T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ÖZEL HUKUK ANA BİLİM DALI
YÜKSEK LİSANS TEZİ

YÜKSEK LİSANS TEZİ

ELEKTRONİK İMZA VE ELEKTRONİK İMZA KANUNU'NA GÖRE SERTİFİKA SAĞLAYICININ ÜÇÜNCÜ KİŞİLERE KARŞI HUKUKİ SORUMLULUĞU

BURCU ERBAYRAKTAR

2501080567

TEZ DANIŞMANI

PROF. DR. BAKİ İLKAY ENGİN

İSTANBUL

2011

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
MÜDÜRLÜĞÜ



TEZ ONAYI

Enstitümüz **ÖZEL HUKUK** Bilim Dalında ders dönemindeki Eğitim - Öğretim Programını başarı ile tamamlayan **2501080567** numaralı **BURCU ERBAYRAKTAR'IN** hazırladığı **"ELEKTRONİK İMZA VE ELEKTRONİK İMZA KANUNU'NA GÖRE SERTİFİKA SAĞLAYICININ ÜÇÜNCÜ KİŞİLERE KARŞI HUKUKİ SORUMLULUĞU"** konulu **YÜKSEK LİSANS/** ~~**DOKTORA TEZİ**~~ ile ilgili **TEZ SAVUNMA SINAVI,** Lisansüstü Öğretim Yönetmeliği'nin 15.Maddesi uyarınca **13.07.2011 ÇARŞAMBA** günü saat **13:00'TE** yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin Kabulü'ne* **OYBİRLİĞİ /**~~**OYÇOKLUĞUYLA**~~ karar verilmiştir.

JÜRİ ÜYESİ	KANAATİ(*)	İMZA
PROF.DR.TEOMAN AKÜNAL	Kabul	
PROF.DR. TUFAN ÖĞÜZ	Kabul	
PROF.DR.GÜLÇİN ELÇİN GRASSİNGER	Kabul	
PROF.DR.BAKİ İLKAY ENGİN	kabul	
DOÇ.DR SUAT SARI	Kabul	

Adres: Besim Ömerpaşa Caddesi Kaptan-ı Derya Sokağı 34452 Beyazıt/İstanbul
Tel: 0212 440 00 00 / 14219-14220-14221-14222-14226-14227-14243
Fax: 0212 440 03 40 e-mail: sbe@istanbul.edu.tr

ÖZ

Bu çalışmada elektronik imza kavramı ve 5070 sayılı Elektronik İmza Kanunu'na göre sertifika sağlayıcıların üçüncü kişilere karşı hukuki sorumluluğu konusu incelenmektedir. Çalışmanın birinci bölümünde elektronik imza kavramsal olarak incelenmekte ve karşılaştırmalı hukukta elektronik imzanın hukuki sonuçlarına ilişkin olarak getirilen temel düzenlemeler ele alınmaktadır. İkinci bölümde, Türk hukukundaki düzenleniş şekli itibariyle güvenli elektronik imza kavramı ve hususiyetle geçerlilik şekli bakımından güvenli elektronik imzanın hukuki sonuçları üzerinde durulmaktadır. Üçüncü ve son bölümde ise, Türk hukukunda sertifika sağlayıcı kavramı ve sertifika sağlayıcının yükümlülükleri incelenerek, bu yükümlülüklere aykırılık sonucu ortaya çıkan zararlardan sertifika sağlayıcının üçüncü kişilere karşı hukuki sorumluluğu Elektronik İmza Kanunu hükümleri çerçevesinde anlatılmaya çalışılacaktır.

ABSTRACT

This thesis provides an analysis of electronic signature and liability of certificate service providers towards third parties according to the Electronic Signature Law numbered 5070. In the first part, concept of electronic signature and essential regulations in comparative law regarding legal consequences of electronic signatures are examined. The second part of the study displays electronic signature concept in accordance with Turkish electronic signature regulation, and explains especially legal effects of electronic signatures on validity of transactions. The third and the last part introduces concept of certificate service provider, and reviews statutory liability of certificate service providers towards third parties arising from infringement of their obligations, in line with Electronic Signature Law.

ÖNSÖZ

"Elektronik İmza ve Elektronik İmza Kanunu'na Göre Sertifika Sağlayıcının Üçüncü Kişilere Karşı Hukuki Sorumluluğu" başlıklı yüksek lisans tezime büyük bir özveriyle yapmış olduğu derin katkılardan ötürü değerli hocam Prof. Dr. Baki İlkay Engin'e, bana bu çalışma konusunu öneren ve çalışmalarım sırasında her zaman rehberliği ile yol gösteren değerli hocam Prof. Dr. Teoman Akünal'a, Işık Önay, Zeynep Özkul ve Beril Özcanlı başta olmak üzere Koç Üniversitesi Hukuk Fakültesi'ndeki tüm çalışma arkadaşlarıma ve desteğiyle hep yanında olan sevgili aileme teşekkürü borç bilirim.

İÇİNDEKİLER

ÖZ.....i
ÖNSÖZ.....ii
İÇİNDEKİLER.....iii
KISALTMALAR CETVELİ.....x
GİRİŞ.....1

BİRİNCİ BÖLÜM

ELEKTRONİK İMZA KAVRAMI VE ELEKTRONİK İMZA ALANINDAKİ DÜZENLEMELERİN GELİŞİMİ

I. ELEKTRONİK İMZA.....3
A. KAVRAM VE TANIM.....3
B. TEKNOLOJİK YAPISINA GÖRE ELEKTRONİK İMZA TÜRLERİ.....7
1. Dijital (Sayısal) İmza.....7
2. Biyometrik İmza.....12

II. ELEKTRONİK İMZANIN DÜZENLENMESİNDE ESAS ALINAN TEMEL İLKELER.....15
A. İŞLEVSEL DENKLİK İLKESİ.....15
1. El Yazısıyla İmzanın İşlevleri.....16
2. Dijital İmza ile El Yazısıyla İmzanın İşlevleri Açısından Karşılaştırılması.....17
a. Kimlik Tespiti İşlevi.....17
b. Sonuçlandırma İşlevi.....18
c. Uyarı İşlevi.....22
B. TEKNOLOJİDEN BAĞIMSIZLIK İLKESİ.....26

III. ELEKTRONİK İMZAYA İLİŞKİN KARŞILAŞTIRMALI HUKUKTAKİ TEMEL DÜZENLEMELER.....31
A. AVRUPA BİRLİĞİ ELEKTRONİK TİCARET YÖNERGESİ.....31
B. AVRUPA BİRLİĞİ ELEKTRONİK İMZA YÖNERGESİ.....32
1. Elektronik İmza ve Hukuki Etkilerinin Düzenlenmesi.....34
a. Elektronik İmza Tanımı ve Çeşitleri.....34
b. Elektronik İmzanın Hukuki Etkileri.....36
2. Sertifika Hizmetlerinin Düzenlenmesi.....39
a. Sertifika Sağlayıcı Kavramı.....39
b. Sertifika Sağlayıcının Sorumluluğu.....43
C. ELEKTRONİK TİCARET HAKKINDA UNCITRAL MODEL KANUNU.....46
D. ELEKTRONİK İMZALAR HAKKINDA UNCITRAL MODEL KANUNU.....48
1. Elektronik İmza ve Hukuki Etkileri.....49
2. Elektronik İmza Sisteminde Yer Alan Taraflar ve Yükümlülükleri.....50
a. İmza Sahibi ve İmza Sahibinin Yükümlülükleri.....51
b. Sertifika Sağlayıcı ve Sertifika Sağlayıcının Yükümlülükleri.....52
c. Güvenen Taraf ve Güvenen Tarafın Yükümlülükleri.....54
3. Yabancı Elektronik İmzaların ve Yabancı Sertifikaların Hukuki Etkisi..55
E. ELEKTRONİK İMZAYA İLİŞKİN İSVİÇRE, ALMANYA VE AMERİKA BİRLEŞİK DEVLETLERİ'NDEKİ DÜZENLEMELER.....55
1. İSVİÇRE.....55
2. ALMANYA.....57
3. AMERİKA BİRLEŞİK DEVLETLERİ.....58

İKİNCİ BÖLÜM

TÜRK HUKUKUNDA ELEKTRONİK İMZANIN DÜZENLENİŞ TARZI VE HUKUKİ İŞLEMLERİN GEÇERLİLİK ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARI

I. TÜRK HUKUKUNDA ELEKTRONİK İMZANIN DÜZENLENİŞ TARZI.....60

A. ELEKTRONİK İMZA KANUNU VE İLGİLİ MEVZUAT.....61

B. BORÇLAR KANUNU.....64

C. HUKUK MUHAKEMELERİ KANUNU.....64

D. TİCARET KANUNU.....66

E. DİĞER KANUNLARDA YER ALAN DÜZENLEMELER.....69

II. ELEKTRONİK İMZA.....71

III. GÜVENLİ ELEKTRONİK İMZA.....76

A. GÜVENLİ ELEKTRONİK İMZA KAVRAMI.....76

B. GÜVENLİ ELEKTRONİK İMZANIN GEÇERLİLİK ŞARTLARI.....78

1. Münhasıran İmza Sahibine Bağlı Olması.....78

2. Sadece İmza Sahibinin Tasarrufunda Bulunan "Güvenli Elektronik İmza Oluşturma Aracı" ile Oluşturulmuş Olması.....80

a. Ürettiği İmza Oluşturma Verilerinin Kendi Aralarında Bir Eşi Daha Bulunmaması.....82

b. Üzerinde Kayıtlı Olan Elektronik İmza Oluşturma Verilerinin Araç Dışına Hiçbir Biçimde Çıkarılamamasını, Gizliliğini ve Bunların Üçüncü Kişiler Tarafından Elde Edilememesini,

Kullanılamamasını ve Elektronik İmzanın Sahteciliğe Karşı Korunmasını Sağlaması……...83
c. İmzalanacak verinin imza sahibi dışında değiştirilememesi ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesi.....84
3. Nitelikli Elektronik Sertifikaya Dayanarak İmza Sahibinin Kimliğinin Tespitini Sağlaması.....85
a. Genel Olarak.....85
b. Nitelikli Sertifikanın Kullanım Alanı ve Kapsamına İlişkin Sınırlamaların Güvenli Elektronik İmzanın Geçerliliği Bakımından Etkisi.....87
c. Yabancı Elektronik Sertifikalar Bakımından Nitelik Elektronik Sertifikaya Dayanma Şartının Gerçekleştirilmesi.....91
4. İmzalanmış Elektronik Veride Sonradan Yapılan Değişikliğin Tespitini Sağlaması.....92
C. GÜVENLİ ELEKTRONİK İMZA KULLANIMINDA İMZA SAHİBİ SIFATININ BELİRLENMESİ.....94
D. YETKİSİZ BİR ÜÇÜNCÜ KİŞİ TARAFINDAN OLUŞTURULMASININ GÜVENLİ ELEKTRONİK İMZANIN GEÇERLİLİĞİNE ETKİSİ.....96

IV. HUKUKİ İŞLEMLERİN GEÇERLİLİK ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARI.....102
A. BORÇLAR HUKUKU BAKIMINDAN ŞEKİL KAVRAMI.....103
1. Kanuna Dayanan (Yasal) Şekil.....104
a. Adi Yazılı Şekil.....105
b. Resmi Yazılı Şekil.....109
2. Tarafların Anlaşmasına Dayanan (İradi) Şekil.....110
B. GEÇERLİLİK ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARI.....112
1. Kanuna Dayanan Şekil Açısından.....112
2. İradi Şekil Açısından.....117

C. GÜVENLİ ELEKTRONİK İMZA İLE YAPILAMAYACAK HUKUKİ İŞLEMLER.....119
1. Geçerliliği Resmi Şekle Tabi Tutulan Hukuki İşlemler.....120
2. Geçerliliği Özel Merasime Tabi Tutulan Hukuki İşlemler.....123
3. Teminat Sözleşmeleri.....124
a. Teminat Sözleşmesi Kavramı.....124
b. Teminat Sözleşmelerine İlişkin İstisnanın Anlamı.....125
c. Teminat Sözleşmelerine İlişkin İstisnanın Sonuçları.....130
D. İSPAT ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN HUKUKİ SONUÇLARINA GENEL BAKIŞ.....137

ÜÇÜNCÜ BÖLÜM

SERTİFİKA SAĞLAYICININ ELEKTRONİK İMZA KANUNU'NDAN DOĞAN YÜKÜMLÜLÜKLERİ VE ÜÇÜNCÜ KİŞİLERE KARŞI HUKUKİ SORUMLULUĞU

I. SERTİFİKA SAĞLAYICI KAVRAMI VE SERTİFİKA SAĞLAYICININ ELEKTRONİK İMZA KANUNU'NDAN DOĞAN YÜKÜMLÜLÜKLERİ...140
A. SERTİFİKA SAĞLAYICI KAVRAMI.....141
B. SERTİFİKA SAĞLAYICININ YÜKÜMLÜLÜKLERİ.....145
1. Nitelikli Sertifika Talep Eden Kişilerin Kimliğini Tespit Etme Yükümlülüğü.....145
2. İmza Oluşturma ve Doğrulama Verilerinin Üretilmesi Yükümlülüğü...148
a. İmza Oluşturma Verisinin Sertifika Sağlayıcı Tarafından Üretilmesi.....149
b. İmza Oluşturma Verisinin İmza Sahibi Tarafından Üretilmesi.....150
(1) İmza Oluşturma Verisinin İmza Sahibi Tarafından

Sertifika Sağlayıcıya Ait Yerlerde Üretilmesi.....150
(2) İmza Oluşturma Verisinin İmza Sahibi Tarafından ve Sertifika Sağlayıcının Sağladığı Güvenli Elektronik İmza Oluşturma Araçlarıyla Üretilmesi.....151
(3) İmza Oluşturma Verilerinin İmza Sahibi Tarafından Sertifika Sağlayıcıya Ait Olmayan Yerlerde ve Araçlarla Üretilmesi.....152
3. Nitelikli Sertifika Düzenleme Yükümlülüğü.....154
4. İmza Doğrulama Verisini İmza Sahibine Özgüleme Yükümlülüğü.....158
5. Elektronik İmza Araçlarını Sağlama Yükümlülüğü.....160
6. İmza Sahibini Bilgilendirme Yükümlülüğü.....161
7. Nitelikli Elektronik Sertifikayı İptal Etme Yükümlülüğü.....167
a. Nitelikli Sertifikanın İptalini Gerektiren Sebepler.....167
(1) Nitelikli Sertifika Sahibinin Talebi.....168
(2) Nitelikli Elektronik Sertifikada Yer Alan Bilgilerin Sahteliğinin veya Yanlışlığının Ortaya Çıkması veya Bilgilerin Değişmesi.....168
(3) İmza Oluşturma Verisinin Çalınması, Kaybolması veya Başka Bir Şekilde İmza Sahibinin İradesi Dışında Elinden Çıkması Sonucu Gizliliğinin Ortadan Kalkması.....169
(4) İmza Oluşturma Verisinin Güvenliğinin Ortadan Kalkması.....170
(5) Nitelikli Sertifika Sahibinin Fiil Ehliyetinin Sınırlandığının, İflasının veya Gaipliğinin ya da Ölümünün Öğrenilmesi.....171
(6) Elektronik İmzanın İmza Oluşturma ve Doğrulama Amacı Dışında Kötüye Kullanıldığının Tespit Edilmesi.....171
(7) Sertifika İlkelerinin Değişmesi.....172
(8) Sertifika Sağlayıcının Faaliyetinin Sona Ermesi.....172
b. Nitelikli Sertifikanın İptaline İlişkin Taleplerin Yapılması.....173

c. Nitelik Sertifikanın İptal Edilmesi ve İptal Kararının Sertifika Sağlayıcı Tarafından Oluşturulan İptal Listesinde Yayınlanması....175
8. Nitelikli Sertifikayı Kamuya Açık Bir Dizinde Yayımlama Yükümlülüğü.....177
9. Zaman Damgası Hizmetini Sağlama Yükümlülüğü.....179
10. Sertifika Sağlayıcının Diğer Yükümlülükleri.....181

II. SERTİFİKA SAĞLAYICININ ÜÇÜNCÜ KİŞİLERE KARŞI SORUMLULUĞU.....183
A. SORUMLULUĞUN NİTELİĞİ VE ŞARTLARI.....185
1. Hukuka Aykırı Fiil.....190
2. Zarar.....194
3. Uygun İlliyet Bağı.....195
4. Kusur.....197
B. SERTİFİKA SAĞLAYICININ ÇALIŞTIRDIĞI KİŞİLERİN DAVRANIŞLARINDAN SORUMLULUĞU.....200
1. Sorumluluğun Anlamı.....200
2. Sorumluluğun Şartları.....201
C. NİTELİKLİ SERTİFİKANIN KULLANIM ALANI VE MADDİ KAPSAMINA İLİŞKİN SINIRLAMALARIN SERTİFİKA SAĞLAYICININ SORUMLULUĞUNA ETKİSİ.....204
D. ZORUNLU SERTİFİKA MALİ SORUMLULUK SİGORTASI.....207

SONUÇ.....210

KAYNAKÇA.....214

KISALTMALAR CETVELİ

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
Abt.	:	Abteilung (kısım)
Art.	:	Artikel (madde)
a.g.e.	:	adı geçen eser
Aufl.	:	Auflage (bası)
AÜHFD	:	Ankara Üniversitesi Hukuk Fakültesi Dergisi
BATİDER	:	Banka ve Ticaret Hukuku Dergisi
BGB	:	Bürgerliches Gesetzbuch (Alman Medeni Kanunu)
BGBl	:	Das Bundesgesetzblatt für die Republik Österreich (Avusturya Resmi Gazetesi)
BGH	:	Bundesgerichtshof (Alman Federal Mahkemesi)
BK.	:	22.4.1926 tarihli ve 818 sayılı Borçlar Kanunu
bkz.	:	bakınız
Bot ZertES	:	Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (İsviçre Elektronik İmza Kanunu Gerekçesi)
C.	:	Cilt
CEN	:	European Committee for Standardization (Avrupa Standardizasyon Komitesi)
CMK.	:	4.12.2004 tarihli 5271 sayılı Ceza Muhakemesi Kanunu
Cardozo Arts Ent. L.J.	:	The Cardozo Arts & Entertainment Law Journal
Computer L. Rev. & Tech	:	Computer Law Review & Technology Journal
CLSR	:	Computer Law and Security Review

çev.	:	çeviren
DG Information Society	:	Directorate General for the Information Society
dn.	:	dipnotu
edit.	:	editör
E.	:	Esas numarası
e-devlet	:	elektronik devlet
e-imza	:	elektronik imza
EC	:	European Commission
EESSI	:	The European Electronic Signature Standardization Initiative (Avrupa Elektronik İmza Standardizasyon Girişimi)
EİK.	:	15.1.2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu
EİY.	:	06.01.2005 tarihli ve 25692 sayılı Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik
E-Sign Act	:	Electronic Signatures in Global and National Commerce Act (ABD Elektronik İmza Kanunu)
ETKK	:	Elektronik Ticaret Koordinasyon Kurulu
ETSI	:	European Telecommunications Standards Institute (Avrupa Telekomünikasyon Standartları Enstitüsü)
GSÜHFD	:	Galatasaray Üniversitesi Hukuk Fakültesi Dergisi
HD.	:	(Yargıtay) Hukuk Dairesi
HGK.	:	(Yargıtay) Hukuk Genel Kurulu
HPD	:	Hukuki Perspektifler Dergisi
Hrsg.	:	Herausgegeben von (yayımlayan)
HMK.	:	12.1.2011 tarihli ve 6100 sayılı Hukuk Muhakemeleri Kanunu

HUMK.	:	18.06.1927 tarihli ve 1086 sayılı Hukuk Usulü Muhakemeleri Kanunu
ICEC'06	:	International Conference on Electronic Commerce 2006
IT & Law Series	:	Information Technology & Law Series
İBK	:	(Yargıtay) İçtihadı Birleştirme Kararı
JILT	:	Journal of International Commercial Law and Technology
K.	:	Karar numarası
Kamu SM	:	Kamu Sertifikasyon Merkezi
LNCS	:	Lecture Notes in Computer Science
m.	:	madde
MK.	:	22.11.2001 tarihli ve 4721 sayılı Türk Medeni Kanunu
NCCUSL	:	The National Conference of Commissioners on Uniform State Laws (Yeknesak Eyalet Hukukları Oluşturulması Hakkında Ulusal Konferans)
N.	:	Not, kenar notu
NJW	:	Neue Juristische Wochenschrift
NOTEV	:	Noterlik Hukuku Araştırma Enstitüsü Vakfı
Noterlik K.	:	18.1.1972 tarihli ve 1512 sayılı Noterlik Kanunu
OCSP	:	Online Certificate Status Protocol (Çevrimiçi Sertifika İptal Durumu Kontrol İmkanı)
OR.	:	Obligationenrecht (İsviçre Borçlar Kanunu)
par.	:	paragraf
PDA	:	Personal Digital Assistant (Kişisel Dijital Asistan)
PIN	:	Personal Indentification Number (Kişisel Kimlik Numarası)
PKI	:	Public Key Infrastructure (Açık Anahtar Altyapısı)

RG	:	Resmi Gazete
s.	:	sayfa
S.	:	Sayı
SigG	:	Gesetz über Rahmenbedingungen für elektronische Signaturen (Alman Elektronik İmza Kanunu)
SigV	:	Verordnung zur elektronischen Signatur (Alman Elektronik İmza Yönetmeliği)
SİL	:	Sertifika İptal Listesi
SPK	:	Sermaye Piyasası Kurulu
T.	:	Tarih
TAKBİS	:	Tapu ve Kadastro Bilgi Sistemi
Tapu K.	:	22.12.1934 tarihli ve 2644 sayılı Tapu Kanunu
TBBD	:	Türkiye Barolar Birliği Dergisi
TBMM	:	Türkiye Büyük Millet Meclisi
TKHK.	:	23.2.1995 tarihli ve 4077 sayılı Tüketicinin Korunması Hakkında Kanun
TTK.	:	29.6.1956 tarihli ve 6762 sayılı Türk Ticaret Kanunu
UEKAE	:	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UNCITRAL	:	United Nations Commission on International Trade Law *(*Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu)
USB	:	Universal Serial Bus (Evrensel Seri Veriyolu)
UYAP	:	Ulusal Yargı Ağı Projesi
vd.	:	ve devamı
Vol.	:	Volume (cilt)
VzertES	:	Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (İsviçre Elektronik İmza

		Yönetmeliği)
Y.	:	Yıl
Yarg.	:	Yargıtay
YKD.	:	Yargıtay Kararları Dergisi
ZertDV	:	Verordnung über Dienste der elektronischen Zertifizierung (İsviçre Elektronik İmza Yönetmeliği)
ZertES	:	Bundesgesetz über Zertifizierungsdienste im Bereich der Elektronische Signatur (İsviçre Elektronik İmza Kanunu)

GİRİŞ

İnternet üzerinden gerçekleştirilen hukuki işlemlerin gittikçe yaygınlaşması neticesinde elektronik imza kavramının yaratılmasına ihtiyaç duyulmuştur. Elektronik imza tekniklerinin geliştirilmesine ve yaygınlaştırılmasına duyulan bu ihtiyaç, özellikle hukuki işlemlerin yasal olarak geçerlilik şekline tabi kılındığı düzenlemeler açısından daha da kendini hissettirmektedir. Bunun dışında, elektronik imza teknikleri, el yazısıyla imzanın sağladığı işlevleri elektronik ortamda ikame etme amacına yönelmektedir. El yazısıyla imzanın sağladığı işlevler esas itibariyle imzalayanın kimlik bilgilerinin tespitine olanak vermesi ve irade açıklamasının yer aldığı metinle bağlanma iradesini ortaya koymasıdır.

Elektronik imza kavramı, şartları itibariyle Türk hukukunda ve karşılaştırmalı hukuklarda yer alan düzenlemelerde teknolojiden bağımsız bir dille tanımlanmakta, bu sayede çeşitli teknikleri kapsayan hukuki bir kavram olarak ortaya çıkmaktadır. Diğer bir ifadeyle, uygulamadaki elektronik imza tekniklerinin (dijital imza, biyometrik imza vb.) hukuki bir etki doğurabilmesi, hukuki düzenlemelerde elektronik imza kavramına ilişkin olarak öngörülen asgari koşulları yerine getirmesine bağlı tutulmaktadır.

Türk hukukunda, meydana getirdiği hukuki sonuçları bakımından, kural olarak el yazısıyla imzayla denk kılınan elektronik imza türü güvenli elektronik imzadır (BK 14 I). Prensip teknolojiden bağımsızlık ilkesi olmakla birlikte, güvenli elektronik imza kavramının uygulamadaki karşılığını dijital imza teknolojileri oluşturmaktadır. Güvenli elektronik imzanın şartları 5070 sayılı Elektronik İmza Kanunu'nun 4. maddesinde tanımlanmaktadır. Bu şartların eksiksiz bir şekilde yerine getirilmesi ve bu sayede güvenli elektronik imzanın kanunda bahşedilen hukuki sonuçları doğurması görevi sertifika sağlayıcıları tarafından üstlenilmektedir.

Sertifika sağlayıcıların Elektronik İmza Kanunu'nda düzenlenen yükümlülükleri gereği gibi ifası, güvenli elektronik imzanın varlığını ve güvenli elektronik imza kullanımına bağlı olarak ortaya çıkacak hukuki sonuçları teminat altına almaktadır.

Güvenli elektronik imzanın geçerliliği ile sertifika sağlayıcıların yükümlülükleri arasında kurulan bu bağlantı birtakım karmaşık sorunları beraberinde getirmektedir. Bunların en önemlisi sertifika sağlayıcının üçüncü kişilere karşı sorumluluğu meselesidir.

Çalışmamız kapsamında ilk olarak, elektronik imza kavramının ortaya çıkışı, bu kavramın gelişiminde esas alınan ilkeler ve karşılaştırmalı hukukta elektronik imza konusunun düzenleniş tarzı genel itibariyle incelenecektir. İkinci bölümde, elektronik imzaya ilişkin Türk hukukundaki düzelemelere ve elektronik imzanın hukuki sonuçları konularına yer verilmektedir. Bu bölümde, elektronik imzanın hukuki sonuçları, hukuki işlemlerin geçerlilik şekli bakımından güvenli elektronik imzanın sonuçlarıyla sınırlı olarak değerlendirilmektedir. Böyle bir sınırlandırmaya başvurmamızın sebebi, yürürlükteki mevzuatımızda elektronik imzanın hukuki sonuçlarının yalnızca güvenli elektronik imzaya münhasır olarak düzenlenmiş olmasıdır. Güvenli elektronik imza dışında kalan basit elektronik imzalı belgelerin delil değeri konusuna ise ayrı bir çalışmaya konu olabilecek kapsamı ve derinliği dolayısıyla tezimizde yer vermemeyi daha isabetli buluyoruz.

Üçüncü ve son bölümde, güvenli elektronik imzanın geçerliliği bağlamında sertifika sağlayıcıların yükümlülükleri konusu detaylı olarak incelenerek, bu yükümlülüklerin ihlali halinde sertifika sağlayıcının güvenli elektronik imzanın geçerliliğine güvenen üçüncü kişilere karşı sorumluluğu konusu ele alınmaktadır. Sertifika sağlayıcının güvenli elektronik imza verdiği kişilerle arasındaki sözleşmeye dayanan sorumluluğu konusu Elektronik İmza Kanunu'nun ve çalışmamızın kapsamı dışında kalmaktadır.

BİRİNCİ BÖLÜM

ELEKTRONİK İMZA KAVRAMI VE ELEKTRONİK İMZA ALANINDAKİ DÜZENLEMELERİN GELİŞİMİ

I. ELEKTRONİK İMZA

A. KAVRAM VE TANIM

Günümüzde karşılıklı irade beyanlarının gönderilmesi elektronik ortamın sağladığı olanaklar sayesinde daha süratli ve masrafsız bir şekilde gerçekleştirilebilmektedir. Bu gelişme sözleşmelerin elektronik ortamda kurulmasını, kağıda dayalı ortamlara kıyasla daha cazip bir hale getirmekteyse de, kağıda dayalı ortamın sağladığı hukuki güven unsurunu aynı şekilde sağlamaya yeterli olmamaktadır. Bunun en önemli sebepleri, elektronik ortamdaki metinlerin kolaylıkla değiştirilebilmesi ve kimden sadır olduğunun güvenilir bir şekilde belirlenememesidir.

Kağıda dayalı ortamda bir metnin mevcut haliyle kimin iradesini yansıttığını belirleyebilmek el yazısıyla imza sayesinde mümkün olur. Elektronik ortamda kayıtlı bulunan bir metnin ise el yazısıyla imzalanabilmesi söz konusu değildir. El yazısıyla imzanın eksikliği nedeniyle de, elektronik ortamdaki bir metnin aslı ve kopyası arasında çoğu zaman bir farklılık bulunmamaktadır. Bunun sonucunda sözleşme metinlerinin değiştirilmesi çok basit bir şekilde ve fark edilmeksizin mümkün olabilmektedir[1]. Bu tür kaygılara cevap vermek amacıyla geliştirilmiş, elektronik ortamda yapılan irade beyanlarının daha sonra yazıcı vasıtasıyla kağıt üzerinde tespit edilip taraflarca imzalanması ve bu şekilde teyit edilmesi şeklinde birtakım

[1] Hatice Özdemir Kocasakal, **Elektronik İmzanın Geçerliliği ve İspat Gücü Açısından Uluslararası Planda Yaşanan Gelişmeler**, Prof. Dr. Ergun Önen'e Armağan, İstanbul, Alkım, 2003, s.217-251, s.217.

uygulamalar mevcuttur. Ancak bu uygulamalar elektronik ortamın sağlamaya çalıştığı kağıt israfının azaltılması, belgelerin saklanmasında yer tasarrufu sağlaması ve özellikle de hukuki ilişkilerin daha süratle kurulması hedefleriyle örtüşmemekte, klasik yöntemlere nazaran yeni bir avantaj ortaya koymamaktadır[2].

Kağıda dayalı belgelerde bulunan el yazısıyla imza unsurunun elektronik ortamda karşılığının bulunmayışı, geçerliliği yazılı şekle tabi tutulan sözleşmelerin elektronik yolla yapılmasına ve elektronik belgelerin ispat aracı olarak kullanılmasına engel oluşturmuştur[3]. Bu engeli aşmak üzere elektronik imza kavramının yaratılmasına ihtiyaç duyulmuş ve birçok ülkede yapıldığı gibi Türk hukukunda da elektronik imzanın şartlarını yeknesak bir şekilde belirleyen ve bunların sağlanması için gereken teknik altyapıyı açıklayan hukuki düzenlemeler meydana getirilmiştir[4].

Elektronik imzanın düzenlenmesinin ardında yatan fikir, elektronik ortamda güvenli bir şekilde bilgi değişimi sağlama ve bu yolla hukuki ilişkiler kurma hususlarında yeni olanaklar yaratmaktır. Bu sayede elektronik imza el yazısıyla imzanın yerini almakta, aynı işlevleri gerçekleştirmek üzere inşa edilmektedir[5]. Elektronik imza kavramı, uluslararası düzenlemelerde birbirine yakın ifadelerle tanımlanmaktadır. Avrupa Birliği Elektronik İmza Yönergesi'nin 2. maddesine göre elektronik imza "*başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan ve bir doğrulama yöntemi oluşturan, elektronik formda bulunan veri*"dir. UNCITRAL Elektronik İmza Model Kanunu'na göre ise elektronik imza, "*bir veri mesajına eklenen veya mantıksal olarak bu mesajla ilişkilendirilen, veri mesajıyla[6] bağlantılı olarak imzalayanın kimliğini belirlemeye yarayan ve imzalayan*

---

2 Zarife Şenocak, "Dijital İmza ve Dijital İmzalı Belgelerin Borçlar Kanunu Hükümleri Açısından Ele Alınması", **AÜHFD**, C.50, S.2, 2001, s.98-135, s.124.

3 Necip Kocayusufpaşaoğlu, **Borçlar Hukuku Genel Bölüm**, C.1, 4. Bası, İstanbul, Filiz Kitabevi, 2008, s.290.

4 Bu düzenlemelerin gelişimi için bkz. s.60.

5 Wolfgang Kilian, "Dijital Communication and Contract Law", **Uluslararası İnternet Hukuku Sempozyumu**, İzmir, Dokuz Eylül Üniversitesi Yayını, 2002, s.145-161, s.155.

6 Model Kanun m.2'ye göre burada geçen veri mesajı, "elektronik, optik veya bunlarla sınırlı olmamak üzere, elektronik veri değişimi, elektronik posta, telgraf, teleks veya telekopi de dahil olmak üzere benzer her türlü araçla üretilen, gönderilen, alınan veya saklanan bilgi"dir.

tarafından söz konusu veri mesajının içeriğini onaylama iradesi ile uygulanan elektronik formattaki veridir[7] *".*

Her iki düzenlemedeki tanımlar dikkate alındığında, elektronik imza, her türlü elektronik ses, sembol veya uygulamayı kapsayan ve kullanılan teknolojiden bağımsız (*technology-neutral*) bir üst kavram olarak ortaya çıkmaktadır[8]. Gerçekten bu kavramın altında, dijital imza, mobil imza, biyometrik imza gibi çeşitli teknolojilerden yararlanılarak oluşturulmuş birbirinden farklı elektronik imza türleri bulunmaktadır.

Ancak günümüzde, farklı elektronik imza çeşitleri arasında hukuki düzenlemelerde aranan güvenlik şartını en büyük ölçüde gerçekleştiren elektronik imza türü dijital imzadır[9]. Buna paralel olarak elektronik imza kavramına ilişkin birçok akademik çalışmada büyük ölçüde dijital imza tekniği esas alınmakta ve bu nedenle elektronik imza ile dijital imza kavramları eş anlamlı olarak kullanılmaktadır[10]. Aslında elektronik imzanın her türünün bilgisayar ortamındaki diğer tüm veriler gibi dijital verilerden oluştuğu dikkate alındığında, elektronik imza

---

7 Türk hukukunda EİK. 3 (a) hükmüne göre elektronik veri "*elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları*" ifade etmektedir. Öğretide elektronik veri bilgisayarın bir sonuca ulaşmak için bilgi işleme sürece içinde, işlem yaptığı rakamlar, sözcükler ve cümleler olarak da tanımlanmaktadır: Ayşe Saadet Arıkan, "Bilgisayar Programlarının Korunması: AB ve Türkiye (1. Bölüm)", **TBBD,** S.3, 1996, s.309-382.

8 Elektronik imza teriminin bir üst kavram olduğu ilk olarak UNCITRAL Elektronik İmza Model Kanunu'nda belirtilmiştir (Uygulama Kılavuzu, par.33 vd). Türk hukukunda da elektronik imzanın bir üst kavram olduğu kabul edilmektedir: Kocayusufpaşaoğlu, **a.g.e**., s.291; Billur Yaltı Soydan, "E-imza ve E-belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk – I", **Vergi Sorunları Dergisi**, S.151, 2001 s.127-135, s.128; Ulvi Altınışık, **Elektronik Sözleşmeler**, İstanbul, Seçkin, 2003, s.78-79; Mine Erturgut, **Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi**, Ankara, Yetkin Yayınları, 2004; Mesut Orta, **Elektronik İmza ve Uygulaması**, İstanbul, Seçkin, 2005, s.36; İpek Sağlam, **Elektronik Sözleşmeler**, İstanbul, Legal, 2007, s.155.

9 Adam White Scoville, "Clear Signature, Obscure Signs, **Cardozo Arts Ent. L.J.,** 1999/17, s.346-412, s. 361; Minyan Wang**,** "The Impact of Information Technology Development on the Legal Concept- A Particular Examination on the Legal Concept of Signatures", **International Journal of Law and Information Technology**, Vol.15, No.3, Oxford University Press, 2006, 253-274, p.254. Ancak, yine de elektronik ortamda gerçekleştirilen işlemlerde güvenlik şartını gerçekleştiren tek elektronik imza türünün dijital imza olduğu düşünülmemelidir: Erturgut, **a.g.e.**, s.54.

10 Bu yaklaşımı benimseyen yazarlar için bkz. Şenocak, a.g.e., s.98; Leyla Keser Berber, **İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza**, Ankara, Yetkin Yayınları, 2002, s.119 vd.; Ergun Özsunay, "Elektronik Ticaret ve E-Sözleşmelerin Temel Sorunları", **Uluslararası İnternet Hukuku Sempozyumu**, İzmir, Dokuz Eylül Üniversitesi Yayını, 2002, s.121-145, s.136.

ve dijital imzanın, hatta daha genel bir ifadeyle dijital ve elektronik deyimlerinin eş anlamlı olarak kullanılmasında teknik açıdan bir yanlışlık yoktur. Fakat günümüzde kazandığı anlam itibariyle dijital imza belirli bir teknolojik yöntemi ve tasarımı ifade etmektedir[11]. Bu dar ve günlük dilde kazandığı anlam itibariyle dijital imza, çeşitli elektronik imza yöntemlerinden sadece birisidir. Elektronik imza ise tüm bu yöntemleri içeren hukuki bir kavram olarak karşımıza çıkmaktadır[12].

Elektronik imzaya ilişkin yasal düzenlemeler, "el yazısıyla imza"nın işlevlerine odaklanmakta ve işlevsel denklik ilkesi çerçevesinde, elektronik imzanın el yazısıyla imzanın işlevlerini yerine getirmesini sağlamayı amaçlamaktadır. Bu sebeple elektronik imza kavramının, teknik bir kavram olan ve elektronik imza yaratma dışında kalan başka amaçlarla da kullanılan dijital imzadan ayrı olarak değerlendirilmesi gerekmektedir[13]. Hangi teknolojik uygulamaların elektronik imza olarak kabul göreceği teknolojiye göre değil, konuya ilişkin hukuki düzenlemelere göre belirlenmektedir[14].

Bu çerçevede, ilk olarak elektronik imzanın hukuken düzenlenmesi ihtiyacını doğuran elektronik imza türlerinin teknolojik yapıları itibariyle açıklanması, ikinci olarak karşılaştırmalı hukukta ve Türk hukukunda elektronik imza düzenlenmelerinde esas alınan teknolojiden bağımsızlık ve işlevsel denklik ilkelerinin incelenmesi gerekmektedir.

---

[11] Emrehan İnal, **E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması,** İstanbul, Vedat Kitapçılık, 2005, s.140, dn.189; Huriye Kubilay / Esen Akıntürk, "Elektronik Konişmento", **Prof.Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı,** İstanbul, Beta, 2001, s.333-354; s.339; Keser Berber, **Dijital İmza**, s.503.

[12] Jos Dumortier / Stefan Kelm / Hans Nilsson / Georgia Skouma / Patrick Van Ecke, **The Legal and Market Aspects of Electronic Signatures, Study for the European Commission – DG Information Society**, (Çevrimiçi) http://ec.europa.eu/information_society/eeurope/2005/all_about //electronic_sig_report.pdf, 04 Ağustos 2010, s.29.

[13] Dijital imza kişiler arasındaki iletişimin güvenliğini sağlayan teknolojilerden biridir. Ancak aynı zamanda makineler arası iletişimi veya bir web sayfasının güvenliğini sağlama amacı ile de kullanılabilir: Jos Dumortier, "E-imza, E-fatura ve E-ticaret", **Ankara Barosu Hukuk Kurultayı 03-07 Ocak 2006, C. IV: Bilişim Hukuku**, 2006, Ankara, s.159-167, s.160. Örneğin, Finlandiya ve Belçika'da uygulanmakta olan elektronik kimlik kartı projeleri (electronic identity card projects) dijital imza teknolojisine dayanmaktadır: Dumortier / Kelm / Nilsson / Skouma / Van Ecke, **a.g.e**., s.29, dn.4.

[14] Lorna Brazell, **Electronic Signatures Law and Regulation**, London, Sweet & Maxwell, 2004, s.35.

B. TEKNOLOJİK YAPISINA GÖRE ELEKTRONİK İMZA TÜRLERİ

Elektronik imza türleri belirli teknolojilerin elektronik imza oluşturmak uğruna kullanılmasıyla meydana gelmektedir[15]. Örneğin, bilgisayar ekranına özel bir kalem aracılığıyla atılan imza veya kağıda dayalı ortamda bulunan el yazısıyla imzanın tarayıcı vasıtasıyla bilgisayara aktarılması ya da bilgisayar ekranındaki "Onaylıyorum" yazısının üzerinde tıklanması birer elektronik imza niteliği taşımaktadır[16]. Yine, elektronik ortamdaki bir satım işlemini gerçekleştirmek amacıyla bir kredi kartının numarasının ve güvenlik kodunun sisteme girilmesi de bir elektronik imza niteliğindedir. Bunlar dışında elektronik postanın altına eklenen isim de elektronik imza sayılmaktadır[17].

