	
ERİŞİM YÖNETİMİ		
6	Veri erişimi yetkili kişilerle ve uygun yetkilendirme ile olmalıdır.	
7	Resmi yöntemler, bilgi sistemleri ve hizmetleri için erişim haklarının ayrılmasını denetlemek üzere yer almalıdır.	(yılda en az bir kez)

8	Yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan, kullanıcıların tüm yaşam döngüsü basamaklarını kapsayan erişim yönetimi uygulanmalıdır.	
9	Sistem yönetimi, veri manipülasyonu ve raporlama sistemlerine erişim için doğrulama gerekmelidir.	
10	Veri transferi güvenli protokoller üzerinden yapılmalıdır.	Örn: SSL Encryption SET
11	Müşteri, kart sağlayıcısı banka ve işyeri arasındaki bilgi akışının güvenliği için 3D Secure (3 Boyutlu Güvenlik) Sistemi'nin kullanılması kuvvetle önerilmektedir	
ERİŞİM SEVİYELERİ VE İZİNLER		
12	E-Ticaret verisine erişme hakkı olan her kullanıcıdan Gizlilik Anlaşması imzalaması istenmelidir.	
13	En15480 standardı gereğince rol tabanlı erişim kontrolü sağlanarak ticari firmaların bilmesi gereken verileri kendisine tanınan yetki ile erişebilmesinin sağlanması ve bunun ötesinde bilmesi gerekmeyen verilere erişememesinin öneminden bahsedilebilir.	
14	Satışlar, alıcının reşit bilgisi göre (+18) yapılmalıdır.	E-Ticaret Uygulamalarında Kişilere Özgü Bilgilerden Biri De Doğum Tarihi Bilgisidir. Günümüzde Telefonla Yapılan Doğrulamalarda Kişisel Bilgi Olarak Doğum Tarihi Sorgulanabilmektedir. Ayrıca, Kişi, Reşit Olmadığı Halde İnternet Üzerinden Ticari Alışveriş Gerçekleştirilebilmektedir. Bu Nedenle E-Ticaret Uygulamalarında Doğum Tarihi Bilgisi Yerine Kimlik Doğrulaması Yapılırken Reşit Bilgisinin (Reşit, Reşit Değil Şeklinde Doğrulanarak) Kullanılması Önemlidir.
DEPOLAMA GEREKLERİ		
15	E-Ticaret verisi güvenli bir sunucu terminalinde saklanmalıdır.	
EĞİTİM GEREKLERİ		
16	Sistem yönetimine, veriye ve raporlama mekanizmalarına erişimi olan tüm çalışanların güvenlik farkındalığı eğitimleri almaları gerekmektedir.	
SİSTEM GÜVENLİĞİ		
17	Sistem konfigürasyonu açıklık analizi yapılarak güvenlik açısından test edilmelidir.	Açıklık analizleri kurum tarafından gerçekleştirilebileceği gibi, dış firmalardan da güvenlik değerlendirme hizmeti kapsamında temin edilebilir.
UZAKTAN ERİŞİM GEREKLERİ		

18	Sisteme Uzaktan erişim VPN ile yapılmalıdır.	
YEDEKLEME		
19	Gerekli iş bilgisi ve yazılımın yedekleme kopyaları düzenli olarak alınmalıdır.	
20	Gerekli tüm iş bilgileri ve yazılımın bir felaket ya da ortamın zarar görmesi sonrası yeniden kurtarılabilmesi için yeterli yedekleme tesisleri bulunmalıdır.	Tüm planların tutarlı olmasını sağlamak, tutarlı şekilde bilgi güvenliği şartlarını ifade etmek ve test ve bakım önceliklerini tanımlamak için tek bir iş sürekliliği planları çerçevesi oluşturulmalıdır.
21	Yazılı koruma prosedürleri ve yedekleme kopyalarının tam ve doğru kayıtlarıyla birlikte en alt yedekleme bilgi seviyesi, ana sitede meydana gelebilecek bir felaketten kaçmaya yetecek kadar uzaklıktaki bir uzaktan erişim istasyonunda saklanmalıdır	Bu altyapı kurum tarafından oluşturulabileceği gibi, alternatif bir kurumdan da temin edilebilir.
22	En az üç yedekleme süresi ya da kuşağı muhafaza edilmelidir.	**Farklı yedek kopyalarının çalışır halde olduğu dönemsel olarak kontrol edilmelidir.**
KOPYALAMA/ÇOĞALTMA		
23	E-Ticaret ile ilgili veriler/bilgiler sadece yetkili ve Gizlilik Anlaşması imzalamış kişiler tarafından yetkileri paralelinde görülebilir, kopyalanır, çoğaltılır.	
24	Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen temizlenmelidir.	
ÇALIŞAN GEREKSİNİMİ		
25	Uygulama geliştirme, operasyon sistem yönetimi ve güvenlik yönetimi ayrı personeller tarafından idame ettirilmelidir.	
VERİ TABANI GEREKLERİ		
26	Veri tabanları uç kullanıcı sistemlerinden fiziksel olarak ayrılmış donanımlar üzerinde muhafaza edilmelidir.	
27	Veri tabanların yapılan tüm işlemlerin izlenebilirliği sağlanmalıdır.	
e-POSTA İLE SİPARİŞ		
28	Müşteri Siparişlerinin e posta yolu ile alındığı süreçleride bilgi PGP veya benzeri bir yazılım ile şifrelenmelidir.	Kimlik doğrulama amacıyla elektronik imza ya da mobil imza kullanılabilir.
KREDİ KARTI İLE ÖDEME – DOĞRULAMA – GEÇERLEME		
29	Kredi kartı bilgileri online alınıp daha sonra işletilecek ise barındırma firmasının web sunucusu güvenliği önemsenmeli, güvenilir bir barındırma firması seçilmelidir.	(güvenlik açısından Kredi kartı bilgilerinin daha sonra işletilmek üzere barındırılması önerilmemektedir) Barındırma firması ile yapılan sözleşmede bilgilerin gizliliğini içeren maddeler eklenmelidir.
30	Kredi kartı bilgileri online alınıp gerçek zamanlı işletiliyor ise; firma ya kendi dijital	