1. Dijital (Sayısal) İmza

Dijital imza yetmişli yılların sonunda ortaya çıkmış bir kavramdır. Açık ağlar üzerinde elektronik ortamda kurulan iletişimde bir veri doğrulama yöntemi olarak kullanılmak üzere geliştirilmiştir[18]. Modern kriptografinin[19] bir sonucu olarak, açık anahtar alt yapısının (*public key infrastructure - PKI*)[20] kullanılması suretiyle

---

[15] Elektronik imza tekniklerinin çeşitliliği teknoloji ve hayal gücüyle sınırlıdır: Mehmet Ertan Yardım, **Elektronik İmza ve Elektronik İmzanın Medeni Usul Hukukumuza Etkileri**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s.6.

[16] Altınışık, **a.g.e**., s.81; Yardım, **a.g.e**., s.8.

[17] ABD hukukunda elektronik postanın altına isim yazılması elektronik imza olarak kabul edilmektedir. Aynı yönde 1997 yılında İngiltere verilmiş bir mahkeme kararı bulunmaktadır. Bkz. Thomas J. Smedinghoff / Ruth Hill Bro**, Electronic Signature Legislation,** (Çevrimiçi) http://library.findlaw.com/1999/Jan/1/241481.html, 12.03.2010.

[18] Jay Forder, "The inadequate legislative response to e-signatures", **CLSR**, Vol.26, 2010, s.418-426, s.418.

[19] Kriptografi gizli yazışma anlamına gelmektedir. Üçüncü kişiler tarafından okunduğunda anlaşılmayacak şekilde yazma tekniğidir. Okunabilir formdaki bir metnin, okunamayacak bir forma ya da bir şifre mesajına dönüştürülmesi kriptografi aracılığıyla yapılmaktadır. Kriptografinin tarihi kökenin binlerce yıl öncesine kadar gitmektedir. Detaylı bilgi için bkz. Brazell, **a.g.e**., s.50.

[20] Açık anahtar yapısı ve gizli anahtar yapısı hakkında detaylı bilgi için bkz. Brazell, **a.g.e**., 51.

elektronik verilerin şifrelenmesi esasına dayanır[21]. Açık anahtar alt yapısı esas itibariyle elektronik verinin kaynağını doğrulamakta ve içeriksel bütünlüğünün sağlanmış olduğunu garanti altına almaktadır. Dijital imza tekniğinin kullanım alanı yerine getirdiği bu işlevler sayesinde çok geniştir. Elektronik imza oluşturmak amacıyla kullanılabileceği gibi bunun yanı sıra, web siteleri, bilgisayar yazılım programları, sunucular ve dijital yolla dağıtılan veya depolanan diğer verilerin kaynağını doğrulamak amacıyla da kullanılmaktadır[22].

Dijital imza elektronik olarak yaratılan belgelerin şifrelenmesi yoluyla oluşturulmaktadır. Bu şifrelemenin gerçekleşebilmesi için, aralarında matematiksel bir bağlantı bulunan ve işlevsel olarak birlik arz eden biri gizli anahtar[23], diğeri herkesçe bilinebilir ve ulaşılabilir nitelikteki açık anahtar olmak üzere iki anahtara ihtiyaç bulunmaktadır.

Dijital imzanın oluşturulmasında iki aşamalı bir prosedür söz konusudur. Karşı tarafa gönderilecek olan metin oluşturulduktan sonra, ilk olarak metnin tamamına şifreleme programı kullanılarak "*hash*" algoritması[24] tatbik edilmektedir[25]. Bunun sonucunda elektronik ortamda oluşturulan metin, harf ve rakamlardan oluşan bir mesaj özetine, teknik adıyla *hash*[26] değerine dönüşmektedir. Oluşan *hash* değeri metnin karakteristik özelliklerinin tümünü (işaretlerin türü, sırası ve sayısı) içermekte

---

21 Şenocak, **a.g.e.**, s.99; Erturgut, **a.g.e**., s.67.

22 Babette Aalberts / Simone van der Hof, **Digital Signature Blindness: Analysis of legislative approaches toward electronic authentication**, (Çevrimiçi) http://cwis.kub.nl/~frw/people/hof/ds-fr.htm, s.8, 03.11.2009.

23 Gizli anahtar (0) ve (1) sayılarından meydana gelen bitlerden oluşmaktadır. Dijital imzanın güvenliği gizli anahtarın uzunluğuna bağlıdır: Brazell, **a.g.e**., s.54, Altınışık, **a.g.e**., s.81.

24 Algoritma, bir bilgisayara, bir program içinde verilen komutların kombine edilme metodudur. Örnek vermek gerekirse 10'luk sayıların ikili sistemde (0 ve 1'ler ile) yazılışının matematiksel aşamaları bir algoritmadır. Bazı yazarlar algoritmayı bir problemin çözümünün mantıksal adımları olarak nitelendirmektedir. Daha fazla bilgi için bkz. Arıkan, **a.g.e.**, s.329.

25 *Hash* algoritmasının işlevi şöyle açıklanabilir: Birbirinden farklı iki metnin aynı *hash* değerine sahip olması, en yüksek seviyede hesaplama donanımı kullanılmasına rağmen imkansız olmalıdır. Bu özelliğin sağlanması bir elektronik imzanın güvenli sayılması için zorunludur. Bkz. Erturgut, **a.g.e**., s.78. Bir *hash* değeri verildiğinde *hash* algoritmasının uygulanması suretiyle mesajın orjinaline ulaşmak mümkün olmamalıdır. bkz. Erturgut, **a.g.e**., s.75; Brazell, **a.g.e**., s.52.

26 Konu ile ilgili yazılan Türkçe eserlerde *hash* değerine karşılık gelmek üzere, öz değeri, özet değeri, mesaj özeti, parmak izi ifadeleri de kullanılmaktadır. Türkçe çevirilerinde bir terim birliği sağlanmamış olduğundan, ayrıca kullanılan terimlerin anlam bakımından karışıklık yaratabileceği sakıncasıyla, *hash* ifadesini aynen kullanmayı tercih ediyoruz.

olduğundan metnin herhangi bir şekilde değiştirilmesi halinde farklılaşacak, metne özgü bir değer niteliği taşımaktadır. Böylelikle, *hash* değeri, veri bütünlüğünün korunduğunun yani metnin imzalandıktan sonra değiştirilip değiştirilmediğinin tespitini sağlayacaktır[27].

Hash değeri saptandıktan sonra, imzalayan bu değer üzerinden, yalnızca kendine ait olan gizli anahtarını kullanarak, dijital imzasını oluşturur. Burada gizli anahtarın kullanılması yoluyla şifrelenen, *hash* değeridir. Birkaç satırlık metin özeti niteliğindeki *hash* değeri yerine uzun içerikli metinlerin şifrelenmesi ve deşifre edilmesi uzun vadelere yayılan ve masraflı bir süreci gerektirmekte ve en önemlisi bu süreç gönderen ve muhatap dışındaki kişilerin müdahalelerine açık olmaktadır. *Hash* değeri kullanımı bu rizikoyu ortadan kaldırmakta, metinde taraflar dışındaki kişilerce değişiklik yapılmasını engellemekte ve ayrıca dijital imzanın uygulanması işlemini birkaç dakikalık basit bir işlem haline getirmektedir[28]. *Hash* değerinin şifrelenmesi sonucu dijital imza meydana gelmektedir[29].

Gönderen dijital imzayı metinle birlikte alıcıya gönderir. Alıcı, gönderenin açık anahtarını kendisine ulaşan şifrelenmiş metni deşifre etmekte kullanır ve *hash* değerine ulaşır. Dijital imzayı doğrulamak amacıyla, kendisine gönderilen düz metin üzerinden *hash* değerini aynı usule uyarak tekrar hesaplar. Bu iki hash değerinin karşılaştırılmasıyla ortaya şu sonuçlar çıkmaktadır: İlk olarak, dijital imzanın gönderenin gizli anahtarı kullanılarak oluşturulmuş olduğu anlaşılmaktadır. Açık ve gizli anahtarın birbiriyle işlevsel birlik taşıması sayesinde bu tespit edilebilmektedir. İkinci sonuç ise mesajın değiştirilmemiş olduğudur ve bu mesajın doğruluğu onaylanmıştır. Çünkü metinde herhangi bir değişiklik yapılmış olsa, bu *hash* değerinin farklı çıkmasına yol açacak ve yapılan karşılaştırma sonunda metne müdahale edilmiş olduğu anlaşılacaktır[30].

---

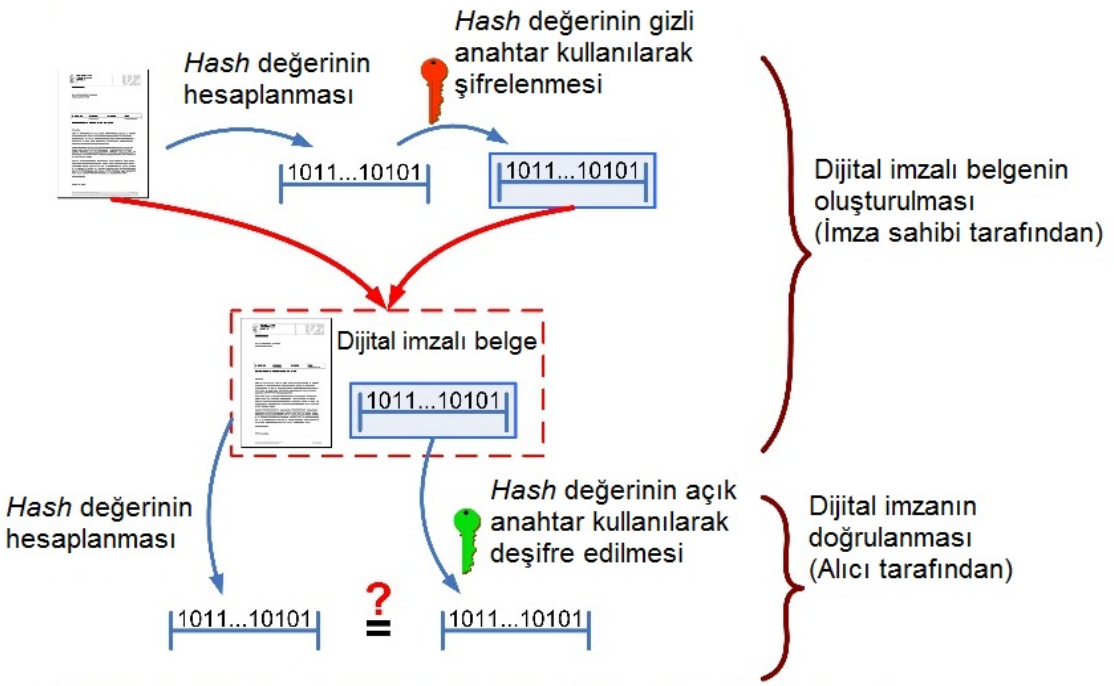
[27] Erturgut, **a.g.e.**, s.69, dn.168.

[28] Sağlam, **a.g.e.**, s.162; Altınışık, **a.g.e**., s.83; İbrahim Kırçova / Pınar Öztürk, **İnternette Ticaret ve Hukuksal Sorunlar,** İstanbul, İstanbul Ticaret Odası Yayını, 2000. s.70.

[29] Altınışık, **a.g.**e., s.84.

[30] Bunlara ek olarak, mesajın gizliliğin de temin edilmesi mümkündür. Bunun çapraz şifreleme yöntemi kullanılmaktadır. Şöyle ki, (A) mesajı önce (B)'nin açık anahtarıyla şifreler, daha sonra kendi gizli anahtarını kullanarak ikinci defa şifreler. (B) mesajı aldığında önce (A)'nın açık

Aşağıda dijital imza tekniğine bir örnek verilmektedir[31]:



Şekilde de görüldüğü gibi, dijital imza gizli anahtarla oluşturulmakta ve bu anahtara karşılık gelen açık anahtarla doğrulanabilmektedir. Açık anahtar gizli anahtarın kullanılıp kullanılmadığını tespite yaramaktadır[32]. Bu sayede dijital imzalı belgenin alıcısına dijital imzanın gizli anahtarın sahibi tarafından oluşturulduğuna dair güven sağlamaktadır. Ancak sertifikaya dayalı olmadıkça bu haliyle dijital imza uygulaması tek başına kimlik tespitini gerçekleştirmeye yaramamaktadır[33]. İmzalayan kişinin kimliğinin tespit edilebilmesi için bir sertifikaya ve bu sertifikayı düzenleyen bir *güvenilir üçüncü kişiye* ihtiyaç vardır. Sertifika imza anahtarı ile imza sahibi ve imza edilen mesaj arasında bağlantı kurulmasını sağlar[34]. Güvenilir üçüncü kişi uygulamada sertifika sağlayıcı olarak ortaya çıkmaktadır. Sertifika sağlayıcıları

---

anahtarını kullarak ilk şifreyi deşifre edecek, daha sonra kendi gizli anahtarını kullarak deşifre etmek yoluyla orijinal metne ulaşacaktır: Altınışık, **a.g.e**., s.83. Bu bakımdan elektronik imza, el yazısıyla imzaya ek yeni bir işlev sunmakta, eski dönemlerde kullanılan mühüre daha çok yaklaşmaktadır.

31 Örnekteki şema "Wikimedia Commons" adlı sayfadan alınarak Türkçe'ye çevrilmiştir. (Çevrimiçi) http://commons.wikimedia.org/wiki/File:Digital_signature _schema.gif, 29 Ocak 2011.

32 Sağlam, **a.g.e**., s.159.

33 Erturgut, **a.g.e**., s.83.

34 Erturgut, **a.g.e**., s.84; Şenocak, **a.g.e.**, s.99.

imza anahtarı çiftini üreterek imza sahibine teslim etmekte, gizli anahtara karşılık gelen açık anahtarın[35] imza sahibi kişiye özgülendiğini onaylamaktadır[36].

Uygulamada sözü edilen dijital imzaların yalnızca bir bölümü sertifikaya dayanmaktadır. Teknik olarak, dijital imzanın her zaman bir sertifikaya dayalı olması mecburiyeti bulunmamaktadır.

Yukarıda belirtilen açıklamalar dikkate alınarak, dijital imzanın oluşturulması ve doğrulanmasının uzun süreli ve zahmetli işlemler olduğu düşünülebilir. Ancak, uygulamada bu işlemler bilgisayar tarafından ve tek bir tuşa basılması suretiyle çok kısa sürede gerçekleştirilmektedir[37]. Hatta bu kadar basit olması nedeniyle dijital imzada yazılı şeklin uyarı işlevinin tam olarak gerçekleşmediği ifade edilmektedir[38]. Bununla birlikte İmzalayan dijital imzanın uygulanması prosedürünü gözle takip edememekte, ancak özel bir program aracılığıyla dijital imzanın içeriğini temsili biçimde görebilmektedir[39].

Dijital imza yoluyla imzalanmış elektronik belge, metinden ve imzadan oluşmaktadır. Bu açıdan daha çok eski dönemlerde kullanılan mühüre benzediği ifade edilmektedir[40].

---

[35] Bir kimsenin dijital imzasının geçerliliği, bu kişinin açık şifresinin bir onay makamı tarafından dijital bir imza ile tasdik edilmesiyle olur (Keser Berber, **a.g.e.**, s.154; Leyla Keser Berber, "Şekil ve Dijital İmza", **Elektronikteki Gelişmeler ve Hukuk Sempozyumu,** Ankara, 2001, s.73).

[36] Erturgut, **a.g.e**., s.83. Sertifika sağlayıcıları elektronik imzanın yaratımı ve kullanımı için gereken altyapıyı oluşturmaktadır: Kilian, **a.g.e.**, s.155. Dijital imzanın kimlik tespiti işlevinin el yazısıyla imza ile karşılaştırması için bkz. s.18.

[37] Kırçova / Öztürk, **a.g.e**., s.70; Turgay Sarıakçalı, **İnternet Üzerinden Akdedilen Sözleşmeler**, Ankara, Seçkin, 2008, s.71.

[38] Şenocak, **a.g.e**., s.127. Dijital imzanın uyarı işlevinin el yazısıyla imza ile karşılaştırması için bkz. s.24 vd.

[39] Şenocak, **a.g.e**., s.99.

[40] Kilian, **a.g.e.**, s.155; Michael Bromby, "Identification, trust and privacy: How biometrics can aid certification of digital signatures", **International Review of Law, Computers & Technology**, Vol.24, Issue 1, March 2010, s.133-141, s.140; Altınışık, **a.g.e**., s.79-80; Leyla Keser Berber, "İmzalıyorum, O Halde Varım! Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri", **TBBD**, S.2, 2000, s. 503-556; Kırçova / Öztürk, **a.g.e**., s.70; ayrıca bkz. yukarıda dn.30.

2. Biyometrik İmza

Biyometrik özellikler belirli bir kişiye özgü olup diğer bir kişiyle aynı olmayan, parmak izi, ses, retina, imza ve yazı dinamikleri gibi fiziksel ve tipik davranış özelliklerini ifade eder[41]. Biyometrik özellikler statik ve dinamik olmak üzere ikiye ayrılır[42]. Statik özellikler, kişinin parmak izi, avuç çizgileri örneği, yüz şekli, kulak kepçesi, iris örneği, vücut sıcaklığı ve koku gibi özellikleridir. Dinamik özellikler ise ses, konuşurken yapılan dudak hareketleri, imza dinamikleri, bilgisayarın klavyesine vuruş davranışları ve ritimleri olabilir[43]. Biyometrik özellikleri ifade eden veriler Kişisel Verilerin Korunmasına ilişkin AB Yönergesi'ne[44] göre kişisel veri olarak kabul edilmektedir[45]. Türk hukukunda 06.02.2004 tarihli ve 25365 sayılı Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'in[46] 3. maddesine göre bir gerçek kişiyi tanımlamaya yarayan fiziksel veriler kişisel bilgi/veri niteliğindedir[47].

Biyometrik özelliklerin kişiye özgü olması sebebiyle, biyometrik yöntemler kimlik tespiti ve kimlik doğrulama amacıyla kullanılmaktadır[48]. Kimlik tespitinde

---

41 Erturgut, **a.g.e.**, s.63.

42 Erturgut**, a.g.e.**, s.63; Vücut özellikleri ve davranış özelliklerine dayanan tanıma yöntemleri olarak da ikiye ayrılmaktadır: Brazell, **a.g.e**., s.39; Leyla Keser Berber / Murat Lostar, **Bilişimde Biyometrik Yöntemler**, Ankara, Yetkin Yayınları, 2006, s.33.

43 Gwen Kennedy, "Thumbs Up for Biometric Authentication", **Computer L. Rev. & Tech.**, Vol.VIII, 2004, s.379-407, s.383-388; Erturgut, **a.g.e**., s.63.

44 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050.*

45 Biometrik verilerin hukuki niteliği hakkındaki değerlendirmeler için bkz. Yue Liu, "Identifying Legal Concerns in the Biometric Context", **JILT,** Vol.3, Issue 1, 2008, s.45-54, s.45

46 RG. 06.02.2004, sayı 25365.

47 Türk hukukunda Kişisel Verilerin Korunması Kanunu Tasarısı'nın "Tanımlar" başlıklı 3. maddesinin (ç) fıkrasına göre kişisel veri deyimi belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgileri ifade etmektedir. Tasarıda veri konusu kişi kavramına konuya ilişkin Avrupa Birliği Yönergesi esas alınarak tüzel kişiler de dahil edilmiştir. Kişisel Verilerin Korunması Kanunu Tasarısı'nın metni için bkz. (Çevrimiçi) http://www2.tbmm.gov.tr/d23/1/1-0576.pdf, 29 Ocak 2011.

48 Biyometrik sistemlerinin uygulama alanları hakkında detaylı bilgi için bkz. Keser Berber / Lostar, **a.g.e**., s.36 vd.

sistemde kayıtlı bütün referans verilerinin aktüel veriyle karşılaştırması yapılırken, kimlik doğrulamada aktüel veri ile sadece daha önceden kayıtlı referans verisi karşılaştırılarak kullanıcının daha önce kaydedilen kullanıcı olup olmadığı belirlenmektedir. Biyometrik özelliklerin karşılaştırılması için, referans örneğinin, öncelikle elektronik veriye dönüştürülmesi gerekmektedir[49].

Biyometrik yöntemlerin imzada kimlik doğrulamayı sağlama amacıyla kullanılması yeni değildir. El yazısıyla imza[50] ve parmak izi uygulamaları da kimlik doğrulama işlevini esas itibariyle biyometriye dayalı olarak sağlamaktadır[51]. Elektronik imzaya ilişkin hukuki düzenlemeler biyometrik yöntemlerin kimlik doğrulamayı sağlama amacıyla kullanılmasını kabul etmektedir. Bunun şartı biyometrik yöntemlerin yeterli güvenliği sağlaması ve dışarıdan gelen saldırılara karşı dayanıklı olmasıdır[52]. Ancak, kimlik doğrulama işlevi görmesine rağmen biyometrik yöntemler tek başına elektronik bir verinin bütünlüğünü sağlamaya yeterli olmamaktadır[53].

Elektronik imza alanında, biyometrik yöntemler daha çok dijital imza teknolojisine ek olarak, giriş kontrollerinde gizli anahtara erişimi sağlamak için PIN kodu yerine veya PIN kodu ile birlikte kullanılmaktadır. Bu şekilde, elektronik imzanın gizli anahtarın yetkili sahibinin bizzat kendisi tarafından uygulanmış olduğu daha güvenli olarak tespit edilebilmektedir[54]. Fakat, bu durumda dahi, sistemde kayıtlı referans verileri dijital formda bulunduğundan, verilerin tahrif edilmesi,

---

49 Erturgut, **a.g.e**., s.64.

50 İmza dinamikleri elektronik imza için geçerli bir teknoloji olarak kabul edilebilir. Bu sistemde, elle yazısıyla imzanın (sadece imzanın şekli değil, aynı zamanda atılma hızı, vurgu, kalemin açısı ve kişinin imzasını atma biçiminin diğer özellikleri) sayısal kaydı oluşturulur ve bu kayıt elektronik bir belgeyi mühürlemekte kullanılabilir (Scoville, **a.g.e**., s.345- 355).

51 Kennedy, **a.g.e.**, s.382.

52 Olaf Henniger / Björn Schneider / Bruno Struif / Ulrich Waldmann, "Improving the Binding of Electronic Signatures to the Signer by Biometric Authentication", **Advances in Biometrics**, ed. David Zhang, Anil K. Jain, Heidelberg, Springer, 2006, s.523-530, s.523.

53 Yardım, **a.g.e**., s.8.

54 Bu noktada, giriş kontrolünde biyometrik usullerin kullanılması, imza usulünü kullanan kişinin imza sahibi olup olmadığını tespit etmek bakımından daha geniş bir garanti sağlamakta, elektronik imzayı daha güvenli hale getirmektedir: Martin Bergfelder, **Der Beweis im elektronischen Rechtsverkehr,** Hamburg, Verlag Dr. Kovač, s.250; Sebastian Jungermann, **Der Beweiswert elektronischer Signaturen,** Frankfurt am Main, Peter Lang, 2002, s.35 vd.; Erturgut, **a.g.e**., s.111; Keser Berber, **a.g.e**., s.196.

kopyalanması ve yetkisiz kişilerce kaydedilmesi tehlikelerinin mevcut olduğu ifade edilmektedir[55].

Kimlik doğrulamada kayıtlı biyometrik verilerden yararlanılması her zaman mümkün olmayabilir. Örneğin, parmak izine dayalı kimlik doğrulama yönteminde, parmağın yaralanması halinde, parmak izi verisi önceden dijital formda kaydedilmiş parmak izi verisine denk gelecek şekilde oluşturulamayacak ve kimlik doğrulama gerçekleştirilemeyecektir[56]. Bu yüzden giriş kontrollerinde kullanılan biyometriye dayalı yöntemlerin, ayrıca PIN kodu gibi bilgiye dayalı yöntemlerle desteklenmesi gerektiği ifade edilmektedir[57].

Sonuç olarak biyometrik yöntemlere dayalı dijital imza teknolojisinin, erişim şifresinin akılda tutulması, kimseyle paylaşılmaması, saklanması gibi gereklilikleri ortadan kaldırması sebebiyle daha güvenli olduğu genel olarak kabul edilmekle birlikte[58], PIN kodu yöntemine göre biyometrik imzanın daha üst seviyede güvenlik sağlamadığı görüşü de bulunmaktadır[59].

---

[55] Erturgut, **a.g.e**., s.65, dn.144. Giriş güvenliğinde biyometrik yöntemlerin uygulanmasında kullanılan araçlar güvenlik açısından farklı seviyelerde sınıflandırılmaktadır. Retina tanıma ve DNA tanıma yöntemleri yüksek seviyede güvenlik sağlarken, imza dinamikleri gibi yöntemler daha düşük güvenliktedir: Aashish Srivastava, "Electronic signatures and security issues: An emprical study", **Computer Law & Security Review**, Vol.25, 2009, s. 432-446, s.439.

[56] Parmak izine dayalı dijital imzayı kullanan kişiler, parmağın yaralı olması sebebiyle elektronik imzayı kullanamadığını belirtmektedir. Diğer taraftan cihazın parmak izini algılaması çok vakit almaktadır: Srivastava, **a.g.e.**, s.439-440.

[57] Biyometrik yöntemler aracılığıyla elektronik imzanın bağlayıcılığının güçlendirilmesi için, dijital imzalı belgenin muhatabının dijital imzanın biyometriye dayalı olduğuna dair bilgilendirilmesi gerektiği belirtilmektedir: Henniger / Schneider / Struif / Waldmann, **a.g.e.**, s.523.

[58] Bromby, **a.g.e.**, s.137; Henniger/ Schneider/ Struif/ Waldmann, **a.g.e.**, s.523;

[59] Bu görüşe göre biyometrik verilerin kullanılması kişiyle olan bağlantısının daha güçlü olması nedeniyle ve kaybolması, unutulması, çalınması ihtimalleri bulunmadığından tercih edilmektedir. Bununla birlikte biyometrik verilerin de dijital ortamda yetkisiz kişilerce ele geçirilmesi, kopyalanması tehlikeleri mevcuttur. Bu sakıncaları itibariyle, biyometrik verilerinin kimlik doğrulama amacıyla kullanılması, elektronik imzanın güvenliğininin yanı sıra, kişisel verilerin korunması bakımından da hukuken önem taşınmaktadır. Detaylı inceleme için bkz. Liu, **a.g.e.**, s.52.

II. ELEKTRONİK İMZANIN DÜZENLENMESİNDE ESAS ALINAN TEMEL İLKELER

Karşılaştırmalı hukukta ve Türk hukukunda elektronik imzaya ilişkin getirilen düzenlemelerde işlevsel denklik ilkesi (*functional equality principle*) ve teknolojiden bağımsızlık ilkesi (*technology neutrality principle*) esas alınmaktadır. Bu bakımdan her iki ilke hakkında açıklamalara yer verilmesi yararlı olacaktır.

A. İŞLEVSEL DENKLİK İLKESİ

İşlevsel denklik ilkesi, genel olarak yazılı belge kullanımının amaç ve işlevlerinin analizi ve bunların elektronik ortamda kullanılan tekniklerle nasıl sağlanabileceğinin belirlenmesine yönelik olarak geliştirilmiş ve ilk defa olarak 1996 tarihli Elektronik Ticaret Hakkında UNCITRAL Model Kanunu'nda ortaya konulmuştur[60].

Elektronik imzaya ilişkin yasal düzenlemeler, işlevsel denklik ilkesi çerçevesinde, el yazısıyla imzanın işlevlerinin, elektronik imza ile yerine getirilmesini sağlamayı amaçlamaktadır. İşlevsel denklik ilkesi, öncelikle el yazısıyla imzanın işlevlerinin tanımlanması, sonrasında da elektronik imzanın bu işlevleri gerçekleştireceği şartların belirlenmesi esasına dayanmaktadır[61].

El yazısıyla imzanın işlevleri tanımlanırken, belirli bir hukuk sistemindeki imza kavramının esas alınması önem taşır. Zira karşılaştırmalı hukukta birçok hukuki düzenlemede el yazısıyla imza bakımından yer alan farklılıklar elektronik imza

---

[60] İşlevsel denklik yaklaşımı için bkz. *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis adopted in 1998*, par.15-18. Benzer bir yaklaşım içeren, teknolojiden bağımsızlık ilkesi doğrultusunda çevrimiçi ve çevrimdışı ortamı düzenleyen temel kuralların denkliği prensibi hakkında bkz. Chris Reed, "Taking Sides on Technology Neutrality", **SCRIPT-ed**, Vol.4, Issue 3, 2007, s.264-284, s.266-267.

[61] Hatice Özdemir Kocasakal, **Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti**, İstanbul, Vedat Kitapçılık, 2003, s.94. Bu sayede, elektronik imzanın hangi şartlar altında el yazısıyla imza ile eşdeğer güvenirlikte olduğu belirlenmiş olacaktır: Yaltı Soydan, **E-imza I**, s.133.

tanımlarının da farklılaşmasına sebep olmaktadır[62]. Bu bakımdan aşağıda el yazısıyla imzanın işlevleri belirlenirken Türk hukuku esas alınacaktır.

1. El Yazısıyla İmzanın İşlevleri

El yazısıyla imza, imzalayan kişiye özgü karakteristik özellikler taşıyan bir yazıdır[63]. El yazısıyla imzanın iki temel işlevi bulunmaktadır[64]:

a. *Kimlik tespiti işlevi*: El yazısıyla imzanın kişiye özgü bir nitelik taşıması sayesinde imzalayanın kimliğini belirlemek mümkündür.

b. *Sonuçlandırma işlevi*: El yazısıyla imza metni sonlandırmakta ve imzanın üstündeki metnin imza sahibinin iradesiyle ve eksiksiz kaleme alındığını göstermektedir[65]. Bu sebeple kural olarak metnin sonuna ve metin yazıldıktan sonra atılmaktadır[66]. Bu sayede el yazısıyla imza, metnin imza sahibi tarafından imzalandığı andaki kapsamı itibariyle kabul edildiğini ve değiştirilmediğini tespite yaramaktadır[67].

Hukuki işlemlerde genel olarak şeklin işlevlerinden biri hukuki işlemde bulunacak kişiyi düşünmeye sevketmesidir. Öğretide uyarı işlevi olarak ifade

---

62 Birsen Acır, **Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi**, SPK Yeterlilik Etüdü, Ankara, 2000, s.23.

63 Erturgut, **a.g.e**., s.100.

64 Öğretide el yazısıyla imzanın işlevleri belirlenirken, yukarıda belirttiğimiz işlevlerine ek olarak ayrıca el yazısıyla imzanın gerçeklik işlevi bulunduğu belirtilmektedir. Buna göre, gerçeklik işlevi, el yazısıyla imzanın beyanın gerçekten imza sahibinden kaynaklandığını temin etmesidir (Şenocak, **a.g.e.**, s.125; Erturgut**, a.g.e**., s.112). Gerçeklik işlevi imzanın sonuçlandırma ve kimlik tespiti işlevleri ile yakından ilgilidir. Gerçeklik işlevinin amacı imzanın beyanı açıklayan kişi tarafından atıldığını, yani imzanın imzalayandan sadır olduğunu ispatlamasıdır (Erturgut, **a.g.e**., s.112).

İmzanın kimlik tespiti ve sonuçlandırma işlevlerini, yalnızca bir yazılı belgeden ilk bakışta görüneni tespite yönelik olarak değil, maddi gerçekliğin araştırılmasında esas alınan, dolayısıyla ispata yönelik işlevlerini de kapsayacak şekilde daha geniş tanımladığımız için, gerçeklik işlevinin ayrı bir başlıkta incelenmesine gerek görmemekteyiz.

65 Şenocak, **a.g.e**., s.125.

66 M. Kemal Oğuzman / M. Turgut Öz, **Borçlar Hukuku Genel Hükümler**, 8. Bası, İstanbul, Vedat Kitapçılık, 2010, s.123; Selahattin Sulhi Tekinay / Sermet Akman / Haluk Burcuoğlu / Atilla Altop, **Borçlar Hukuku Genel Hükümler**, 7. Bası, İstanbul, Filiz Kitabevi, 1993, s.117; Kocayusufpaşaoğlu, **a.g.e**., s.280; Ali Naim İnan, **Borçlar Hukuku Genel Hükümler,** Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, Sevinç Matbaası,1979, s.138.

67 Kocayusufpaşaoğlu, **a.g.e.,** s.280.

edilen[68] bu işlevin elektronik imzalı belgeler bakımından ne ölçüde gerçekleştirildiğinin ayrı bir başlıkta incelenmesi gerekmektedir. Çünkü bu işlevin elektronik imzada tam olarak yerine getirildiği konusunda ortaya çıkan tereddütler, elektronik imzanın uygulama alanının şeklin uyarı işlevinin önem taşıdığı bazı hukuki işlemler bakımından sınırlandırılmasında rol oynamaktadır[69]. Bu nedenle aşağıda nitelikli sertifikaya dayanan dijital imzanın el yazısıyla imzanın kimlik tespiti ve sonuçlandırma işlevlerini ne ölçüde yerine getirdiği karşılaştırmalı olarak incelendikten sonra, üçüncü olarak uyarı işlevi üzerinde durulacaktır.

2. Dijital İmza ile El Yazısıyla İmzanın İşlevleri Açısından Karşılaştırılması

El yazısıyla imzanın işlevlerini büyük ölçüde yerine getiren elektronik imza tekniği günümüzde yalnızca nitelikli sertifikaya dayanan dijital imzadır[70]. Dijital imza tekniği, elektronik imza oluşturma amacıyla kullanıldığı takdirde, elektronik mesajın kim tarafından imza edildiğini göstermekte ve içeriksel bütünlüğünü temin etmektedir[71]. Böylece el yazısıyla imzadan beklenen işlevleri yerine getirmekte[72] ve bu itibarla da, el yazısıyla imzanın dijital ortamda yaratılmış *surrogatı* olarak tarif edilmektedir[73]. Günümüzde nitelikli sertifikaya dayanan dijital imzanın (ya da

---

[68] Kenan Tunçomağ, **Türk Borçlar Hukuku C.1: Genel Hükümler,** 6. Bası, İstanbul, Sermet Matbaası, 1976, s.216; Feyzi Necmettin Feyzioğlu, **Borçlar Hukuku C.I: Genel Hükümler,** 2. Bası, İstanbul, Fakülteler Matbaası, 1976, s.303; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.99; Oğuzman / Öz, **a.g.e.**, s.117.

[69] Türk hukukunda teminat sözleşmelerine ilişkin getirilen istisna hakkında bkz. s.25 ve s.125.

[70] Özdemir Kocasakal, **a.g.e**., s.99; Şenocak, **a.g.e**., s.125.

[71] Aalberts / van der Hof, **a.g.e.**, s.8; Erturgut, **a.g.e.**, s.67. Dijital imza, kimliği belirlenebilir bir kişinin, mevcut bir belgenin görüldüğünü ve imza edildiğini ispat edebilir şekilde garanti etme amacını taşımaktadır: Keser Berber, **a.g.e.**, s.137.

[72] Sağlam, **a.g.e**., s.156.

[73] *Surrogat* ikame unsur anlamına gelmekte olup, bir hukuk kuralının asıl unsur olarak kabul ettiği şeyin veya değerin yerini alan unsur (öğe) için kullanılır. Günümüzde dijital imzanın konvansiyonel anlamdaki imzanın *surrogatı* haline geldiği belirtilmektedir (Bülent Sözer, "Elektronik İmza Kanunu'na Göre Digital İmza", **Prof. Dr. Ergon A. Çetingil ve Prof. Dr. Rayegân Kender'e 50. Birlikte Çalışma Yılı Armağanı**, Ankara, Çizgi Basım, 2007, s.994-1030, s.997).

sayısal imzanın) diğer elektronik imza türlerine göre en yüksek seviyede güvenlik sağladığı genel olarak kabul edilmektedir[74].

Bu sebeple, bu bölümde yalnızca nitelikli sertifikaya dayanan dijital imza ile el yazısıyla imzanın sağladığı işlevler karşılaştırmalı olarak incelenecektir.

a. Kimlik Tespiti İşlevi

El yazısıyla imza sayesinde imzalayanın kimliği tespit edilir. El yazısıyla imza, yazı şeklinin karakteristik olması sebebiyle sahibini belirlenebilir kılmaktadır[75]. El yazısıyla imza taklit edilme ihtimaline karşın mutlak bir koruma sağlamasa da, imzanın karakteristik oluşu taklit edilmesini güçleştirmektedir. İtiraz durumunda imza karşılaştırması yapılabilir[76]. El yazısıyla imzanın üzerine yazıldığı şeyle olan cismani bağlılığı bu tür manipülasyonların tespit edilmesini mümkün kılmaktadır[77].

Elektronik imzada kimlik tespitinin güçlüğü en önemli sorundur[78]. Dijital imza elektronik verilerden meydana geldiğinden, gizli anahtarın gerçek hak sahibi tarafından kullanılmış olup olmadığı, doğrudan doğruya imza tetkik edilerek anlaşılamamaktadır[79]. Diğer bir ifadeyle dijital imza ile imzalayan arasındaki bağlantı esas itibariyle, el yazısıyla imzadaki gibi biyometrik bir usule dayanmadığından[80] böyle bir inceleme söz konusu değildir. Bunun yerine kimlik

---

74 Scoville, **a.g.e.**., 361; Brazell, **a.g.e**., s.49; Wang**, a.g.e.**, s.254; Nuray Ekşi, "Elektronik İmzalara İlişkin UNCITRAL Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme", **Yasa Hukuk Dergisi**, S.3, 2001, s.333-340, s. 338. Dijital imzanın kör imza, tuzak imza, vekalet imza, inkar edilemez imza gibi kendi içinde başka çeşitleri de olduğu belirtilmektedir: Acır, **a.g.e**., s.30.

75 Şenocak, **a.g.e.**, s.125; Erturgut, **a.g.e**., s.109.

76 Erturgut, **a.g.e**., s.112.

77 Şenocak, **a.g.e**., s.124.

78 Minyan Wang, "A Review of Electronic Signatures Regulations: Do They Faciliate of Impede International Electronic Commerce?", **ICEC'06**, Fredericton Canada, ACM, s.548-552, s.548.

79 Hakan Karan, **Elektronik Konişmento**, Ankara, Turhan Kitabevi, 2004, s.143.

80 Bergfelder, **a.g.e**., s.250.

tespitinin gerçekleştirilmesinde matematiksel temele dayalı birtakım prosedürler kullanılmaktadır[81].

Dijital imzada, matematiksel olarak, gizli anahtar kullanılarak imzalanmış metne dayanılarak, yalnızca metnin gizli anahtarı elinde bulunduran kişi tarafından imzalandığı tespit edilebilebilmektedir[82]. Ancak kimin gizli anahtarı elinde bulundurduğu, yani imza sahibinin kimliği, tek başına dijital imzadan anlaşılamamaktadır[83].

Dijital imzanın kim tarafından uygulandığının tespiti iki şartın yerine getirilmesine bağlıdır: Birincisi, gizli anahtarın tek olması; ikincisi ise gizli anahtarın belirli bir kişiye özgülenmiş ve üçüncü kişiler tarafından kullanılmasının engellenmiş olmasıdır[84]. Gizli anahtar üzerinde sadece imza sahibi tasarruf edebiliyorsa, bu takdirde elektronik belgenin gizli anahtar sahibi tarafından oluşturulduğu sonucuna varılabilecektir[85]. Bu şekilde dijital imza ile imzalayanın kimliği arasında bağlantı kurulması için, bunu garanti eden ve üstlenen, bağımsız[86] ve güvenilir bir üçüncü kişiye, sertifika sağlayıcılarına ihtiyaç bulunmaktadır. Sertifika sağlayıcıları, imza sahibinin kimliğini güvenilir bir şekilde tespit ederek[87] bu kimlik bilgilerine dayalı olarak bir sertifika düzenlemekte ve bu sertifika aracılığıyla imza sahibi ve gizli anahtar arasında bağlantı kurmaktadır[88]. Dolayısıyla dijital imzada imzalayanın

---

81 Sofie Bianka Dörr, **Elektronische Signaturen und Haftung der Anbieter von Zertifizierungsdiensten**, Zürich, 2002, s.13.