	sertifikasını veya barındırma firması tarafından sağlanan dijital sertifikayı kullanmalıdır.
ANAHTAR YÖNETİMİ	
31	Tüm anahtarlar değiştirilmeye ve tahrip edilmeye karşı korunmalıdır
32	Anahtarları üretmek, saklamak ve arşive kaldırmak için kullanılan ekipmanın korunması için fiziki koruma kullanılmalıdır.
33	Anahtar boyları seçilirken kriptografik kapsamda güvenlik zafiyeti oluşturmayacak anahtar boyları seçilmelidir. Anahtar boylarının yeterliliği hususunda şifreli yazı konusunda otorite olan bir kurumdan onay alınmalı ve/veya TSE-CAVP ve TSE-CMVP programlarına referans standartları olan TS ISO/IEC 19790: Kripto Modülleri için Güvenlik Gereksinimleri ve TS ISO/IEC 24759: Kripto Modülleri Test Gereksinimleri`nden sertifikalanmak önerilir.
ÜRÜN GÜVENLİĞİ	
35	E-Ticaret Yazılımlarının, Bilgi Teknolojileri Ürün Güvenliği Standardı olan TS ISO/IEC 15408-Ortak Kriterler (Common Criteria) standardından bağımsız akredite laboratuvarlar tarafından teste tabi tutulması ve sertifikasyonu kuvvetle önerilir.
36	PCI DSS & PA DSS Ödeme Uygulaması Güvenliği Kart sahibinin gizli bilgisinin korunması için önemlidir.
37	Tedarik Zinciri Güvenliği (Supply Chain Security) de yukarıda sayılan güvenlik önlemlerine ek olarak düşünülebilinir.

Tablo 1: E-Ticaret Güvenlik Gereksinimleri

BÖLÜM 3

TÜRKİYE'DE ELEKTRONİK TİCARET HUKUKU VE MEVZUATTAKİ GELİŞMELER

3.1. Elektronik Ticaret Hukuku

Bilindiği üzere 90'lı yılların ortalarından itibaren Dünya'da ve Avrupa'da e-ticaret kanunları şekillendirilmektedir. Söz konusu kanunların şekillenmesinde elektronik veriyle ilgili düzenlemelerin temel teşkil ettiği görülmektedir. Zira elektronik ticarette alıcı ve satıcı arasında teşkil edecek bir sözleşme bakımından; taraflar arasındaki elektronik veri değişimi sırasında verilerin alınması, kabulü, hukuki geçerlilikleri ve uygulanabilirliği, delil niteliği ve tarafların sorumlulukları gibi hususların düzenlenmiş bulunması gerekmektedir. Bu çerçevede birçok ülkede öncelikle elektronik veriyle ilgili düzenlemeler yapılmış ve ardından elektronik ticarete ilişkin düzenlemeler şekillenmiştir.

3.2. AB'de Elektronik Ticaret Hukuku

AB elektronik ticarete ilişkin yasal düzenlemeler konusunda en etkin çalışan örgütlenmelerden biridir. AB'nin elektronik ticaret hukuku ortamının oluşturulması bakımından temel önceliği güven ortamının tesisidir. Tüketiciler ve işletmeler bakımından elektronik ticaretin güvenilirliğinin sağlanması gerektiği aksi halde elektronik ticaretin gelişemeyeceği Birlik içerisinde önemle vurgulanmıştır. Bu çerçevede elektronik ticaretle alakalı hukuki çerçevenin oluşturulmasında güvenilirlik ve "Ortak Pazar" serbestisi hususları öncelikle göz önünde bulundurulmuştur.

AB'de elektronik ticarete ilişkin düzenlemeler doğrudan elektronik ticaret veya elektronik imza yasaları ile başlamamıştır. Elektronik ticarete ilişkin mevzuatın oluşturulmasında, bilgi toplumuyla ilgili direktifler ve tüketicinin korunması direktiflerinin mesafeli satışlarla ilgili maddelerinde yapılan değişiklikler başta olmak üzere bazı yasal düzenlemelerin elektronik ticarete ilişkin düzenlemelerden çok daha evvel yapıldığı görülmektedir. Doğrudan elektronik ticarete ilişkin düzenlemeler bu alandaki gelişmeleri takiben 90'lı yıllarda çıkartılmaya başlanmıştır.

AB mevzuatı içerisinde elektronik ticareti düzenlemek ve belirli standartlar getirmek amacıyla çok sayıda düzenleme bulunmaktadır. Bu kapsamda yer alan en önemli AB direktifleri aşağıdaki konuları kapsamaktadır:

3.2.1 Kişisel Bilgilerin İşlemler ve Veri Transferi Sırasında Korunması Direktifi(95/46/EC)

Direktif kapsamında düzenlenen konular temel olarak aşağıdadır:

- Kişisel verilerin toplanması ve işlenmesi ancak şartlar altında hukuken mümkündür olacağı düzenlenmektedir.

"l) Veri sahibinin açık rızası bulunması,

2) İşlemin sebebi veri sahibinin onay verdiği bir sözleşme, veri sahibinin hayati çıkarları, kamu çıkarları ve güvenliği için gerekli olması."

- Bazı durumlar hariç dil, din, ırk, politik görüşler, sağlık, yasal örgütler gibi konulara ilişkin kişisel veri toplanamaz ve işlenemez.
- Verilerin sahibine hangi bilgilerin toplandığı, kim tarafından ne şekilde kullanılacağı konusunda açık bilgi verilmelidir.
- Kişisel verilerin güvenliğini sağlayacak tüm önlemler alınmalıdır.

2012 yılında Direktifte yapılan bir takım güncellemelerle kişisel verilerin daha iyi korunması için aşağıda ifade edilen hususlarda bazı ek güvenceler getirilmektedir. Bu kapsamda:

- Tüketiciler istedikleri takdirde kendilerine ait verilen dijital ortamdan silinmesini isteyebilir.
- Veri toplanması için tüketicinin rızasının gerektiği durumlarda bu rızanın açıkça verilmesi aranır.
- Verileri toplayan ve işleyen kurum ve kuruluşların sorumlulukları arttırılır.
- Kişiler, kendilerine ait verilerin yanlış kullanıldıklarını düşündüklerinde ülkelerindeki veri koruma kurumlarına başvurabilirler.

- AB kanunları, AB'de aktif olan farklı ülke firmaları içinde geçerlidir.

3.2.2 Verinin İşlenmesi ve Mahremiyetinin Korunması Direktifi(97/66/EC)

Bu Direktif kapsamında 95/46/EC sayılı Direktife pek çok açıdan ek yapılarak gerçek kişilerin iletişimlerinde mahremiyetin ve özel hayatların korunmasını ayrılmaz haklar olduğu ifade edilmektedir. Bu hakların korunması için hizmet sağlayıcılara gerekli tüm güvenlik önlemlerini alma yükümlülüğü getirilmektedir.

3.2.3 Mesafeli Satış Sözleşmelerinde Tüketici Haklarının Korunması Direktifi (97/7/EC)

Bu Direktif kapsamında:

- Tüketici alış veriş öncesi satıcı firmanın kimliği, ürünün ya da hizmetin özellikleri, fiyatlandırma, teslim zamanı ve iptal şartlan hakkında bilgilendirilmelidir.
- Tüm satış sözleşmeli detayları vazıh olarak tüketiciye bildirilmelidir.
- Tüketicilerin satın aldıkları ürünleri iade etmek için en az 7 günleri vardır.
- Satıcı ürünleri en geç 30 gün içerisinde teslim etmelidir.

3.2.4 Bilgi Toplumu Hizmetlerinin, Özellikle Elektronik Ticaretin Ortak Pazardaki Bazı Yönleri Hakkındaki Direktif (2000/31/EC)

Bu Direktif Hükümlerine göre:

- Tüketiciler satıcı firmalara ulaşabilecekleri erişim bilgilerine sahip olmalıdır.
- Ürün reklam ve tanıtımları tam ve doğru bilgi vermeli; ürünlerin fiyatlandırması varsa promosyonlar açıkça anlaşılabilir olmalıdır.
- Üye ülkeler internet üzerinden sözleşme yapılmasını sağlayacak yasal düzenlemeleri yapmalıdır.
- Satıcı firma verilen siparişin alındığını ve sözleşme şartlarını gecikme olmadan tüketiciye bildirmelidir.
- Oluşabilecek anlaşmazlıkları hızlıca çözebilecek mekanizmalar ve prosedürler oluşturulmalıdır.

3.2.5 Elektronik İşlemlerde Mahremiyetin Korunması Direktifi(2002/58/EC)

Bu Direktif kapsamında:

- Elektronik haberleşme hizmet sağlayıcıları, kişisel bilgilere sadece yetkili kişilerin erişimini sağlamaktan, verinin değişilmesini ya da silinmesini engellemekten ve tüm güvenlik politikalarının uygulanmasından sorumludur.
- Üye devletler kamuya açık elektronik iletişimin izinsiz olarak dinlenmesini ya da kayda alınmasını engelleyecek düzenlemeleri yerine getirmelidir.
- Tüketiciye ait kişisel bilgiler artık onlara ihtiyaç kalmadığında ya silinmeli ya da isimsiz hale getirilmelidir.
- Tüketiciler önceden talep etmedikleri elektronik iletişimleri almayı istediklerini bildirmelidir.
- Tüketicilerin cihazlarına herhangi bir bilgi yüklenmeden (örn. cookies) tüketicinin onayı alınmalıdır.
- Halka açık rehberlere tüketicilere ait bilgiler onayları dışında eklenemez.

Yukarıda özetle anlatılan AB mevzuatıyla Birlik bölgesindeki ülkelerin e-ticaret alanındaki yasal uygulamalarının ve ticari prosedürlerinin ortak standartlar altında toplanması ve uyumlaştırılması amaçlanmaktadır.

Bu mevzuata ek olarak AB tarafından bilgi ve iletişim teknolojilerinin kullanım ve erişiminin daha da yaygınlaşmasını sağlamak ve AB'nin bu alandaki rekabetçiliğini arttırmak amacıyla **"Avrupa Sayısal Gündem"**i oluşturmuştur. Bu Gündem kapsamında kişisel bilgilerin gizliliği, tüketici hakları ve elektronik ticari sözleşmeler, güvenli ödeme sistemleri, e-imza ve e-kimlik, vergilendirme, güven damgası ve pazarlara erişim engellerinin kaldırılması gibi konularda düzenlemeler yapılması öngörülmektedir.

Sayısal Gündem kapsamında yayımlanan **"AB Sayısal Haklar Kanunu"** pek çok açıdan OECD Tüketici Hakları Yönlendirmesiyle benzerlik göstermektedir. Bu kanun kapsamında internette reklam/e-posta gönderimi, tüketici hakları ve sözleşmeler ile güvenli ödeme konuları düzenlenmiştir.
Buna göre:

- Tüketiciler satılan ürün veya hizmetle ilgili tam, eksiksiz ve gerçek bilgiye ulaşabilmelidir.
- Tüketiciyi yanıltıcı reklam faaliyetleri (örneğin ürün ya da fiyatıyla ilgili yanlış yönlendirme) yasaklanmıştır.
- Satıcı kendisine kolay ulaşımı sağlamak amacıyla firma adını, adresini, erişim bilgilerini, varsa bağlı bulunduğu profesyonel kuruluşları paylaşmalıdır.