82 Dörr, **a.g.e**., s.14; Erturgut, **a.g.e**., s.109.

83 Brazell, **a.g.e**., s.53; Erturgut, **a.g.e**., s.109; Altınışık, **a.g.e**., s.84.

84 Erturgut, **a.g.e**, s. 108-109.

85 Erturgut, **a.g.e**., s.69.

86 Bağımsızlık, sertifika sağlayıcının imza üretimi sırasında ilgililerden ve imza üretiminde kullanılan araçları üreten ve satanlardan bağımsız olmasını gerektirir. Bunun yanında, sertifika sağlayıcı devletin kurumlarına karşı da bağımsız olmalıdır. Bu sayede, özel hukuk ilişkileri hakkında devletin doğrudan bilgi sahibi olması ve bu ilişkilere etki etmesi engellenmiş olacaktır: Erturgut, **a.g.e**., s.109.

87 Sertifika sağlayıcı, imza anahtarı sahibinin kimliğini tespit ederken mevzuatta belirtilen usule uymak zorundadır. Örneğin Türk Elektronik İmza Kanunu m.10 (b)'ye göre sertifika sağlayıcı, nitelikli sertifika verdiği kişilerin kimliğini resmi belgelere göre (kimlik kartı, pasaport vb.) güvenilir bir biçimde tespit etmekle yükümlüdür.

88 Altınışık, **a.g.e.**, s.85; Sağlam, **a.g.e**., s.165; Erturgut, **a.g.e.**, s.82-83, s.109. Sertifikanın elektronik ortamda bir nüfus cüzdanı ile benzerlik gösterdiği söylenebilir: İnci Biçkin, "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler", **TBBD**, S.63, Mart-Nisan 2006, s.109-125, s.113.

kimliğinin belirlenmesi sertifika aracılığıyla mümkün olmaktadır[89]. Sertifika düzenlenmeden bir dijital imzanın herhangi bir kişiden sadır olduğunun belirlenebilmesi günümüz şartlarında neredeyse imkansızdır[90].

Bununla birlikte, bir sertifika sağlayıcı tarafından imza sahibinin kimliğinin güvenilir biçimde tespit edilmiş olması ve sertifikaya dayalı bir dijital imza kullanılmış olması dahi, gizli anahtarın gerçekten özgülendiği imza sahibi tarafından kullanılmış olup olmadığını mutlak surette belirlemeye yetmemektedir[91]. Dijital imzanın güvenliği anahtarın ne derece iyi korunduğuna bağlı tutulmaktadır[92]. Bu açıdan kimlik tespiti bakımından ortaya çıkan riskler ve bunları ortadan kaldırmak için geliştirilen çözüm önerileri şunlardır:

Öncelikle, imza sahibinin gizli anahtarını bilgisayarın sabit sürücüsüne saklaması halinde, gizli anahtarı ele geçiren bir kimse, imza sahibinin adına ve hesabına yetkisiz bir biçimde işlemlerde bulunabilir. Uygulamada, bu riski azaltmak için, sertifika sağlayıcı ürettiği gizli anahtarı ve kimlik bilgilerini bir akıllı karta yerleştirmekte ve imza sahibine bu şekilde teslim etmektedir[93]. Böylece gizli anahtar bir araç içinde taşınabilir bir hale geldiğinden, bilgisayarın sabit sürücüsüne göre daha güvenli bir ortamda saklanmış olmaktadır[94]. Ancak imza anahtarının saklanması için taşınır nitelikteki bu tür imza araçlarının kullanılması halinde, bu

---

89 Bergfelder, **a.g.e**., s.250; Erturgut, **a.g.e**., s.82.

90 İnal, **a.g.e**., s.139; Şenocak, **a.g.e**., s.126, Karan, **a.g.e**., s.143. Karşı görüşte: Keser Berber, **a.g.e**., s.136-138. Dijital imza bir bilginin bütünlüğü bozulmadan ve başka kişilere kapalı bir ortamda iletildiğini ve ileten tarafın kimliğini doğrulayan, diğer bir ifade ile gönderen kişinin kimliğini açıkça teyit edip iletilen bilgilerin güvenilirliği ve orijinalliğini ortaya koyan, harf, karakter veya sembollerden oluşmuş bir settir: Şebnem Akipek, **Özel Hukuk ve İnternet**, Ankara Üniversitesi'nde İNET-TR'99 Programı çerçevesinde düzenlenen "Internet ve Hukuk" konulu panelde sunulan Tebliğ, 19-21 Kasım 1999, (Çevrimiçi) http://inet-tr.org.tr/inetconf5/tammetin/hukuk.html, 12.02.2011.

91 Bu nedenle, elektronik imza kanunlarında imza sahiplerine, imza araçlarının korunmasına ilişkin ağırlaştırılmış özen yükümlülükleri getirilmektedir: Şenocak, **a.g.e**., s.1126. Türk hukukunda da imza sahibinin imza oluşturma verisini başkalarına kullandırmamakla ve bu konuda gerekli tedbirleri almakla yükümlü olduğu Elektronik İmza Yönetmeliği'nin 15. maddesinin (e) fıkrasında belirtilmektedir.

92 Sağlam, **a.g.e**., s.157.

93 Gizli anahtarın güvenli olarak saklanması, günümüzde gizli anahtarın akıllı kartta veya taşınabilir bellek çubuğunda kaydedilmesi yöntemiyle gerçekleştirilmektedir: Bromby, **a.g.e.**, s.136.

94 Bromby, **a.g.e.**, s.136.

araçların kaybolması veya çalınması tehlikeleri ortaya çıkmaktadır[95]. Gizli anahtara yetkisiz kişiler tarafından ulaşılamaması için, yani gizli anahtarın elinde bulunduran herkes tarafından kullanılmasının engellenmesine yönelik olarak, sıklıkla başvurulan tedbir imza araçlarına giriş kontrollerinin kurulmasıdır[96].

Giriş kontrollerinde genellikle iki yöntem kullanılmaktadır. Bunlardan ilki ve en yaygın olanı, gizli anahtara erişimin bir şifre ile sağlanmasıdır. Erişim şifresi bir kelime veya PIN şeklinde olabilir. Şifre kelime veya PIN (*Personal Identification Number*- Kişisel Kimlik Numarası) kullanıcı tarafından seçilebileceği gibi, sadece kullanıcının bilgisi dahilinde kalmak üzere sertifika sağlayıcı tarafından kullanıcıya bildirilebilir[97]. Ancak giriş kontrollerinde kullanılan erişim şifrelerinin başkaları tarafından öğrenilmesi halinde, bu şifrelerin klavye aracılığıyla herhangi bir kişi tarafından girilmesi mümkündür. PIN veya şifrenin giriş kontrolünde kullanılmasının el yazısıyla imzada olduğu gibi işlemi yapan kişiyle kişisel olarak bir bağlılığı yoktur. Dolayısıyla, giriş kontrolleri gizli anahtarının güvenliğini arttırmakla birlikte, yine de tam olarak gerçekleştirememektedir[98].

Giriş kontrollerinde kullanılan ikinci yöntem, imza anahtarına erişimde biyometrik usullerden yararlanılmasıdır. Giriş kontrolünde biyometrik usullerin kullanılmasının dijital imza tekniğini daha güvenli hale getireceği ifade edilmektedir[99].

---

[95] İmza araçlarının kaybolması veya çalınması halinde eğer kullanıcı bu durumu fark ederse, aynen kredi kartları uygulamasında olduğu gibi sertifika sağlayıcıya yapacağı bildirim ile sertifikanın iptalini talep edecektir: Apol·lónia Martínez Nadal / Josep Lluís Ferrer Gomila, "Liability of Certification Authorities: A Juridical Point of View", **Information Security, 4th International Conference: ISC 2001**, ed. George I. Davida, Yair Frankel, Berlin Heidelberg, Springer-Verlag, s.204-219, s.206.

[96] Erturgut, **a.g.e,** s.110; Bromby, **a.g.e.**, s.136.

[97] Aynı şekilde PIN ve şifrenin sertifika sağlayıcı tarafından da bilinmemesi gerekmektedir (Erturgut, **a.g.e**., s.110).

[98] Erturgut, **a.g.e**., s.111.

[99] Şenocak, **a.g.e**., s.126; Erturgut, **a.g.e**., s.111; Bromby, **a.g.e**., s.136; Srivastava, **a.g.e**., s.439; Kişiyle biyometrik bir veriye dayalı olarak bağlantı kurulmadığı takdirde dijital imza kimlik doğrulama işlevinin tam olarak gerçekleştirelemeyecektir: Bergfelder, **a.g.e**., s.249. Biyometrik usullerin tanımı ve dijital imza ile birlikte kullanılmının ne şekilde gerçekleştirildiği hakkında bkz. s.12.

Sonuç olarak, kimlik tespiti işlevi dijital imzanın en zayıf yönü olduğunu vurgulamak gerekir. Bunun nedeni her halükarda gizli anahtarın belli bir araçta kayıtlı olmasının ve saklanmasının gerekli oluşudur[100]. El yazısıyla imzanın imzalayanla olan kişisel bağlılığı elektronik imzada bulunmamaktadır[101]. Dijital imza imzalayanın şahsına değil, gizli anahtara bağlı olarak oluşturulmaktadır[102].

b. Sonuçlandırma İşlevi

Metnin, sahip olduğu içerikle imzalanıp imzalanmadığı meselesi imzanın sonuçlandırma işleviyle ilgilidir[103]. El yazısıyla imza, üstünde yazılı beyanın hukuken bağlayıcı olduğunu ve sonradan yapılan değişikliklerin ve eklemelerin imzalayan için bağlayıcı olmadığını ifade eder[104]. Dijital imzanın da, metnin tamamını kapsayacak şekilde oluşturulduğu, ayrıca metin üzerinde değişikliklerin yapılmasını engelleyerek metnin içeriksel bütünlüğünü temin ettiği, bu bakımdan el yazısıyla imzanın sonuçlandırma işlevini yerine getirdiği kabul edilmektedir[105].

Elektronik Ticaret Hakkında UNCITRAL Model Kanunu'nda el yazısıyla imzanın sonuçlandırma işleviyle yakından ilişkili olarak kağıda dayalı ortamdaki "orjinallik" kavramı üzerinde durulmaktadır. Model Kanun'un 8. maddesinde bu kavramın elektronik ortamda veri mesajları açısından karşılanabilir olduğu, bunun için veri mesajında yer alan bilginin oluşturulduğu tarihten itibaren bütünlüğünün korunduğu konusunda kesin olarak güvenilir bir garanti sağlaması gerektiği kabul edilmektedir.

---

[100] Bromby, **a.g.e.**, s.134.

[101] Erturgut, **a.g.e**., s. 111; Bromby, **a.g.e.**, s136.

[102] Brazell, **a.g.e**., s.53. İmza sahibi imza aracı üzerindeki hakimiyetini kaybetmediği müddetçe, dijital imzanın taklidini yapmak mümkün değildir: Biçkin, **Elektronik İmza**, s.114.

[103] Erturgut, **a.g.e.**, s.106.

[104] Turhan Esener, **Borçlar Hukuku C.1: Akitlerin Kuruluşu ve Geçerliliği,** Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1969, s.174; Tunçomağ, **a.g.e**., s.228; Feyzioğlu, **a.g.e**., s.320; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.117; Kocayusufpaşaoğlu, **a.g.e**., s.280-281; Şenocak, **a.g.e.,** s.125.

[105] Erturgut, **a.g.e.**, s.106; Şenocak, **a.g.e.,** s.125; Altınışık, **a.g.e.**, s.93; Kırçova / Öztürk, **a.g.e**., s.69.

Dijital imza tekniğinde, ilk olarak metin hazırlanmakta, daha sonra metne *hash* usulü uygulanarak metnin özeti niteliğindeki *hash* değeri yaratılmaktadır. Daha sonra imzalama prosedürü tamamen bu *hash* değeri üzerinden gerçekleşmekte, imzalanan metin ve dijital imza arasında mantıksal bir bağlantı kurulmaktadır[106]. Bu şekilde dijital imza metnin tamamını kapsayacak biçimde uygulanmış olmaktadır. Dijital imzalı metnin içeriğinde sonradan yapılan en küçük değişikliklerin, *hash* fonksiyonu sayesinde *hash* değerleri karşılaştırılarak, belirlenmesi mümkün olmaktadır[107]. Metnin içeriksel bütünlüğünün kontrolü için onun *hash* değerinin çıkarılması ve öncekiyle karşılaştırılması yeterlidir[108]. Bu sayede dijital imza açısından sonuçlandırma işlevi gerçekleştirilmiş olmaktadır[109].

Dijital imzanın sonuçlandırma işlevinin el yazıyla imzadan çok daha farklı bir anlamı bulunmaktadır. *Hash* fonksiyonu metnin maddi içeriğini ve anlamını ayırt edebilecek bir teknik içermemektedir. Elektronik ortamdaki metni yalnızca sayısal bir veri olarak algılamakta ve bu veriyi başka bir sayısal veri niteliğindeki *hash* değerine dönüştürmektedir. Örneğin, metinde, irade açıklaması bakımından bir farklılık yaratmayan, yalnızca bir satır boşluk bırakılması halinde dahi böyle bir değişiklik *hash* değerinin farklılaşmasına sebep olacaktır. Bu durumda da, gerçekte hukuken hiçbir değeri olmamasına rağmen, metnin tahrif edildiği ve imza sahibinin iradesini yansıtmadığı sonucu ortaya çıkacaktır. Dolayısıyla, yalnızca *hash*

---

[106] Erturgut, **a.g.e**., s.69. Bu bağ dolayısıyla dijital imzanın sonuçlandırma işlevinin, el yazısıyla imzadan daha kesin şekilde gerçekleştiği ileri sürülmektedir (Şenocak, **a.g.e.,** s.125). *Hash* fonksiyonu kullanılması sayesinde sonuçlandırma işlevi diğer elektronik imza türlerine göre en iyi şekilde sağlanmaktadır, bkz. Bergfelder, **a.g.e**., s.252. Dijital imza dışındaki elektronik imza yöntemlerinde ise metin ile imza arasındaki mantıki bağ bu kadar belirgin şekilde kurulamamaktadır (Sarıakçalı, **a.g.e.**, s.88). Dijital imza, metnin belgenin yazarı tarafından düzenlendiğini belirtmek kadar, başkası tarafından bozulmadığını da göstermek amacını güder ve dolayısıyla da metnin tamamı dijital imzaya dönüşmüş olur (Bülent Sözer, **Elektronik Sözleşmeler**, İstanbul, Beta, 2002, s.127).

[107] Erturgut, **a.g.e**., s.75; Acır, **a.g.e**., s.32.

[108] Karan, **a.g.e**., s.143.

[109] Dörr, **a.g.e**., s.14; Erturgut, **a.g.e.**, s.106. Elektronik imzanın tek başına bir metnin doğruluğunu ve bütünlüğünü teyit edebilmesi için, imzayı oluşturan verinin metne ayrılmaz bir biçimde iliştirilmiş olması gerekmektedir. Bkz. Karan, **a.g.e**., s.143.

değerlerinin karşılaştırılması, tamamen matematiksel bir uygulamaya dayalı olduğundan sonuçlandırma işlevi bakımından aldatıcı olabilecek bir yöntemdir[110].

Bunun yanı sıra, dijital imzalı belgelerin uzun yıllar saklanması gerekli olan hallerde (örneğin ticaret sicilinde), sonuçlandırma işlevinin belirli bir süre sonra zayıflaması tehlikesi ortaya çıkmaktadır. Çünkü dijital imza kullanılarak imzalanmış belgenin imzalanmasından birkaç yıl sonra, daha hızlı işlemciler ve gelişmiş şifre çözme teknikleriyle iz bırakılmaksızın değiştirilmesi daha kolay olabilecektir[111]. Buna engel olmak üzere, elektronik belgelerin arşivlenmesi ve uzun süre saklanması gerekli olan durumlarda, dijital imzalı belgenin formatının daha güncel bir formata dönüştürülmesi imkanı (teknik adıyla *migration* yöntemi) bulunmaktadır[112].

c. Uyarı İşlevi

Yazılı şeklin en önemli işlevlerinden birisi de hukuki işlemde bulunmak isteyen kişiyi düşünmeye sevketmesidir[113]. Klasik anlamıyla bir senedin imzalanması belirli bir çabayı gerektirmekte ve bu şekilde taraflar acele kararlar vermekten korunmuş olmaktadır[114].

Dijital imza bakımından uyarı işlevinin yerine getirilip getirilmediği konusunda iki farklı görüş bulunmaktadır. Bir görüşe göre, irade beyanlarını elektronik olarak ileten kişilerin büyük çoğunluğu bu beyanlara klasik anlamda yazılı beyanlara olduğu kadar önem vermediğinden, elektronik imza el yazısıyla imzanın sahip olduğu uyarı işlevini taşımamaktadır[115]. Genel olarak elektronik ortamda

---

[110] Lucien Pauliac, **The Hiddden Truth About Electronic Signatures**, çev. Nicholas Allen, (Çevrimiçi) http://www.megapreuve.org/cariboost_files/Hidden_20Truth_20About_20Electronic 20Signatures.pdf, 27 Eylül 2010, Erişim Tarihi:11.03.2011, s.3.

[111] Şenocak, **a.g.e.**, s.127. Yazar burada gerçeklik işlevinin zayıfladığını belirtmektedir.

[112] Bu şekilde, örneğin *Microsoft Word 97* programı ile oluşturulan bir belge Windows Word 2003 kullanılarak daha yeni bir formata dönüştürülebilir ve bu sayede zamana dayanıklılığı sağlanabilir. Ancak bu yöntemin uygulanmasının, dijital imzanın geçerliliğini yitirmesine sebep olduğu açıklanmakta, bunun önemli hak kayıplarına yol açabileceği tehlikesine dikkat çekilmektedir. Detaylı bilgi için bkz. Pauliac, **a.g.e**, s.4.

[113] Genel olarak Türk hukukunda şeklin işlevleri hakkında aşağıda bkz. s.103-104.

[114] Erturgut, **a.g.e**., s.115.

[115] Şenocak, **a.g.e.**, s.127.

yapılan işlemler, klavye veya fareye dokunularak verilen bir komutla basit bir şekilde yapılmaktadır. Hukuki işlemde bulunan kişinin, gerek imzaladığı metin ile gerekse hukuki işlemin karşı tarafı ile fiziksel bir temasın bulunmaması nedeniyle uyarı işlevi tam olarak gerçekleşememektedir. Bu görüşe paralel olarak, Türk Elektronik İmza Kanunu'nun 5. maddesinde teminat sözleşmelerinin elektronik imza yoluyla kurulamayacağı belirtilmiştir. Maddeye ilişkin gerekçede elektronik imzanın kullanımının kolaylığı nedeniyle doğması muhtemel zararların önüne geçilmesi amacı gözetilerek böyle bir düzenlemenin yapıldığı belirtilmektedir.

Diğer bir görüşe göre ise, nitelikli sertifikaya dayalı gelişmiş elektronik imzanın kullanılması artık basit bir işlem olmaktan uzaklaşarak daha karmaşık bir sürece dönüştüğü için uyarı işlevinin sağlanmaktadır[116]. İmza sahibinin dijital imzayı kullanmak için yaptığı hazırlıklar (sertifika sağlayıcıya başvurulması, sertifika sağlayıcı tarafından imza sahibinin yazılı olarak bilgilendirilmesi, anahtar çiftinin teslim alınması, imzalama prosedürü vb.) dikkate alınarak, imzanın hukuki sonuçlarının bilincinde olduğu kabul edilebilir. İmza usulü ne kadar karışıksa, uyarı fonksiyonu da o ölçüde mevcuttur[117]. Özellikle, gizli anahtarın akıllı kartta veya başka bir taşıyıcıda kayıtlı bulunması, bu kartın okuyucuya yerleştirilerek imzalama usulünün başlatılması, akıllı kartın kullanımının PIN veya biyometrik usulde bir korumayla güvenilir hale getirilmesi durumlarında uyarı fonksiyonunun yerine getirildiğini kabul etmek gerekir[118].

Elektronik imzanın uyarı işlevini el yazısıyla imzayla eşit şekilde gerçekleştirildiğinin kabul edilmesi ve hukuki düzenlemelerde belirli hukuki işlemler açısından öngörülen sınırlamaların kaldırılması, elektronik imzanın kullanımına ve hukuki sonuçlarına ilişkin olarak toplumda yeterli bilincin oluşturulmasına bağlıdır[119]. Bu açıdan bakılırsa, mutlak bir eşitliğin sağlanmasında elektronik imza kullanıcılarının geçen zaman içinde ortaya koydukları davranışların, edinilen

---

[116] Erturgut, **a.g.e**., s.116; Keser Berber, **Şekil ve Dijital İmza**, s.131; Altınışık, **a.g.e.**, s.93.
[117] Erturgut, **a.g.e**., s.115-116.
[118] Erturgut, **a.g.e**., s.115-116.
[119] Bergfelder, **a.g.e**., s.254; Şenocak, **a.g.e**., s.127.

alışkanlıkların ve tecrübelerin belirleyici olacağını kabul etmek gerekmektedir[120]. El yazısıyla imzanın hukuki sonuçları hakkında toplumda yerleşik bulunan anlayışa paralel bir anlayışın elektronik imza bakımından da geliştiğini kabul etmek şartıyla, belirli hukuki işlemlerin elektronik imza yoluyla gerçekleştirilemeyeceğine dair düzenlemelerin geçerli bir temele dayanmadığını ve kaldırılması gerektiğini ileri sürmek mümkün olabilecektir[121].

B. TEKNOLOJİDEN BAĞIMSIZLIK İLKESİ

Bilgi ve iletişim teknolojileri alanında getirilen yasal düzenlemelerde teknolojiden bağımsızlık ilkesi esas alınmakta, teknolojiyle ilişkili kavramlar ve kurallar bu ilke ışığında tanımlanmaktadır. Teknolojiden bağımsızlık ilkesinden hareketle, hukuk kurallarının belli bir teknoloji türüne münhasır düzenlemeler getirmemesi, bir teknoloji türünün diğerlerine üstün tutulmayarak farklı teknolojik gelişmeleri kapsayacak genel tanımlar ve kurallar konulması amaçlanmaktadır[122]. Böylelikle hukukun teknolojinin gerisinde kalmaması ve yeniliklerin kanun değişikliğine gerek olmaksızın uygulanabilmesi, diğer bir ifadeyle hukuki düzenlemelerin göreceli de olsa zaman yönünden kalıcılığı, devamlı uygulanabilirliği sağlanacaktır[123]. Bu yönüyle teknolojinin kendisi değil, teknoloji

---

[120] Şenocak, **a.g.e**., s.127.

[121] Bu yaklaşıma paralel olarak, AB Elektronik Ticaret Yönergesi'nin 9. maddesinin III. fıkrası uyarınca üye devletler, elektronik ortamda gerçekleştirilemeyeceği öngörülen hukuki işlemlerin hangi gerekçeyle halen daha kapsam dışında bırakıldığını her beş yıllık süre sonunda Komisyon'a hazırladıkları raporda bildirmekle yükümlü kılınmıştır. Benzer şekilde ABD'deki Eyaletlerarası veya Dış Ticarette Elektronik Kayıtların ve İmzaların Kullanılmasını Kolaylaştıracak Kanun Bölüm 103'de, elektronik imzanın şimdilik kullanılamayacağı alanlar belirlenmiş, ancak 103 (c) hükmünde ise Ticaret Bakanının üç yıllık süre içinde bu sınırlamanın tüketicilerin korunması için gerekli olmaya devam edip etmediğini kontrol edeceği düzenlenmiştir.

[122] Bert Jaap Koops, "Should ICT Reguation be Technology-Neutral", **IT&Law Series,** Vol.9, The Hague: T.M.C. Asser Press 2006, s.77-108, s.85-86; Reed, **a.g.e.**, s.269.

[123] Koops, **a.g.e.**, s.88; *Koops* teknolojiden bağımsızlık ilkesinin kanun koyucu tarafından gözetilmesi gereken dört esas amacını şu şekilde sıralamaktadır:

1. Kişilerin davranışları ve bu davranışların sonuçları bakımından belirli etkilerin gerçekleştirilmesi,
2. Özellikle çevrimiçi ve çevrimdışı ortam anlaşılmak üzere, farklı davranış şekilleri arasında fonksiyonel eşitliğin sağlanması,
3. Etkileri yönünden eşitlik arz eden teknolojiler arasında ayrım yapılmaması,

kullanımının hukuken yarattığı etki ve sonuçların düzenlenmesi gerektiği ifade edilmektedir[124].

Teknolojiden bağımsızlık ilkesi ile elektronik imza kavramı ve elektronik imza uygulamasını düzenleyen kurallar belli bir teknoloji türüne ilişkin ayrım yapılmaksızın genel olarak tanımlanmaktadır. Böylelikle mevcut ve gelişmekte olan teknolojilerinin tamamını kapsayan yasal bir düzenlemenin gerçekleştirilmesi amaçlanmaktadır.

Geçmişe bakıldığında, birçok ülkede elektronik imza kanunlarının oluşturulmasında ilk olarak dijital imzayı esas alan teknoloji odaklı (*technology-specific*) düzenlemeler getirildiği görülmektedir. Bu durum, dijital imza türünün, diğer elektronik imza türlerine nispetle daha güvenilir olduğunun kabul edilmesinin sonucudur[125]. *Dijital imza yaklaşımı (Digital signature approach)*[126] olarak adlandırılan bu yöntem, elektronik imzaya ilişkin dünyadaki ilk hukuki düzenleme olan, 1995 tarihli Utah Dijital İmza Kanunu'nda ve bunu takiben 1997 tarihli Alman Dijital İmza Kanunu'nda benimsenmiştir[127]. Utah Dijital İmza Kanunu ilk bakışta genel tanım ve kurallar içeren lafzı itibariyle teknolojiden bağımsız bir düzenleme olarak görülebilirse de, kuralları incelendiğinde dijital imzayı hukuken geçerli kılmak amacını taşıması yönünden teknoloji odaklı olduğu anlaşılmaktadır[128]. Kanun açık anahtar alt yapısına dayalı dijital imzayı hukuken el yazılı imza ile denk kılmış,

---

4. Hukukun iki anlamda zamana dayanırlığının sağlanması:
    a. Kanunların teknolojide meydana gelecek yeniliklere engel olmayacak esnek biçimde kaleme alınması,
    b. Kanunların teknolojik yenilikleri kapsayacak, çok sayıda değişikliğe gitmeye gerek olmayacak şekilde sürekliliğinin sağlanması.

[124] "Hukuki düzenleme sonuçları itibariyle teknolojiden bağımsız olmalıdır. Çevrimiçi ve çevrimdışı ortama ilişkin düzenlemeler, ceza hukuku ve medeni hukuk da dahil olmak üzere, mümkün olduğunca benzer olmalıdır. Ancak, bu ortamlar arasında eşitliği gerçekleştirmek adına farklı düzenlemelerin gerektiği durumlar söz konusu olabilecektir"; İngiliz hükümeti tarafından belirlenen bu yaklaşım için bkz. Koops, **a.g.e.**, s.78.

[125] Koops, **a.g.e.**, s.13. Bu sistemde elektronik imza sisteminde yer alan tarafların hakları ve yükümlülükleri oldukça detaylı bir şekilde düzenlenmektedir (Wang, **Electronic Commerce**, s.550).

[126] Dijital imza yaklaşımı ve bu yaklaşımın benimsendiği diğer ülkelerdeki düzenlemeler için bkz. Aalberts / van der Hof, **a.g.e.**, s.25.

[127] Koops, **a.g.e.,** s.13.

[128] Aalberts / van der Hof, **a.g.e.**, s.27

diğer elektronik imza türlerinin hukuken geçerliliğine ilişkin bir düzenleme getirmemiştir[129]. Alman Dijital İmza Kanunu'nda daha ileri gidilerek, açık anahtar altyapısına dayalı dijital imza tekniği güvenlik standardı olarak kabul edilmiş, böylelikle elektronik ticaretin gelişebilmesi için gereken güvenlik ortamının oluşturulması amaçlanmıştır[130]. Ancak bu Kanun, teknolojiden bağımsızlık ilkesini benimseyen 1999 tarihli AB Elektronik İmza Yönergesi'nin milli hukuka dönüştürülmesiyle, geçerliliğini yitirmiştir. ABD'de 2000 yılında yürürlüğe giren ve tüm eyaletlerde uygulanan, teknolojiden bağımsız nitelikteki Küresel ve Ulusal Ticarette Elektronik İmzalar Kanunu da (*Electronic Signatures in Global and National Commerce Act / E-Sign Act*) da Utah Dijital İmza Kanunu'nun yerine geçmiştir[131]. Karşılaştırmalı hukuktaki bu düzenlemeler dikkate alınarak teknoloji tarafsız bir yaklaşımla kaleme alınan 5070 sayılı Türk Elektronik İmza Kanunu da 23.01.2004 tarihli Resmi Gazete'de yayımlanarak, yayımından altı ay sonra yürürlüğe girmiştir.

Dijital imza yaklaşımı benimsenerek teknoloji odaklı bir düzenlemeye gidilmesinin avantajı, teknolojiden bağımsızlık ilkesinden hareketle yapılan birçok düzenlemeye göre hukuken daha kesin ve öngörülebilir bir durumun yaratılmasındadır[132]. Kavram ve kurallar belirli bir imza teknolojisini detaylı olarak düzenlemekte, hukuki boşluklar ve teknolojik gelişmelere bağlı olarak yorumlanacak soyut mahiyetteki kavram ve kurallar asgari düzeyde kalmaktadır. Oysa *fonksiyonalist/minimalist yaklaşım (functionalist/minimalist approach)*[133] olarak da

---

[129] Aalberts / van der Hof, **a.g.e.**., s.26-27; Scoville, **a.g.e.**, s.13-14.

[130] Dijital imza standardının yerine getirilmesi için gerekli koşullar İmza Yönetmeliği'nde (*Signaturverordnung*) ve Teknik Katalog'da (*Massnahmenkatalog*) belirlenmiştir. Teknik standardın yerleştirilmesinde hukuki bir araçtan, kanundan yararlanılması, Alman sisteminin şekle ilişkin katı kurallarının yansıması olarak değerlendirilmiştir. Bkz. Aalberts / van der Hof, **a.g.e.**., s.25-27.

[131] "Dijital imza" kavramının "elektronik imza" kavramı yerine kullanılması muhtemelen elektronik imza konusundaki ilk düzenlemelerden olan 1996 tarihli Utah ve 1997 tarihli Alman kanunlarının "Dijital İmza Kanunu" adıyla sadece dijital imzayı esas almış olmasından kaynaklanmaktadır. Ancak, dijital imza üst kavram olan elektronik imzanın sadece bir çeşidini oluşturmaktadır. Bkz. Şenocak, **a.g.e**., s.98; Altınışık, **a.g.e**., s.79; Sağlam, **a.g.e**., s.141-142.

[132] Koops, **a.g.e.,** s.13-14.

[133] Fonksiyonalist / minimalist yaklaşım ile ilgili detaylı bilgi için bkz. Aalberts / van der Hof, **a.g.e.**, s.35; Koops, **a.g.e.**, s.13-15. Bu yaklaşımın benimsendiği ülkelerde elektronik imzanın hukuken imza kavramı üzerinde meydana getirdiği değişiklikler hakkında bkz. Wang, **a.g.e.**, s.254.

ifade olunan teknolojiden bağımsızlık ilkesi ışığında hazırlanan düzenlemelerde (örneğin ABD Elektronik İmza Kanunu) soyut kavram ve kurallardan yola çıkılarak daha fazla yoruma açık alan bırakılmaktadır[134]. Ancak bu düzenlemelerin avantajı ise, daha uzun süre yürürlükte kalabilmeleri ve teknolojik ilerlemelerin önünü kapatmamalarıdır[135].

Teknoloji odaklı dijital imza yaklaşımını ve teknolojiden bağımsızlık ilkesini benimseyen fonksiyonalist yaklaşımı bir araya getiren *karma yaklaşım (mixed approach / two-prong approach)*[136], 13 Aralık 1999 tarihli Avrupa Birliği Elektronik İmza Yönergesi'nde benimsenmiştir[137]. Elektronik İmza Yönergesi, teknolojiden bağımsızlık ilkesinin kısmen de olsa benimsendiği ilk Avrupa Birliği düzenlemelerinden biridir. Yönerge, elektronik imzayı "başka bir elektronik veriye eklenen ve onunla mantıksal bağlantısı bulunan ve doğrulama aracı olarak hizmet veren elektronik veri" olarak tanımlanmakta ve elektronik imzanın hukuki geçerliliğini herhangi bir teknoloji türüne ilişkin ayrım yapmaksızın genel olarak kabul etmektedir. Diğer taraftan el yazısıyla imza ile aynı hüküm ve sonuçları doğuracak güçlü hukuki etkiye sahip "gelişmiş elektronik imza" kavramını yaratmakta, bu kavrama ilişkin yerine getirilmesi gereken ek kriterler belirlemektedir. İmzanın işlevleri göz önüne alınarak belirlenmiş bu kriterler şunlardır: (a) Elektronik imza, onu imzalayana bağlanabilmelidir; (b) imzalayanın kimliğinin tanımlanmasını mümkün kılmalıdır; (c) yalnızca imzalayanın kontrolünde tutabileceği araçların kullanılması suretiyle yaratılabilmelidir; (d) ilişkili olduğu

---

[134] Koops, **a.g.e.**, s.14. Bu yaklaşımın benimsendiği ülkelerde, esas itibariyle elektronik imzanın hukuki etki doğurmasına engel olunamayacağı düzenlenmektedir. Taraflar hangi elektronik imza teknolojisini kullanmak istediklerine yapacakları hukuki işlemin niteliğine bağlı olarak serbestçe karar verebilmektedir. Bu sistemde imza sahibinin, üçüncü kişinin ve sertifika sağlayıcının hak ve yükümlülükleri kanun yoluyla düzenlenmemektedir. ABD, Kanada, İngiltere, Avusturalya teknolojiden bağımsızlık ilkesinin en geniş şekilde benimsendiği ülkeler arasındadır (Wang, **Electronic Commerce**, s.549).

[135] Buna karşılık zaman kavramının göreceliği olduğu ve kanunların zamana dayanırlığının bilişim çağındaki hızlı değişim göz önüne alınarak yeniden anlaşılması, geçmişte olduğu gibi uzun yıllar yürürlükte kalacak hukuki düzenlemelerin teknolojinin devamlı ilerlediği böyle bir dönemde beklenemeyeceği, teknoloji-spesifik düzenlemelerdeki kesinliğin ve öngörülebilirliğin kalıcılığa üstün tutulması gerektiği görüşünde: Koops, **a.g.e.**, s.10.

[136] Karma yaklaşım hakkında detaylı bilgi için bkz. Aalberts / van der Hof, **a.g.e.**, s.29; Koops, **a.g.e.**, s.15

[137] Koops, **a.g.e.**, s.15; Forder, **a.g.e.**, s.422.

verilere, verilerde sonradan yapılan değişikliklerin anlaşılmasını sağlayacak şekilde bağlı[138] olmalıdır.

AB Elektronik İmza Yönergesi bu işlevlerin yerine getirilmesine odaklanırken, lafzı itibariyle belirli bir teknolojiye üstünlük tanımamaktadır. Bununla birlikte, Yönerge'nin Ek'leri incelendiğinde gelişmiş elektronik imza sayılabilmek için yerine getirilmesi gerekli objektif şartların aslında açık anahtar alt yapısına dayalı dijital imzayla yakından ilgili olduğu dikkati çekmektedir. Yönerge bir taraftan teknolojik gelişmelerden bağımsız, imzadan beklenen işlevleri esas alan, teknolojik yenilikleri de kapsayacak genel kurallar içermekte, diğer taraftan Ekler kısmında hukuki kesinliği sağlamak amacıyla, dijital imza teknolojisinin yaygın şekilde kullanıldığı gerçeğinden hareketle, dijital imzaya yönelik teknoloji odaklı kurallar getirmektedir[139].

Karma yaklaşım 2001 tarihli Elektronik İmzaya ilişkin UNCITRAL Model Kanun'da da benimsenmiştir[140]. Model Kanunun biyometrik gibi diğer imza teknolojilerini kullanımını destekleyecek biçimde elektronik imzayı genel çerçevede düzenlediği kabul edilebilirse de, özel olarak ele aldığı konular itibariyle açık anahtar alt yapısına dayalı olduğu, dijital imza teknolojisinin kullanımından doğan problemleri çözüme ulaştırdığı tespit edilmektedir[141].

Sonuç olarak, genel yaklaşım elektronik imza kanunlarının teknolojiden bağımsızlığı olmakla birlikte, yine de gerek Türk hukukunda gerekse karşılaştırmalı

---

[138] Özellikle bu şartın dijital imzayla büyük ölçüde ilişkili olduğu ifade edilmektedir: Aalberts / van der Hof, **a.g.e.**, s.33.

[139] Koops, **a.g.e.**, s.15. Bazı yazarlar bu düzenleme şekli itibariyle AB Elektronik İmza Yönergesi'nde benimsenen teknolojiden bağımsızlık prensibinin yanıltıcı olduğu ve görünüşte kaldığı düşüncesindedirler. Bu yazarlara göre, elektronik imza tanımı, imza yaratım ve doğrulama verileri açısından pratik olarak hiç önem arz etmeyen genel düzenleme tarzı, bunların teknolojiden bağımsızlığı anlamına gelmemelidir. Buna karşılık pratik olarak önem arz eden ve gerek şartları gerekse hukuki etkisi bakımından ayrı olarak düzenlenen gelişmiş elektronik imza ve nitelikli gelişmiş elektronik imza kavramları ve Yönerge'nin eklerinde belirtilen şartlar, isim olarak belirtilmese bile, açık anahtar altyapısına dayalı dijital imzayı tanımlamakta ve düzenlemektedir. Bu bakımdan yönergenin teknolojiden bağımsızlık ilkesine dayandığından bahsedilemez. AB Elektronik İmza Yönergesi'nde esas olarak dijital imza düzenlenmiştir ve gelecekte kullanıma girecek farklı teknolojilerin ayrıca düzenlenmesi gerekecektir: Dörr, **a.g.e**., s.55.

[140] Brazell, **a.g.e.**, s.77. Koops, **a.g.e.,** s.15

[141] Brazell, **a.g.e.**, s.77.

hukuktaki yasal düzenlemelerde teknolojiden bağımsızlık ilkesinin tam anlamıyla esas alınmış olduğu söylenemez. Bu durum, günümüzde dijital imza tekniğinin elektronik imza meydana getirmek amacıyla en yaygın şekilde kullanılan teknoloji türü olmasından kaynaklanmaktadır. Hukuki düzenlemelerde teknolojiden bağımsızlık ilkesi benimsenerek, el yazısıyla imzanın işlevlerine odaklanan ve buların elektronik ortamda sağlamayı hedef tutan, teknolojik gelişmelerden bağımsız kurallar getirilirken, diğer taraftan günümüzdeki hakim teknoloji uygulamasının dijital imza olduğu gerçeği kabul edilerek, dijital imzaya münhasır kurallara da yer verilmektedir. Bu nedenle teknolojiden bağımsızlık ilkesi ile teknoloji odaklı dijital imza yaklaşımını bir araya getiren karma bir yaklaşımın benimsendiğini ifade etmek daha isabetli olacaktır.

III. ELEKTRONİK İMZAYA İLİŞKİN KARŞILAŞTIRMALI HUKUKTAKİ TEMEL DÜZENLEMELER

A. AVRUPA BİRLİĞİ ELEKTRONİK TİCARET YÖNERGESİ

Avrupa Parlamentosu ve Avrupa Konseyi'nin 8 Haziran 2000 tarihli ve 2000/31/EC sayılı Elektronik Ticaret Yönergesi[142], üye devletlerin hukuk sistemlerinin elektronik ortamda sözleşmelerin imzalanmasına imkan verecek şekilde düzenlenmesini ve özellikle sözleşmelerin kurulmasına ilişkin hukuk kurallarının elektronik ortamda sözleşmelerin kurulmasına engel olmamasını ve bu sözleşmelerin sadece elektronik ortamda yapılmış olmaları gerekçe gösterilerek hukuki etkiden ve geçerlilikten yoksun bırakılmamasını öngörmektedir (m.9/1).

Yönerge m.9/2 hükmünde üye devletlerin belirli sözleşme kategorileri bakımından m.9/1'in düzenlemesine istisna getirebilecekleri belirtilmektedir. Bu maddede yer alan sözleşme kategorileri şunlardır:

---

[142] *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market Official Journal L 178 , 17/07/2000 P. 0001 – 0016.*

a) Kira sözleşmeleri hariç olmak üzere taşınmaz mallar üzerinde haklar doğuran ve bu hakları devreden sözleşmeler,

b) Kanunen mahkemelerin veya kamu makamlarının katılımı öngörülen sözleşmeler,

c) Ticari, iş veya mesleki amaçları dışında hareket eden kişiler tarafından verilen teminatlara ilişkin sözleşmeler ve bu kişilerin borç altına girdiği kefalet sözleşmeleri

d) Aile ve miras hukukuna ilişkin sözleşmeler.

Üye devletlerin ulusal hukuklarında yukarıda sayılan türdeki sözleşmelerin elektronik yolla kurulamayacağını kabul etmeleri mümkündür. Ancak hangi gerekçeyle 9/1 hükmünü sınırlandıran bu istisnaları uyguladıklarını veya uygulamaya devam ettiklerini her beş yıllık sürenin bitiminde Komisyon'a bir rapor sunarak açıklamaları gerekmektedir (m. 9/3).

B. AVRUPA BİRLİĞİ ELEKTRONİK İMZA YÖNERGESİ

1999/93/EC sayılı Avrupa Birliği Elektronik İmza Yönergesi[143] (Yönerge)[144] 13 Aralık 1999 tarihinde kabul edilmiş ve 19 Ocak 2000'de Topluluk Resmi Gazetesi'nde yayımlanmıştır[145]. Elektronik İmza Yönergesi ile birlikte EESSI[146]

---

[143] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L 013, 19.01.2000 P. 0012 – 0020.*

[144] Bu başlık altında, AB Elektronik İmza Yönergesi'nin çeşitli maddelerine sıklıkla atıf yapılacak olması nedeniyle, söz konusu düzenleme "Yönerge" olarak kısaltılmaktadır.

[145] Avrupa Komisyonu 8 Ekim 1997 tarihinde "Elektronik Haberleşmede Güvenin ve Güvenliğin Sağlanması: Dijital imza ve Şifreleme" başlıklı Tebliğ'i kabul etmiştir (*COM(97)503 "Ensuring Security and Trust in Electronic Communication. Towards a European Framework for Digital Signatures and Encryption"*. Tebliğ metnine ulaşmak için bkz. (Çevrimiçi) http://configura.gva.es/ sistemes/seguridad/norm-europa/97503toc.html, 30 Temmuz 2010). Bu Tebliğ'de bildirilen kararlardan birisi şudur: "Elektronik ticaretin teşvik edilmesi, Avrupa endüstrisinde rekabetin arttırılması, serbest dolaşımın önündeki engellerinin kaldırılması ve dijital imzanın milli sınırları aşan kullanımının sağlanması amacıyla, Topluluk çapında ortak bir çerçevenin benimsenmesi acil olarak gerekmektedir ve bu çerçeve en geç 2000 yılında yürürlüğe konulacaktır". Konsey'in 1 Aralık 1997 tarihli toplantısında Avrupa Komisyonu tarafından hazırlanan plan kabul edilmiştir. Konsey'in talebi üzerine Avrupa Komisyonu iki belge hazırlamıştır: 1) Elektronik İmzalar için Topluluk Çerçevesi'ne ilişkin Yönerge Önerisi ve 2) Avrupa standardizasyon kuruluşları tarafından elektronik imzayla ilgili standardizasyon gereklilikleri hakkında inceleme yapılmasına dair talimat. Bu konuda bkz. Jos Dumortier, "The European Regulatory Framework for Electronic

standardizasyon belgeleri elektronik imzanın Avrupa'daki düzenleyici çerçevesini oluşturmaktadır[147].

AB Elektronik İmza Yönergesi'nin 1. maddesine göre Yönerge'nin iki temel amacı bulunmaktadır: 1) Elektronik imzanın hukuki etkilerinin üye devletler tarafından tanınması, 2) elektronik imza kullanımının kolaylaştırılması. Bu amaçları gerçekleştirmek ve iç pazarın uygun şekilde işleyişini temin etmek üzere elektronik imzalar ve sertifika hizmetlerinin sunumu hakkında temel düzenlemeler getirilmektedir.

Yönerge'nin gerekçe kısmında, belirli sayıda kişiler arasında bir özel hukuk anlaşmasına dayalı olarak oluşturulan kapalı ağ sistemlerinde kullanılan elektronik imzalar açısından Yönerge'nin uygulanmayacağı belirtilmektedir[148]. Böylece Yönerge'nin uygulama alanı açık ağ olarak adlandırılan internet üzerinde meydana getirilen hukuki ilişkilerle sınırlandırılmış olmaktadır[149].

Aşağıda, Yönerge'nin belirlediği amaçların gerçekleştirilmesine yönelik olarak benimsenen yasal çerçeve ve bu yasal çerçevenin üye ülkelerin iç hukukun dönüştürülmesi sürecinde benimsenen ilkeler genel hatlarıyla incelenecektir.

Signatures: A Critical Evaluation", **EU Electronic Commerce Law**, edit. Ruth Nielsen, Søren Sandfeld Jacobsen, Jan Trzaskowski, Copenhagen, Djøf Publishing, 2004, s. 69-93; s.69. Ayrıca Yönerge'nin 1996 yılı itibariyle geliştirilen tasarıları hakkında değerlendirmeler için bkz. Brazell, **a.g.e**., s.87-90.

146 Yönergenin kabul edilmesi ile birlikte, Avrupa standardizasyon kuruluşları tarafından oluşturulan Avrupa Elektronik İmza Standandardizasyonu İnsiyatifi (*European Electronic Signature Standardization Initiative* – EESSI) çalışmalarına başlamıştır. EESSI elektronik imza hakkında birtakım teknik standartlar belirlemiş ve bu standartları, Avrupa Telekomünikasyon Standartları Enstitüsü Teknik Şartnameleri (*European Telecommunications Standards Institute – ETSI Technical Specifications*) ve Avrupa Standardizasyon Komitesi Çalıştay Kararları (*European Committee for Standardization - CEN Workshop Agreements*) şeklinde yayımlanmıştır. EESSI tarafından yürütülen çalışmalarda belirlenen standartların bir bölümü Avrupa Birliği'nin Resmi Gazetesi'nde 2003/511/EC sayılı Komisyon Kararı ile yayınlanmıştır. Oluşturulan teknik standartların tamamının yayımlanmasını takiben, Ekim 2004 tarihinde misyonunu yerine getirmiş olduğu gerekçesiyle EESSI kapatılmıştır. Elektronik imzaya ilişkin standardizasyon faaliyetleri halen daha Avrupa Birliği bünyesindeki standardizasyon kuruluşları tarafından daha dar kapsamlı olarak devam ettirilmektedir. Detaylı bilgi için bkz. (Çevirimiçi) http://www.ict.etsi.org/ Working_Groups/EESSI 31 Temmuz 2010.

147 Dumortier, **a.g.e**., s.70.

148 Bkz. Yönerge'nin 16. nolu gerekçesi.

149 Özdemir Kocasakal, **Elektronik İmza**, s.229.

1. Elektronik İmza ve Hukuki Etkilerinin Düzenlenmesi

a. Elektronik İmza Tanımı ve Çeşitleri

Yönerge m.2'ye göre elektronik imza "başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan ve bir doğrulama yöntemi (*method of authentication*) oluşturan, elektronik formda bulunan veri"dir.

Yönerge gelişmekte olan teknolojileri de kapsayacak şekilde elektronik imzayı geniş olarak ve teknolojiden bağımsız bir şekilde tanımlamaktadır[150]. Yönerge'de yer alan "elektronik imza" kavramı, teknik değil hukuki bir kavramı ifade etmekte ve elektronik imza tanımı, bugün kullanılmakta olan ve gelecekte ortaya çıkabilecek teknolojilerin tamamını kapsamaktadır[151].

Yönerge'nin öngördüğü modele göre tüm elektronik imzalar el yazısıyla imza ile hukuken eşdeğer kabul edilmemektedir[152]. Yönerge'de elektronik imza hukuki etkilerine göre genel olarak elektronik imza ve nitelikli sertifikaya dayanan ve güvenli elektronik imza oluşturma aracı ile oluşturulan gelişmiş elektronik imza olmak üzere iki ayrı kategoriye ayrılmıştır[153].

Yönerge m.2/1'deki tanım kapsamına giren, başka bir elektronik veriye eklenen veya onunla mantıksal bağlantısı bulunan ve bir doğrulama yöntemi oluşturan, elektronik formda bulunan her veri genel olarak elektronik imza kavramına girmektedir.

---

[150] Dörr, **a.g.e.**, s.54.

[151] "İmza" kavramı her üye devlette aynı hukuki anlamı taşımamaktadır. Örneğin bir belge üzerinde basılı olarak (el yazısıyla değil) adın belirtilmesi veya bir şirketin kaşesi İngiltere'de hukuken geçerli bir imza olarak değerlendirilirken, Fransa, Almanya ve Belçika'da yalnızca el yazısıyla imza geçerli bir imzanın hüküm ve sonuçlarını doğurmaktadır. Bu yönüyle, Yönerge'nin kabul ettiği "elektronik imza tanımı, üye devletlerde kullanılan "imza" kavramının büyük ölçüde birleştiği bir alan yaratmaktadır. Bu konuda bkz. Dumortier, **a.g.e.**, s.71.

[152] Fatih Bilgili, "Özel Hukukta Elektronik İmza ve Elektronik Ticaret", **Prof.Dr. Ömer Teoman'a Armağan**, C.II, İstanbul, Beta, 2002, s.991-1012, s.993.

[153] Brazell, **a.g.e**., s.90. Yönerge'de elektronik imzanın güvenlik ve güvenilirlik derecesine göre hiyerarşik olarak üç ayrı kategoriye ayrıldığı ifade edilmektedir: İnal, **a.g.e**., s.64.

Nitelikli sertifikaya dayanan ve güvenli elektronik imza oluşturma aracı ile oluşturulan gelişmiş elektronik imza (kısaca "nitelikli elektronik imza") ise, Yönerge'nin 5. maddesinin 1. fıkrasında tanımlanmaktadır. Buna göre nitelikli elektronik imza:

1. Yönerge m.2/2'de belirtilen şartları taşıyan gelişmiş elektronik imza[154] niteliğinde olmalıdır. Gelişmiş elektronik imza, Yönerge m.2/2'de tanımlanmaktadır. Bu tanıma göre bir elektronik imzanın gelişmiş elektronik imza olarak kabul edilebilmesi için; a) münhasıran imza sahibine bağlı olması, b) imza sahibinin kimliğini belirlemeye yaraması, c) yalnızca imza sahibinin kontrolü altında bulunabilen araçlarla oluşturulmuş olması, d) ilişkili olduğu verilere, bu verilerde sonradan yapılan değişiklikleri tespit edebilecek şekilde bağlı olması gerekmektedir. Gelişmiş elektronik imzanın uygulamadaki dijital imzaya karşılık gelmek üzere düzenlendiği konusunda öğretide görüş birliği bulunmaktadır[155].

2. Nitelikli sertifikaya dayanmalıdır (nitelikli sertifika Ek 1'deki[156] şartları taşıyan sertifikadır ve Yönerge Ek II'de belirtilen şartları yerine getiren bir sertifika sağlayıcı tarafından düzenlenmesi gerekmektedir).

---

[154] Öğretide "*gelişmiş elektronik imza*" kavramı "*ileri elektronik imza*" olarak da ifade edilmektedir (Bilgili, **a.g.e**., 994 vd). Biz burada gelişmiş elektronik imza çevirisini kullanmayı daha açıklayıcı olması sebebiyle tercih ediyoruz.

[155] Özdemir Kocasakal, **Elektronik İmza**, s.231.

[156] **Yönerge Ek I: Nitelikli sertifikada bulunması gereken bilgiler**

Tüm nitelikli sertifikalar aşağıdaki hususları içermelidir:

1. Sertifikanın nitelikli bir sertifika olarak düzenlendiğine dair bir ibare;
2. Sertifika sağlayıcının ve bulunduğu ülkenin adı;
3. İmzalayan sahibinin adı ya da takma adı;
4. Sertifikanın veriliş amacına bağlı olarak, gerektiğinde imza sahibinin özel sıfatı
5. İmza sahibinin kontrolü altında, imza oluşturmak için gerekli verilere karşılık gelen imza doğrulama verileri;
6. Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihine ilişkin bir ibare;
7. Sertifikanın kimlik kodu;
8. Nitelikli sertifikayı veren sertifika sağlayıcının gelişmiş elektronik imzası;
9. Gerektiği takdirde, sertifikanın kullanım alanına ilişkin sınırlamalar;
10. Gerektiği takdirde, sertifikanın kullanılabileceği hukuki işlemlerin değerlerine ilişkin sınırlamalar.

3. Güvenli imza oluşturma aracı (Yönerge Ek III'teki[157] şartları yerine getiren imza oluşturma aracı) ile oluşturulmuş olmalıdır.

b. Elektronik İmzanın Hukuki Etkileri

AB Elektronik İmza Yönergesi elektronik imzanın hukuken tanınmasını amaçlamaktır. Bu amaç çerçevesinde getirilen düzenlemeler elektronik imzanın nitelikli elektronik imza olup olmamasına göre iki açıdan incelenmelidir:

Yönerge m.5/1, nitelikli elektronik imzanın üye devletlerin ulusal hukukunda el yazısıyla imza ile aynı hukuki etkiyi doğurmasını ve yargılamada delil olarak kullanılabilmesini öngörmektedir[158]. Bu düzenleme, nitelikli elektronik imzanın hukuki etkilerini uyumlaştırmaya yönelik olmayıp, üye devletlerin hukukunda nitelikli elektronik imzanın hukuki etkilerinin farklılık göstermesi mümkündür. Öncelikle üye devletlerin hukuk sistemlerinde veya Topluluk mevzuatından sözleşmelerin kuruluşu açısından öngörülen şekil kuralları aynen geçerliliğini koruyacaktır[159]. Örneğin, AB üyesi bir ülkede herhangi bir sözleşmenin geçerliliği el yazısıyla imzaya ek olarak başka katı kurallara bağlamışsa, bu kurallar nitelikli elektronik imzanın uygulanabilirliği açısından da etkili olacaktır[160]. Yönerge ile bu

---

[157] **Yönerge Ek III: Güvenli İmza Oluşturma Araçlarına İlişkin Şartlar**

1. Güvenli imza oluşturma araçlarının, uygun teknik ve usuli araçlar vasıtasıyla, asgari olarak aşağıdaki şartları taşıması gerekmektedir:

a. İmzayı oluşturmak için kullanılan imza oluşturma verileri, fiili olarak yalnızca bir kez oluşabilmeli ve bunların gizliliği yeterli derecede sağlanmalıdır;

b. İmzayı oluşturmak için kullanılan imza oluşturma verilerinin elde edilememesi yeterli derecede güvenlikle sağlanmalı ve imza güncel teknolojinin kullanılmasıyla sahteciliğe karşı korunmalıdır;

c. İmzayı oluşturmak için kullanılan imza oluşturma verileri, meşru imzalayan tarafından, başkalarının kullanımına karşı güvenilir bir şekilde korunabilmelidir.

2. İmza oluşturma araçları, imzalanacak verileri değiştirmemeli ve bu verilerin imzalama işlemi öncesinde imzalayana sunulmasını (imzalayan tarafından görülmesini) engellememelidir.

[158] Dumortier, **a.g.e**., s.86; Ivo Geis, "Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce", **MMR**, Heft 11, 2000, 667-674, s.670.

[159] Özdemir Kocasakal, **Elektronik İmza**, s.230.

[160] Dumortier, **a.g.e**., s.86; Josh Bell / Ruben Gomez / Paul Hodge / Viktor Mayer-Schönberger, "Elektronic Signature Regulation: An Early Scorecard – Comparing Electronic Signatures Legislation in the US and the European Union", **Computer Law and Security Report**, Vol.17, Issue 6, 2001, s.399-402, s.400.

konuda sağlanan tek imkan, el yazısıyla imza şartı öngörülen durumlarda, bu koşulun belirli şartlarla elektronik imza ile de gerçekleşebileceğinin kabul edilmesidir[161]. Bu açıdan el yazısıyla imzanın hukuki etkilerini düzenleyen kuralların, nitelikli elektronik imzanın hukuki etkilerinin belirlenebilmesi bakımından, her ülke açısından bir referans noktası oluşturduğu belirtilmektedir[162]. Yönerge, nitelikli elektronik imza dışında kalan elektronik imzaların, hukuki etkilerini belirlemeyi üye devletlerin seçimine bırakmaktadır.

Yönerge'nin uygulama alanı 1. maddenin son fıkrasında açıkça sınırlandırılmaktadır. Buna göre; "Yönerge, sözleşmelerin kuruluşuna ve geçerliliğine[163] veya ulusal ya da Topluluk mevzuatı tarafından öngörülen şekle ilişkin diğer şartları içermediği gibi, belgelerin kullanımıyla ilgili, ulusal ya da Topluluk hukukunda belirtilen düzenlemeleri etkilemez"[164]. Diğer bir ifadeyle, Yönerge, elektronik imzanın hukuki etkilerini düzenlerken, elektronik imzalı belgenin hangi alanlarda kullanılacağına ilişkin bir düzenleme getirmemektedir[165]. Buna göre her üye devlet elektronik imzalı belgelerin kullanılabileceği alanları belirleme konusunda serbesttir[166]. Örneğin, kağıt temelli belgeler yerine elektronik belge kullanımının ulusal hukuka göre mümkün olmadığı hallerde elektronik imza

---

[161] Özdemir Kocasakal, **Elektronik İmza**, s.230.

[162] Bu yaklaşıma göre, nitelikli elektronik imzanın şekil bakımından hukuki etkisi, el yazısıyla imzanın tek başına şekil şartını gerçekleştirebilmesiyle doğru orantılı olacaktır. Detaylı bilgi için bkz. Dumortier, **a.g.e**., s.86.

[163] Elektronik ortamda kurulan sözleşmelerin geçerliliği meselesi Elektronik Ticaret Yönergesi'nde düzenlenmektedir. Bkz. s.32.

[164] Yönerge'nin kapsamının bu şekilde sınırlandırılmış olması yabancı doktrinde "büyük ve talihsiz bir sınırlama" olarak değerlendirilmekte, bu sebeple Yönerge'de yer alan düzenlemelerin çok sınırlı bir alanda etki doğuracağı belirtilmektedir. Detaylı bilgi için bkz. Aalberts / van der Hof, **a.g.e**., s.32.

[165] Martien Schaub, **European Legal Aspects of E-Commerce**, Europa Law Publishing, 2004, s.131; İnal, **a.g.e**., s.68.

[166] Her ne kadar AB Elektronik İmza Yönergesi'ne göre üye devletler elektronik imza yoluyla imza edilen belgelerin kullanılabileceği alanları belirleme konusunda serbest bırakılmışsa da, özel hukuk açısından bu serbesti Avrupa Birliği'nin Elektronik Ticaret Yönergesi ile önemli ölçüde sınırlandırılmış bulunmaktadır (Aalberts / van der Hof, **a.g.e**., s.32). Elektronik Ticaret Yönergesi'nin 9. maddesine göre üye devletler ulusal hukuklarına göre sözleşmelerin elektronik yolla kurulmasını sağlamakla yükümlüdür. Bu sebeple üye devletler bu alanda elektronik imzaların geçerliliğini kabul edip etmemek konusunda serbestiye sahip olmayıp, nitelikli sertifikaya dayanan elektronik imza ile imzalanmış sözleşmelerin tıpkı el yazısıyla imzalanmış gibi geçerliliğini tanımak zorundadır (İnal, **a.g.e.**, s.68-69).

kullanılmayacaktır[167]. Elektronik belge kullanımının mümkün olması halinde ise, belgenin nitelikli elektronik imza ile imzalanması, imzalanan elektronik belgenin el yazısıyla imzalanmış bir belge ile aynı hukuki sonuçları doğurmasını sağlayacaktır[168].

Yönerge'de usul hukuku bakımından, elektronik imzalı belgelere belirli bir ispat gücü atfedilmemiş ve ispat gücünün belirlenmesi tamamen üye devletlerin ulusal hukukuna bırakılarak, nitelikli elektronik imza ile imzalanan bir belge ispat kuvveti açısından el yazısıyla imzalanmış bir belge ile eş değer kılınmamıştır[169]. Yönerge, üye devletlerin elektronik imzalı belgelerin delil olarak değerlendirilmesi hakkında ulusal hukuklarında yer alan mevcut düzenlemelerini etkilememektedir. Bu konuda yalnızca elektronik imzalı belgelerin mahkemede delil olarak kabul edilmesi gerektiğini kurala bağlanmakta ve bu bakımdan "ayrımcılık yasağı" öngörülmektedir[170]. Buna göre, bir elektronik imzanın sadece elektronik formda olması, nitelikli bir sertifikaya dayanmaması, akredite edilmiş bir sertifika sağlayıcı tarafından verilmiş bir nitelikli sertifikaya dayanmaması veya güvenli bir imza oluşturma aracı ile üretilmemiş olması sebeplerinden birine dayanılarak hukuki etki doğurmasına veya yargılamada delil olarak kullanılmasına engel olunamayacaktır (Yönerge m.5). Bu şekilde kağıt belge üzerinde yer alan el yazısıyla imzaya, sırf bu özelliğinden ötürü üstünlük tanınmaması kabul edilmiş olmaktadır.

---

[167] Schaub, **a.g.e.**, s.131.

[168] Ayrıca, üye devletin ulusal hukukunda yasak söz konusu değilse, Yönerge bir özel hukuk sözleşmesine dayalı olarak tarafların aralarında elektronik imzalı belgeleri kabul etme kural ve koşullarını kararlaştırmaya ilişkin irade serbestisini kısıtlamamaktadır (Yönerge'nin 16 nolu gerekçesi). Bu durum özellikle belirli sayıda katılımcı arasındaki özel hukuk anlaşmalarına dayalı sistemler (kapalı ağ sistemleri) içinde kullanılan elektronik imzalar açısından önemlidir. Bu konuda bkz. Dumortier, **a.g.e**., s.86; ayrıca bkz. Bilgili, **a.g.e**., s.993, dn.12.

[169] Bu durumda elektronik imzaya dayanan taraf, ispat gücü konusunda hakimi ikna etmelidir: Özdemir Kocasakal, **Elektronik İmza**, s. 233.

[170] Özsunay, **a.g.e**., s.136; Erturgut, **a.g.e**., s.140.

2. Sertifika Hizmetlerinin Düzenlenmesi

a. Sertifika Sağlayıcı Kavramı

Yönerge m.2/9'a göre sertifika, "imza doğrulama verisini[171] bir kişiye bağlayan ve bu kişinin kimliğini doğrulayan elektronik belgedir". Nitelikli sertifika kavramı ise m.2/10'da tanımlanmaktadır. Bir sertifikanın nitelikli sertifika kabul edilmesi için Yönerge Ek I'de öngörülen şartları gerçekleştirmesi ve Ek II'deki şartları haiz bir elektronik sertifika sağlayıcı tarafından düzenlenmesi gerekmektedir.

Sertifika sağlayıcı kavramı Yönerge m.2/11'de çok geniş şekilde tanımlamaktadır. Buna göre sertifika sağlayıcı "sertifika düzenleyen ve elektronik imzaya ilişkin diğer hizmetleri sunan bir gerçek veya tüzel kişi ya da bir kuruluştur"[172]. Yönerge ile sertifika sağlayıcıları, nitelikli sertifika düzenleyenler ve düzenlemeyenler olarak ikiye ayrılmaktadır[173].

Yönerge m.3/1'de üye ülkelerin sertifika hizmetlerinin sağlanmasını önceden verilecek bir izne tabi tutamayacağı belirtilmiştir. Yönerge'in 10 numaralı gerekçesinde açık ağlar kanalıyla sertifika hizmetlerinin Topluluk çapında sağlanabilmesi için sertifika sağlayıcılarının, önceden izin almak zorunda olmaksızın, serbestçe faaliyette bulunmaları gerektiği belirtilmektedir. Önceden izin alma, yalnızca faaliyete başlamadan önce sertifika sağlayıcının ulusal otoritelerden sertifika hizmetini sunabilmesi için onay almasını değil, aynı etkiyi gösterecek diğer tüm tedbirleri de kapsamaktadır[174].

---

[171] Yönerge m.2/7'de "elektronik imzaların doğrulanması için kullanılan, şifre ya da açık kriptografik anahtarlar gibi veriler" şeklinde tanımlanan imza doğrulama verisi, dijital imza tekniğindeki açık anahtara karşılık gelmek üzere kullanılmaktadır.

[172] Yönerge'nin 9 numaralı gerekçesi böyle bir geniş tanıma başvurulmuş olmasını şu şekilde açıklamaktadır: "Elektronik imzalar, bu imzalarla ilgili ya da bu imzaları kullanan yeni ürün ve hizmetlerin ortaya çıkmasına sebep olan çok çeşitli durumlarda ve uygulamalarda kullanılacaktır; bu ürün ve hizmetlerin tanımı, sertifika verilmesi ve bu sertifikaların yönetimiyle sınırlı kalmamalı, aynı zamanda, elektronik imzaları kullanan ya da elektronik imzalarla ilişkili olan kayıt hizmetleri, zaman damgası hizmetleri, rehber hizmetleri, bilişim hizmetleri veya elektronik imzayla ilgili danışma hizmetleri gibi tüm hizmetleri kapsamalıdır.

[173] İnal, **a.g.e.**, s.70.

[174] Dumortier / Kelm / Nilsson / Skouma / van Ecke, **a.g.e.,** s.40.

Sertifika hizmetlerinin sunulması önceden izin alma şartına bağlanmamakla birlikte, her üye devletin "nitelikli sertifika" düzenleyen sertifika sağlayıcılarını denetlemek için uygun bir sistem oluşturması gereği Yönerge m.3/3'de düzenlenmiştir. Yönerge m.3/3'e göre her üye devlet, ülkelerinde kurulan ve kamuya nitelikli sertifika veren sertifika sağlayıcılarının EK II'de[175] belirtilen şartlara uygunluğunu denetlemek üzere uygun bir sistemi kurmakla yükümlüdür. Kurulması

[175] **Yönerge Ek II: Nitelikli sertifika veren sertifika sağlayıcılarının yerine getirmesi gereken şartlar**

Sertifika sağlayıcıları:

1. Sertifika hizmeti sağlamak için yeterli güvenilirlikte olduklarını göstermek;

2. Hızlı ve güvenli bir rehber hizmeti ile güvenli ve çabuk bir iptal hizmetinin işleyişini temin etmek;

3. Sertifikaların verildiği veya iptal edildiği tarih ve saatin kesin olarak belirlenebilmesini temin etmek;

4. Ulusal hukuk çerçevesinde uygun araçlarla, nitelikli sertifikanın verildiği kişinin kimliğini ve gerektiğinde, bu kişiye özel sıfatları doğrulamak;

5. Uzmanlık bilgisine, deneyime ve hizmetlerin sağlanması açısından gerekli niteliklere, özellikle idari yönden yeterliliğe, elektronik imza teknolojisi konusunda özel bilgilere ve uygun güvenlik prosedürleri alanında deneyime sahip personel çalıştırmak; personelin aynı zamanda kabul edilmiş standartlar çerçevesinde yeterli ve bunları karşılayacak idari prosedürleri de uygulayabilmeleri gereklidir;

6. Değiştirmeye karşı korumalı güvenilir sistem ve ürünlerin kullanımı ile bunlar tarafından desteklenecek işlemin teknik ve kriptografik güvenliğinin temin etmek;

7. Sertifikanın taklidine karşı önlemler almak ve sertifika sağlayıcının imza oluşturma verisini üretmesi halinde, bu verilerin üretilmesi sırasında gizliliği temin etmek;

8. Yönerge'de öngörülen şartlara uygun olarak faaliyet gösterilmesi açısından, özellikle meydana gelebilecek zararlardan sorumluluğunun üstlenilebilmesi için, örneğin uygun bir sigorta sözleşmesi yapma yoluyla, yeterli mali kaynakların bulundurmak,

9. Sertifikanın özellikle yargılamada delil olarak kullanılabilmesi amacıyla, nitelikli sertifikaya ilişkin tüm kayıtları uygun bir süre boyunca saklamak; bu kayıtların elektronik yollarla yapılması mümkündür;

10. Sertifika sağlayıcı tarafından anahtar yönetimi hizmeti verilen kişiye ait olan imza oluşturma verilerinin saklamamak veya kopyalamamak;

11. Elektronik imzasını desteklemek için sertifika telep eden kişiyle sözleşme ilişkisi kurulmadan önce, kalıcı iletişim yollarıyla, sertifika kullanımına ilişkin, kullanımdaki kısıtlamalar da dahil olmak üzere, kesin kural ve koşulların neler olduğu, ihtiyari bir akreditasyon hizmet sisteminin varlığı, şikayet usullerinin ve uyuşmazlıkların çözümü prosedürleri hakkında bu kişiyi bilgilendirmek; elektronik yolla da iletilebilecek bu bilgiler, yazılı olarak ve kolayca anlaşılabilir bir dille yapılmalıdır, talep etmeleri halinde bu bilgilerin ilgili bölümü sertifikaya güvenen üçüncü kişilere sunulabilmelidir;

12. Sertifikaları doğrulanabilir bir şekilde saklamak üzere güvenilir sistemler kullanmak ve böylece
· Sadece yetkili kişilerin ekleme ve değişiklik yapabilmesini,

· Bilgilerin doğruluğunun kontrol edilebilmesini,

· Sadece sertifika sahibinin rızasının varlığı halinde sertifikaların tekrar kullanılabilir olmasının teminini,

öngörülen denetim sistemi, izin mahiyetinde etki doğurarak sertifika hizmetlerinin kamuya serbestçe sunumunu kısıtlamamalı, aynı zamanda nitelikli sertifikanın ayırt edilebilirliğini sağlayarak, üçüncü kişiyi kendisine sunulan sertifikanın nitelikli olduğu hususunda yanıltılması ihtimaline karşı korumalıdır[176]. Bu bağlamda önerilen denetim sistemi, sertifika sağlayıcılarının faaliyetlerine başlamadan önce bir kamu otoritesine bildirimde bulunmalarıdır[177]. Bildirim, hukuken idari bir yükümlülük niteliğinde olması şartıyla Yönerge'ye uygun kabul edilmektedir. Sertifika sağlayıcının bildirimde bulunduktan sonra faaliyete başlayabileceğine ilişkin olumlu veya olumsuz bir cevabı beklemek zorunda olması izin mahiyetinde değerlendirme göreceğinden Yönerge m.3/1'e aykırı olacaktır[178].

Yönerge m.3/2'e göre sertifika hizmetlerinin sağlanmasının izin şartına bağlanamayacağı kuralı saklı kalmak kaydıyla, üye devletler sunulan sertifika hizmetlerinin standardını yükseltmek amacıyla ihtiyari akreditasyon sistemleri kurabilecek veya mevcut olanları sürdürebilecektir[179]. Akreditasyon sistemleri, sertifika sağlayıcı tarafından verilen hizmetin güvenirliğini artırmaya yöneliktir ve

---

· Bu güvenlik gerekliliklerini tehlikeye sokabilecek tüm teknik değişikliklerin işleten tarafından fark edilmesinin mümkün olmasını sağlamak;

ile yükümlüdür.

[176] İlk bakışta Yönerge m.3/1 ile çelişkili görünen bu düzenlemeyle aslında ticari hayatın gereklilikleri ile tüketicinin korunması amacı arasında bir denge yaratılmaya çalışılmaktadır (14 nolu gerekçesi); ayrıca bkz. Dumortier / Kelm / Nilsson / Skouma / Van Ecke, **a.g.e.,** s.40. Bu maddede belirtilen denetim sistemleri her üye devlette birbirinden farklı ağırlıkta düzenlenmektedir. Sertifika sağlayıcıların genellikle yerleşik oldukları ülkede hizmet vermeleri sebebiyle günümüzde bu farklılıkların etkileri sınırlı olmakla birlikte, sertifika hizmetlerinin sınır ötesinde verilmesi arttığı takdirde bu farklılıklar olumsuz etkiler doğuracak niteliktedir. Detaylı bilgi için bkz. Dumortier, **a.g.e**., s.77.

[177] Dumortier / Kelm / Nilsson / Skouma / Van Ecke, **a.g.e.,** s.40; Bildirim zorunluluğu AB'ye üye ülkelerde genellikle benimsenmiş olmakla birlikte, farklı uygulamaların bulunduğu görülmektedir. Bazı ülkelerde tüm sertifika sağlayıcılarının bildirimde bulunması gerekliyken, bazılarında ise sadece nitelikli sertifika düzenleyenlerin bildirimde bulunması gerekmektedir: **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu** (çalışma grubu: Leyla Keser, Yasin Beceni, Tugrul Sevim), Temmuz 2004, İstanbul, (Çevrimiçi) http://www.tk.gov.tr/eimza/doc/diger/e-imza%20hukuk%20calisma%20grubu%20raporu.pdf, 10.06.2011.

[178] Dumortier / Kelm / Nilsson / Skouma / Van Ecke**, a.g.e.,** s.40.

[179] Yönerge m.2/13'e göre "ihtiyari akreditasyon; sertifika hizmeti sağlanmasıyla ilgili tüm hak ve yükümlülükleri belirleyen, ilgili sertifika sağlayıcının isteği üzerine, bu hak ve yükümlülüklerin geliştirilmesi ve denetimi ile ilgili kamu kurumu ya da özel bir kurum tarafından verilen her türlü izindir ve sertifika sağlayıcının bu izinden kaynaklanan haklarını kullanmasına, ilgili kararın kendisine ulaşmasına dek, engel olmaktadır". İsteğe bağlı akreditasyon sistemlerine ilişkin tüm şartlar; objektif, saydam, orantılı ve ayrım gözetmeyen nitelikte olmalı (m.3/2) ve sertifika hizmetlerinin sunulmasında rekabeti azaltıcı etki yaratmamalıdır (12 nolu gerekçesi).

ulusal otoritelerin onayı ile kurulmaktadır[180]. Bu düzenleme ile Yönerge'de benimsenen yapıda akredite edilmiş sertifika sağlayıcıları ile akredite edilmiş olmayanlar birlikte ortaya çıkmaktadır[181]. Belirtmek gerekir ki, sertifika sağlayıcının akredite edilmiş olması, bu sertifika sağlayıcının nitelikli elektronik sertifika verdiği anlamına gelmemektedir. Bir sertifika sağlayıcının nitelikli sertifika verebilmesi için Ek II'teki şartları yerine getirmesi gerekmektedir.

Üye devletlerden birinde yerleşik bulunan, akredite edilmiş bir sertifika sağlayıcı tarafından düzenlenen bir nitelikli sertifika ile akredite edilmiş olmayan bir sertifika sağlayıcı tarafından düzenlenen nitelikli sertifika ve bunlara dayanan elektronik imzalar arasında hukuki açıdan hiçbir fark bulunmamaktadır[182].

Avrupa Birliği üyesi olmayan bir devlette yerleşik bulunan bir sertifika sağlayıcı tarafından düzenlenen nitelikli sertifikaların, Topluluk içerisinde yerleşik bir sertifika sağlayıcı tarafından düzenlenen nitelikli sertifikalarla hukuken eş değer kabul edilebilmesi mümkündür[183].

İç pazarda sunulan sertifika hizmetlerini düzenleyen temel hüküm "İç Pazar İlkeleri" başlıklı 4. maddenin 1. fıkrasıdır[184]. Bu hükme göre; "her üye devlet, bu Yönerge uyarınca iç hukukta öngördüğü kuralları, ülkesi dahilindeki sertifika sağlayıcılarına ve onların sunduğu hizmetlere uygulayacaktır. Üye devletler bu

---

[180] Brazell, **a.g.e**, s.89.

[181] İsteğe bağlı akreditasyon kavramı üye devletler tarafından büyük ölçüde yanlış anlaşılmış gözükmektedir. Birçok Avrupa ülkesi ihtiyari akreditasyon sistemlerini, yanlış olarak, Yönerge'nin şartlarının gerçekleşip gerçekleşmediğini denetlemek üzere bir araç olarak değerlendirmektedir. Ayrıca pek çok Avrupa ülkesinde ihtiyari akreditasyon sistemleri gerçekte ihtiyari olarak uygulanmamaktadır. Örneği e-devlet uygulamalarında yalnızca akredite edilmiş sertifika sağlayıcıları kabul edilmekte, böylelikle dolaylı olarak sertifika sağlayıcıları akredite edilmeye zorlanmaktadır, bkz. Dumortier, **a.g.e**., s.77.

[182] İnal, **a.g.e**., s.70.

[183] Bunun için;

a) sertifika sağlayıcının bu Yönerge'deki şartları yerine getirmesi ve bir üye devletteki ihtiyari akreditasyon sistemi çerçevesinde akredite edilmiş olması; veya

b) Topluluk içerisinde yerleşik bulunan ve Yönerge'deki şartları yerine getiren bir sertifika sağlayıcının bu sertifikayı garanti etmesi; veya

c) sertifika veya sertifika sağlayıcının, Topluluk ile üçüncü ülkeler veya uluslararası kuruluşlar arasında yapılan ikili veya çok taraflı anlaşmalarca tanınmış olması gerekmektedir (Yönerge m.7/1).

[184] Dumortier, **a.g.e**., s.80

Yönerge kapsamındaki alanlarda bir diğer üye devletten kaynaklanan sertifika hizmeti sunumunu kısıtlayamazlar". Yönerge'yi iç hukukuna dönüştürürken, üye devletlerin tamamı sertifika sağlayıcılarına ilişkin düzenlemelerinde bu hükme bağlı kalmış ve başka bir üye devlette kurulan sertifika sağlayıcı tarafından sağlanan sertifika hizmetini önceden verilecek bir izne bağlı tutmamıştır. Böylece başka ülkede kurulan bir sertifika sağlayıcı ulusal otoritelerden izin almak zorunda olmaksızın sertifika hizmeti verebilecektir[185].

b. Sertifika Sağlayıcının Sorumluluğu

Yönerge elektronik imza kullanımının yaygınlaşmasına ve elektronik imzanın hukuken tanınmasına katkıda bulunmak üzere sertifika sağlayıcılarının sorumluluğunu düzenlemekte ve bu alanda üye devletlerin ulusal hukuklarındaki mevcut düzenlemeleri asgari düzeyde uyumlaştırmayı amaçlamaktadır[186].

Yönerge'nin 6. maddesi sertifika sağlayıcıların sertifikaya güvenen üçüncü kişilere karşı hukuki sorumluluğunu düzenlemektedir[187]. Yönerge, sertifika sağlayıcıların sorumluluğunu düzenlerken, imza sahibi ve üçüncü kişinin hak ve yükümlülüklerine ilişkin kurallar getirmemektedir. Ayrıca, sertifikanın düzenlenmesi, dağıtımı, kullanımı, iptal edilmesi, askıya alınması ve geçerliliğinin sona erdirilmesi durumlarından doğacak imza sahibinin veya sertifika sağlayıcının fiillerinden ötürü üçüncü kişinin uğrayacağı zararlardan doğan sorumluluğu gerek sertifika sağlayıcı gerekse imza sahibi açısından özel bir şekilde düzenlememektedir[188].

---

[185] Bu sayede Yönerge öngördüğü en önemli hedeflerinden birini gerçekleştirmiş sayılmaktadır (Dumortier, **a.g.e**., s.81).

[186] Apol·lónia Martínez Nadal / Josep Lluís Ferrer Gomila, "Critical Comments on the European Directive on a Common Framework for Electronic Signatures and Certification Service Providers", **LNCS: Financial Cryptography,** Vol.1962, 2001, Springerlink, s.225-244, s.237.

[187] Bu düzenleme ile bir elektronik imzayı doğrulama amacıyla nitelikli sertifika kullanan kişiler ve sertifika sağlayıcı arasındaki tartışmalı konu çözüme kavuşturulmaktadır: Martínez Nadal / Ferrer Gomila, **a.g.e**., s.205.

[188] Martínez Nadal / Ferrer Gomila, **European Directive**, s.238.

Yönerge sertifika sağlayıcıların, düzenledikleri nitelikli sertifikaya haklı olarak (*reasonably*) güvenerek hukuki işlemlere girişen üçüncü kişilerin uğradığı zararlardan sorumluluğuna ilişkindir[189]. "Haklı güven" ifadesinin ne şekilde belirleneceği Yönerge metninden anlaşılmamakla birlikte, gereken özenin gösterilmesi şartıyla sertifikaya güvenilmesi şeklinde yorumlanması gerekmektedir[190].

Bu sorumluluk sadece sertifika sağlayıcının nitelikli sertifika düzenlemesi halinde söz konusu olacaktır[191]. Adi sertifika sebebiyle üçüncü kişilerin uğradığı zararlardan sorumluluk konusunda Yönerge'da hüküm bulunmamakta, bu konunun çözümü üye devletlerin ulusal hukukundaki mevcut düzenlemelere bırakılmaktadır[192].