- Tüketiciye ürünle ilgili tüm maliyetler ayrı ayrı gösterilmeli ve satışın sözleşmesinin ana şartları (süresi, fiyatlandırma şekli gibi) iptal, iade, garanti ve varsa satış sonrası servis imkânları yazılı ya da e-posta ortamında paylaşılmalıdır.
- Tüketiciye satış sözleşmesinden doğan hakları net ve eksiksiz anlatılmalıdır.
- Tüketici haksız sözleşme şartlarından (örneğin tüketicinin yasal haklarını kısıtlayan, otomatik uzayan sözleşmelerde iptali zorlaştıran yöntemler) korunmaktadır.
- Satılan mallar en geç 30 gün içerisinde teslim edilmeli, hasarlı gönderilen ürünler ya değiştirilmeli ya da müşteriye indirim uygulanmalıdır.
- Tüketicilerin satım sözleşmesini iptal etmek için en az 7 günlük süresi vardır. Finansal hizmetler için bu süre 14 gündür.
- Ödemeler İçin güvenli bir sistem sunulmalı ve herhangi bir hatada tüketiciye hemen geri ödeme yapılmalıdır.

Yeni 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanunun amaçlarından birisi de yukarda genel çerçevesi ile anlatılan AB mevzuatına uyumun sağlanmasıdır. Söz konusu kanunun hazırlanması çalışmaları sırasında, yukarıda anılan Direktif hükümlerinin yanı sıra AB tarafından bu Direktifi değiştiren yeni Direktif hükümleri de değerlendirilmiştir.

3.3. Türkiye'de Elektronik Ticaret Hukuku

Dünya genelindeki ekonomik gelişmelere paralel olarak elektronik ticarete ilişkin çalışmalar ülkemizde de 90'lı yılların ikinci yarısında başlamıştır. Dış Ticaret Müsteşarlığı koordinatörlüğünde 1997 yılında elektronik ticaret ağının kurulması ve yaygınlaştırılması çalışmaları başlatılarak her yıl düzenlenen istişare toplantılarında öncelikle hukuk, teknik alt yapı çalışmaları ve finansal konular olmak üzere birçok konu ele alınmıştır.

2008 yılında Elektronik Ticaret Direktif Grubu tarafından yayımlanan raporda ülkemiz mevzuatında yer alan elektronik ticaret düzenlemelerinin AB'nin 2000/31/EC sayılı direktifine kısmen uyumlu olduğu, bununla birlikte dağınık bulunduğu ve genellikle direktifle doğrudan örtüşmediği ifade edilmiştir.

Bu çerçevede yapılan çalışmalar neticesinde AB mevzuatına uyum sağlamak adına ilk kez Adalet Bakanlığı tarafından 26.07.2010 tarihinde "Elektronik Ticaretin Düzenlenmesi Hakkındaki Kanun Tasarısı" hazırlanarak Türkiye Büyük Millet Meclisi

Başkanlığı'na gönderilmiştir. Bu çalışmaların neticesinde 23.10.2014 tarihinde Meclis Genel Kurulu'nda kabul edilen 6563 sayılı "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun" 5.11.2014 tarih ve 29166 sayılı Resmi Gazetede yayımlanarak 1.5.2015 tarihinde yürürlüğe girmiştir.

Yukarıda ifade edilen 6563 sayılı Kanununun yanı sıra ülkemizde elektronik ticaret faaliyetinde bulunmak isteyen firmaların uyması gereken bir dizi yasal düzenleme bulunmaktadır. Bu düzenlemeler ticaret hukuku, borçlar hukuku, tüketicinin korunması hukuku, vergi hukuku, elektronik haberleşme mevzuatı, elektronik imza mevzuatı, internette yapılan yayınlara ilişkin düzenlemeler ve fikri sınaî hakların korunması hukuku gibi birbirinden farklı pek çok alanın kapsamı içerisinde yer almaktadır.

3.3.1 Türkiye'de Elektronik Ticarete İlişkin Mevzuat (Mevcut Durum)

Ülkemizde elektronik ticarete ilişkin hükümlerin yer aldığı düzenlemeler aşağıdadır.

- 1982 tarihli "Türk Anayasası",
- 14.2.2011 tarih ve 27846 sayılı Resmi Gazetede yayımlanan 6102 sayılı "Türk Ticaret Kanunu",
- 4.2.2011 tarih ve 27836 sayılı Resmi Gazetede yayımlanan 6098 sayılı "Türk Borçlar Kanunu",
- 5.11.2014 tarih ve 29166 sayılı Resmi gazetede yayımlanan 6563 sayılı "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun",
- 8.3.1995 tarih ve 22221 sayılı Resmi Gazetede yayımlanan 4077 sayılı "Tüketicinin Korunması Hakkında Kanun",
- 14.3.2003 tarih ve 25048 sayılı Resmi Gazetede yayımlanan 4822 sayılı "Tüketicinin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun",
- 12.10.2004 tarih ve 25611 sayılı Resmi Gazetede yayımlanan 5237 sayılı "Türk Ceza Kanunu",
- 4.5.2007 tarih ve 26530 sayılı Resmi Gazetede yayımlanan 5651 sayılı "Internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun",
- 10.11.2008 tarih ve 27050 sayılı Resmi Gazetede yayımlanan 5809 sayılı "Elektronik Haberleşme Kanunu",

- 23.1.2004 tarih ve 25355 sayılı Resmi Gazetede yayımlanan 5070 sayılı "Elektronik İmza Kanunu",
- 27.6.2013 tarih ve 28690 sayılı Resmi Gazetede yayımlanan 6493 "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun"
- 6.6.2006 tarih ve 26190 sayılı Resmi Gazetede yayımlanan İhracat Yönetmeliği.
- 26.08.2015 tarih ve 29457 sayılı Resmi Gazete'de yayımlanan "Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik",
- 30.11.2007 tarih ve 26716 sayılı Resmi Gazetede yayımlanan "Internet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik",
- 14.6.2003 tarih ve 25137 sayılı Resmi Gazetede yayımlanan "Mesafeli Sözleşmelere Dair Yönetmelik".

Ayrıca e-ticarete ilişkin düzenlemelere aslî etkisi bulunan "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" yasalaşmasına ilişkin süreçlerin tamamlanmasının ardından yukarıda yer alan listeye eklenecektir.

3.3.2 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanununu ile Düzenlen Temel Konular:

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun AB'nin ilgili direktiflerine uyum sağlanması ve Türk Hukukunda borçlar, ticaret ve tüketicinin korunması hakkında mevzuat hükümleri tekrar edilmeksizin bilgi toplumu hizmetleri ile elektronik ticaretin genel ilkelerinin düzenlenmesini amaçlamaktadır. Kanunda öncelikle ticari elektronik sözleşmelerde bilgilendirme yükümlülüğü, ticari elektronik iletişim ve istenmeyen elektronik iletiler ile elektronik ticarette kişisel verilerin korunması olmak üzere üç temel husus düzenlenmektedir.

3.3.2.1 Bilgi Verme Yükümlülüğü:

Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ile elektronik ortamda hizmet sağlayıcılarla sözleşme yapılırken bilgi verme, sözleşme metnine sonradan erişilebilmesi ve hataların sonradan düzeltilebilmesine imkân verilmesi konularında bir takım yükümlülükler getirilmektedir. Kanun'un "Bilgi Verme Yükümlülüğü" başlıklı 3 ve "Siparişler" başlıklı 4'üncü maddeleriyle hizmet sağlayıcıların bilgi verme

yükümlülüğü ve siparişlerde geçerli esaslar düzenlenmektedir. Kanunun bu maddeleriyle hizmet sağlayıcılara farklı konularda bilgi verme yükümlülüğü getirilmekte ve bu sayede sitelerinin ve uygulamalarının güvenilirliği ve güvenliği konularında daha şeffaf olmalarının sağlanması amaçlanmaktadır. Burada hizmet sunuculara elektronik ortamda sözleşme yapılırken bilgi verme, sözleşme metninin sonradan erişilebilir kılınması ve hataların sonradan uygun, etkili ve erişilebilir teknik araçlarla düzeltilebilmesi gibi hususlarda bir takım yükümlülükler getirilmektedir. Bu düzenlemelerin amacı alıcının satın alacağı mal ya da hizmeti tanıyabilmesinin, yanıltılmasının engellenmesinin sağlanmasıdır. Aynı zamanda hizmet sağlayıcının alıcının siparişini aldığını gecikmeksizin elektronik iletişim araçlarıyla teyit etmesi şart koşulmaktadır. Böylece gerçekleştirilen siparişin detaylarının da gecikmeksizin paylaşılması zorunlu kılınmaktadır. Kanun ile sipariş verilmeden önce yapılan veri girişlerinin de etkili bir biçimde sunulması ve varsa hataların sonradan düzeltilebilmesi öngörülmektedir.

Kanunun 9. maddesinin ikinci fıkrasıyla bilgi verme yükümlülüğü de dâhil olmak üzere yaptırımların aracı hizmet sağlayıcılara da uygulanmasına ilişkin usul ve esasların, çıkarılacak yönetmelikle belirleneceği hüküm altına alınmıştır. Bu kapsamda Gümrük ve Ticaret Bakanlığı tarafından hazırlanan “Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik” 26.08.2015 tarih ve 29457 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir. Söz konusu Yönetmelik kapsamında hizmet sağlayıcı ve aracı hizmet sağlayıcıların ağ üzerinde mal veya hizmet satışına ilişkin sözleşme ve siparişlerdeki bilgi verme yükümlülükleri ile elektronik ticarete ilişkin bir takım tedbirler düzenlenmektedir.

3.3.2.2 Ticari Elektronik İletişim ve İstenmeyen Elektronik Postalar:

Elektronik Ticaretin Düzenlenmesi Hakkında Kanunla düzenlenen diğer bir konu ise ticari elektronik iletişim ve istenmeyen elektronik postalar hususudur. Kanunun “Ticari İletişime İlişkin Esaslar” başlıklı 5. Maddesi ve “Ticari Elektronik İleti Gönderme Şartı” başlıklı 6. maddesiyle ticari iletişime ilişkin temel kurallar belirlenmektedir. Buna göre ticari elektronik iletişim sırasında iletişimin ve bu iletişimin adına yapıldığı gerçek ya da tüzel kişinin açıkça belirlenebilir olmasını gerekmekte, satıcıya bu bilgileri sunma yükümlülüğü getirilmektedir.

Kanunun 6. maddesinde yer alan hükümle kişilere, önceden onayları alınmaksızın ticari nitelikli elektronik posta, faks, SMS, vb. iletilerin gönderilmesi engellenmektedir. Maddeye göre ticari elektronik iletiler alıcılara yalnızca önceden

onayları alınmak kaydıyla gönderilebilecektir. Bu onayın yazılı yahut elektronik iletişim araçlarıyla alınması kaydı getirilerek hukuki geçerlilik şekli de kanunla belirlenmiştir. Bununla birlikte ticari hayatın gereklilikleri göz önünde bulundurularak, esnaf ve tacirlere önceden onayları alınmaksızın ticari nitelikli elektronik iletilerin gönderilebilmesi hususunda imkân tanınmıştır. Kanunun 8. Maddesine göre esnaf ve tacirler de dâhil tüm alıcılar diledikleri zaman, hiçbir gerekçe belirtmeksizin ticari elektronik iletileri almayı reddetme hakkına sahiptir.