Yönerge'nin 6. maddesi çerçevesinde sertifika sağlayıcının sorumluluğunu doğuran sebepler şu şekilde sıralanabilir:

1. Nitelikli sertifikada yer alan bilgilerin gerçeğe uygun olması gerekmektedir (Yönerge m.6/1-a). Sertifika sağlayıcı sertifikada yanlış bilgi yer alması sebebiyle meydana gelecek zararlardan sorumlu olacaktır.

2. Nitelikli sertifika olduğu beyan edilen sertifikanın Yönerge Ek I'de öngörülen tüm ayrıntıları içermesi ve sertifikayı düzenleyen sertifika sağlayıcının Yönerge Ek II'de belirtilen şartları yerine getirmesi gerekmektedir (Yönerge m.6/1-a)[193]. Aksi takdirde sertifika sağlayıcı meydana gelecek zararlardan sorumlu olacaktır.

---

[189] Claduia von Seck, **Die elektronische Signatur im Hinblick auf die Haftung der Zertifizierungsdiensteanbieter**, Marburg, 2003, s.47; Martínez Nadal / Ferrer Gomila, **European Directive**, s.238; İnal, **a.g.e**., s.71. Taraflar arasındaki ilişki prensip olarak sözleşmeye dayanmamakla birlikte, sözleşmeye dayandığı haller de söz konusu olabilir: Martínez Nadal / Ferrer Gomila, **a.g.e**., s.205.

[190] Üçüncü kişi nitelikli sertifikadan anlaşılabilenlerle sınırlı olmak üzere nitelikli sertifikanın gerekli şartları taşıyıp taşımadığını, bu sertifikaya dayanarak işlemde bulunmadan önce incelemekle yükümlüdür: von Seck, **a.g.e**, s.47-48.

[191] von Seck, **a.g.e.**, s.47; Bell / Gomez / Hodge / Mayer-Schönberger, **a.g.e**., s.400; İnal, **a.g.e**., s.71

[192] Bell / Gomez / Hodge / Mayer-Schönberger, **a.g.e**., s.400.

[193] von Seck, **a.g.e.**, s.47.

3. Sertifika sağlayıcı, sertifikanın düzenlendiği sırada, nitelikli sertifikada belirtilen imza sahibinin, sertifikada verilen veya tanımlanan imza doğrulama verisine karşılık gelen imza oluşturma verisine sahip olmasını sağlamalıdır (Yönerge m.6/1-b). Bu hükümden anlaşıldığı üzere imza oluşturma verisinin en geç sertifikanın düzenlenmesi anında imza sahibine teslim edilmesi gerekmektedir[194]. Hüküm esas itibariyle imza oluşturma verisinin yetkisiz kullanımından meydana gelecek zararlardan sorumluluğu düzenlemektedir.

4. Sertifika sağlayıcı, her ikisini de kendisinin meydana getirmesi halinde, imza oluşturma verisinin ve imza doğrulama verisinin tamamlayıcı şekilde kullanılabilmelerini sağlamakla yükümlüdür (Yönerge m.6/1-c)[195].

5. Sertifika sağlayıcı düzenlediği nitelikli sertifikanın iptal edilmesi halinde, bu iptal durumunu kayıt altına almakla yükümlüdür. Sertifikanın iptalinin kayıt altına alınmaması ve bu yüzden sertifikanın geçerli bir sertifika görünümünü taşıyarak hukuki işlemlerde kullanılması halinde, iptal durumunda haberi olmayan üçüncü kişilerin uğradığı zararlardan sertifika sağlayıcı sorumlu olacaktır (Yönerge m.6/2).

Yönerge m.6/3 ve m.6/4'te nitelikli sertifikada, sertifikanın kullanılacağı işlemlerin türüne ve değerine ilişkin sınırlamaların öngörülebileceği belirtilmektedir. Bir sertifika sağlayıcı, üçüncü kişiler tarafından anlaşılabilir olması şartıyla, sertifikaların bu sınırlamaları aşan işlemlerde kullanılması sebebiyle sorumlu olmayacaktır[196].

Sertifika sağlayıcılar Yönerge m.6.1 ve m.6/2'de belirtilen sebeplerin gerçekleşmesi dolayısıyla meydana gelen zararlardan, kusurlu olmadıklarını ispat

---

[194] İnal, **a.g.e**., s.72.

[195] Bu verilerin tamamlayıcı şekilde kullanılabilmeleri, ancak teknik kriterlerin gereği gibi yerine getirilmesine bağlıdır. Buna göre sertifika sağlayıcının Yönerge Ek II ve Ek III'te belirtilen şartları yerine getirmesi gerekmektedir: İnal, **a.g.e.**, s.72.

[196] Bunun işlemin değeri bakımında getirilen sınırlamalarla ilgili olarak tartışma yaratacak bir düzenleme olduğu ifade edilmektedir. Çünkü, bir nitelikli sertifikanın kullanılacağı işlemin değeri kavramıyla, bir sertifika yüzünden uğranılacak zarar kavramı birbirinden farklıdır: Martínez Nadal / Ferrer Gomila, **a.g.e**., s.216.

edemedikleri takdirde sorumlu tutulmaktadır. Burada öngörülen sorumluluğun ispat yükü yer değiştirilmiş bir tür kusur sorumluluğu olduğu ifade edilmektedir[197].

C. ELEKTRONİK TİCARET HAKKINDA UNCITRAL MODEL KANUNU

UNCITRAL (*United Nations Commission on International Trade Law* - Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu) tarafından elektronik ortamda hukuki ilişkilerin kurulmasına ve elektronik imzaya ilişkin olarak tüm dünyada kabul gören temel prensipleri içeren iki model kanun hazırlanmıştır: Elektronik Ticaret Hakkında Model Kanun ve Elektronik İmza Model Kanunu. Bunların doğrudan doğruya bir hukuki etkisi bulunmayıp, devletlerin elektronik imzaya ilişkin belirsizlikleri ve hukuki engelleri kaldırmak amacıyla kendi mevzuatlarında getirecekleri düzenlemelerde yararlanabilecekleri bir örnek niteliğindedir. Dolayısıyla devletler bu kanunları kapsamını genişleterek veya değiştirerek iç hukuka aktarabilirler[198].

Bu başlık altında incelenecek olan ilk model kanun 1996 tarihli Elektronik Ticaret Hakkındaki UNCITRAL Model Kanunu'dur. Bu kanun devletlerin ulusal hukuklarında yapacakları düzenlemelerde örnek teşkil etmek ve bu sayede hukukların yakınlaştırılmasına ve birleştirilmesine katkıda bulunmak, elektronik

---

[197] Dörr, **a.g.e.**, 73. Yönerge'nin ilk taslağında sertifika sağlayıcının sorumluluğu tehlike sorumluluğu olarak düzenlenmiştir, ancak bu şekilde düzenlenmesi büyük tartışmalara sebep olmuştur. Sertifika sağlayıcılarının üçüncü kişilere karşı sorumluluğunun bu kadar katı kurallara tabi tutulması iki açıdan eleştirilmiştir: İlk olarak, Yönerge'nin böyle bir düzenlemeyle amacını aşmış olacağı, böyle bir düzenlemenin (asgari uyumlaştırma amacını aşarak) genel olarak üye devletlerin sorumluluk kurallarının uyumlaştırması sonucunu doğuracağı belirtilmiştir. İkinci olarak ise tehlike sorumluluğunun Avrupa Birliği üyesi devletlerde yerleşik sertifika sağlayıcılarının Asya ülkelerinde ve ABD'de yerleşik sertifika sağlayıcılarına kıyasla aleyhine bir durum yaratacağını, rekabet edebilirliklerini azaltacağı ifade edilmiştir, detaylı bilgi için bkz. Christopher Kuner, **Remarks of the German Government on the EU Draft Directive concerning Electronic and Digital Signatures**, 1998, (Çevrimiçi) http://www.kuner.com/data/sig/ gov_ger_eu-draft.htm, 1.02.2011.

[198] Ekşi, **a.g.e**., s.339.

ticaretin gelişimine yönelik yasal engelleri ortadan kaldırarak daha güvenli bir ortam oluşturmak amacıyla hazırlanmıştır[199].

Bu Kanun'da modern iletişim araçlarının gelişimine yönelik en büyük engelin yazılı belge kullanımını zorunlu kılan hukuk kuralları ile oluşturulduğu ifade edilmektedir. Bundan hareketle ulusal hukuklarda yer alan "yazılı", "imza", "orijinal" kavramlarına ilişkin tanımların bilgisayar teknolojisini de kapsayacak şekilde genişletilmesine yönelik düzenlemeler getirilmiştir[200].

Kağıda dayalı ortama ilişkin bu kavramların amaçları ve işlevlerinin analizi ve bu amaç ve işlevlerin elektronik ortamda nasıl sağlanacağının belirlenmesi esasına dayanan işlevsel denklik ilkesi ilk defa olarak bu düzenleme ile ortaya konulmaktadır[201]. Kanun'un 7. maddesi, elektronik ortamda hukuki işlemlerin güven içinde meydana getirilmesi amacıyla, el yazısıyla imzanın işlevlerinin elektronik ortamda gerçekleşmiş sayılabilmesini iki koşula bağlamaktadır. Buna göre, elektronik imza bir yandan imza atan kişinin kimliğinin tespitine, diğer yandan elektronik belgede yer alan irade beyanının bu kişiye ait olduğunu belirlemeye imkan veren güvenilir bir yöntem kullanılarak atılmış olmalıdır.

Model Kanun m.11'de, sözleşmelerin kuruluşuna ilişkin olarak karşılıklı irade beyanlarının, taraflar arasında aksine bir sözleşme yapılmadığı takdirde, elektronik araçlar kullanılarak açıklanabileceği kabul edilmiştir. Buna göre, sırf irade beyanlarının elektronik yolla açıklanmış olması sözleşmenin geçerliliğini ve bağlayıcığını etkilemeyecektir.

Elektronik belgelerin ispat gücü meselesi ise Kanun'un 9. maddesinde düzenlenmektedir. Buna göre elektronik belgede yer alan bilgiler ispat gücüne sahiptir; ancak delil değeri belirlenirken elektronik belgenin oluşturulması, saklanması ve iletiminde kullanılan yolların güvenilirliği, bilginin bütünlüğünün

---

[199] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998,* (Çevrimiçi) http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf, 10.03.2011.

[200] Özdemir Kocasakal, **Elektronik İmza**, s.223.

[201] Özdemir Kocasakal, **Elektronik İmza**, s.224.

korunmasına ilişkin yöntemin güvenilirliği, gönderilen kişinin belirlenmesinde kullanılan yöntem ve diğer şartlar dikkate alınarak değerlendirilecektir. Dolayısıyla her elektronik belgenin değerinin somut olay bakımından değerlendirilmesi gerekli olup, bu madde ile bir belgenin sırf elektronik formda olması nedeniyle delil olma niteliğine zarar verilmemesi gerektiği açıklığa kavuşturulmaktır.

D. ELEKTRONİK İMZALAR HAKKINDA UNCITRAL MODEL KANUNU

UNCITRAL tarafından, ulusal hukuklarca getirilecek elektronik imzaya ilişkin düzenlemelere örnek teşkil etmek ve bu sayede hukukların yakınlaştırılmasına ve birleştirilmesine katkıda bulunmak üzere Elektronik İmza Model Kanunu'nu[202] (Model Kanun) hazırlanmış ve 5 Temmuz 2001'de kabul edilmiştir.

Model Kanunu m.1'e göre, Kanun elektronik imzanın ticari faaliyetlerde kullanımını düzenlemekte olup, ticari nitelikte olmayan faaliyetlerde (örneğin e-devlet uygulamalarında) elektronik imza kullanımını kapsamamaktadır[203]. Elektronik İmza Model Kanunu'nun Yasalaştırılmasına İlişkin Uygulama Kılavuzu'nda (Uygulama Kılavuzu) "ticari faaliyet" ifadesinin geniş anlamda kullanıldığı, bu ifadenin sözleşmeye dayalı olan veya olmayan ticari faaliyetlerin tamamını kapsadığı ifade edilmektedir[204].

---

[202] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment.* Model Kanun'un İngilizce metni için bkz. (Çevrimiçi) http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf, 1.02.2011; Türkçe çevirisi için bkz. Internet ve Hukuk (der. Yeşim Atamer), Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.780.

[203] Apol·lónia Martínez Nadal / Josep Lluís Ferrer Gomila, "Comments to the UNCITRAL Model Law on Electronic Signatures", **LNCS: Information Security,** Vol.2433, 2002, Springerlink, s.229-243, s.231.

[204] Model Kanun m.1'de Kanun'da yer alan düzenlemelerin tüketicinin korunmasına ilişkin kuralları yürürlükten kaldırmadığı belirtilmektedir. Bu sebeple, "ticari faaliyet" ifadesinin geniş yorumlanması gerekmekle birlikte, bir tarafın tüketici konumunda olduğu hukuki işlemlerin, Model Kanun'un iç hukuka dönüştürülmesinde uygulama alanı dışında bırakılması mümkündür. Detaylı inceleme için bkz. Martínez Nadal/Ferrer Gomila, **UNCITRAL Model Law**, s.232.

1. Elektronik İmza ve Hukuki Etkileri

Model Kanun ticari ilişkilerde elektronik imzanın ve elektronik belgelerin kullanılmasını kabul etmekte ve bu araçlara hukuken meşruluk kazandırmaktadır[205]. Elektronik imza, Model Kanunu'nun 2. maddesinde şu şekilde tanımlanır: "*Elektronik imza bir veri mesajına eklenen veya mantıksal olarak bu mesajla ilişkilendirilen, veri mesajıyla*[206] *bağlantılı olarak imzalayanın kimliğini belirlemeye yarayan ve imzalayan tarafından söz konusu veri mesajının içeriğini onaylama iradesi ile uygulanan elektronik formattaki veridir"*.

Elektronik imza kavramı, el yazısıyla imzanın kullanımından doğan hukuki etkilerin tamamını meydana getirmesine imkan verecek şekilde geniş olarak ve teknolojiden bağımsız bir ifadeyle tanımlanmaktadır[207]. Uygulama Kılavuzu'nda mevcut ve gelecekteki uygulamaların tamamını kapsamak üzere, teknolojiden bağımsızlık ilkesinin benimsenmiş olduğu, ancak aynı zamanda uygulamadaki hakim teknoloji türü olan dijital imzaya Model Kanun'un hazırlanmasında büyük önem verildiği belirtilmektedir (Uygulama Kılavuzu, par.14).

Model Kanun, el yazısıyla imzanın işlevlerinin elektronik ortamda gerçekleştirilmesine yönelik olarak işlevsel denklik ilkesi temelinde oluşturulmuştur. Model Kanun m. 6/1 işlevsel denkliğin sağlanmasını elektronik imzanın güvenilirliğine bağlı tutmaktadır. Model Kanun m.6/2'ye göre bir elektronik imzanın güvenilir sayılabilmesi için;

a) imza oluşturma verisinin, kullanıldıkları koşullar içerisinde, sadece imzalayana bağlı olması,

---

[205] Billur Yaltı Soydan, "E-imza ve E-belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk – II", **Vergi Sorunları Dergisi**, S.152, 2001, s.156-165, s.157.

[206] Model Kanun m.2'ye göre burada geçen veri mesajı, "elektronik, optik veya bunlarla sınırlı olmamak üzere, elektronik veri değişimi, elektronik posta, telgraf, teleks veya telekopi de dahil olmak üzere benzer her türlü araçla üretilen, gönderilen, alınan veya saklanan bilgi"dir. Elektronik veri değişimi; "bir bilginin, üzerinde mutabakata varılan standartlara uygun olarak, bir bilgisayardan diğerine elektronik olarak transferi" olarak tanımlanmaktadır (UNCITRAL Elektronik Ticaret Model Kanunu m.1 b).

[207] Martínez Nadal / Ferrer Gomila, **UNCITRAL Model Law**, s.232; Yaltı Soydan, **E-imza II**, s.157.

b) imza oluşturma verisinin imzalama anında yalnızca imzalayanın hakimiyetinde olması,

c) imzalama anından sonra, elektronik imzadaki herhangi bir değişikliğin tespit edilebiliyor olması,

d) imzanın hukuken şart koşulmasının amacının ilişkin olduğu verinin bütünlüğünün teminini sağlamak olduğu durumlarda, imzalama anından sonra bu bilgideki herhangi bir değişikliğin tespit edilebilir olması gerekmektedir.

Bu madde ile elektronik imzanın el yazısıyla imzaya denkliği dört objektif şarta bağlanmaktadır. Bu şartlar Avrupa Birliği Direktifi'nde düzenlenen gelişmiş elektronik imzanın şartlarına paraleldir[208]. Hangi teknoloji ile yerine getirilirse getirilsin, bu şartları haiz bir elektronik imza el yazısıyla imzaya hukuki etkileri itibariyle eşit kabul edilecektir[209]. Kanun kullanılan elektronik imza tekniğinin güvenilir olup olmadığını takdir etme konusunda hakime yetki verdiğinden, buna göre elektronik imzadan yararlanan tarafın onun güvenilir olduğunu ispat etmesi gerekecektir[210].

Model Kanun ile elektronik imzanın hukuki etkileri kabul edilirken, elektronik imza kullanılma zorunluluğu getirilmemektedir. Bu açıdan hiç kimse elektronik bir belgeyi ve elektronik imzayı kabul etmek zorunda değildir[211]

2. Elektronik İmza Sisteminde Yer Alan Taraflar ve Yükümlülükleri

Uluslararası alanda genel bir mutabakat sağlamak ve teknolojik yenilikleri de kapsamak amacıyla, Model Kanun elektronik imza sisteminde yer alan tarafların her biri açısından yerine getirilmesi gereken özel yükümlülüğünün çerçevesini belirleyen asgari bir yaklaşım sergilemektedir. Bu yaklaşım gereğince, özen yükümlülüğünün ihlali halinde meydana gelecek zararlardan sorumluluğun türü, kapsamı ve sınırları

---

208 Martínez Nadal / Ferrer Gomila, **UNCITRAL Model Law**, s.232.

209 Martínez Nadal / Ferrer Gomila, **UNCITRAL Model L**aw, s.235; Yardım, **a.g.e**., s.28.

210 Özdemir Kocasakal, **a.g.e**., s.97.

211 Yaltı Soydan, **E-imza II**, s.157.

ise Model Kanun'da düzenlenmemekte, bu konuların çözümü taraf devletlerin ulusal hukukuna bırakılmaktadır.

a. İmza Sahibi ve İmza Sahibinin Yükümlülükleri

İmza sahibi, Model Kanun m.2 (d)'ye göre imza oluşturma verisini elinde bulunduran ve kendi adına veya temsil ettiği kişi adına davranan kişidir. Bu tanıma göre imza sahibinin gerçek veya tüzel kişi olması mümkündür[212].

İmza sahibinin yükümlülükleri Model Kanun'un 8. maddesinin 1. fıkrasında düzenlenmektedir. Bu maddede belirtilen yükümlülükler şunlardır:

a) İmza sahibi, imza oluşturma aracının yetkisiz kullanımını önlemek için gereken özeni göstermekle yükümlüdür. Bu yükümlülüğün kapsamı, taşınabilir araçlara ilişkin olarak fiziksel anlamda özenin gösterilmesini ve elektronik ortamda kayıtlı verilere erişimin engellenmesini içermektedir (m.8/1 a)[213].

b) İmza sahibi, imza oluşturma verisinin (yetkisiz kullanımına yol açacak şekilde) tehlikede olması veya tehlike doğurabilecek risklerin meydana gelmesi halinde, haklı olarak elektronik imzaya güvenebilecek kişileri ve elektronik imzayı desteklemek üzere hizmet sağlayan kişileri (sertifika sağlayıcılar) durumdan haberdar etmekle yükümlüdür (m.8/1 b).

c) Bir sertifikanın elektronik imzayı desteklemek için kullanıldığı durumlarda, sertifikada yer alan ve sertifikanın geçerli olduğu süre zarfında sertifika ile ilgili olarak sunduğu belgelerde yer alan bildirimlerin eksiksiz ve doğru olduğunu sağlamak için gereken özeni göstermelidir (m.8/1 c). Model Kanun'da belirtilmemiş olmakla birlikte sertifikada yer alan bildirimler, sertifika sahibinin kimlik bilgileri, mesleki bilgileri, adresi gibi bilgilerden

---

[212] Uygulama Kılavuzu'nda "kişi" kavramının herhangi bir ayrım yapılmaksızın tüm gerçek ve tüzel kişileri kapsadığı belirtilmektedir.

[213] Brazell, **a.g.e**., s.80.

oluşmaktadır[214]. İmza sahibinin yükümlülüğü bu bilgileri gerçeğe uygun ve tam bir şekilde iletmek ve herhangi bir değişiklik halinde sertifika sağlayıcının bundan haberdar olmasını ve sertifikadaki bilgilerin değiştirilmesini sağlamaktadır. Yoksa sertifikada yer alan bilgileri devamlı olarak kontrol etmek gibi bir yükümlülüğü bulunmamaktadır[215].

b. Sertifika Sağlayıcı ve Sertifika Sağlayıcının Yükümlülükleri

Model Kanun m.2'ye göre; "sertifika", imza sahibi ile imza oluşturma verisi[216] arasındaki bağlantıyı onaylayan bir veri mesajını veya diğer bir kaydı ifade eder.

Sertifika sağlayıcı, sertifikaları düzenleyen ve elektronik imzaya ilişkin diğer hizmetleri sağlayan kişidir. Bu tanım, sertifika hizmetlerinin sağlanmasına ilişkin faaliyet veren tüm kişi ve kuruluşları kapsamakta olup, sertifika hizmetinin ana faaliyet konusu olması ve devamlılık arz etmesi gerekliliğine ilişkin olarak bir sınırlama getirmemektedir.

Sertifika sağlayıcının sorumluluğunu doğuran sertifikanın imza sahibinin kimliğini belirleme ve doğrulama işlevi görmesidir. Model Kanun, diğer düzenlemelerden farklı olarak sertifikanın imza sahibinin kimliğini belirleme veya doğrulama işlevine sertifika tanımında yer vermemektedir[217].

Model Kanun m.9'da sertifika sağlayıcının yükümlülükleri düzenlenmektedir. Bu maddede belirtilen yükümlülüklerin, sertifika sağlayıcının, imzanın hukuki

---

[214] Brazell, **a.g.e**., s.80.

[215] Brazell, **a.g.e**., s.80.

[216] Bu tanımda geçen imza oluşturma verisi kavramı Model Kanun'da tanımlanmamaktadır. Uygulama Kılavuzu'nda Model Kanun'da geçen imza oluşturma verisinin elektronik imza oluşturma amacıyla kullanılan ve elektronik imza ile imza sahibinin kimliği arasında güvenli bir bağlantı kuran, gizli kriptografik anahtar gibi gizli anahtarları, kodları ve benzeri diğer unsurları ifade ettiği belirtilmektedir. İmza oluşturma verisi kavramının elektronik imza alt yapısına ilişkin olarak tanımlandığı yasal düzenleme AB Elektronik İmza Yönergesi'dir.

[217] Örneğin, Yönerge m.2'de yer alan tanıma göre, sertifika, imza doğrulama verisini bir kişiye bağlayan ve bu kişinin kimliğini doğrulayan elektronik belgedir.

etkilerini doğuracak nitelikteki bir elektronik imzaya destek verme amacıyla hizmet vermesi halinde yerine getirilmesi gerekmektedir (m.9/1). Bu maddede belirtilen yükümlülükler sırasıyla şunlardır:

a) Sertifika sağlayıcı işletme politikalarına ve uygulamaları hakkında yaptığı beyanlara uygun şekilde davranmalıdır. Sertifika sağlayıcı verdiği hizmete ilişkin vaatlerini yerine getirmekle yükümlüdür.

b) Sertifikada yer alan veya sertifikanın geçerli olduğu süre zarfında sertifika ile ilgili olarak sunduğu belgelerde yer alan bildirimlerin eksiksiz ve doğru olduğunu sağlamak için gereken makul özeni göstermelidir.

c) Sertifikaya güvenen tarafa, (i) sertifika sağlayıcının kimlik bilgileri, (ii) sertifikada tanımlanan imza sahibinin sertifikanın düzenlendiği tarihte imza oluşturma verisini hakimiyetinde bulundurduğu, (iii) sertifikanın düzenlendiği tarihte veya düzenlendiği tarihten önce imza oluşturma verisinin geçerli olduğu hususlarına ilişkin olarak; sertifika ile ilgili incelemelerde bulunmasına imkan sağlayacak erişim yollarını sağlamalıdır.

d) Sertifikaya güvenen tarafa, (i) imza sahibinin kimliğinin tespit edilmesi için kullanılan yöntemi, (ii) imza oluşturma verisinin veya sertifikanın kullanım amacına ya da değerine ilişkin olarak getirilen sınırlamaları, (iii) imza oluşturma verisinin geçerli olduğu ve güvenliğinin tehlikede olmadığı, (iv) sertifika sağlayıcı tarafından üstlenilen sorumluluğun kapsamı ve genişliğine ilişkin her türlü sınırlandırmaları, (v) imza oluşturma verisinin tehlikede olması halinde imza sahibi tarafından başvurulacak yöntemleri, (vi) iptal hizmetinin sunulup sunulmadığı bilgilerini gerektiğinde sertifikadan veya başka yerlerden edinebilmesi için uygun erişim yollarını sağlamakla yükümlüdür.

e) İmza oluşturma verisinin tehlikede olması durumunun imza sahibi tarafından bildirilmesine imkan veren yöntemleri sağlamalı ve gerektiğinde iptal hizmetinin verilmesini temin etmelidir.

f) Sertifika hizmetlerinin yerine getirilmesinde güvenilir sistemleri, uygulamaları ve insan kaynaklarını kullanmalıdır.

Model Kanun sertifika sağlayıcının yükümlülüklerini yukarıdaki gibi belirledikten sonra, bu yükümlülüklerin yerine getirilmemesi halinde hukuki sonuçlarının ne olacağına ilişkin bir düzenleme getirmemektedir. Model Kanun m.8/2'de yalnızca, sertifika sağlayıcının par.1'de belirtilen yükümlülükleri yerine getirmediği takdirde bundan doğan hukuki sonuçlara katlanacağı belirtilmekte, sorumluluğun türünün, kapsamının ve sınırlarının ne şekilde tayin edileceği taraf devletlerin ulusal hukukuna bırakılmaktadır[218].

c. Güvenen Taraf ve Güvenen Tarafın Yükümlülükleri

Model Kanun m.2 (f)'ye göre güvenen taraf (*relying party*), bir sertifikayı veya elektronik imzayı esas alarak hareket eden kişidir. Model Kanun'a göre güvenen taraf, yalnızca sertifikaya güvenen kişi olmayıp, sertifikaya dayalı olup olmadığı ayırt edilmeksizin elektronik imzaya güvenen kişiyi de kapsamaktadır[219].

Model Kanun m.11'e göre güvenen taraf; (a) elektronik imzanın güvenilirliğini araştırmak için gerekli davranışlarda bulunmalı ve (b) elektronik imzanın bir sertifika ile desteklenmesi halinde sertifikanın geçerliliğini, askıya alınma veya iptal durumunu araştırmalı, sertifikaya ilişkin herhangi bir sınırlamanın mevcut olup olmadığını kontrol etmelidir. Aksi takdirde meydana gelecek hukuki sonuçlara katlanması gerekmektedir. Bu şekilde Model Kanun m.11, sertifikaya veya elektronik imzaya güvenerek işlemde bulunan kişinin, söz konusu güveninin hangi koşullar altında haklı olarak değerlendirileceğini açıklığa kavuşturmuş olmaktaktadır[220].

---

[218] Martínez Nadal / Ferrer Gomila, **UNCITRAL Model Law**, s.241.

[219] Elektronik imzaya ilişkin düzenlemelerde güvenen taraf kavramına ilişkin bir tanım genellikle bulunmamaktadır (Martínez Nadal / Ferrer Gomila, **UNCITRAL Model Law**, s.235).

[220] Model Kanun m.11 bu yönüyle güvenen kişi açısından özen yükümlülüğü öngörmekle birlikte, bu yükümlülüğün tüketici konumundaki güvenen kişiler lehine daraltılması mümkündür. Bunun dayanağı uygulama alanını ticari faaliyetler olarak belirleyen ve tüketicinin korunmasına ilişkin

3. Yabancı Elektronik İmzaların ve Yabancı Sertifikaların Hukuki Etkisi

Model Kanun'un 12. maddesinde yabancı elektronik imzaların ve yabancı sertifikaların tanınması konusu düzenlenmiş bulunmaktadır. Buna göre, Model Kanun'un yürürlükte olduğu ülke dışında düzenlenen sertifikalar ve oluşturulan veya kullanılan elektronik imzalar eşit seviyede güven sağlamaları halinde, Kanun'un yürürlükte olduğu ülke içinde düzenlenen sertifikalar ve oluşturulan veya kullanılan elektronik imzalar ile eşit hukuki etkiye sahip olurlar (m.12/2 ve m.12/3)[221].

Yabancı sertifikaların veya elektronik imzaların eşit seviyede güven sağlayıp sağlamadığı kabul edilmiş uluslararası standartlara ve diğer ilgili faktörlere göre belirlenecektir (m.12/4). "Diğer ilgili faktörler" Model Kanun m.6, m.9 ve m.10'da belirlenen kriterlere uygunluk açısından değerlendirilecektir[222].

E. ELEKTRONİK İMZAYA İLİŞKİN İSVİÇRE, ALMANYA VE ABD'DEKİ DÜZENLEMELER

1. İSVİÇRE

İsviçre'de elektronik imza hakkında yapılan ilk hukuki düzenleme 1 Mayıs 2000 tarihli "Elektronik Sertifika Hizmetleri Hakkında Yönetmelik[223]"tir. Bu yönetmelikte dijital imza teknolojisi esas alınarak sertifika sağlayıcıların faaliyetleri düzenlenmiştir. 19.12.2003 tarihinde "Elektronik İmza Alanındaki Sertifika

---

kuralların yürürlüğünü saklı tutan Model Kanun'un 1. maddesidir. Detaylı inceleme için bkz. Martínez Nadal / Ferrer Gomila, **UNCITRAL Model Law**, s.235.

[221] Model Kanun m.12/1'e göre, yabancı bir elektronik imzanın veya sertifikanın hukuki etkiye sahip olup olmadığına karar verilmesinde aşağıdaki hususlar dikkate alınmamalıdır:

a) Sertifikanın düzenlendiği veya elektronik imzanın oluşturulduğu veya kullanıldığı coğrafi yer veya

b) Sertifikayı düzenleyenin veya imza sahibinin iş yerinin bulunduğu coğrafi yer.

Bu hükümde belli bir coğrafi yer dikkate alınarak, sertifikanın veya elektronik imzanın hukuki etkilerinin belirlenmesinde ayrım yapılmaması kurala bağlanmış olmaktadır: Brazell, **a.g.e**., s.84.

[222] Bkz. Uygulama Kılavuzu, par.158.

[223] *Verordnung über Dienste der elektronischen Zertifizierung (ZertDV)*. Yönetmelik'in metni için bkz. http://www.admin.ch/ch/d/as/2000/1257.pdf.

Hizmetlerine İlişkin Federal Kanun[224]" kabul edilmiş ve bu Kanun 01.01.2005 tarihinde yürürlüğe girmiştir. Kanun'da Tüzük'ten farklı olarak teknolojiden bağımsız bir yaklaşımla elektronik imza kavramı düzenlenmektedir. Elektronik imza, Avrupa Birliği Elektronik İmza Yönergesi'ndeki yaklaşıma paralel olarak basit elektronik imza (Art. 2 a), gelişmiş elektronik imza (Art. 2 b) ve nitelikli elektronik imza (Art. 2 c) şeklinde üç türe ayrılmaktadır. Bu kavramların tanımı unsurları itibariyle Yönerge'deki karşılıklarıyla örtüşmektedir.

Elektronik İmza Alanındaki Sertifika Hizmetlerine İlişkin Federal Kanun diğer bazı kanunlarda değişiklik yapılmasını öngörmüştür. Bu çerçeve Borçlar Kanunu'nun 14. maddesinde yapılan değişiklikle nitelikli elektronik imzanın el yazısıyla imzayla denkliği kabul edilmiştir.

Borçlar Kanunu'nun 59 (a) hükmünde yapılan değişiklikle özel bir düzenlemeye yer verilmiştir. Bu hükme göre, nitelikli elektronik sertifika sahibi olan imza sahipleri elektronik imza araçlarının yetkisiz kişilerce kullanılması sonucu üçüncü kişilerin uğramış oldukları zararlardan kusursuz olarak sorumlu tutulmaktadır.

Sertifika sağlayıcıların imza sahiplerine ve üçüncü kişilere karşı sorumluluğu konusu ZertES § 16 hükmünde düzenlenmektedir. Bu hükmün birinci fıkrasına göre sertifika sağlayıcıları Kanun'dan veya ikincil nitelikteki düzenlemelerden doğan yükümlülüklerine aykırı davranmaları dolayısıyla imza sahiplerinin ve nitelikli sertifikaya güvenen üçüncü kişileri uğradıkları zararlardan sorumludur. Hükmün ikinci fıkrasında hukuka aykırılık şartının ispat yükü tersine çevrilmektedir. Buna göre sertifika sağlayıcının söz konusu yükümlülüklerine yerine getirildiğini ispat ederek sorumluluktan kurtulması mümkündür.

---

[224] *Das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES), 19.12.2003*. Kanun'un metni için bkz. http://www.admin.ch/ch/d/sr/943_03/index.html.

2. ALMANYA

Almanya'da elektronik imzaya ilişkin ilk düzenleme 1997 tarihli Dijital İmza Kanunu'dur. Bu Kanun'da yalnızca dijital imza teknolojisini esas alan düzenlemeler getirilmiştir. AB Elektronik İmza Yönergesi'yle birlikte 16.05.2001 tarihinde teknolojiden bağımsız bir dille kaleme alınan ve Yönerge'de belirlenen temel esaslara uygun yeni bir Elektronik İmza Kanunu[225] ve bu Kanun'un 24. maddesine dayalı olarak düzenlenen Elektronik İmza Yönetmeliği[226] yürürlüğe girmiştir.

Alman Elektronik İmza Kanunu'nda basit elektronik imza, gelişmiş elektronik imza ve nitelikli elektronik imza olmak üzere üç elektronik imza türüne yer verilmektedir. Alman Medeni Kanunu'na eklenen 126a maddesinde, Kanun'da öngörülen yazılı şekil şartının elektronik şekil yoluyla gerçekleştirilebileceği, bunun için, imzalayanın ismini belirterek elektronik belgeyi nitelikli elektronik imza yoluyla imzalamasının gerekmekte olduğu hükme bağlanmıştır.

Kanun'da sertifika sağlayıcının yükümlülükleri ve elektronik imza araçlarının yerine getirmesi gereken şartlar ayrıntılı olarak düzenlenmektedir. Kanun'da ayrıca elektronik imza teknolojisinin yükseltilmesi amacına yönelik olarak akreditasyon sistemine yer verilmektedir. Akredite edilmiş nitelikli elektronik imzalar ile akredite edilmemiş olanlar arasında hukuki sonuçları bakımından bir farklılık öngörülmemektedir.

Sertifika sağlayıcıların sorumluluğu konusu SigG § 11 hükmünde, AB Elektronik İmza Yönergesi m.6'ya paralel olarak, kusuru ispat yükü tersine çevrilmiş bir haksız fiil sorumluluğu olarak düzenlenmektedir. Bu hükme göre, sertifika hizmet sağlayıcı, bu Kanun veya ilgili Yönetmelik hükümlerinin ihlali veya verdiği imza araçlarının ayıplı olması ya da diğer teknik güvenlik altyapısındaki eksikler

---

[225] *Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz –SigG).* Kanun'un metni için bkz. (Çevrimiçi) http://www.gesetze-im-internet.de/bundesrecht/sigg_2001/gesamt.pdf, 01.05.2011.

[226] *Verordnung zur elektronischen Signatur (Signaturverordnung - SigV)* Yönetmelik'in metni için bkz. (Çevrimiçi) http://www.gesetze-im-internet.de/bundesrecht/sigv_2001/gesamt.pdf, 01.05. 2011.

sebebiyle, nitelikli sertifikaya ya da nitelikli zaman damgasına güvenen bir üçüncü kişinin bu yüzden uğradığı zararlardan sorumludur.

3. AMERİKA BİRLEŞİK DEVLETLERİ

Amerika Birleşik Devletleri'nde elektronik imza hakkındaki kanunlar ilk önce eyaletler düzeyinde çıkarılmaya başlanmıştır. Elektronik imzaya ilişkin ilk düzenleme 1995 tarihli Utah Dijital İmza Kanunu'dur. Bu Kanun'u Kaliforniya Eyaleti tarafından çıkarılan elektronik imza kanunu izlemiştir. Utah Kanunu dijital imza teknolojisini esas alırken, Kaliforniya Kanunu teknolojiden bağımsız bir yaklaşım benimsemiştir. Bu gelişmeleri takip eden diğer eyaletlerin elektronik imza kanunlarında da teknolojiden bağımsızlık ilkesi esas alınarak tüm teknolojileri kapsayan düzenlemelere yer verilmiştir. Eyaletler düzeyinde çıkarılan kırk dokuz ayrı kanunda konuya ilişkin birbirinden farklı düzenlemeler getirilmiştir[227].

Bu gelişmeler takiben, eyaletler tarafından kabul edilen düzenlemelerin yerine geçecek olan Küresel ve Ulusal Ticarette Elektronik İmzalar Kanunu[228] 01.10.2000 tarihinde yürürlüğe girmiştir. Bu Kanun teknolojiden bağımsızlık ilkesine göre hazırlanmış olup, yeni teknolojilerin gelişim ve kullanımına olanak veren bir yaklaşım içermektedir.

Bu Kanunla birlikte elektronik ortamda yapılan sözleşmelerin, elektronik imzaların ve elektronik belgelerin hukuki etkisi ve geçerliliği genel olarak kabul edilmektedir (Sec. 101 (a) 1). Buna ek olarak irade serbestisi ilkesi (*party autonomy*) çerçevesinde hiç kimsenin bir sözleşmenin elektronik ortamda yapılmasına veya elektronik imza kullanımına zorlanamayacağı belirtilmektedir (Sec 101 (a) 2).

Kanun veya başka bir hukuk kuralının, sözleşme veya belgenin kağıt üzerinde yazılı olmasını emrettiği durumlarda, sözleşme veya belgenin elektronik şekilde

---

[227] Smedinghoff / Bro, **Electronic Signature Legislation**, (Çevrimiçi) http:// library.findlaw. com/1999/Jan/1/241481.html, 12.03.2010.

[228] *Electronic Signatures in Global and National Commerce Act* (E-Sign Act). Kanun'un metni için bkz. (Çevrimiçi) http://www.ftc.gov/os/2001/06/esign7.htm, 12.03. 2010.

olması, sonradan başvurulmak üzere tüm taraflar ya da kanun veya diğer bir hukuk kuralı tarafından belgeye ulaşmaya yetkili kılınmış olan diğer kişiler tarafından, saklanmasına ve tam ve doğru olarak kopyalanmasına elverişli değilse, söz konusu belgenin yasal etkisinin, geçerliliğinin ve cebri icra kabiliyetinin göz ardı edilebileceği belirtilmektedir (Sec. 101 e).

İKİNCİ BÖLÜM

TÜRK HUKUKUNDA ELEKTRONİK İMZANIN DÜZENLENİŞ TARZI VE HUKUKİ İŞLEMLERİN GEÇERLİLİK ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARI

I. TÜRK HUKUKUNDA ELEKTRONİK İMZANIN DÜZENLENİŞ TARZI

Türk hukukunda elektronik ortamda kurulan sözleşmeler bakımından Borçlar Kanunu hükümlerinin yetersizliği yazılı şekil şartının elektronik ortamda sağlanması konusunda ortaya çıkmıştır[229]. Elektronik ortamda kurulan sözleşmelerin geçerliliği konusunda, şekil serbestisi ilkesi elektronik ortama uyum sağlarken, bu kuralın istisnasını oluşturan şekle tabi sözleşmeler önemli bir sorun teşkil etmiştir. Aynı sorun ispat şeklinin arandığı durumlarda da söz konusu olmuştur. Teknolojik gelişmeler nedeniyle ortaya çıkan bu boşluğun, el yazısıyla imzayla aynı işlevleri gerçekleştiren bir elektronik imza tekniğinin[230] kullanılması yoluyla doldurulmasına,

---

[229] Hatice Özdemir Kocasakal, "Elektronik Sözleşmeler", **GSÜHFD**, S.1, 2006, s.49-53, s.49.