Bu kapsamda Kanunun elektronik ticari iletiler ve istenmeyen elektronik postalar konusunda AB'nin düzenlemeleri doğrultusunda *"Önceden İzin Alma Yöntemi"* esasını benimsediği görülmektedir.

3.3.2.2 Kişisel Verilerin Korunması

Elektronik Ticaretin Düzenlenmesi Hakkında Kanununun ele aldığı son önemli konu ise elektronik ticarette kişisel verilerin korunması hususudur. Söz konusu kanun kapsamında hizmet sağlayıcılarının müşterilerinin kişisel verilerini onayları olmaksızın kullanması engellenmektedir. Kanunun "Kişisel Verilerin Korunması" başlıklı 10. maddesiyle hizmet sağlayıcı ve aracı hizmet sağlayıcıların yapmış oldukları işlemler nedeniyle elde ettikleri kişisel verilerin saklanmasından ve güvenliğinden sorumlu oldukları ifade edilmektedir. Bu çerçevede hizmet sağlayıcı ve aracı hizmet sağlayıcılar kendilerinde bulunan kişisel verileri ilgili kişinin onayı bulunmaksızın üçüncü kişilere iletemeyecek ve başka amaçlarla kullanamayacaktır.

BÖLÜM 4

SONUÇ

4.1 Türkiye'de Elektronik Ticaret Güvenliğine İlişkin Yapılması Gerekenler

E-Ticarette tüketicilerin güven ve güvenlik endişelerini gidermek ve tüketicileri rahatlıkla alışveriş yapabilecekleri e-ticaret sitelerine yönlendirmek amacıyla Avrupa'da ve dünyanın farklı ülkelerinde devlet ve özel sektör kurumlarınca çalışmalar yapılmış ve "güven damgası" uygulamaları oluşturulmuştur. Bu kurumlar e-ticaret sitelerinin işleyişlerini değerlendirerek belirlenen standartlara uyup uymadıklarını denetlemekte ve belirli minimum standartlara uyum gösteren e-ticaret sitelerini "güven damgası" ile onaylayarak tüketicilerce ayırt edilmesini sağlamaktadır.

Yurt dışında birçok ülkede güvenlik ve /veya gizlilik konularında bağımsız kurumlar tarafından yapılan değerlendirmeler sonucu elde edilen sertifikalar tüketicilere o sitenin ne kadar "güvenilir" olduğunu göstermektedir.

Avrupa Birliği de Sayısal Gündem çerçevesinde "güven damgası" verecek kurumların oluşturulmasını ve işleyişinin düzenlenmesini öngörmektedir. Avrupa Birliği uluslararası e-ticareti geliştirme çalışmaları sırasında var olan kurumları da incelemiş ve örnek kurumları listelemiştir. Bu kurumlar değerlendirmeye ek olarak tüketicilerle e-ticaret şirketleri arasındaki anlaşmazlıkların çözümlenmesinde rol almak, sitelerle ilgili müşteri değerlendirmeleri ve notlamaları oluşturmak gibi farklı işlevler de üstlenmektedir.

Ülkemizde de tüketicilerin güven ve güvenlik endişelerini gidermek ve tüketicileri rahatlıkla alışveriş yapabilecekleri e-ticaret sitelerine yönlendirmek amacıyla bu türlü uygulamaları oluşturulmasının faydalı olacaktır.

Bu noktada ulusal akreditasyon kurumu olması durumundan mütevellit Türk Standardları Enstitüsü bünyesinde ve belirlenen diğer kurumların katılımı ile oluşturulacak yeni bir sertifikasyon programının oluşturulması (güven damgası) ve/veya en asgaride bu dokümanın 2. bölümünde tanımlanan gereksinimlerin denetiminin yapılması gerekmektedir.

Güven Damgası çerçevesinde;

a) E-ticaret yapacak olan kurum ve kuruluşların BT alt yapılarının (kaynak kodları, veri elemanları, sitenin ağ ve sistem altyapısı) güvenlik açısından Sızma testlerine ve Güvenlik Değerlendirme Programlarına tabii tutulması, bu testlerden geçer sonuç alması gerekmektedir. (Geliştirilen Güvenlik Değerlendirme Programları ile e-ticaret yapılarında bulunan açıklıkların tehdit unsuru oluşturmasını önlemenin hedeflenmesi gerekmektedir.)

b) Bununla birlikte söz konusu firmaların Bilgi Güvenliği Yönetim Sistemi sertifikasına sahip olmaları istenebilir. Bilgi Güvenliği Yönetim Sistemi sertifikasına (TS ISO IEC 27001) sahip olan organizasyonlar müşteri bilgilerinin gizliliğini ve güvenliğinin sağladıklarını, BT altyapılarının uygun güvenlik seviyesinde olduğunu taahhüt etmiş olurlar. Ayrıca bu sertifika herhangi bir güvenlik olayı tespitinde yapılması gereken iş sürekliliği planlarının, sistemin yeniden ayağa kaldırılmasının, olay yönetiminin, güvenlik güncellemelerinin de kontrol altında olduğunun; saldırı tespit sistemlerinin çalıştığının da göstergesidir.

c) Güvenli E-Ticaret yazılımları için hazırlanan Koruma Profiline uyumu sağlanıp, TS ISO/IEC 15408: Bilgi Teknolojileri Ürün Güvenliği - Ortak Kriterler (Common Criteria) standardına göre bağımsız akredite laboratuvarlar tarafından teste tabi tutulup ve "YETKİLENDİRİLMİŞ" Sertifikasyon kurumları tarafından da sertifikasyonu gerçekleştirilmelidir. Türk Standardları Enstitüsü Ortak Kriterler Belgelendirme Sistemi (TSE-OKBS) TS ISO/IEC 15408-Ortak Kriterler alanında dünyada 26 ülkenin taraf olduğu CCRA (Common Criteria Recognition Arrangament – Ortak Kriterler Tanıma Anlaşması)'na "YETKİLENDİRİLMİŞ ÜYE" statüsünde üye olup, verdiği sertifikalar bu 26 ülkede tanınmakta, yani TSE-OKBS tarafından sertifikalanan bilişim ürünleri "uluslararası güvenli ürün" olmaktadırlar. E-Ticaret yazılımları, bu kapsamda sertifikalanarak uluslararası tanınır güvenliğe sahip

olacaktır, bu konuda Güvenli E-Ticaret Koruma Profili de TSE tarafından hazırlanmıştır.