[230] Türkiye'de elektronik imza konusunda herhangi bir yasal düzenleme bulunmazken, bazı ticari kuruluşlar kendi iç bünyelerinde dijital imzayı kullanmışlardır. Örneğin bir banka internet şubesini kullanarak işlem yapan müşterilerine işlem bilgilerini dijital imzalı dekont şeklinde göndermekteydi: Leyla Keser Berber, "E-Sözleşme Bağlamında Dijital İmza ve ETKK Yasa Taslağı Açısından Türkiye'de Durum", **İnternet ve Hukuk**, ed. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2004, s. 49-64.

Bunun dışında Türk Sermaye Piyasası bakımından, elektronik iletişim araçlarının gelişmesi ve internetin oluşması ile birlikte Türk sermaye piyasasının bu gelişmelere uyum sağlaması ve Dünya sermaye piyasaları ile entegrasyonuna katkı sağlamak amacıyla 2499 sayılı Sermaye Piyasası Kanunu'nun 22. maddesinin Sermaye Piyasası Kurulunun başlıca görev ve yetkilerini düzenleyen (u) bendine 15.12.1999 tarihinde 4487 sayılı Kanun ile yapılan değişiklik ile şu hüküm eklenmiştir: "*İnternet de dahil, her türlü elektronik bilgi iletişim araç ve ortamı ve benzeri araçlar üzerinden gerçekleştirilen ihraç ve halka arzlar ile sermaye piyasası faaliyetleri ve işlemlerini; genel hükümler çerçevesinde bu Kanun kapsamına giren işlemlerde elektronik imza kullanım esaslarını düzenlemek ve denetlemek*". Sermaye Piyasası Kanunu'nda yapılan bu değişiklik ile 5070 sayılı Elektronik İmza Kanunu kabul edilmeden çok önce Türk mevzuatına elektronik imza kavramı girmiştir. Ancak bu tarihten sonra Sermaye Piyası Kurulu tarafından bu yönde bir çalışma

imzanın üzerine borç alan kimsenin el yazısıyla olmasını emreden BK. 14 II hükmü engel olmuştur[231].

Bu ihtiyaca cevap vermek, hangi elektronik imza tekniklerinin el yazısıyla imzayla aynı işlevleri yerine getireceğini yasal bir dayanağa kavuşturmak ve elektronik imzanın hukuki sonuçlarını düzenlemek amacıyla Elektronik İmza Kanunu hazırlanmıştır. Elektronik imzanın teknik altyapısının ve genel olarak hukuki etkilerinin Elektronik İmza Kanunu ile birlikte yasal bir dayanağa kavuşturulmasını takiben, Borçlar Kanunu, Hukuk Mukameleri Kanunu, Ticaret Kanunu başta olmak üzere, diğer kanunlarda da elektronik imza kullanımına ilişkin özel düzenlemelere yer verilmeye başlanılmıştır. Aşağıda Elektronik İmza Kanunu ve ilgili mevzuatta elektronik imzanın düzenleniş şekli genel esasları itibariyle incelendikten sonra, Türk hukuku bakımından elektronik imzanın uygulama alanını belirleyen bu temel nitelikli düzenlemelerde yer alan hükümlere özetle yer verilecektir.

A. ELEKTRONİK İMZA KANUNU VE İLGİLİ MEVZUAT

5070 sayılı Türk Elektronik İmza Kanunu (EİK.) 15.01.2004 tarihinde kabul edilerek 23.01.2004 tarihli ve 25355 sayılı Resmi Gazete'de yayımlanmış ve 25. maddesi gereği yayımından itibaren altı ay sonra yürürlüğe girmiştir. Elektronik İmza Kanunu'nun uygulanması ve nitelikli sertifika hizmetlerinin verilmeye başlanılması için ikincil nitelikteki yasal düzenlemelerin yapılması gerekmiştir. Bu amaçla Bilgi Teknolojileri ve İletişim Kurumu[232] tarafından hazırlanan "Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik" (EİY.) ve "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ" 06.01.2005 tarihinde, 25692 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu düzenlemelerin yürürlüğe girmesiyle birlikte sertifika hizmetlerinin

---

yapılmamıştır (Tamer Soysal, "Teknik ve Hukuki Açıdan Elektronik İmza", **Legal Hukuk Dergisi**, Mart 2006, s.697-733, s.721, dn.100). Bu konuda ayrıca bkz. s.69.

231 Şenocak, **a.g.e**., 134.

232 2813 sayılı Telsiz Kanunu'nda değişiklik yapan 27.1.2000 tarihli ve 4502 sayılı Kanun'la kurulan Telekomünikasyon Kurumu, 10.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu (RG 10.11.2008, sayı 27050 (Mükerrer) ile yeni bir düzenlemeye tabi olmuş ve adı "*Bilgi Teknolojileri ve İletişim Kurumu*" olarak değiştirilmiştir.

verilmesine ilişkin çalışmalar başlamış ve sonuç olarak bu hizmetlerin sunulmasına yönelik kuruluşlar faaliyete geçmiştir[233].

EİK. 1 hükümünde Kanun'un amacı, "*elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemek*" olarak ifade edilmektedir. Bu amacı gerçekleştirmek üzere getirilen düzenlemeler, "*elektronik imzanın hukukî yapısını, elektronik sertifika hizmet sağlayıcılarının*[234] *faaliyetlerini ve her alanda elektronik imzanın kullanımına ilişkin işlemleri*" kapsamaktadır (EİK. 2). Elektronik imzanın teknik yönleri ise daha detaylı olarak bu Kanun'a bağlı olarak çıkarılan Elektronik İmza Yönetmeliği'nde düzenlenmektedir.

EİK. 5 I hükmünde, güvenli elektronik imzanın el yazısıyla imza ile aynı hukuki sonucu doğuracağı belirtilmektedir. Bu hükme göre her tür elektronik imza el yazısıyla imzaya hukuken eşdeğer kılınmamış, yalnızca, el yazısıyla imzanın işlevlerini gerçekleştirdiği kabul edilen güvenli elektronik imzanın el yazısıyla imza ile aynı hukuki sonucu doğuracağı düzenlenmiştir. Güvenli elektronik imza kavramının yerine getirmesi gereken şartlar EİK. 4 hükmünde yer almaktadır. Güvenli elektronik imzanın en temel şartı bir nitelikli sertifiya dayanmasıdır. Nitelikli sertifikaya dayanması şartı başta olmak üzere, EİK. 4 hükmünde belirtilen diğer şartların da teknik olarak yerine getirilmesi sertifika sağlayıcılar tarafından üstlenilmektedir. Bu çerçevede, hukuken soyut bir anlam ifade eden güvenli elektronik imza kavramının uygulamadaki teknik karşılığının oluşturulması görevi sertifika sağlayıcıları tarafından üstlenilmiş olmaktadır.

---

[233] Elektronik imza ile ilgili mevzuatın yürürlüğe girdiği tarihten bugüne kadar geçen sürede Türkiye'de toplam dört sertifika sağlayıcı kurulmuştur. Bir ticaret şirketi olarak kurulan sertifika sağlayıcıları, faaliyete başladıkları tarih itibariyle, şunlardır: Elektronik Bilgi Güvenliği A.Ş. (24.06.2005), Türktrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (16.07.2005) ve EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (1.09.2006). Elektronik imza sertifikası hizmetini kamu kurumlarında vermek üzere oluşturulan TÜBİTAK-UEKAE (Kamu Sertifikasyon Merkezi) de 30.06.2005 tarihinden itibaren faaliyete geçmiştir.

[234] Elektronik İmza Kanunu'nda ve Elektronik İmza Yönetmeliği'nde "*elektronik sertifika hizmet sağlayıcı*" yerine "*elektronik sertifika hizmet sağlayıcısı*" ifadesi kullanılmaktadır. "*Sağlayıcı*" kelimesinin sonuna eklenen "-(s)ı" yapım eki dilbilgisi yönünden hatalıdır. Nitekim, bilişim hukuku alanındaki başka düzenlemelerde de doğru olarak "*içerik sağlayıcı*", "*yer sağlayıcı*", "*erişim sağlayıcı*" şeklindeki ifadeler tercih edilmektedir. Bu nedenle Kanun'un hatalı kullanımını benimsemeyerek, "*sağlayıcı*" ifadesini kullanmayı uygun görmekteyiz. Diğer yandan, Kanun'un "*elektronik sertifika hizmet sağlayıcısı*" şeklindeki uzun ifadesi yerine daha sade ve anlaşılır olması nedeniyle kısaca "*sertifika sağlayıcı*" ifadesini kullanmayı tercih ediyoruz.

Elektronik İmza Kanunu'nda sertifika sağlayıcıların yükümlülükleri detaylı bir şekilde düzenlenmekte ve bu yükümlülüklerin gereği gibi ifasını, dolayısıyla oluşturulan elektronik imzaların güvenliğini teminat altına almak üzere, sertifika sağlayıcıları ağırlaştırılmış bir hukuki sorumluluğa tabi tutulmaktadırlar. İmza sahibinin ve üçüncü kişinin yükümlülükleri konusuna ise Elektronik İmza Kanunu'nda yer verilmemekte, bu konunun düzenlenmesi Yönetmelik hükümlerine bırakılmaktadır.

Elektronik İmza Kanunu'nda ve buna bağlı olarak çıkarılan Yönetmelik'te elektronik imza kavramı ve unsurları teknolojiden bağımsız bir dil kullanılarak düzenlenmektedir. Ancak, bu düzenlemelere yakından bakıldığında, birçoğunun dijital imza teknolojisinin unsurlarını daha objektif bir dil kullanarak tanımladığı dikkati çekmektedir. Örneğin, EİK. 4 hükmünde şartları belirtilen güvenli elektronik imzanın gerçekteki karşılığı nitelikli sertifikaya dayanan dijital imza tekniği olarak ortaya çıkmaktadır[235]. Nitekim, Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan tebliğlerde dijital imza tekniği (açık ve gizli anahtar üretiminde kullanılacak algoritmalar gibi güvenlik unsurları bakımından) doğrudan düzenlenmektedir.

Teknolojiden bağımsız ifadeler kullanılarak, güvenli elektronik imzanın yerine getirmesi gereken işlevlere odaklanılmış olması, diğer teknoloji türlerinin bu doğrultuda geliştirilmesi açısından esnek bir tutum benimsendiğini göstermektedir. Diğer taraftan, elektronik imza uygulamaları açısından belirli bir güvenlik standardının oluşturulması amacıyla, günümüz uygulamasında hakim olan dijital imza tekniğinin özelliklerinin esas alınmış olması isabetlidir. Türk hukukunda elektronik imzaya ilişkin benimsenen bu düzenleme tarzı, teknolojiden bağımsızlık ilkesi uygulanırken karma yaklaşımının kabul edildiğini ortaya koymaktadır[236].

---

[235] Aynı görüşte: Kocayusufpaşaoğlu, **a.g.e**., s.291; Keser Berber, **E-Sözleşme Bağlamında Dijital İmza,** s.52 (Yazar bu görüşten hareket ederek Kanun'un adının "Dijital İmza Kanunu" olması ve dijital imza kavramına üstünlük tanınması gerektiğini ifade etmektedir).

[236] Teknolojiden bağımsızlık ilkesi ve karma yaklaşım hakkında değerlendirmeler için yukarıda bkz. s.26 vd.

B. BORÇLAR KANUNU

Elektronik İmza Kanunu'nun 22. maddesiyle Borçlar Kanunu'nun "İmza" başlıklı 14. maddesine şu hüküm eklenmiştir: "Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir"[237].

11.01.2011 tarihli ve 6098 sayılı yeni Türk Borçlar Kanunu[238] da bu değişikliklere paralel düzenlemeler öngörmektedir. Kanun'un 15. maddesinde, daha düzgün bir ifadeyle, güvenli elektronik imzanın el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğuracağı belirtilmektedir. Bu hükme ilave olarak BK. 14 II hükmü, kanunda aksi öngörülmedikçe, güvenli elektronik imza ile gönderilip saklanabilen metinlerin de yazılı şekil yerine geçeceğini düzenlemektedir.

Yürürlükteki ve yeni Borçlar Kanunu'nun güvenli elektronik imzaya ilişkin yukarıda belirtilen hükümlerinin hukuki işlemlerin geçerlilik şekli bakımından yarattığı sonuçlar aşağıda detaylı olarak incelenecektir.

C. HUKUK MUHAKEMELERİ KANUNU

12.01.2011 tarihli ve 6100 sayılı yeni Hukuk Muhakemeleri Kanunu (HMK.) elektronik imzalı belgelerin delil olarak incelenmesi ve ispat gücüne ilişkin önemli düzenlemeler getirmektedir[239]. Ayrıca Ulusal Yargı Projesi'nin çalışma usulleri düzenleyen hükmünde güvenli elektronik imzaya özel bir fonksiyon yüklemektedir.

HMK. 199 I hükmüne göre, elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları belge niteliğini haizdir. Adi senetlerin ispat gücünü düzenleyen HMK. 205 II hükmü, usulüne göre güvenli elektronik imza ile oluşturulan elektronik verilerin senet hükmünde olduğunu ifade etmektedir.

---

[237] Bu hükümde kullanılan ifadenin eleştirisi için bkz. s.114-115.

[238] RG 4.02.2011, sayı 27836.

[239] Hukuk Muhakemeleri Kanunu'nun 448. maddesine göre, bu Kanun hükümleri, tamamlanmış işlemleri etkilememek kaydıyla derhal uygulanacaktır.

Taraflarca delil olarak dayanılan elektronik belgelerin, kağıda dayalı ortamda çıktıları alınarak ve talep edildiğinde incelemeye elverişli şekilde elektronik ortama kaydedilerek mahkemeye ibraz edilmeleri gerekmektedir (HMK. 219 I). Hakim, mahkemeye delil olarak ibraz edilen elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen incelemekle yükümlü kılınmıştır (HMK. 205 III). Güvenli elektronik imzalı belgenin inkarı halinde ise, hakim veriyi inkar eden tarafı dinlendikten sonra bir kanaate varamadığı takdirde, bilirkişi incelemesine başvuracaktır (HMK. 210 I).

"*Elektronik işlemler*" başlıklı HMK. 445 hükmünde Ulusal Yargı Ağı Projesi (UYAP)'nin işleyişi düzenlenmektedir. UYAP, adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bir bilişim sistemidir. Dava ve diğer yargılama işlemlerinin elektronik ortamda gerçekleştirildiği hallerde UYAP kullanılarak veriler kaydedilir ve saklanır (HMK. 445 I). Bu madde uyarınca, elektronik ortamda, güvenli elektronik imza kullanılarak dava açılması, harç ve avans ödenmesi, dava dosyalarının incelenmesi mümkündür. Hukuk Muhakemeleri Kanunu kapsamında fiziki olarak hazırlanması öngörülen tutanak ve belgeler güvenli elektronik imzayla elektronik ortamda hazırlanabilir ve gönderilebilir. Güvenli elektronik imza ile oluşturulan tutanak ve belgeler ayrıca fiziki olarak gönderilmez, belge örneği aranmaz (HMK. 445 II).

Günümüzde elektronik devlet uygulamalarının en önde gelen uygulamaları arasında UYAP'ı göstermek mümkündür. UYAP kapsamında yer alan uygulamalar sayesinde hakim ve savcılar ile kalem personeli gerekli yazı ve kararlarını elektronik imza ile imzalamakta ve elektronik yolla gerekli mercilere göndermektedir. Avukatlar UYAP sistemini ve elektronik imzaları kullanmak suretiyle hukuk mahkemelerinde dava açma, icra takipi başlatma, mevcut davalarını takip etme imkanına sahiptir. Bunun yanı sıra vatandaşlar da haklarında açılmış davalarla icra takiplerini bu sistemden öğrenebilmekte ve davanın seyrini bu sistem üzerinden takip edebilmektedir[240].

[240] UYAP uygulamaları kapsamında Yargıtay'ın bazı daireleri dosyaların fiziksel olduğu kadar elektronik olarak da gönderilmesini istemekte ve üyeleri ilamlarını elektronik imza ile imzalayarak yerel mahkemelere göndermektedirler. Hakimler ve Savcılar Yüksek Kurulu'nun ve Adalet

D. TİCARET KANUNU

Halihazırda yürürlükte bulunan Türk Ticaret Kanunu'nun çeşitli hükümlerinde, 29 Mart 2011 tarihli ve 6215 sayılı "Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" hükümleri aracılığıyla, elektronik ortamdaki araçların kullanımına ilişkin olarak, güvenli elektronik imzayı da kapsayan birçok değişiklikler yapılmıştır. Bu değişiklikler 1 Temmuz 2012 tarihinde yürürlüğe girecek 6102 sayılı Yeni Türk Ticaret Kanunu'nunda yer alan düzenlemelere paralel niteliktedir. Böyle bir yönteme başvurularak e-devlet hizmetlerinin şimdiden uygulamaya konulmasının amaçlandığı anlaşılmaktadır.

Yeni Ticaret Kanunu'nda elektronik ortamdaki araçların kullanımına ilişkin pek çok düzenlemeye yer verilmektedir. Bunların bir bölümü Ticaret Kanunu'nda düzenlenen temel hukuki işlemlerin – örneğin, ihtar, ihbar ve beyanların yapılması (m.18), ticaret sicili kayıtlarına elektronik ortamda erişim (m.24), elektronik arşivleme (m.64 II), elektronik ortamda ticari defterin tutulması (m.64-65), cari hesap (m.94), elektronik ortamda kurullar (m.1527) – elektronik araçlar kullanılarak ne şekilde yapılacağını düzenlemektedir. Bunların yanı sıra yeni Ticaret Kanunu'nun bazı hükümleri elektronik ortamdaki araçların kullanımını zorunlu kılmaktadır. Örneğin, Kanun'un 1524 I hükmüne göre, her sermaye şirketi, bir internet sitesi açmak, şirketin internet sitesi zaten mevcutsa bu sitenin belli bir bölümünü, bu maddede belirtilen hususların (örneğin ticaret şirketlerinin birleşmesi, bölünmesi, tür değiştirmesi halinde, ortakların ve menfaat sahiplerinin incelemesine sunulan bilgiler, tablolar, belgeler; sermaye arttırımı, azaltılması dahil, esas sözleşme değişikliklerine ait belgeler, kararlar; imtiyazlı pay sahipleri genel kurulu kararları, menkul kıymet çıkarılması gibi işlemler dolayısıyla hazırlanan raporlar) yayımlanmasına özgülemek zorundadır.

Bakanlığı Teftiş Kurulu Başkanlıkları ile Bilgi İşlem Dairesi Başkanlığının ortak çalışmaları sonucu yakın zamanda mahkemeler, cumhuriyet başsavcılıkları ile diğer adalet dairelerinin denetimini UYAP üzerinden elektronik olarak gerçekleştirilmesi ve denetime ilişkin tüm raporların elektronik ortamda oluşturulması ve ilgili müfettişin elektronik imzasıyla imzalaması planlanmaktadır: Gürsel Orer, **Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu**, Ankara, Adalet Yayınevi, 2011, s.71.

Yeni Ticaret Kanunu'ndaki bu düzenelemelere paralel olarak, 6215 sayılı Kanun'la yürürlükteki Ticaret Kanunu hükümlerinde güvenli elektronik imzaya ilişkin yapılan değişiklikler şunlardır:

6215 sayılı Kanun'un 16. maddesiyle yürürlükteki Ticaret Kanunu'nun sonuna eklenen "*Çevrimiçi İşlemler*" başlıklı Ek madde 2 hükmünün I. fıkrasına göre; poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetler güvenli elektronik imza ile düzenlenemez. Bu senetlere ilişkin kabul, aval ve ciro gibi senet üzerinde gerçekleştirilen işlemler güvenli elektronik imza ile yapılamaz. Aynı maddenin II. fıkrasında konşimentonun, taşıma senedinin ve sigorta poliçesinin imzası elle, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla da atılabileceği düzenlenmektedir. Düzenlendikleri ülke kanunlarının izin verdiği ölçüde bu senetlerde yer alacak kayıtlar el yazısı, telgraf, teleks, faks ve elektronik diğer araçlarla yazılabilir, oluşturulabilir, gönderilebilir (EK madde 2 II son)[241].

Ek madde 2'nin III. fıkrasında, ticaret şirketleri ile gerçek ve tüzel kişi diğer tacirlere ilişkin olarak, bu Kanunun zorunlu tuttuğu bütün işlemlerin elektronik ortamda güvenli elektronik imza ile de yapılabileceği açıkça hükme bağlanmıştır. Bu işlemlerin dayanağı olan belgeler de aynı usulle elektronik ortamda düzenlenebilir. Zaman unsurunun belirlenmesi gereken ve yönetmelikte düzenlenen hallerde güvenli elektronik imzaya eklenen zaman damgasının tarihi, diğer hallerde merkezi veri tabanı sistemindeki tarih esas alınacaktır (TTK. Ek madde 2 III) .

Ek madde 2'nin IV. fıkrasında şirket adına imza yetkisini haiz kişilerin şirket namına kendi adlarına üretilen güvenli elektronik imzayla imza atabileceği belirtilmektedir. Bu durumda, kullanılacak nitelikli elektronik sertifikalarda sertifika sahibi alanı içerisine, sertifika sahibinin ismiyle birlikte temsil ettiği tüzel kişinin de ismi yazılacak ve bu husus tescil ve ilan edilecektir (Ek madde IV) . Ek madde 2'nin son fıkrasında bu maddenin uygulanmasına dair usul ve esasların Sanayi ve Ticaret Bakanlığınca çıkarılacak yönetmelikle düzenleneceği belirtilmektedir. Yeni Ticaret

[241] Bu konuda ayrıca bkz. s.117, dn.391.

Kanunu'nun "Güvenli Elektronik İmza" başlıklı 1526. maddesinde, Ek madde 2 hükmüne, aynı ifadeyle ve kapsamla yer verilmektedir.

Ticaret sicilinin tutulmasına ve ticaret sicili memurluğu teşkilatına ilişkin usul ve esasların bir tüzükle düzenlenmesini öngören "Nizamname" başlıklı TTK. 28 hükmünün II. fıkrasında, ticaret sicilinin elektronik ortamda tutulması imkanı dikkate alınarak, buna ilişkin usul ve esasların Sanayi ve Ticaret Bakanlığı tarafından çıkarılacak yönetmelikle düzenleneceği hükme bağlanmaktadır. Böyle bir sistemin kurulması halinde ticaret sicili kayıtlarına elektronik ortamda erişmek mümkün hale gelecektir. TTK 28 II hükmünde ticaret sicili kayıtları ile tescil ve ilan edilmesi gerekli içeriklerin düzenli olarak elektronik ortamda depolanan ve sunulabilen merkezi ortak veri tabanının, Sanayi ve Ticaret Bakanlığı ile Türkiye Odalar ve Borsalar Birliği nezdinde oluşturulacağı belirtilmektedir. Yeni Ticaret Kanunu'nun "Ticaret Sicili" başlıklı 14. maddesinin II. fıkrasında hüküm aynı şekilde muhafaza edilmiştir .

Sanayi ve Ticaret Bakanlığı, Türk Ticaret Kanunu'nun 28. maddesine böyle bir hüküm getirilmesinden yaklaşık bir yıl önce, Türk Ticaret Kanunu'nun 27. ve 274. maddelerine ve Sanayi ve Ticaret Bakanlığının Teşkilat ve Görevleri Hakkında Kanun'un 33. maddesine dayanılarak bir tebliğ yayımlanmıştır. "Merkezi Tüzel Kişilik Bilgi Sisteminin Oluşturulması Hakkında Tebliğ" başlıklı bu düzenlemede ticaret sicili memurlukları tarafından yapılan tescil, tadil ve terkin işlemlerine ilişkin kayıtların elektronik ortamda merkezi bir sistemde tutulmasına ve sicil işlemlerinin çevrimiçi ortamda yapılmasına ilişkin uygulamaların esaslarının belirlenmesi amaçlandığı (m.1) ve 2010 yılı itibariyle (ilk uygulaması 19.4.2010 tarihinde Mersin'de başlatılmak üzere) ticaret sicili kayıtlarının elektronik ortamda tutulmaya başlanacağı belirtilmektedir (m.5). Tebliğ'in 6. maddesinde, bir ticari işletme veya bir ticaret şirketi kurmak isteyen kişilerin, Bakanlıkça hazırlanan Merkezi Tüzel Kişilik Sistemine "www.icticaret.gov.tr" adresinden erişerek, her türlü kuruluş işlemlerine ilişkin başvuruları bu sistem üzerinden alınacak kullanıcı adı ve şifrelerini kullanarak veya güvenli elektronik imzanın kullanılması suretiyle gerçekleştirebileceği belirtilmektedir. Kuruluş dışındaki ticaret sicili işlemlerine

ilişkin başvurular ise (kullanıcı adı ve şifre alınması imkanı bulunmaksızın) sadece güvenli elektronik imzanın kullanılarak yapılacaktır (m.6).

Bunların yanı sıra Yeni Türk Ticaret Kanunu'nda yer alan güvenli elektronik imzaya ilişkin bazı özel düzenlemeler şunlardır: Kanun'un 18. maddesine göre, tacirler arasında, diğer tarafı temerrüde düşürmeye, sözleşmeyi feshe, sözleşmeden dönmeye ilişkin ihbarlar veya ihtarlar noter aracılığıyla, taahhütlü mektupla, telgrafla veya bunların yanında güvenli elektronik imza kullanılarak kayıtlı elektronik posta sistemi ile de yapılabilecektir. Aynı şekilde her takvim yılının sonunda hesap devresinin kapatılması ve artan bakiyenin belirlenmesine ilişkin 94. maddede, saptanan artan tutarı gösteren cetveli alan tarafın, aldığı tarihten itibaren bir ay içinde, noter aracılığıyla, taahhütlü mektupla, telgrafla veya güvenli elektronik imza içeren bir yazıyla itirazda bulunmamışsa, bakiyeyi kabul etmiş sayılacağı belirtilmektedir.

E. DİĞER KANUNLARDA YER ALAN DÜZENLEMELER

2499 sayılı ve 28.07.1981 tarihli Sermaye Piyasası Kanunu'na[242], 15.12.1999 yılında yapılan değişiklikle Sermaye Piyası Kurulu'nun görev ve yetkilerini düzenleyen 22. maddeye (u) bendi eklenmiştir. Bu hükme göre, sermaye piyasası kurulu genel hükümler çerçevesinde bu Kanun kapsamına giren işlemlerde elektronik imza kullanım esaslarını düzenlemek ve denetlemekle yetkilidir.

Sermaye Piyasası Kurulu tarafından hazırlanan, 30/5/2009 tarihli ve 27243 sayılı Resmi Gazete'de yayımlanan VIII/61 sayılı Bilgi, Belge ve Açıklamaların Elektronik Ortamda İmzalanarak Kamuyu Aydınlatma Platformuna Gönderilmesine İlişkin Esaslar Hakkında Tebliğ'in 3 üncü maddesinde değişiklik yapan Tebliğ 1 Nisan 2011 tarih ve 27892 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu değişiklik ile yatırım fonlarının her türlü bilgi, belge ve raporlarının elektronik ortamda imzalanması ve Kamuyu Aydınlatma Platformu kullanılarak kamuya

[242] RG 30.07.1981, sayı 17416.

açıklanması sağlanacaktır. Bu şekilde kamuyu aydınlatmanın daha etkin bir şekilde yapılmasının yanı sıra, yatırım fonlarının ilanlarına ilişkin maliyetlerin azaltılması ve yatırım fonları için de periyodik raporlara merkezi bir sistemden ulaşılmasını sağlayan bir yapının kurulması amaçlanmaktadır.

Hükümet tarafından 11.03.2010 tarihinde TBMM'ye sevk edilen "*Kamu Hizmetlerinin Hızlandırılması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı*" ile elektronik devlet uygulamalarının yaygınlaştırılması planlanmakta, bu çerçevede güvenli elektronik imzanın uygulama alanını büyük ölçüde genişleten hükümler öngörülmektedir[243].

Tasarı'nın 4. maddesi Tapu Kanunu'da değişiklik yaparak, tapu sicilinin elektronik ortamda tutulmasının önünü açmaktadır. Tasarı'nın getirdiği başka bir önemli değişiklik Noterlik Kanunu'na ilişkindir. Tasarı'nın 11. maddesine göre, güvenli elektronik imza ile yapılması kanunen yasaklanan hukuki işlemler saklı kalmak kaydıyla, noter huzurunda veya noter huzurunda olmadan yapılabilecek belirli noterlik işlemlerinin elektronik ortamda güvenli elektronik imza kullanılarak yapılabileceği düzenlenerek, söz konusu noterlik işlemlerinin neler olduğunun Adalet Bakanlığı'nın uygun görüşü alınarak Türkiye Noterler Birliği tarafından belirleneceği belirtilmektedir[244].

Bunun yanı sıra, 4077 sayılı Tüketicinin Korunması Hakkında Kanun çerçevesinde tüketici sorunları hakem heyeti kararlarının güvenli elektronik imza ile imzalanmasını öngörmekte ve güvenli elektronik imza altyapısına dayalı olarak işletilen "Tüketici Bilgi Sistemi" oluşturulmasını düzenlemektedir.

Tasarıyla, ayrıca, Ceza Muhakemesi, İdari Yargılama Usulü, İcra ve İflas Kanunlarında yapılacak değişikliklerle UYAP sisteminin çalışma esaslarının alt yapısının ve uygulama alanının yasal bir dayanağa kavuşturulması, ayrıca adli işlemlerde elektronik imza kullanımının yaygınlaştırılması hedeflenmektedir.

---

[243] Tasarı metni için bkz. (Çevrimiçi) http://www.basbakanlik.gov.tr/Forms/pDraftOfALaw.aspx, 10.06.2011.

[244] Bu konuda bkz. s.121-122 ve dn.410.

II. ELEKTRONİK İMZA

Elektronik imza kavramı EİK. 3 (b) hükmünde oldukça geniş şekilde tanımlanmaktadır: "*Elektronik imza başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*"dir[245].

Bu tanım AB Elektronik İmza Yönergesi'nin m.2/1 hükmünde yer alan tanımın Türkçe çevirisi niteliğinde olup, elektronik imza kavramına ilişkin asgari unsurları belirlemektedir. Bu tanımda verilen asgari unsurları yerine getiren elektronik imza türü basit elektronik imza olarak adlandırılmaktadır. Elektronik İmza Kanunu'nun genel gerekçesinde elektronik imza kavramının dijital imza ve biyometrik tanıma yöntemlerinin kullanımına olanak veren bir üst kavram olduğu belirtilmektedir[246].

Elektronik İmza Kanunu'nda, EİK. 3 (b) hükmünde belirtilen asgari unsurları taşıyan elektronik imza kavramına ilişkin olarak ikili bir ayrım yapılmaktadır: Güvenli elektronik imza ve güvenli elektronik imzanın özelliklerini taşımayan basit elektronik imza[247]. Güvenli elektronik imza olarak adlandırılan gelişmiş elektronik imza türünün şartları EİK. 4 hükmünde yer almaktadır. Basit elektronik imzanın asgari olarak EİK. 3 (b) tanımında yer alan şartları taşıması zorunlu olup, bunlara ek olarak başka gelişmiş işlevleri de yerine getirmesi mümkündür. Böyle bir ayrıma gidilmesi, elektronik imzanın hukuki sonuçlarının belirlenmesi bakımından önem

---

[245] Elektronik imza kavramı daha önce ETKK Hukuk Çalışma Grubu raporlarında şu şekilde tanımlanmıştır: "Bir bilginin, üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşmuş bir seti ifade eder". Bkz. Kubilay / Akıntürk, **a.g.e**., s.338. Bu tanım aslında birebir dijital imza tekniği örnek alınarak hazırlanmış, bu nedenle basit elektronik imzanın şartlarını ağırlaştıran bir tanımdır. Bununla birlikte EİK.3 (b)'de yer alan tanımla karşılaştırıldığında, el yazısıyla imzanın işlevlerine odaklanması ve sadeliği sayesinde daha hukuki bir ifadeye sahip olduğunu itiraf etmek gerekir.

[246] Teknolojik yapılarındaki farklılık nedeniyle dijital imza ve biyometrik imzanın aynı kanunda ve aynı hukuki sonuçları meydana getirmek üzere düzenlenmesinin mümkün olmadığı, Elektronik İmza Kanunu'nun esas itibariyle dijital imza tekniğini düzenlediği, bu nedenle biyometrik imzanın ayrı bir kanunda düzenlenmesinin gerekli olduğu görüşünde: Leyla Keser Berber, **Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi**, (Çevrimiçi) http://www.hukukcu.com/bilimsel/kitaplar/e_imza_ tasarielestiri.htm, 14.02.2011.

[247] EİK. 3 (b) hükmüne ilişkin madde gerekçesinde de elektronik imza kavramı bakımından Türk hukukunda ikili bir ayrım yapıldığı bu şekilde ifade edilmektedir.

taşımaktadır. Güvenli elektronik imza kural olarak hukuki sonuçları itibariyle el yazısıyla imzaya eş değer kılınırken (EİK. 5 I), basit elektronik imzaya, güvenlik seviyesi ne kadar gelişmiş olursa olsun, böyle bir sonuç bağlanmamaktadır.

Buna göre, EİK. 3 (b) hükmü çerçevesinde, basit elektronik imzanın iki ana unsuru bulunmaktadır. Birinci olarak, elektronik imzanın "*başka bir elektronik veriye eklenen*" veya "*başka bir elektronik veri ile mantıksal bağlantısı bulunan*" bir elektronik veri niteliğinde olması gerekmektedir. Elektronik veri, EİK 3 (a) hükmünde "*elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar*" olarak ifade edilmektedir[248]. İkinci olarak, bu şartları taşıyan bir elektronik verinin kimlik doğrulama amacıyla kullanılması gerekmektedir.

Başka bir elektronik veriye eklenme ifadesinin teknik olarak nasıl bir yapıya karşılık gelmek üzere kullanıldığı pek anlaşılamamaktadır. Çünkü elektronik ortamda meydana getirilen bir belgeyi oluşturan unsurlar arasında, el yazısıyla imza ile belge arasındaki fiziksel bağa benzer bir bağ bulunmamaktadır[249]. ***Mantıksal bağlantısı bulunması*** halinde de yine elektronik imza ile belgenin geri kalanı arasında fiziksel bağdan farklı nitelikte bir bağlantı bulunmaktadır. Bu halde elektronik imza, imza edilen metnin dahilindedir ve elektronik imza ile imza edilen metin bilgisayar tarafından tek bir belge olarak algılanmaktadır[250]. Bu iki koşuldan birini gerçekleştiren elektronik imzanın kendisinin de bir elektronik veri niteliğinde olması gerekmektedir (EİK. 3 b)[251].

Basit elektronik imza tanımının hukuki olarak önem taşıyan unsuru, elektronik imzanın ***"kimlik doğrulama amacıyla kullanılması"***nın şart olmasıdır[252].

---

[248] Kanun elektronik veri kavramını kullanılan yönteme ilişkin bir sınırlama yapmaksızın, teknolojik gelişmeler sayesinde gelişen yeni yöntemleri de kapsayak şekilde tanımlamıştır. Bu bakımından teknoloji tarafsız bir yaklaşım içermektedir. Aynı görüşte: Orta, **a.g.e**., s.94.

[249] Brazell, **a.g.e**., s.92.

[250] Brazell, **a.g.e**., s.92.

[251] Dijital imzanın bir elektronik veri değil şifreleme programı olduğu bu nedenle bu tanım kapsamına girmediği ifade edilmektedir. Bkz. Keser Berber, **Tasarı.**

[252] Öğretide basit elektronik imzanın biri maddi diğeri manevi nitelikte iki unsuru olduğu belirtilmiştir. "Başka bir veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan bir elektronik veri" oluşu elektronik imzanın maddi unsurudur. "Kimlik doğrulama amacıyla kullanılması ise manevi unsuru ifade etmektedir. Bkz.Yardım, **a.g.e**., s.57.

Kimlik doğrulama amacıyla kullanılması elektronik imzanın temel özelliğidir[253]. Çünkü bu şart, el yazısıyla imzanın, bir kişinin kimliğini belirlenebilir kılması dolayısıyla bir irade açıklamasını sahibine atfedilir kılan, bir beyanın kimden kaynaklandığını açıklayan yönünü ortaya koymaktadır. Kimlik doğrulama amacıyla kullanılması şartının aranması sayesinde, başka bir elektronik veriye eklenen veya mantıksal bağlantısı bulunan her elektronik veri bir basit elektronik imza sayılmayacaktır.

AB Elektronik İmza Yönergesi'nin İngilizce metninde yer alan "*authentication*" ifadesi[254] EİK. 3 (b)'ye "kimlik doğrulama" ifadesiyle aktarılmıştır.

"Kimlik doğrulama" ifadesinin basit elektronik imzanın unsurlarının belirlenmesi açısından soru işareti yarattığı belirtilmektedir. Bir görüşe göre, "*authentication*" ifadesine karşılık gelmek üzere EİK. 3 (b)'ye "kimlik doğrulama" şeklinde yapılan çeviri, aslında imza sahibinin kimlik bilgilerinin tespiti anlamındaki *"identification*" ifadesine karşılık gelmekte, "*identification*" şartı ise elektronik imza sayılabilmeye ilişkin daha yüksek bir kriter belirlemektedir. Gerçekten de kimlik

---

Bu karşılık elektronik imzanın üç unsuru olduğu görüşünde: Orta, **a.g.e**., s.39. Yazar, birinci olarak elektronik imzanın elektronik veriden ayrı olması ve ona eklenmesi, ikinci olarak eklendiği veriyle mantıksal bir bağlantı kurması, üçüncü olarak başka bir veriye eklenme ve mantıksal bağlantı kurulmasının kimlik doğrulama amacıyla yapılması şeklinde ayırdığı üç ayrı unsur tanımlamaktadır.

253 Bu tanımdan da anlaşılacağı üzere basit elektronik imza esas itibariyle kimlik doğrulama amacını taşımaktadır: Sanem Aksoy, "Borçlar Hukukunda Güvenli Elektronik İmza", **HPD**, S.5, 2005, s.252, s.254.

254 Buradaki "*authentication*" ifadesinin bir verinin doğruluğunun, bütünlüğünün, kaynağının ve bunun gibi özelliklerinin başka bir veri tarafından doğrulanması anlamındaki "veri doğrulama" (*data authentication*) olarak anlaşılması gerektiği ifade edilmektedir. Yani elektronik imzanın dayandığı tekniğin veri doğrulama işlevi görmesi gerekmekte, bu işlevin elektronik imza yaratmak ve imza edilen belgeyle hukuken bağlı olmak amacıyla kullanılması gerekmektedir. Elektronik ortamda doğrulama işlevini yerine getirmek üzere veri doğrulamanın yanı sıra, varlık doğrulama (*entity authentication*) yöntemi de kullanılmaktadır. PIN kodu girilerek elektronik ortamda banka hesabına bağlanılması varlık doğrulamaya örnek olarak verilebilir. (Böyle bir uygulama bir kimseye özel bir anahtar verilerek, kendisine istediği zamanlarda belirli bir ortama giriş yapabilmesi konusunda yetki verilmesine benzetilebilir.) Bu ayrım, varlık doğrulamaya yönelik teknik ve uygulamaların bir tür basit elektronik imza olarak kabul görmeyecek olması bakımından önem taşımaktadır. Çünkü bu esnada bir elektronik imza meydana getirilmiş olmayıp, yalnızca bir web sayfasına giriş kontrolü sağlanmaktadır. Diğer taraftan, aynı PIN kodunun internet üzerinden yapılan bir ödeme işlemini onaylamak maksadıyla kullanılması sırasında, veri doğrulama yönteminden yararlanılarak, bir tür basit elektronik imza meydana getirilmektedir. Dumortier / Kelm / Nilsson / Skouma / Van Ecke, **a.g.e**., s.29; Brazell, **a.g.e**., s.92.

bilgilerinin doğrulanması şartı, AB Elektronik İmza Yönergesi m.2/b hükmünde gelişmiş elektronik imzanın şartları arasında sayılmaktadır[255].