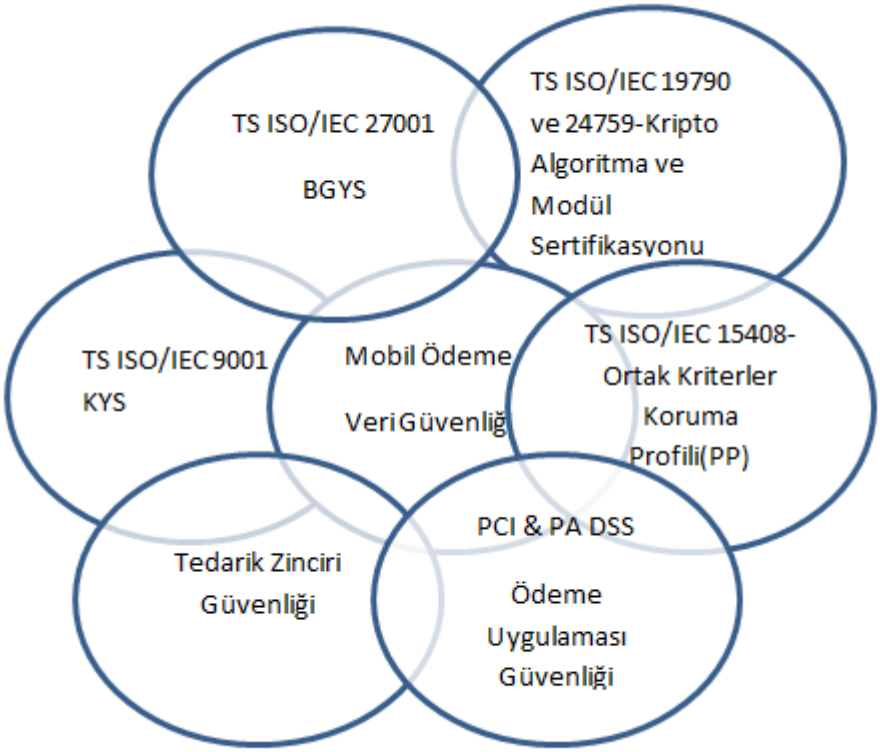
d) Kullanılacak olan Kripto Algoritma ve Modüllerinin, TSE-CAVP ve TSE-CMVP programlarına referans standartlar olan TS ISO/IEC 19790: Kripto Modülleri için Güvenlik Gereksinimleri ve TS ISO/IEC 24759: Kripto Modülleri Test Gereksinimlerinden sertifikalanmaları kuvvetle önerilir.

e) PCI & PA DSS Ödeme Uygulaması Güvenliği Kart sahibinin gizli bilgisinin korunması için önemlidir.

f) Tedarik Zinciri Güvenliği (Supply Chain Security) de yukarıda sayılan güvenlik önlemlerine ek olarak düşünülebilinir.

g) Müşteri memnuniyetinin sağlanması açısından (sipariş onaylama ve iptal etme süreçleri, ürünlerin zamanında teslimi, tüketici şikâyetinin iletilip şikâyetlere yanıt verilebilmesi) ve Sosyal Sorumluluklar hususlarında da e-ticaret yapan firmaların Kalite Yönetim Sistemi sertifikasına sahip olmaları beklenebilir.

Aşağıdaki tabloda E-Ticaret Güvenliği ilgili standartlarla özetlenmiştir.



Tablo 2: E-Ticaret Sertifikasyon Bileşenleri

Yine kurulacak sertifikasyon programı bünyesinde herhangi bir problem ortaya çıktığı durumlarda müşteri mağduriyetini önlemek üzere tüketiciler için tüm vatandaşlarımızın ulaşımına açık bir şikâyet sistemi kurulmalıdır.

E-ticaret sisteminin yaygınlaştırılması için bilgilendirme toplantıları, çeşitli seminerler ve eğitimler düzenlenebilir, özellikle dijital imza kullanma sürecinin kullanıcılara anlatılması, vatandaşlarımızda bilinçlilik sağlanması konularına önem verilmelidir.

4.2 Türkiye'de Elektronik Ticaret Mevzuatına İlişkin Yapılması Gerekenler

a) Türkiye'de var olan yasal mevzuat e-ticareti ana hatlarıyla düzenlemektedir. Ülkemizde var olan yasal mevzuat (Türk Ticaret Kanunu, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun, Tüketicinin Korunması Hakkında Kanun, Mesafeli Sözleşmelere dair Yönetmelik gibi) e-ticaretteki gizlilik, müşteri hakları, güvenlik/güvenilirlik, güvenli ödeme gibi konuları ana hatlarıyla düzenlemektedir. Ancak kişisel verilerin korunmasını sağlayan kanun henüz tasarı aşamasındadır ve sonuçlandırılamamıştır.

- *Kişisel Verilerin Korunması Hakkında Kanun Tasarısı:* Kişisel verilerin yasal ve dürüst bir şekilde toplanması ve işlenmesi ve kullanım amaçlarına uygun süre için muhafaza edilmesi, verilerin amaca aykırı olarak paylaşılmaması, veri sahibi kişinin hakkındaki verileri öğrenme, değiştirme ve gerekirse silme haklarını düzenlemektedir. Türkiye'de kişisel verilerin korunmasıyla ilgili mevcut bir kanuni düzenleme bulunmamaktadır. Türk Ceza Kanunu'nun 135. Maddesinde "Kişisel verilerin kaydedilmesi" konusu ele alınmakta ve hukuka aykırı olarak kaydedenlere ceza öngörülmektedir. Türkiye'nin, Avrupa Konseyi'nin 108 sayılı Sözleşmesi'ne imza koyan ve Avrupa Birliği'ni hedefleyen, bu nedenle de mevzuatını AB mevzuatı ile uyumlaştırmaya çalışan bir ülke olmasından hareketle, kişisel verilerin korunması ile ilgili bir mevzuat çalışması planlanmış ve bu kanun tasarısı hazırlanmıştır.

  Söz konusu kanun tasarılarının hazırlanmasının üzerinden zaman geçmiştir; teknolojinin ve pazarın gelişimiyle birlikte yeni ihtiyaçlar ortaya çıkmaktadır. Hem bu konulardaki AB çalışmaları ve yönlendirmeleri hem de gelişmiş ülkelerin ilgili mevzuatlarının incelenmesiyle güncelleme gerektirmektedir.

b) Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı tarafından hazırlanan "2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı"nda yer alan " e- Ticaret Mevzuatının Tamamlanması" başlıklı 51 numaralı eylem ile; ülkemizde, e-ticaretin daha güvenli bir zeminde yapılması ve bu konudaki yasal eksikliklerin giderilmesi adına, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun çerçevesinde vergilendirme, tüketici hakları, kişisel bilgilerin gizliliği, fikri mülkiyet, güvenli ödeme sistemleri ve benzeri alanlarda, e-ticaret ortamının gelişimini destekleyecek ikincil düzenlemelerin yapılacağı ve gerekli tedbirlerin alınacağı ifade edilmiştir.

Türkiye'de e-ticaretin yaygınlaşmasının önündeki en önemli engellerden biri, bu alandaki yasal düzenlemelerin yetersizliğidir. E-Ticaret alanında başarılı ve gelişmiş ülkelerin tümünde, e-ticareti düzenleyen ana kanunlar yürürlüğe sokulmuş durumda olup, bu alandaki belirsizlikler büyük ölçüde giderilmiştir. Örneğin ABD, OECD'nin e-ticaretle ilgili ilkelerini benimseyerek e-ticaretin gelişimini artırmak için zaman içinde gerekli tüm düzenlemeleri gerçekleştirmiştir. ABD'de internette tüketici bilgilerinin gizliliğinin ve genel tüketici haklarının korunması, güvenli ödemenin sağlanması, internette yapılan reklam faaliyetleri ve e-posta gönderiminin düzenlenmesi, elektronik imza ve kayıtlar ile vergilendirme konuları belirli kurumlarca düzenlenmekte ve denetlenmektedir. Türkiye'nin AB'ye katılım müzakereleri sürecinde, AB tarafından e-ticareti düzenleyen direktiflere uyum sağlanması amacı ile "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısının" hazırlanması ihtiyacı ortaya çıkmıştır. Bu kanun tasarısı ile ticari iletişimin, elektronik iletişim araçlarıyla yapılan sözleşmelerin ve e-ticarete ilişkin bilgi verme yükümlülükleri ile uygulanacak yaptırımların düzenlenmesi amaçlanmıştır. Söz konusu Kanun 23.10.2014 tarihinde Meclis Genel Kurulunda kabul edilerek 6563 sayılı "Elektronik Ticaretin Düzenlenmesi Hakkında Kanun" adı ile 5.11.2014 tarih ve 29166 sayılı Resmi Gazetede yayımlanmıştır. Kanun 1.5.2015 tarihinde yürürlüğe girmiştir. 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun çerçevesinde ikincil düzenlemeler ile rehber ve kılavuzların hayata geçirilmesi gerekmektedir.

Strateji Uygulama Adımları çerçevesinde:

- *Gümrük ve Ticaret Bakanlığı koordinasyonunda, e-ticaretin önündeki engelleri tespit ederek buna yönelik tedbirleri belirleyecek bir yapı oluşturulacaktır.*
- *e-Ticarete ilişkin mevzuat altyapısı, teknolojik gelişmeler ışığında gözden geçirilecek; özel sektörün gereksinimleri doğrultusunda ilave öneriler geliştirilecektir.*
- *Başta vergilendirme ve tüketici haklarının korunması olmak üzere e-ticaretin gelişimini ilgilendiren alanlarda ikincil mevzuat düzenlemeleri hazırlanacak ve gerekli tedbirler alınacaktır.*
- *Mevzuata uygun olarak, kılavuz niteliğinde e-ticaret sözleşmeleri oluşturulacaktır.*
- *Mevzuata ilişkin bilgilendirme ve yaygınlaştırma etkinlikleri düzenlenecek ve mevzuatın işletmeler ve tüketiciler tarafından benimsenmesi sağlanacaktır.*

c) Başta Avrupa Birliği'nin e-ticaretle ilgili direktifleri olmak üzere AB Sayısal Gündemi'nin ana başlıklarından biri olan “Sayısal Tek Pazar” başlığı altında yer alan kişisel bilgilerin gizliliği, güvenli ödeme, e-imza/e-kimlik ve vergilendirme gibi e-ticaret konuları hakkında tek bir AB standardı belirlenmekte ve üye ülkelerin uyumu istenmektedir. Avrupa Sayısal Gündemi çerçevesinde yayımlanmış bulunan “Avrupa Sayısal Haklar Kanunu” da ülkemizin uyum sağlamasının faydalı olacağı düzenlemeler arasında yer almaktadır.

d) 6563 sayılı “Elektronik Ticaretin Düzenlenmesi Hakkında Kanun” ile elektronik ticaretin güvenlik boyutu ile ilgili kapsamlı bir düzenleme getirilmemektedir. Bilgi güvenliğinin sağlanmasına ilişkin kriter, standart ve yaptırımların mevzuatla belirlenmesinin faydalı olacağı değerlendirilmektedir.