Bir görüşe göre, kanunumuzun benimsediği bu farklı tercih sebebiyle, basit elektronik imzanın imza sahibinin bilgilerini göstermesi gerekmektedir. Bu bakımdan hukukumuzda ABD hukukundan farklı olarak, örneğin internette sözleşmenin kabulü amacıyla "Tamam" ikonunun tıklanması elektronik imza kabul edilmeyecektir[256]. Başka bir görüş, AB Elektronik İmza Yönergesi'nde kullanılan "*authentication"* ifadesinin "kimlik tespiti" şeklinde anlaşılması gerektiğini belirtmektedir. Buna göre, EİK. 3 (b)'de yer alan "kimlik doğrulama" ifadesi kimlik tespitini de kapsayan daha geniş bir ifade içermekte, bu nedenle basit elektronik imzanın şartlarını ağırlaştıran bir yönü bulunmamaktadır[257].

AB Elektronik İmza Yönergesi'ndeki basit elektronik imza tanımında yer alan "*authentication*" deyimi bazı eserlerde "*ispat aracı*" olarak dilimize çevrilmektedir[258]. Bu çeviriyi benimseyen *Özdemir Kocasakal*'a göre, Yönerge'nin bu tanımı imzanın geleneksel işlevlerini içermemekte, sadece elektronik imzanın ispat aracı olarak kullanılacağını belirtmek suretiyle teknik bir anlam taşımaktadır. Bu ispat elektronik verilerin kaynağına, bütünlüğüne, servis sağlayıcı veya yazılım programı gibi diğer unsurlara ilişkin olabilir[259].

Kanaatimize göre, "kimlik doğrulama" ifadesinin lafzi yorumundan yola çıkarak, kanun koyucunun yalnızca imzalayanın kimlik bilgilerini ortaya koyan elektronik imza teknolojilerine üstünlük tanıyarak bunlara hukuki sonuç bağlamayı amaçladığı, bunun dışında kalanları basit elektronik imza kavramının dışında bıraktığı yargısına varılamaz. Öncelikle EİK. 3 (b) hükmünde "kimlik doğrulama" şartı değil, "kimlik doğrulama amacıyla kullanılma" şartı arandığı gözden

---

[255] Bu görüş için bkz. **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu**, s.23.

[256] Yardım, **a.g.e**., s.58.

[257] Erturgut, **a.g.e**., s.59

[258] Özdemir Kocasakal, **Elektronik İmza**, s.230.

[259] Özdemir Kocasakal, **Elektronik İmza**, s.230 ve dn.32. Öğretide "*authentication*" ifadesinin "ispat aracı" olarak Türkçeleştirildiği başka bir akademik çalışma için bkz. Kırçova / Öztürk, **a.g.e**., s.65.

kaçırılmamalıdır. Bu, imzalama ve bu şekilde belirli bir hukuki işlemle bağlanma iradesinin arandığını açıklığa kavuşturan bir şarttır. Bu nedenle, basit elektronik imza bir irade beyanını sonuçlandırmak ve bu beyanla bağlı kalmak amacıyla kullanılan teknolojilerinin tamamını kapsayacak şekilde mümkün olduğunca geniş yorumlanmalıdır. Kullanılan teknolojinin herhangi bir yöntemle bir irade beyanının ve bu irade beyanının kimden kaynaklandığını tespite imkan vermesi halinde, basit elektronik imzanın şartları yerine getirilmiş sayılacaktır[260].

Diğer taraftan, "ispat aracı" şeklindeki çevirinin, elektronik imzanın diğer teknik uygulamalardan ayırt edilebilmesine olanak veren imzalama niyetine ilişkin unsuru içermemesine rağmen, basit elektronik imzanın hukuki sonuçları itibariyle arz ettiği önemi açıklayan bir yönü bulunduğunu ifade etmek gerekir. Çünkü yürürlükteki mevzuatımızda basit elektronik imzanın önemi aslında yalnızca ispat hukuku açısından ortaya çıkmaktadır. Şöyle ki, basit elektronik imza, kimlik doğrulamayı sağlayabilir. Elektronik belgeye eklendiği veya onunla mantıksal bağlantısı kurulabildiği sürece o belgeye ilişkin olduğu sonucuna da varılabilir. Ancak bu sonuçlar, mutlak değildir. Basit elektronik imza verinin bütünlüğü veya belgeyi düzenleyenin kimliği konusunda bir garanti sunmamaktadır[261]. Kullanılan belirli bir basit elektronik imza teknolojisinin el yazısıyla imzadan beklenen işlevleri ne ölçüde yerine getirdiğinin her davada ayrı olarak incelenmesi gerekmektedir.

Elektronik imza teknikleri arasında bilgisayar ekranına atılan imza[262], tarayıcıdan bilgisayara aktarılan imza[263], ATM ve kredi kartlarının şifrelerinin elektronik ortamda bir hukuki işlemi sonuçlandırmak amacıyla kullanılması basit elektronik imzaya örnek olarak gösterilebilir. Basit bir elektronik postanın metnin sonuna isim yazılarak gönderilmesi işleminin dahi, kimden kaynaklandığı tespit edilebilir olduğu takdirde basit elektronik imza olarak kabul edilmesi mümkündür[264].

---

[260] EİK 3 (b)'deki bu tanımın elektronik imzaya mümkün olduğunca geniş bir anlam yüklediği ve teknoloji tarafsız bir yaklaşım benimsediği görüşünde: Orta, **a.g.e**., s.95

[261] Erturgut, **a.g.e**., s.61.

[262] Erturgut, **a.g.e.**, s.61-62

[263] Erturgut, **a.g.e.**, s.61-62, von Seck, **a.g.e.**, s.29.

[264] Amerika'da verilen bir mahkeme kararında bu iki örnek bir elektronik imza olarak kabul edilmiştir. Elektronik imzanın ayırt edici şartı bir metni imzalama iradesinin tespit edilebilirliği

Basit elektronik imza güvenli elektronik imzanın şartlarını gerçekleştirmeyen elektronik imza türlerinin tamamını kapsamaktadır. Bu bakımdan nitelikli sertifikaya dayanmayan bir dijital imza da basit imza olarak değerlendirilecektir[265].

III. GÜVENLİ ELEKTRONİK İMZA

A. GÜVENLİ ELEKTRONİK İMZA KAVRAMI

Türk hukukunda el yazısıyla imza ile aynı işlevleri gerçekleştirmek üzere tasarlanan elektronik imza türü güvenli elektronik imzadır. EİK. 5 I hükmüne göre, yalnızca güvenli elektronik imza niteliğini taşıyan elektronik imzalar el yazısıyla imza ile aynı hukuki sonucu doğuracaktır.

Bir elektronik imzanın güvenli elektronik imza niteliği taşıması için, EİK. 4 hükmüne göre;

a) münhasıran imza sahibine bağlı olması,
b) sadece imza sahibinin tasarrufunda bulunan "güvenli elektronik imza oluşturma aracı" ile oluşturulmuş olması,
c) nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlaması,
d) imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlaması gerekmektedir.

Türk hukukunda güvenli elektronik imza kavramı AB Elektronik İmza Yönergesi'nin 5. maddesinde tanımlanan "nitelikli elektronik imza" kavramına karşılık gelmektedir[266]. Yönerge'ye göre nitelikli elektronik imza, nitelikli sertifikaya

---

olarak ifade edilmektedir: Smedinghoff / Bro, **Electronic Signature Legislation**, (Çevrimiçi) http:// library.findlaw. com/1999/Jan/1/241481.html, 12.03.2010.

[265] Aksi görüşte: Yardım, **a.g.e**., s.6. Yazar, basit elektronik imzayı dijital imza yöntemi ile oluşturulamayan elektronik imzalar olarak tanımlamaktadır. Böyle bir tanım Elektronik İmza Kanunu'nun benimsediği sistemle örtüşmemektedir. Dijital imza bir hukuki kavram olmadığı gibi, nitelikli sertifikaya dayanmayan tek başına bir dijital imza da bir basit elektronik imzadır.

[266] Güvenli elektronik imzanın, Yönerge m.2'deki gelişmiş elektronik imzanın aynısı olduğu görüşünde: Sağlam, **a.g.e**., s.173. Yönerge'deki nitelikli elektronik imza kavramı için bkz. s.35. "*Güvenli elektronik imza*" terimine karşılık gelmek üzere, Alman Elektronik İmza Kanunu (SigG

dayanan, güvenli elektronik imza oluşturma aracı ile oluşturulmuş, bir tür gelişmiş elektronik imzadır. EİK. 4 hükmünde yer alan güvenli elektronik imza kavramı incelendiğinde, Yönerge'nin gelişmiş elektronik imza kavramının çatısı altında nitelikli elektronik imzanın şartlarını açık hale getirerek tanımlamakta olduğu tespit edilmektedir. EİK. 4 (a), (b) ve (d) bentlerinde yer alan şartlar gelişmiş elektronik imzanın şartlarının aynısıdır. Yalnızca (b) bendinde, gelişmiş elektronik imza tanımındaki "bir araç" ifadesi yerine "güvenli elektronik imza oluşturma aracı" ifadesi yerleştirilmiştir. Nitelikli sertifikaya dayanma şartı da (c) bendi olarak ilave edilmiş, böylelikle nitelikli elektronik imzanın şartlarının tamamı güvenli elektronik imza bakımından benimsenmiştir.

AB Elektronik İmza Yönergesi'nden farklı olarak, hukuki etkileri bakımından basit elektronik imzadan farkının bulunmaması nedeniyle gelişmiş elektronik imzaya Elektronik İmza Kanunu'nda ayrı bir maddede yer verilmemiş olması isabetli bir seçimdir. Elektronik İmza Kanunu el yazısı ile imzanın hüküm ve sonuçlarını doğurması amacıyla doğrudan güvenli elektronik imzayı düzenlemektedir[267].

EİK. 4 hükmünde belirtilen şartlar incelendiğinde, güvenli elektronik imza kavramının, el yazısıyla imzanın yerine getirdiği işlevlerin esas alınması suretiyle tanımlandığı görülmektedir[268]. El yazısıyla imzanın işlevlerini günümüzde en yakın şekilde gerçekleştiren elektronik imza tekniği dijital imzadır[269]. Zaten, teknolojiden bağımsız bir şekilde ifade edilmiş olmasına rağmen, güvenli elektronik imza oluşturma aracının şartları, imza oluşturma ve doğrulama verilerine ilişkin tanımlarla birlikte bir bütün olarak incelendiğinde, gerçekte bu kavramın nitelikli sertifikaya dayanan dijital imza tekniğini düzenlendiği açıkça tespit edilmektedir[270].

---

§2/3), İsviçre Elektronik İmza Kanunu (ZertEs §2 c) ve Avusturya Elektronik İmza Kanunu'nda (Signaturgesetz §2/3a) "*nitelikli elektronik imza*" (*qualifizierte elektronische Signatur*) terimi kullanılmaktadır.

267 Güvenli elektronik imzanın hukuki sonuçları hakkında bkz. s.112.

268 Özdemir Kocasakal, **Elektronik Sözleşmeler**, s.54.

269 Güvenli elektronik imza kavramının yorumunda dijital imza kavramı esas alındığı takdirde el yazısıyla imza ile aynı hukuki sonucu doğurması mümkün olacaktır: Özdemir Kocasakal, **a.g.e.,** s.101.

270 Aynı görüşte: Sözer, **a.g.e.**, s.1020. Güvenli elektronik imza belirli bir teknolojinin isim verilmeden fakat doğrudan temel alınmasıyla tanımlanmıştır: Mete Özgür Falcıoğlu, **Türk Hukukunda Elektronik Satım Sözleşmesi ve Kuruluşu,** Ankara, Yetkin Yayınları, 2004, s.96.

B. GÜVENLİ ELEKTRONİK İMZANIN GEÇERLİLİK ŞARTLARI

1. Münhasıran İmza Sahibine Bağlı Olması

Elektronik imzanın münhasıran imza sahibine bağlı olması şartı, imza oluşturma verisinin bir eşinin daha bulunmamasını ve tek bir kişiye özgülenmiş olmasını ifade eder[271].

İmza oluşturma verisi EİK. 3 d'ye göre; "*imza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri*" ifade eder. İmza oluşturma verisi kavramı Yönerge'den (m.2/4) alınmış, Türkçe'ye tercüme edilmiştir. Teknolojiden bağımsız bir ifadeyle tanımlanmış olmasına rağmen, gerçekte dijital imza tekniğinde kullanılan gizli anahtarı[272] karşılamakta olduğu, tanımında verilen örnekten (*kriptografik gizli anahtar*) de anlaşılmaktadır.

İmza oluşturma verisinin bir eşinin daha bulunmaması şartı, dijital imzada, gizli anahtarın teklik fonksiyonu olarak da ifade edilmektedir[273]. İmza oluşturma verisinin bir eşinin daha bulunmadığının mutlak olarak belirlenebilmesi, dünya üzerindeki bütün elektronik imza kullanıcılarına özgülenmiş bulunan imza oluşturma verilerinin karşılaştırması yoluyla mümkün olabilir. Böyle bir karşılaştırmanın yapılabilmesi uygulamada söz konusu değildir[274]. Bu sebeple imza oluşturma verisinin bir eşinin daha bulunmaması şartının gerçekleşmiş sayılması için, imza oluşturma verisinin teknik ve güvenlik kriterlerine uygun şekilde raslantısal olarak üretilmesi ve başka bir kişiye daha önce özgülenmemiş olduğunun bilinmesi yeterlidir[275].

---

[271] Erturgut, **a.g.e**., s.311.

[272] Dijital imzada gizli anahtar, genellikle harflerden ve rakamlardan oluşan karakterler diziliminden meydana gelen bir şifredir: Brazell, **a.g.e**., s.98.

[273] Erturgut, **a.g.e**., s.311.

[274] Brazell, **a.g.e**., s.98.

[275] Brazell, **a.g.e**., s.98.

İmza oluşturma verisi uygulamada sertifika sağlayıcı veya imza sahibi tarafından üretilmektedir[276]. İmza oluşturma verisinin üretilmesi ve imza oluşturma aracına kaydedilmesi sırasında, başkaları tarafından öğrenilmemesi ve kopyalanmaması konusunda gerekli tedbirlerin alınması gerekmektedir. Sertifika sağlayıcı dahi üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz (EİK. 10 II)[277].

İkinci olarak, *imza oluşturma verisinin münhasıran imza sahibine özgülenmiş olması* gerekmektedir. Bu şartın yerine getirilmesi için, bir eşi daha bulunmayan imza oluşturma verisinin, EİK. 6'da belirtilen nitelikleri haiz bir güvenli elektronik imza oluşturma aracında kayıtlı olarak, bir nitelikli sertifika aracılığıyla imza oluşturma verisiyle arasında bağlantı kurulan imza sahibine teslim edilmesi gerekmektedir[278]. Aslında bu şartın yerine getirilmesi güvenli elektronik imzanın aşağıda incelenecek EİK 4 (b) ve (c) hükümlerinde belirlenen diğer şartlarının tam olarak gerçekleştirilmesiyle doğrudan bağlantılı bir şarttır. Kullanılan aracın güvenli elektronik imza oluşturma aracı niteliği taşıması sayesinde imza oluşturma verisinin tek olduğu, başka bir kopyasının daha üretilemeyeceği ve yetkisiz kimselerce kullanılamayacağı şartları temin edilmekte, bu sayede güvenli elektronik imzanın münhasıran imza sahibine bağlı olduğu kabul edilebilmektedir. Diğer taraftan imza oluşturma verisinin tek bir kişiye özgülenmiş olduğu nitelikli sertifika aracılığıyla kamuya açıklanmaktadır[279].

Dijital imzada gizli anahtarın tek bir kişinin kontrolüne özgülenmesi, kriptografik güvenlikle ilişkilidir. Kriptografik güvenlik, diğer bir ifadeyle

---

[276] Mathias Hansen, **Die ausservertragliche Haftung von Zertifizierungsdiensteanbietern,** Hamburg, Verlag Dr. Kovač, 2008**,** s.47.

[277] Gizli anahtarın başkaları tarafından öğrenilmesinin engellenmesi için, anahtar çiftini üreten bilgisayar güvenli bir ortamda bulunmalı ve başka bilgisayarlarla veri alışverişini sağlayan bir bağlantısı bulunmamalıdır. Bilgisayarın bulunduğu ortama girişin güvenlik önlemleri alınmış kapılarla sağlanması gerekmektedir (Erturgut, **a.g.e**., s.94). Sertifika sağlayıcının anahtarın bir kopyasını aldığı, anahtarın kurtarılması (*key recovery)* adı verilen işlem hakkında bkz. s.150.

[278] Hansen, **a.g.e.**, s.129. El yazısıyla imzada el yazısının karakteristiği sayesinde yerine getirilen bu şart, elektronik imzada, imzanın ve imzalamada kullanılan araçların münhasıran imza sahibine bağlı olduğunun garanti edilmesi ile gerçekleşecektir (Sarıakçalı, **a.g.e**., s.74).

[279] Hansen, **a.g.e**., s.47. "*Münhasıran imza sahibine bağlı olma*" ifadesiyle elektronik sertifikaya işaret edilmektedir: Orta, **a.g.e**., s.104.

matematiksel güvenlik, gizli anahtarın üretiminde kullanılan algoritmaların, kırılıp kırılmadığına bağlıdır[280]. Algoritmaların kriptografik güvenlik açısından uygunluğu, Bilgi Teknolojileri ve İletişim Kurumu tarafından belirlenmektedir. Kurum tarafından hazırlanan ve 06.01.2005 tarihli ve 25692 sayılı Resmi Gazete yayımlanan *Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ*'in[281] 6. maddesinde imza oluşturma ve doğrulama verilerinin üretilmesinde hangi algoritmaların ve parametrelerin kullanılması gerektiği gösterilmektedir[282].

2. Sadece İmza Sahibinin Tasarrufunda Bulunan "Güvenli Elektronik İmza Oluşturma Aracı" ile Oluşturulmuş Olması

Güvenli elektronik imzanın ikinci şartı, sadece imza sahibinin tasarrufunda bulunan EİK. 6'da belirtilen şartları taşıyan güvenli elektronik imza oluşturma aracı kullanılarak oluşturulmuş olmasıdır.

Bir aracın güvenli elektronik imza oluşturma aracı niteliğinde olduğunun kabul edilebilmesi için, sertifika sağlayıcı tarafından münhasıran imza sahibinin tasarrufuna özgülenmiş olması ve yetkisiz kulllanımların engellenmesi için teknik ve güvenlik yönünden gerekli tedbirlerin alınmış olması gerekmektedir[283]. Bunun için güvenli elektronik imza oluşturma aracına PIN veya parola ya da biyometrik yöntemlere dayalı çalışan giriş kontrollerinin kurulması mümkündür[284]. Bu nitelikleri taşıyan bir güvenli elektronik imza oluşturma aracının imza sahibine teslim edilmesiyle "sadece imza sahibinin tasarrufunda bulunma" şartı yerine getirilmiş olacaktır.

---

[280] Erturgut, **a.g.e**., s.97.

[281] RG 18.06.2005, sayı 25849.

[282] Bu tebliğde belirtilen algoritmalar ve parametrelerin geçerlilik süresi, bunların üretilmesinde kullanılan teknik standartların güvenlik seviyesi dikkate alınarak, her yılın sonunda Bilgi ve İletişim Teknolojileri Kurumu tarafından yayımlanan tebliğler aracılığıyla uzatılmaktadır. 06.01.2005 tarihli bu tebliğde belirtilen algoritma ve parametrelerin geçerliliği, tekrar uzatılmadığı takdirde, 31.12.2011 tarihinde sona erecektir.

[283] Güvenli imza oluşturma aracının sadece imza sahibinin kontrolünde bulunması şartı, hem gizli anahtarın kayıtlı olduğu veri taşıyıcıları hem de imza programını işleten araçları kapsamalıdır: Erturgut, **a.g.e**., s.314.

[284] Giriş kontrollerinin elektronik imzanın kimlik tespiti işlevini yerine getirmesi bakımından önemi hakkında bkz. s.21.

İmza sahibinin bu aracı başkalarına kullandırmaması ve aynı şekilde bu konuda gerekli tedbirleri almış olması gerekmektedir (EİY. 15 e). Tahmin edildiği üzere, PIN veya parolanın klavye aracılığıyla girilmesi herhangi bir kişi tarafından yapılabilir. Uygulamada imza sahibinin güvenli elektronik imza oluşturma aracı niteliğindeki USB çubuğu ve parolasını bir başka kişiye vererek kendi adına imza atmasını istediği durumlarla çok sık karşılaşılmaktadır. Örneğin, bir şirkette, şirketi temsile yetkili bir çalışana ait elektronik imza aracı, bu çalışan dışında başka kişiler tarafından da kullanılarak (şirketi temsile yetkili çalışan imza sahibi olarak görülecek şekilde) şirket adına elektronik imza oluşturulmakta olabilir[285].

Prensip olarak, sertifika sağlayıcının güvenli elektronik imza oluşturma aracını imza sahibine özgülemiş olması, burada incelenen şartın gerçekleşmesi, dolayısıyla güvenli elektronik imzanın el yazısıyla imzanın hukuki sonuçlarını doğurması bakımından yeterlidir. İmza sahibinin kendi isteği ile başka bir kişiye USB çubuğu verdiği yukarıdaki gibi durumlarda, bu kişinin meydana getirdiği elektronik imzanın imza sahibinden sadır olduğu kabul edilecektir[286].

İmza oluşturma aracı genel olarak EİK. 3 (e) hükmünde tanımlanmaktadır. Bu hükme göre basit imza oluşturma aracı; *"elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını ifade eder"*. Akıllı kart, akıllı kalem, mobil telefon, PDA (*Personal Digital Assistant* – Dijital Özel Sekreter) veya bir bilgisayar sabit disk sürücüsü imza oluşturma aracının uygulamadaki örneklerinden bazılarıdır[287].

Güvenli elektronik imza oluşturma aracının taşıması gereken şartlar ise EİK. 6 hükmünde yer almaktadır. Bu hükme göre güvenli elektronik imza oluşturma araçları;

---

[285] Elektronik İmza Kanunu'nun yalnızca gerçek kişilerin imza sahibi olabileceğini düzenleyen EİK. 3 (c) hükmü dolayısıyla, maddi hukuktaki imza sahibi kavramından farklılaşan bir kavram yaratılmıştır. Nitelikli sertifikada bir gerçek kişinin bir tüzel kişiyi temsile yetkili olduğunun belirtildiği hallerde, imza sahibi EİK 3 (c) uyarınca gerçek kişi, adına ve hesabına hukuki işlemde bulunulan, diğer bir ifadeyle yapılan işlemin tarafı olan niteliki sertifikada temsil olunan olarak belirtilen tüzel kişidir. Güvenli elektronik imza kullanımında imza sahibi sıfatının belirlenmesi hakkında bkz. s.94.

[286] Güvenli elektronik imza oluşturma aracının üçüncü bir kişi tarafından kullanımı dolayısıyla ortaya çıkan hukuki sorunlar hakkında bkz. s.96 vd.

[287] Erturgut, **a.g.e**., s.313.

"a) Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamalıdır;

b) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini sağlamalıdır;

c) Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,

d) İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini sağlayan imza oluşturma araçlarıdır".

Bu şartlar Elektronik İmza Kanunu'na genel olarak AB Elektronik İmza Yönergesi Ek III'den alınmıştır. Burada, açıkça ifade edilmiş olmamasına rağmen, imza oluşturma verisinin teklik fonksiyonun ve belirli bir kişinin kontrolüne özgülenmesinin sağlanması için kayıtlı olduğu imza oluşturma aracının taşıması gereken özellikler düzenlenmektedir[288]. Aşağıda bu şartların amacı ve uygulamada neye karşılık geldiği özetle incelenenecektir.

a. Ürettiği İmza Oluşturma Verilerinin Kendi Aralarında Bir Eşi Daha Bulunmaması

EİK.6 (a) hükmünde imza oluşturma verisinin imza sahibi tarafından güvenli imza oluşturma aracı kullanılarak üretilmesi konusu düzenlenmektedir. Güvenli imza oluşturma aracının sertifika sağlayıcı tarafından imza sahibine teslim edilmesi halinde, bu aracın ürettiği imza oluşturma verisinin teklik fonksiyonunu yerine getirmesi sertifika sağlayıcı tarafından üstlenilmektedir.

Gizli anahtarın sertifika sağlayıcının hakimiyetindeki bilgisayarda üretilmesi halinde, görevli personelin yeterli özeni göstermemesi nedeniyle gizli anahtarın gizliliğinin ortadan kalkması, kopyalanması ve bir kopyasının saklanması riskleri

[288] Başka bir görüşe göre, burada düzenlenen dijital imza teknolojisine özgü gizli anahtar unsurudur: Yardım, **a.g.e**., s.65.

güvenlik açısından halen daha mevcuttur[289]. Bu nedenle gizli anahtarın üretiminin imza oluşturma aracı içinde yapılması ve oradan dışarı çıkmasının engellenmesi, başka bir ortamda üretilerek sonradan veri taşıyıcıya kaydedilmesi yöntemine göre, daha güvenlidir. Bu şekilde gizli anahtarın veri taşıyıcısı dışında başka bir ortamda belirli süreyle bulunması ve bu esnada kopyalanması tehlikesi engellenmektedir[290].

b. Üzerinde Kayıtlı Olan Elektronik İmza Oluşturma Verilerinin Araç Dışına Hiçbir Biçimde Çıkarılamamasını, Gizliliğini ve Bunların Üçüncü Kişiler Tarafından Elde Edilememesini, Kullanılamamasını ve Elektronik İmzanın Sahteciliğe Karşı Korunmasını Sağlaması

EİK.6 (b) ve (c) bentlerinde imza oluşturma verisinin tekliğinin ve gizliliğinin güvenli bir şekilde temin edilmesi, üzerinde kayıtlı olduğu imza oluşturma aracı dışına çıkarılmamasına ve hiçbir şekilde kopyalanamamasına bağlı tutulmaktadır. Bu amaca yönelmesi bakımından, bu iki hükmün tek bir başlık altında incelenmesinde sakınca görmemekteyiz.

Bu şartların sağlanabilmesi için bir akıllı kartın kayıtlı olduğu bir USB çubuk kullanılması önerilmektedir[291]. Bu veri taşıyıcıları günlük olarak elektronik verileri kaydetmek amacıyla kullanılan veri taşıyıcılarından farklıdır. Öncelikle elektronik imzanın oluşturulması, veri taşıyıcısında kayıtlı akıllı kart içinde gerçekleştirilmektedir. Bu şekilde gizli anahtar ve gizli anahtar kullanılarak oluşturulan *hash* değeri, akıllı kart dışına çıkmamaktadır. İşlem akıllı kart içinde gerçekleştirildiğinden, akıllı kartın takılı olduğu bilgisayarın merkezi işletim biriminin gizli anahtara erişimine ihtiyaç bulunmamaktadır. Akıllı kartın kendisi küçük bir bilgisayar niteliğindedir ve kendi içindeki yazılım programı sayesinde imzalama işlemini tek başına gerçekleştirmektedir.

Gizli anahtarın akıllı kartın dışına çıkmasının engellenebilmesi için bu kartın (günlük kullanımdaki veri taşıyıcılarının aksine) elektronik verilerin kopyalanması,

---

[289] Bkz. EİK. 10 II: "*Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz*".

[290] Erturgut, **a.g.e**., s.94.

[291] Geis, **a.g.e**., s.668.

kaydedilmesi ve okunmasına karşı korumalı olması gerekmektedir. Bu sayede taşıyıcı aracı ele geçiren bir kimse, bu aracın içinden akıllı kartı söküp çıkarsa dahi, bu kartta kayıtlı olan imza oluşturma verisini başka bir ortama kopyalayamayacaktır. Bu özelliğin yalnızca yetkisiz üçüncü kişilere kaşı değil, imza sahibine karşı da sağlanmış olması gerekmektedir[292]. Akıllı kartın bu özelliği donanım araçlarına bağlı olarak geliştirilen bir özelliktir. Sadece yazılım programlarından yararlanılarak bu özelliğin sağlanması mümkün değildir[293].

c. İmzalanacak Verinin İmza Sahibi Dışında Değiştirilememesi ve Bu Verinin İmza Sahibi Tarafından İmzanın Oluşturulmasından Önce Görülebilmesi

İmzalacak verinin, elektronik belgenin, imza sahibi dışında değiştirilememesi imza oluşturma verisine bağlı bir özelliktir. İmza oluşturma verisi mevcut teknolojiye göre aranan güvenlik standardına uygun olarak üretilmiş olmadır. Bilimin ve tekniğin o günkü durumuna göre ne kadar çaba gösterilirse gösterilsin, herkesçe bilinebilir açık anahtardan gizli anahtarın yeniden hesaplanması veya herhangi bir yolla şifrelemenin kırılması mümkün olmamalıdır[294].

Bununla birlikte, elektronik imza oluşturulmadan önce, imzalanmak istenen metin imza sahibi tarafından görülebilmeli, bunun için gerekli teknik bileşenler güvenli bir şekilde sağlanmalıdır[295]. Metnin imza sahibi tarafından görülebilmesinin el yazısıyla imzanın uyarı işlevinin elektronik imzada sağlanması bakımından önem taşımaktadır.

---

[292] Jörg aus der Fünften, **Die Haftung der Zertifizierungsstellen nach dem Signaturgesetz,** Münster, LIT Verlag, 2000**,** s.106.

[293] Geis, **a.g.e**., s.668.

[294] Hansen, **a.g.e**., s.47; Erturgut, **a.g.e**., s.47.

[295] İmza sahibinin ekranda gördüğü ve imzalamak istediği metin ile teknik olarak gerçekte imzaladığı metin birbirinden farklı olabilir. Bunu engellemek için imza usulünde kullanılan belgenin temsiliyle ilgili bileşenlerin güvenli olması gerekmektedir. Detaylı bilgi için bkz: Erturgut, **a.g.e**., s.95.

3. Nitelikli Elektronik Sertifikaya Dayanarak İmza Sahibinin Kimliğinin Tespitini Sağlaması

a. Genel Olarak

Güvenli elektronik imzanın şartlarından biri de nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlamasıdır (EİK. 4 c). EİK. 3 (ı) hükmüne göre; elektronik sertifika, "*imza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı*" ifade eder. Elektronik sertifika imza doğrulama verisi ile imza sahibi arasında bağlantı kurulması yoluyla kimlik tespitini sağlamaktadır. Bu bağlantının kurulması imza doğrulama verisinin, kimliği sertifika sağlayıcı tarafından tespit edilen kişiye özgülenmesi yoluyla olmaktadır[296].

Sertifika sağlayıcı tarafından düzenlenen nitelikli sertifikanın geçerliliği belirli bir süre ile sınırlıdır (EİK. 9 e). Bir sözleşmenin imza edildiği sırada nitelikli sertifikanın geçerli olup olmadığının belirlenebilmesi için nitelikli sertifikada zaman damgasının yer alması gerekmektedir[297].

Elektronik İmza Kanunu'nun kapsamı ve ilgili mevzuat incelendiğinde nitelikli elektronik sertifikanın sertifika sağlayıcı tarafından verilen, EİK. 9'da belirtilen bilgileri ihtiva eden ve Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'deki teknik şartları gerçekleştiren bir tür elektronik sertifika olarak düzenlendiği tespit edilmektedir.

---

[296] Erturgut, **a.g.e**., s.84. Bu niteliği ile elektronik sertifika, imza oluşturma verisinin imza sahibi olarak görünen kişiye ait olduğunu doğrulamaktadır: Sözer, **a.g.e.**, s.1014.

[297] Sertifikanın geçerlilik süresi içinde oluşturulmuş olan imza, bu sertifikanın geçerlilik süresi dolduğunda veya sertifika iptal edildiğinde geçersiz duruma düşecektir. İmza sahibinin belirteceği tarih bilgisi, imza sahibinin bu tarihi istediği şekilde belirlemesi mümkün olduğundan dolayı güvenli değildir. Bu noktada; imzada, imza tarihi dışında güvenilir bir zaman verisinin ve sertifikanın bu güvenilir tarihte geçerli olduğuna dair bir ispatın bulunmasının önemi belirginleşmektedir: Gonca Hülya Selçuk, **E-Devlet Uygulamaları için Elektronik İmza Formatları**, TÜBİTAK UEKAE Kamu Sertifikasyon Merkezi, (Çevrimiçi) http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/Makaleler/EDevletUygulamalariIcinElektronikImzaFormatlari.pdf, 08.03.2011. Aynı görüşte: Altınışık, **a.g.e**., s.88.

Nitelikli elektronik sertifikanın taşıması gereken bilgilerin neler olduğu EİK. 9'da düzenlenirken, bu bilgilerin sertifika sahibi ve elektronik imzaya güvenen üçüncü kişiler tarafından açıkça görülebilir olması amaçlanmaktadır[298].

EİK. 9'da belirtilen şartlar AB Elektronik İmza Yönergesi Ek II'ye paralel bir düzenleme içermektedir. EİK. 9'a göre nitelikli elektronik sertifikada bulunması gereken bilgiler şunlardır:

a) Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare,

b) Sertifika sağlayıcının kimlik bilgileri ve kurulduğu ülke adı,

c) İmza sahibinin teşhis edilebileceği kimlik bilgileri,

d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi,

e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri,

f) Sertifikanın seri numarası,

j) Sertifika sağlayıcının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası.

EİK. 9 hükmüne göre nitelikli sertifikada şu bilgilerin de yer alması mümkündür: Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi (EİK. 9 g)[299], sertifika sahibinin mesleki veya diğer kişisel bilgileri (EİK. 9 h)[300]

---

[298] Brazell, **a.g.e.**, s.94.

[299] Nitelikli sertifikada belirtilen temsil yetkisinin imza sahibi kavramının belirlenmesi bakımından ortaya çıkardığı sorunlar hakkında bkz. s.94.

[300] İmza sahibini üçüncü kişiyi temsil yetkisi ve mesleki bilgileri gibi kimlik bilgileri dışında kalan benzeri ek bilgilerin nitelikli sertifikaya bağlı ayrı bir sertifikaya kaydedilmesi imkanı bulunmaktadır. Uygulamada buna görev sertifikası (*attribute certificate – Attributzertifikat*) adı verilmektedir (Spiegelhalder, **a.g.e**., s.61; Hansen, **a.g.e**., s.47). Görev sertifikasına başvurulmasının amacı ana sertifikanın iptaline gidilmeksizin, bilgilerin güncellenmesini sağlamaktır. Kimlik bilgileri dışında kalan ek bilgilerin duruma göre yenilenmesi veya kaldırılması gerekebilir. Örneğin, üçüncü kişiyi temsil yetkisi açısından sertifikada değişiklik yapılması sıklıkla gündeme gelebilir. Üçüncü kişiyi temsil yetkisinin sona ermesi halinde, sertifikanın iptal edilmesi ve yeni bir sertifikanın üretilmesi gerekmektedir. Üçüncü kişiyi temsil yetkisinin görev sertifikasında belirtilmesi halinde sadece bu sertifikanın iptali yeterli olacaktır. Görev sertifikası sayesinde, ana sertifikanın iptaline veya değiştirilmesine gerek bulunmamaktadır (Torsten Spiegelhalder, **Rechtsscheinhaftung im Stellvertretungsrecht bei der Verwendung elektronischer Signaturen, Hamburg,** Verlag Dr. Kovač, 2007**,** s.61). Türk hukukunda görev sertifikası kanun veya yönetmelik hükümleriyle ayrıca düzenlenmiş değildir. Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan nitelikli sertifikaya ilişkin teknik kriterleri belirleyen rehberde (Bilgi Teknolojileri ve İletişim Kurumu 2007/DK-77/207 Sayılı ve 18.04.2007 Tarihli Kurul Kararı ve buna ek olarak çıkarılan Ek: Nitelikli Elektronik Sertifika, SİL ve OCSP İstek / Cevap Mesajları Profilleri) temsil yetkisinin, mesleki ve diğer kişisel bilgilerin sertifikaya bağlı bir

ve sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgiler (EİK. 9 ı). Bu bilgilerin nitelikli sertifikaya işlenmesi imkanı kabul edilmiş olmakla birlikte, nitelikli sertifikada bu bilgilerin yer alması zorunlu değildir[301]. Bunlar dışında kalan EİK. 9 hükmünde sayılan bilgilerin sertifikada bulunması ise nitelikli sertifika unusurunun gerçekleşmesi ve elektronik imzanın hukuken bağlayıcı bir etki doğurabilmesi için zorunludur[302]. EİK. 9 hükmünde belirtilen bilgileri ihtiva etmeyen bir elektronik sertifika nitelikli elektronik sertifika olarak kabul edilmeyecek ve bunun sonucu olarak, güvenli elektronik imzanın varlığından bahsedilemeyecektir[303].

Bir sertifikanın geçerli olabilmesi için imza sahibi adına düzenlenen nitelikli sertifikadan kök sertifikaya[304] kadar giden tüm sertifikaların geçerli olması gerekmektedir [305].

b. Nitelikli Sertifikanın Kullanım Alanı ve Kapsamına İlişkin Sınırlamaların Güvenli Elektronik İmzanın Geçerliliği Bakımından Etkisi

Nitelikli sertifikanın kullanılacağı işlemlere ilişkin getirilecek olan sınırlamalar, bu işlemlerin türü ve maddi kapsamı bakımından getirilecek sınırlamalar olmak üzere iki türlü olabilir. Elektronik İmza Kanunu'nda açıkça belirtilmemiş olmamakla birlikte, işlemin türü bakımından sınırlamaya gidilebileceği EİY. 15 (d) hükmünün ifadesinden anlaşılmaktadır. Öğretide, imza sahibinin nitelikli

---

eklentiye (özne dizin nitelikleri eklentisi) kaydedileceği gösterilmektedir. Bu ifadeden, belirtilen eklentinin bir tür görev sertifikası niteliğinde olup olmadığı anlaşılamamaktadır.

301 Sertifika esas itibariyle imza doğrulama verisi ile imza sahibinin "adı" arasında bağlantı kurmaktadır. Temsil yetkisi, mesleki yeterlilik belgesi, sertifikanın kullanımına ilişkin maddi sınırlamalar benzeri bilgilerin sertifikada bulunması zorunlu değildir: Hansen, **a.g.e**., s.47.

302 Hansen, **a.g.e**., s.49.

303 Sözer, **a.g.e.**, s.1015.

304 Kök sertifika kavramı hakkında bkz. s.178.

305 Gülen Çelebi Başçi, **Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi**, TÜBİTAK UEKAE Kamu Sertifikasyon Merkezi (Çevrimiçi) http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/Makaleler/Sertifika%20Gecerlilik%20Kontrolundeki%20Sorunlarin%20Giderilmesi.pdf, 28.05.2011.

sertifikada öngörülen sınırlamalara aykırı türde veya değerde bir işlemde bulunması halinde, böyle bir elektronik imzanın nitelikli sertifikada yer alan diğer bilgiler sayesinde yalnızca kimlik doğrulama işlevini yerine getireceği, bunun dışında geçerli bir güvenli elektronik imzanın varlığından söz edilemeyeceği ifade edilmektedir [306].

Güvenli elektronik imza kullanılarak imzalanan bir metinde yer alan irade beyanının içeriği, nitelikli sertifikada yer alan sınırlamalarla uyuşmadığı takdirde, söz konusu irade beyanı geçerli olarak hukuki sonuç doğurmaz. Başka bir ifadeyle el yazısıyla imzanın sonuçlandırma işlevi böyle bir durumda güvenli elektronik imza bakımından yerine getirilmiş olmamaktadır[307]. Bunun nedeni üçüncü kişiye karşı hukuken çelişkili bir görünüş yaratılmış olmasından kaynaklanmaktadır. Böyle bir çelişkinin varlığı halinde üçüncü kişinin elektronik imzanın yetkili imza sahibi tarafından kullanıldığına ilişkin olarak nitelikli sertifikaya haklı bir güveni bulunmamaktadır. Zira üçüncü kişinin kendisinden beklenen özen külfetini yerine getirerek nitelikli sertifikada yer alan bilgileri kontrol etmesi (EİY. 16) ve bu sınırlamaları irade beyanının içeriği ile karşılaştırması halinde, kendi başına güvenli elektronik imzanın yetkisiz bir kişi tarafından kullanıldığından şüphe duyacağı bir görünüş söz konusudur.

İmza sahibi nitelikli sertifikadaki sınırlamaları aşan bir teklif gönderirken, bu sınırlamaların beyan muhatabı üçüncü kişi açısından hüküm ifade etmeyeceğini açıkça belirtmiş dahi olsa, sözleşme sınırlamaları aşan değer üzerinden kurulamaz. Çünkü nitelikli sertifika imza sahibi tarafından değil, sertifika sağlayıcı tarafından hazırlanmakta ve sertifikada yer alan bilgilerin doğruluğu ve geçerliliği sertifika sağlayıcı tarafından üçüncü kişilere karşı garanti edilmektedir. Aksi bir yoruma başvurarak, imza sahibinin kendi iradesiyle sertifikadaki sınırlamaların etkisini

---

[306] Hans-Christoph Thomale, **Haftung und Prävention nach dem Signaturgesetz,** Baden-Baden, 2003, s.152; İnal, **a.g.e**., s.150-151. Uygulamada sertifikadaki sınırlamaların üçüncü kişiler tarafından istenirse dikkate alınabileceği şeklinde bir yaklaşım bulunmaktadır. Örnek için bkz. (Çevrimiçi) http://www.kamusm.gov.tr/tr/Urunler/Nes/, 10.03.2011. Oysa ki, yukarıda da belirttiğimiz gibi, nitelikli sertifikayı aşan değerdeki bir hukuki işlem irade beyanı ile nitelikli sertifikadaki kaydın uyumsuzluğu dolayısıyla geçersiz olacaktır. Bu nedenle, üçüncü kişi tarafından her zaman nitelikli sertifikadaki sınırlamaların kontrol edilmesi gerekmektedir.

[307] Aynı yönde: Stefanie Fischer-Dieskau / Gerrit Hornung, "Erste höchstrichterliche Entscheidung zur elektronischen Signatur", **NJW**, Heft 40, 2007, s. 2897 – 2899, s.2899.

bertaraf edebileceğini kabul etmek, nitelikli sertifikanın bu işlevini ortadan kaldırmak anlamına gelir.

Nitelikli sertifikadaki sınırlamalar, özellikle çalınma veya kaybolma gibi imza aracının imza sahibinin iradesi dışında elinden çıkmış olduğu hallerde imza sahibinin sorumluluğunun sınırlandırılması bakımından önem taşımaktadır[308]. Çünkü böyle bir durumda üçüncü kişinin nitelikli sertifikaya güveni koruma görmeyeceğinden, nitelikli sertifikadaki sınırlamaların aşan zararlardan ötürü, üçüncü kişi imza sahibinin sorumluluğuna başvuramayacaktır[309].

Diğer taraftan ticari hayatın doğurduğu ihtiyaçlar sebebiyle bazen bir nitelikli elektronik sertifikanın belirli kişilere karşı üzerinde yer alan sınırlamaları aşan bir şekilde kullanıldığı haller ortaya çıkabilir. Örneğin, (A) kendisine ait nitelikli sertifikayı 1000 lira değerindeki işlemlerle sınırlandırmış olmasına rağmen, bu sertifikaya dayanan elektronik imzasını kullanarak (B)'ye ara sıra 1000 lirayı aşan değerdeki bir sözleşme teklifleri gönderiyor ve (B) bu teklifleri kabul ediyor olabilir. Sertifikayı aşan kullanımların bu şekilde tekrarlanması halinde, nitelikli sertifikayla beyan arasındaki uyumsuzluğun bilmesine rağmen, (B)'nin bu sınırlamaların kendisi bakımından hüküm ifade etmediği düşüncesiyle nitelikli sertifikanın geçerliliğine ilişkin haklı bir güveni oluşabilir. Bu durumda hemen belirtelim ki, yine yukarıdaki gerekçeyle, elektronik imza geçerli bir hukuki sonuç doğurmayacak ve yazılı şekil şartı böyle bir elektronik imza kullanılarak tamamlanmış olmayacaktır. Ancak böyle bir ihtimalde şekle aykırılığın imza sahibi tarafından üçüncü kişiye karşı ileri sürülmesi hakkın kötüye kullanımı teşkil edecektir.

Alman Federal Mahkemesi'nin elektronik imza konusunda vermiş olduğu ilk karar, nitelikli sertifikadaki sınırlamaların elektronik imzanın geçerliliği bakımından yarattığı hukuki etkilere ilişkindir[310]. Bu kararda bir avukat adına düzenlenmiş ve 100 Euro değerindeki işlemlerle sınırlandırılmış olan bir nitelikli elektronik sertifika

---

[308] Fischer-Dieskau / Hornung, **a.g.e**., s.2897.

[309] Nitelikli sertifikadaki sınırlamaların sertifika sağlayıcının sorumluluğu bakımından etkisi hakkında bkz. s.204.

[310] Bu karar hakkında detaylı inceleme için bkz. Fischer-Dieskau / Hornung, **a.g.e**., s. 2897 – 2899.

inceleme konusudur. Karara konu olayda, avukatın açmış olduğu davanın masrafları 100 Euro'yu aştığından, ilk derece mahkemesi, elektronik imzanın geçersiz olduğunu ve bu durumda da aranan şekil şartının yerine getirilmemiş olduğunu ileri sürerek avukatın açtığı davayı dikkate almamıştır.

Alman Federal Mahkemesi, elektronik imzanın bir avukat tarafından dava açma amacıyla kullanılması halinde, nitelikli sertifikadaki parasal sınırlamaların bu işlemin geçerliliğini etkilemeyeceği gerekçesiyle, ilk derece mahkemesinin kararını bozmuştur. Federal Mahkeme bozma kararında nitelikli sertifikadaki sınırlamaların koruyucu etkisini dikkate alarak, bunların elektronik imzanın geçerliliğini ne şekilde etkileyeceğinin belirlenmesi gerektiği esasından hareket etmektedir. Buna göre, nitelikli sertifikadaki parasal sınırlamalar imza sahibinin malvarlığını doğrudan yükümlülük altında sokan borçlandırıcı işlemler (bir banka hesabından başka bir hesaba yapılan EFT işlemi gibi) açısından etki doğurmalıdır. Avukat bakımından ise dava harcının yatırılması avukatın malvarlığında değil, müvekkilin malvarlığında etki yaratacak niteliktedir. Bunun yanında, avukatın nitelikli sertifikasındaki parasal sınırın güvenli elektronik imzayı geçersiz kıldığının kabul edilmesi halinde, avukat davayı açamamakta ve müvekkiline karşı sorumluluğu ortaya çıkmaktadır. Böyle bir durumda nitelikli sertifikadaki sınırlama imza sahibi konumundaki avukatı koruyucu bir işlev görmemekte, bilakis onun aleyhine bir etki doğurmaktadır. Bu yaklaşım neticesinde, Federal Mahkeme bir avukat tarafından imzalanan dava dilekçesinin geçerliliği bakımından, avukatın elektronik imza sertifikasında yer alan maddi sınırlamaların hiçbir etki doğurmayacağına karar vermiştir. Mahkemeye göre böyle bir dilekçenin geçerli olmadığının ileri sürülebilmesi için avukatın nitelikli sertifikasında, dava açma yetkisinin bulunmaması gibi, işlemin türüne ilişkin bir sınırlamanın mevcut olması gerekmektedir[311].

[311] Fischer-Dieskau / Hornung, **a.g.e**., s.2898 vd.

c. Yabancı Elektronik Sertifikalar Bakımından Nitelik Elektronik Sertifikaya Dayanma Şartının Gerçekleştirilmesi

Uluslararası alanda ticari ilişkilerin kurulmasında elektronik ortam tarafların bir araya gelme mecburiyetini ortadan kaldırması bakımından avantaj yaratmaktadır. Bununla birlikte karşı karşıya gelmeyen ve farklı ülkelerin hukukuna tabi taraflar arasında güven temeline dayalı bir hukuki ilişkinin sağlanması güçtür. Nitelikli sertifika bu ihtiyaca cevap vermek üzere geliştirilmiş bir kavram olmasına rağmen, tüm dünyada üretilen nitelikli sertifikaların her zaman aynı standartları yerine getirmesi beklenemez. Yabancı sertifikaların geçerliliğine ve içerdiği bilgilerin doğruluğuna güvenin sağlanabilmesi, bunların Türkiye'de kurulu sertifika sağlayıcıları tarafından garanti edilmiş olmalarına bağlıdır[312].

Nitekim, EİK. 14 hükümde, yabancı bir ülkede kurulan bir sertifika sağlayıcı tarafından verilen elektronik sertifikaların Türk hukukuna göre geçerli kabul edilmesini öngören bir düzenleme getirilmektedir. Bu hükme göre, yabancı elektronik sertifikaların geçerlilikleri ve hukuki sonuç doğurabilmeleri milletlerarası anlaşmaların varlığına veya Türkiye'de kurulu bir sertifika sağlayıcı tarafından garanti edilmelerine bağlıdır.

İlk olarak EİK. 14 I yabancı bir ülkede kurulu bir sertifika sağlayıcı tarafından verilen elektronik sertifikaların hukuki sonuçlarının milletlerarası anlaşmalarla belirleneceğini ifade etmektedir[313]. İkinci olarak EİK. 14 II'ye göre yabancı bir ülkede kurulu sertifika sağlayıcı tarafından verilen elektronik sertifikaların, Türkiye'de kurulu bir sertifika sağlayıcı tarafından kabul edilmesi durumunda, bu elektronik sertifikalar nitelikli elektronik sertifika sayılacaktır[314].

---

[312] Altınışık, **a.g.e**., s.85; Keser Berber, **Dijital İmza**, s.530.

[313] Milletlerarası anlaşmalara ilişkin EİK. 14 I'deki bu düzenlemeyle ilgili olarak EİY. 32 I yabancı elektronik sertifikaların hukuki sonuçlarına ve hukuken kabul edilebilirliğine ilişkin şartların milletlerarası anlaşmalara göre belirleneceğini açıklamaktadır. Burada Kanun'un açıkça yapmış olmadığı bir tercihin Yönetmelik ile benimsenmesinin yetki aşımı teşkil ettiği konusundaki eleştiri için bkz. Sözer, **a.g.e.**, s.1017.

[314] Kanun'da yabancı elektronik sertifikaların Türk hukukuna göre geçerliliğinin sağlanması için başvurulabilecek seçenekler birbirinden bağımsız olarak tarif edilmiş olmasına rağmen, Yönetmelik Türkiye'de kurulu bir sertifika sağlayıcı tarafından yabancı elektronik sertifikaların

EİK. 14 II'ye göre Türkiye'de kurulu bir sertifika sağlayıcı tarafından kabul edilen sertifikalar, kendi ülkelerinde nitelikli elektronik sertifika niteliğini taşıyıp taşımadığına bakılmaksızın, Türk hukukuna göre EİK. 5 çerçevesinde nitelikli elektronik sertifikanın hukuki sonuçlarını meydana getirebilecektir[315]. EİY. 32 II'ye yabancı sertifikaların Türkiye'de kurulu bir sertifika sağlayıcı tarafından kabul edilmesi için asgari olarak şu şartların yerine getirilmesi gerekmektedir: a) Yabancı elektronik sertifika, Kanun'da ve bu Yönetmelik'te yer alan nitelikli elektronik sertifikanın teknik şartları taşımalıdır; b) yabancı sertifika sağlayıcı kurulu bulunduğu ülkede sertifika sağlayıcı olarak faaliyet göstermelidir[316].

Bu elektronik sertifikaların kullanılması sonucunda doğacak zararlardan, Türkiye'deki sertifika sağlayıcı da sorumlu olacaktır (EİK. 14 II). Her iki durumda da yabancı elektronik sertifikalar, Türkiye'de hukuki geçerliliği kabul edilen nitelikli elektronik sertifika ile aynı hukuki değere sahip olmaktadır.

4. İmzalanmış Elektronik Veride Sonradan Yapılan Değişikliğin Tespitini Sağlaması

Elektronik imza, imza oluşturma verisiyle oluşturulur ve imza doğrulama verisiyle doğrulanır. Elektronik imza bu şekilde elektronik ortamda hazırlanan metnin imza sahibinden sadır olduğunu, değiştirilmediğini, içeriksel bütünlüğünün sağlandığını belirlemeye yarar[317].

---

garanti edilmesi seçeneğini konuya ilişkin milletlerarası anlaşma bulunmaması şartına bağlamıştır: Sözer, **a.g.e.**, s.1017.

315 Orta, **a.g.e**., s.116.

316 EİY. 32'ye göre Türkiye'de kurulu bir elektronik sertifika hizmet sağlayıcı, kabul edeceği yabancı elektronik sertifika ile ilgili aşağıdaki belgeleri, sertifikaların kullanımına başlanmadan bir (1) ay önce Kuruma verir:

a) Elektronik sertifikalarını kabul edeceği yabancı elektronik sertifika hizmet sağlayıcının kendi sertifikasının örneği,

b) Yabancı elektronik sertifika hizmet sağlayıcının kurulu bulunduğu ülkede elektronik sertifika hizmet sağlayıcı olduğuna dair yetkili merciden alınmış belge,

c) Yabancı elektronik sertifikanın, Kanun ve bu Yönetmelikte yer alan nitelikli elektronik sertifikanın teknik şartlarını taşıdığına dair bilgi ve belgeler.

Kurum, yabancı elektronik sertifika hizmet sağlayıcıya ait bilgileri internet sayfasında yayınlar.

317 Erturgut, **a.g.e**., s.82.

EİK. 3 (f)'ye göre imza doğrulama verisi, "elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler"dir. İmza doğrulama verisi AB Elektronik İmza Yönergesi'nden (m.2/7) alınmış, Türkçe'ye tercüme edilmiştir. Teknolojiden bağımsız bir ifadeyle tanımlanmış olmasına rağmen, gerçekte dijital imza tekniğinde kullanılan açık anahtarı karşılamakta olduğu, tanımında verilen örnekten anlaşılmaktadır.

Dijital imzada açık anahtar gizli anahtara karşılık gelmekte ve gizli anahtar ile açık anahtar arasında matematiksel bir bağlantı bulunmaktadır[318]. Açık anahtar kural olarak herkesin erişimine açıktır, en azından dijital imzalı belgenin gönderildiği karşı tarafın erişimine açık olması gerekmektedir[319]. Açık anahtar imza oluşturulmasında değil, imza edilen metinde değişiklik yapılıp yapılmadığını kontrol amacıyla kullanılmaktadır[320]. Bu kontrol sonucunda değişkliğin tespit edilebilmesi için anahtar çiftinin birbiriyle uyumlu olarak kullanılabilir olması gerekmektedir[321].

Esas itibariyle imzalı metinde sonradan yapılan değişikliklerin tespiti sağlayan metnin şifrelenmesinde kullanılan *hash* usulüdür. *Hash* fonksiyonunun matematiksel özelliği sayesinde değişiklikler oluşturulan *hash* değerine yansımakta ve *hash* değerleri karşılaştırılak bu durum tespit edilebilir olmaktadır. Değişikliklerin güvenilir bir şekilde belirlenebilmesi için hash fonksiyonunun gereken güvenlik kriterine sahip olması gerekmektedir[322].

---

[318] Hansen, **a.g.e**., s.47

[319] Erturgut, **a.g.e**., s.81. Açık anahtar imza sahibi tarafından üçüncü kişiye bizzat iletilebileceği gibi, üçüncü kişi bu sertifika sağlayıcıdan da temin edebilir: İnal, **a.g.e**., s.142.

[320] Kontrol sonucu negatif çıkarsa o metnin gönderen kişiden kaynaklanmadığı veya metnin ya da dijital imzanın iletim sırasında değişikliğe uğradığı sonucuna ulaşılır. Açık anahtar gizli anahtara karşılık geliyorsa kontrol sonucu pozitif, karşılık gelmiyorsa negatif çıkar. Detaylı bilgi için bkz. Erturgut, **a.g.e**., s.81.

[321] Erturgut, **a.g.e**., s.81. İmza oluşturma ve doğrulama verilerinin birbiriyle uyumlu olarak kullanılabilmesi kriterinin sağlanmamış olması, AB Elektronik İmza Yönergesi m.6/c'de sertifika sağlayıcı açısından bir sorumluluk dayanağı olarak gösterilmektedir.

[322] Teorik olarak, iki ayrı metnin, aynı hash değerine sahip olması mümkündür. Sadece teoride olan bu tehlikenin pratikte önlenmesi, hash algoritmasının gücüne bağlıdır: Erturgut, **a.g.e**., s.324. Böyle bir durumda, metinde sonradan yapılan bir değişiklik tespit edilemeyecektir. Hash algoritmalarının güvenilirliği konusu, Bilgi Teknolojileri ve İletişim Kurumu tarafından çıkarılan 06.01.2005 tarihli ve 25692 sayılı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'e göre değerlendirilmektedir.

İmza doğrulama verilerinin uygulanması ve elektronik imzalı metnin değiştirilemediğinin tespiti imza doğrulama aracı kullanılarak gerçekleştirilmektedir. EİK. 3 (g) hükmü imza doğrulama aracını elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı olarak tanımlamaktadır[323]. Elektronik imzanın değiştirilmediğinin güvenilir bir şekilde tespit edilebilmesi için, üçüncü kişi tarafından güvenli elektronik imza doğrulama aracı kullanılması gerekmektedir (EİY. 16 b).

C. GÜVENLİ ELEKTRONİK İMZA KULLANIMINDA İMZA SAHİBİ SIFATININ BELİRLENMESİ

EİK. 3 (c) hükmüne göre imza sahibi "*elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi*" ifade eder[324].

EİK. 3 (c) hükmüne göre yalnızca gerçek kişiler imza sahibi olabilir. Tüzel kişilere imza sahibi olma imkanı tanınmamaktadır[325]. Hükmün elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanma şartını esas alan ifadesi basit elektronik imza bakımından yeterli kabul edilebilir. Güvenli elektronik imza kullanımı söz konusu olan hallerde ise, imza sahibinin, kendisine nitelikli sertifika aracılığıyla bir imza oluşturma verisi özgülenen kişi olarak anlaşılması gerekmektedir.

Borçlar hukukunun genel hükümleri çerçevesinde değerlendirildiğinde, Elektronik İmza Kanunu'nda düzenlenen imza sahibi kavramının, bir hukuki işlemle borç altına giren imza sahibi kavramıyla (BK. 14 I) örtüşmemediği haller ortaya

---

[323] Bu tanım AB Elektronik İmza Yönergesi m.2/8'de aynı ifadeyle yer almaktadır.

[324] İmza sahibi kavramına karşılık gelmek üzere, Kanun'da "*nitelikli elektronik imza sahibi*", "*nitelikli elektronik sertifika sahibi*", "*elektronik sertifika sahibi*" deyimleri bir arada kullanılmaktadır. Bu değişik kullanımların özel bir sebebe dayanıp dayanmadığı Kanun'dan veya gerekçe metninden anlaşılamamakta, Kanun'un özensiz bir dille kaleme alındığını düşündürmektedir.

[325] Bu düzenlemeyle tüzel kişilerin de imza sahibi olmasına imkan veren AB Elektronik İmza Yönergesi'nden ve UNCITRAL Elektronik İmza Model Kanunu'ndan farklılaşılmakta, Alman Elektronik İmza Kanunu'na paralel bir düzenleme getirilmektedir.

çıkabilir. Örneğin, EİY. 4 hükmünde bir tüzel kişiliğin çalışanları, müşterileri, üyeleri veya hissedarları adına nitelikli elektronik sertifika başvurusu (kurumsal başvuru) yapabileceği belirtilmektedir. Kurumsal başvuruda bulunan tüzel kişinin, çalışanları adına düzenlenecek nitelikli sertifikalarda temsil olunan olarak gösterilmeyi talep etmesi sıklıkla karşılaşılabilecek bir durumdur. Böyle bir kaydın nitelikli sertifikada yer alması halinde, çalışanın güvenli elektronik imzayı meydana getirmesiyle tüzel kişinin kaşesini kullanması arasında aslında hiçbir farklılık bulunmamaktadır. Güvenli elektronik imza kullanılarak yapılan hukuki işlemin tarafı konumundaki kişi çalışan değil tüzel kişidir. Kıyas yoluyla imza sahibinin de aslında çalışan değil tüzel kişi olduğu şeklinde yapılacak bir yoruma, yalnızca gerçek kişilerin imza sahibi olabileceğini öngören EİK. 3 (c) hükmü engel teşkil edecektir.

Sertifika sağlayıcı ile imza sahibi arasındaki hukuki ilişki taraflar arasında kurulan bir özel hukuk sözleşmesine dayanmaktadır. İmza sahibi uygulamada genellikle sözleşmenin karşı tarafı olarak ortaya çıkmakla birlikte, yukarıda belirtildiği şekilde, bir ticaret şirketinin sertifika sağlayıcı ile sözleşme yaparak çalışanları adına güvenli elektronik imza temin etmesi halinde, BK. 111 II çerçevesinde üçüncü kişi (imza sahibi) yararına tam sözleşme söz konusu olacaktır[326]. Üçüncü kişi yararına tam sözleşme olarak nitelendirmemizin sebebi, böyle bir sözleşmenin varlığı halinde, adına nitelikli sertifika düzenlenecek olan çalışanın Elektronik İmza Kanunu'na göre imza sahibi sıfatını taşıyacak ve bu sıfatına bağlı olarak tek başına çeşitli talepler (örneğin, sertifika iptal talebi) ileri sürebilecek olmasıdır.

[326] Böyle bir imkan bulunmakla birlikte, tezin bu kısmında karışıklığa yer vermemek bakımından sözleşmenin karşı tarafını işaret etmek üzere "*imza sahibi"* kavramını kullanacağız.

D. YETKİSİZ BİR ÜÇÜNCÜ KİŞİ TARAFINDAN OLUŞTURULMASININ GÜVENLİ ELEKTRONİK İMZANIN GEÇERLİLİĞİNE ETKİSİ

Birinci bölümde işlevsel denklik ilkesi incelenirken, elektronik imzanın kimlik tespiti işlevini, yalnızca biyometrik doğrulama yöntemlerinin kullanılması halinde, el yazısıyla imzayla eşit güçte yerine getirdiğinin kabul edilebileceğini belirtmiştik[327]. Biyometrik yöntemler dışında kalan bilgiye dayalı PIN veya şifre gibi yöntemlerden yararlanılması halinde ise, güvenli elektronik imza oluşturma aracının imza sahibi dışındaki kişiler tarafından kullanılması her zaman mümkündür. Böyle bir durumda imza sahibinin "imzalayan kişi ben değilim" şeklindeki bir iddiası gündeme gelebilecektir.

Yukarıda EİK. 4 (b) hükmünde geçerli bir güvenli elektronik imzanın varlığından söz edebilmek için aranan imzanın "*sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulması*" şartını incelemiştik[328]. İmza aracının imza sahibi dışında bir kişi tarafından kullanılması halinde, ortada geçerli bir güvenli elektronik imzanın bulunmadığı savunmak mümkün müdür? Bu hükmün yanı sıra, nitelikli sertifikaya güvenerek hukuki işlemde bulunan ve imza aracını kimin kullandığını bilebilecek durumda olmayan üçüncü kişi tarafından da konuya yaklaşıldığında, bu soruya kesin bir cevap vermek mümkün değildir. Çünkü, güvenli elektronik imza alt yapısı, esas itibariyle, kişilerin anonim bir şekilde hareket etmekte olduğu elektronik ortamda, nitelikli sertifika aracılığıyla güven unsurunu sağlamlaştırma amacına yönelik olarak yaratılmış bir kavramdır. Yalnızca EİK. 4 (b) şartının yorumundan hareket edilerek, üçüncü kişiye karşı yaratılan hukuki görünüşün sonuçlarının göz ardı edilmesi, güvenli elektronik imza kavramının ayırt edici unsuru olan nitelikli sertifikanın kimlik bilgilerini sergileyerek taraflar arasında güven sağlamaya yönelen işlevini yok saymak anlamına gelir. Bununla birlikte, EİK. 4 (b) hükmünün yorumu ile nitelikli sertifika kavramının bağdaştırılmaya çalışılması önemli sorunları beraberinde getirmektedir:

---

[327] Bu konuda bkz. s.22.
[328] Bkz. s.80 vd.

Akla gelen ilk ihtimal, imza sahibinin bir üçüncü kişiye imza aracını teslim etmesi ve üçüncü kişinin kendisine verilen yetkiye uygun olarak imza aracını kullanması halidir. Böyle bir durumda EİK. 4 (b) şartının yerine getirilmediği kabul edilerek, güvenli elektronik imzanın geçersiz olduğu savunulabilir mi? Temsil hükümleri kıyasen uygulanarak bu soruya olmusuz cevap verilmesi ve elektronik imzanın geçerliliğinin bundan etkilenmeyeceği sonucuna varılması mümkündür.

İkinci ihtimal, imza sahibinin imza aracının kendi isteğiyle bir üçüncü kişiye vermesi ve üçüncü kişi tarafından imza sahibinin verdiği yetki aşılarak bir işlemde bulunulması halidir. Ayrıca, imza aracının çalınma, kaybolma gibi imza sahibinin iradesi dışında çıkmış ve yetkisiz bir üçüncü kişi tarafından imza sahibi adına bir güvenli elektronik imza meydana getirilmiş olabilir. Bu şekilde, yetkisiz kimseler tarafından güvenli elektronik imza oluşturulması halinde, bu durumdan haberi olmayan üçüncü kişinin güveni ne ölçüde koruma görecektir? Beyan muhatabı konumundaki üçüncü kişinin güveninin hukuken korunması gerektiği kabul edildiği takdirde bunun hangi hukuki sebebe dayalı olarak gerçekleştirilebileceği meselesi ortaya çıkmaktadır. Bu ihtimallerde imza sahibi ve beyan muhatabı arasında bir sözleşmenin kurulduğu kabul edilebilir mi? İmza sahibinin imza anahtarını kimseye kullandırmamakla ve bu konuda gerekli tedbirleri almakla yükümlü kılınmış olmasına rağmen (EİY. 15 e), bu yükümlülüğünü tam olarak yerine getirmemesi, yani gerekli özeni göstermemesi dolayısıyla böyle bir kullanımın meydana gelmiş olması bu konuda nasıl bir etki doğuracaktır?

Bu soruların cevaplandırılmasında akla gelen çözümlerden ilki imza sahibinin üçüncü kişinin zararını haksız fiil hükümlerine göre karşılamakla yükümlü olmasıdır. İkinci çözüm, hukuki görünüşün korunması prensipleri çerçevesinde sözleşmenin kurulduğunun kabülü ve üçüncü kişi tarafından imza sahibinden ifa menfaatinin talep edilmesi şeklindedir. İsviçre hukukunda haksız fiil sorumluluğuna dayalı çözüm şekli benimsenirken, Alman hukukunda bu konuya ilişkin çalışmalarda hukuki görünüşe güvenin korunması prensibi esas alınarak çözüm önerileri getirilmektedir.

İsviçre Borçlar Kanunu'na, 1.1.2005 tarihinde yapılan bir değişiklikle, imza anahtarı sahibinin üçüncü kişilere karşı sorumluluğunu düzenleyen özel bir

sorumluluk maddesi (OR. 59a) eklenmiştir[329]. Bu hükme göre, imza anahtarı sahibi bir sertifika sağlayıcı tarafından düzenlenen geçerli bir nitelikli sertifikaya güvenen üçüncü kişilerin bu yüzden uğradığı zararlardan dolayı sorumludur[330]. İmza anahtarı sahibinin bu sorumluluktan kurtulabilmesi için, imza anahtarının yetkisiz olarak kullanılmasına engel olmak için, somut olaya göre alınması gereken ve kendisinden beklenen güvenlik tedbirlerini yerine getirdiğini inandırıcı bir şekilde ortaya koyarak, gerekli özeni göstermiş olduğunu ispat etmesi gerekmektedir[331]. Hakim, özen

---

[329] OR. 59a hükmünün Almanca ve Fransızca metinleri sırasıyla aşağıdaki şekildedir:

"F. Haftung für Signaturschlüssel

[1]Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des Bundesgesetzes vom 19. Dezember 2003 über die elektronische Signatur verlassen haben.

[2] Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.

[3] Der Bundesrat umschreibt die Sicherheitsvorkehrungen im Sinne von Absatz 2".

"F. Responsabilité en matière de clé de signature

[1] Le titulaire d'une clé de signature répond envers les tiers des dommages que ces derniers ont subis parce qu'ils se sont fiés à un certificat qualifié valable délivré par un fournisseur de services de certification reconnu au sens de la loi du 19 décembre 2003 sur la signature électronique.

[2] Le titulaire de la clé de signature est libéré de sa responsabilité s'il peut établir de manière crédible qu'il a pris les mesures de sécurité raisonnablement imposées par les circonstances pour éviter une utilisation abusive de la clé de signature.

[3] Le Conseil fédéral arrête les mesures de sécurité à prendre au sens de l'al. 2".

[330] İsviçre öğretisinde, OR 59a hükmünde düzenenlenen sorumluluğun bir tür basit sebep sorumluluğu (*einfache/milde Kausalhaftung*) olduğu görüşü (Roland Brehm, **Berner Kommentar, Band IV: Das Obligationenrecht, 1. Abt, 3.Teilband, 1. Urteilband Art.41-61 OR,** 3. Aufl., Bern, 2006, Art. 59a N.5) yanında, ispat yükü tersine çevrilmiş bir kusur sorumluluğu olduğu görüşü de savunulmaktadır (Andreas Furrer / Markus Müller-Chen, **Obligationenrecht Allgemeiner Teil**, 1. Aufl., Zurich, Schulthess, 2008, §12 N.76). Bir tür basit sebep sorumluluğu olduğu görüşü, kanunun imza sahibinin "somut olaya göre alınması gereken ve kendisinden beklenen güvenlik tedbirlerinin yerine getirdiğini" ispat ederek sorumluluktan kurtulmasının mümkün olduğunu öngören OR. 59a I hükmüne dayandırılmaktadır. Bu hükümde yer alan ifadenin, kusursuzluğun ispatı söz konusu olan hallerde arananın aksine, objektif özen yükümlülüğünün yerine getirildiği şeklinde daha ağır ölçüde yorumlanmasını gerektiren bir anlam taşıdığı, zira imza anahtarının kullanılması dolayısıyla meydana gelebilecek muhtemel zararların, bu şekilde ağır bir sorumluluk düzenlemesine başvurulmasını haklı gösterdiği ifade edilmektedir (Brehm, **a.g.e.**, Art.59a N.5). Bu sorumluluğun yalnızca malvarlığı zararlarına ilişkin olduğu, mutlak hak ihlalinden ötürü meydana gelen zararların genellikle bu sorumluluğun kapsamında değerlendirilmeyeceği görüşünde: Ingeborg Schwenzer, **Schweizerisches Obligationenrecht Allgemeiner Teil**, 5. Aufl., Bern, 2009, N.53.29a.

[331] Bu hükümde kullanılan inandırıcı bir şekilde ortaya koyma anlamına gelen *"glaubhaft darlegen"* deyiminin diğer kusursuz sorumluluk düzenlemelerinde kullanılan ispat etme anlamındaki *"nachweisen"* deyiminden hukuki sonuçları bakımından bir farkı olmadığı belirtilmektedir (Brehm, **a.g.e**., Art.59a N.9).

yükümlülüğünün ne ölçüde yerine getirildiğini tespit ederken, öncelikle "*gereken güvenlik tedbirlerinin*" neler olduğunu belirleyecek, daha sonra somut olaya göre ve olası tehlikeleri göz önünde bulundurarak, bunların hangilerinin imza sahibi tarafından yerine getirilmesinin beklenebileceğini değerlendirecektir[332].

OR. 59a hükmünde düzenlenen sorumluluğun yalnızca imza anahtarının yetkisiz bir üçüncü kişi tarafından kullanıldığı hallerle sınırlı olarak, sertifika dolayısıyla yaratılan hukuki görünüşe güvenen ve bu yüzden zarara uğrayan üçüncü kişiye karşı ortaya çıkacağı belirtilmektedir. Böyle bir hukuki görünüşün yaratılması, imza sahibinin, imza anahtarının yetkisiz kişiler tarafından kullanılması tehlikesini engellemek için gereken tedbirleri yeterli ölçüde almamış olmasından kaynaklanmaktadır[333]. Bunun dışında örneğin, imza sahibinin güvenli olmayan bir imza oluşturma aracı kullanması ve bu yüzden bir üçüncü kişinin zarara uğraması halinde, bu hükmün kapsamına girmeyen, başka bir sorumluluk temelinin daha ortaya çıkacağı belirtilmektedir[334].

İmza sahibinin güvenerek imza anahtarını teslim ettiği üçüncü kişilerin vermiş olduğu zararlardan da sorumlu olacağı ve bu kişilerin istihdam ettiği kişiler olması halinde OR. 55'teki kurtuluş kanıtlarını ileri sürerek bu sorumluluktan kurtulamayacağı ifade edilmektedir. Çünkü, imza sahibinin özen yükümlülüğünü yerine getirip getirmediği belirlenirken, imza anahtarının müstahdeme devredilmiş olması zaten tek başına gereken güvenlik tedbirinin alınmış olduğunun ispatına engel teşkil edecektir[335]. Diğer taraftan, burada koruma gören üçüncü kişi nitelikli sertifikaya güvenen kişidir. İmza anahtarını kullanan kişinin imza sahibi veya

---

[332] Brehm, **a.g.e**., Art.59a N.10.

[333] Brehm, **a.g.e**., Art.59a N.7. Bot ZertES 2001, 5708-5709.

[334] Brehm, **a.g.e**., Art.59a N.7

[335] OR. 59a hükmünün son fıkrasında bu maddede sözü edilen güvenlik tedbirlerinin neler olduğunun özel bir yönetmelikte düzenleneceği belirtilmiştir. Buna dayarak hazırlanan 3.12.2004 tarihli İsviçre Elektronik İmza Yönetmeliği'nde (VzertES), imza sahibi tarafından yerine getirilmesi öngörülen güvenlik tedbirlerinin neler olduğu gösterilmektedir. Bunlar arasında belirtilen başlıca güvenlik tedbiri imza oluşturma aracının hiçbir zaman başka bir kimseye teslim edilmemesi, imza oluşturma aracına giriş kontrolü sağlayan PIN gibi verilerin kimseyle paylaşılmamasıdır. Burada belirtilen tedbirlerin örnek niteliğinde olduğu, yalnızca bunların yerine getirilmiş olduğunu ispat ederek imza sahibinin sorumluluktan kurtulmasının mümkün olmadığı belirtilmektedir: Brehm, **a.g.e**., Art.59a N.18 vd.

müstahdem olması sertifikaya güvenen üçüncü kişi bakımından hiçbir farklılık yaratmamaktadır[336].

İmza anahtarının yetkisiz bir üçüncü kişi tarafından kötü niyetli olarak veya zorla ele geçirildiği hallerde, imza sahibinin gerekli güvenlik tedbirlerini almaması ile zararın oluşumu arasında illiyet bağının bulunmadığının tartışılabileceği belirtilmektedir. Buna göre, eğer imza sahibi gereken ve kendisinden beklenen güvenlik tedbirlerini yerine getirmediği için başka bir kimse zarara uğradıysa bu durumda illiyet bağının kesildiği ileri sürülemez. Zaten bu tedbirlerin eksiksiz yerine getirilmesi böyle bir ihtimalin ortadan kaldırılması amacına yöneliktir. Ancak, hayatın olağan akışının dışında kalan bir şekilde imza anahtarının ele geçirilmesi halinde, örneğin bir silahlı soygun olayında, illiyet bağının bulunmadığı, imza sahibi özen yükümlülüğünü gerektiği şekilde meydana getirseydi dahi zararın meydana geleceğini kabul etmek mümkün olacaktır[337].

Görüldüğü gibi İsviçre Borçlar Kanunu'na eklenen 59a hükmü kapsamında, imza sahibinin, nitelikli sertifikaya güvenen üçüncü kişilerin bu yüzden uğradıkları zararlara ilişkin olarak, haksız fiile dayalı tazminat borcu düzenlenmektedir.

İsviçre hukukundan farklı olarak, bu konuda özel bir yasal düzenleme içermeyen Alman hukukunda ise, imza sahibinin, elektronik imzanın yetkisiz bir kişi tarafından kullanılmasından kaynaklanan sorumluluğu, hukuki görünüşe güveninin korunması prensibi çerçevesinde ve yukarıda belirtilen üç ayrı ihtimal dikkate alınarak incelenmektedir. Birinci ihtimal, imza sahibi tarafından bir üçüncü kişi imza anahtarını kullanmaya yetkili kılınması ve üçüncü kişinin imza sahibinin verdiği yetkiye uygun olarak hareket etmesi halidir. Bu halde, temsil hükümlerinin (BGB §164 vd.) kıyasen uygulanması gerektiği, bunun sonucunda imza sahibinin imzalanan irade açıklamasıyla borç altına gireceği kabul edilmektedir[338].

---

[336] Brehm, **a.g.e**.,Art.59a N.14.

[337] Brehm, **a.g.e**., Art.59a N.17.

[338] Karl Larenz / Manfred Wolf, **Allgemeiner Teil des deutschen bürgerlichen Rechts,** 9. Aufl., München, Beck, 2004, s.497; Heinrich Dörner, **Rechtsgeschäfte im Internet**, AcP 202, 2002, s.388; Ulrich Noack, "Elektronische Form und Text Form", **Das Neue Schuldrecht**, Barbara Dauner-Lieb, Thomas Heidel, Gerhard Ring (Hrsg.), Heidelberg, C.F.Müller, 2002, §15 N.15;

İkinci ihtimal, imza sahibinin bir üçüncü kişiye imza anahtarını kullanarak işlemde bulunması için yetki vermesi, ancak üçüncü kişinin kendisine verilen bu yetkinin sınırlarını aşarak bir hukuki işlemde bulunması halidir. Bu şekilde, imza anahtarını ve şifresini üçüncü kişiye kendi isteğiyle vererek, imza sahibi üçüncü kişinin onun adına işlem yapabileceği bir hukuki görünüş yaratmasına imkan vermiş olmakta, onu görünüşte bir yetkiyle donatmış olmaktadır. Bu nedenle de, imza anahtarı üçüncü kişi tarafından kötüye kullanmışsa, imza sahibi ile beyan mutahatabı arasında hukuki görünüş esasına göre sözleşme kurulacak ve beyan muhatabı sorumlu olacaktır[339].

Son olarak, imza anahtarının imza sahibinin elinden iradesi dışında çıktığı (örneğin çalınma, kaybolma) ve bir üçüncü kişi tarafından yetkisiz olarak kullanıldığı hallerde, ihmal suretiyle yaratılan hukuki görünüş dolayısıyla verilen bir temsil yetkisi (*Anscheinsvollmacht*) bulunduğunun kabul edilebileceği ifade edilmektedir. Bunun şartları beyan muhatabının hukuki görünüşe güvenmekte haklı olması ve imza sahibinin hukuki görünüş yaratan olguları gerekli özeni göstererek fark edebilecek ve bunu engelleyebilecek durumda olmasıdır. Eğer bu şartlar gerçekleştiyse, yetkisiz üçüncü kişi tarafından yapılan bir işlemin imza sahibini bağlayacağı belirtilmektedir[340].

İmza sahibinin nitelikli sertifikaya güvenen üçüncü kişinin bu yüzden uğradığı zararlardan dolayı haksız fiile dayalı sorumluluğunun gündeme gelebilmesi için hukuka aykırı bir fiilinin bulunması gerekmektedir. Hatırlanacağı üzere, haksız

---

Gerald Spindler / Katharina Anton, "BGB §126a: Elektronische Form", **Recht der elektronischen Medien**, Gerald Spindler, Fabian Schuster (Hrsg.), 2. Aufl., München, C.H. Beck, 2011, N.10. Yazarlar, imza anahtarının bir üçüncü kişi tarafından kullanılması halini, temsilcinin başkası adı altında işlem yapması (*Noack*) ve temsilcinin başkası adına imzalaması hallerine (*Larenz / Wolf*) benzetmektedir.

339 Spindler / Anton, **a.g.e**., N.10. Burada katlanma suretiyle yaratılan hukuki görünüşe dayalı bir temsil yetkisinin bulunmadığı belirtilmektedir. Bir üçüncü kişinin imza anahtarını kullanmasına imza sahibinin katlanması beyan muhatabına karşı dışarı vurulmamaktadır. Bu yüzden bu ihtimalde kendine özgü bir hukuki görünüş hali olduğu ifade edilmektedir. Detaylı bilgi için bkz. Dörner, **a.g.e**., s.389.

340 İmza sahibinin şifreyi imza oluşturma aracının üstüne yazması halinde, böyle bir sorumluluğun doğmasını gerektiren bir özen eksikliği bulunduğunun kabul edilebileceği belirtilmektedir: Dörner, **a.g.e**., s.393. Aynı yönde: Noack, **a.g.e**., §15, N.15. Spindler / Anton, **a.g.e**., N.10. Hukuki görünüş esasının uygulanmaması ve haksız fiil hükümlerine gidilmesi halinde tüm riskin üçüncü kişi tarafından üstlenileceği belirtilmektedir: Dörner, **a.g.e**., 391.

fiil sorumluluğunda hukuka aykırılık unsuru bir mutlak hak ihlali bulunduğu takdirde veya bir koruyucu hukuk normuna aykırılık söz konusu olan hallerde ortaya çıkmaktadır[341]. Üçüncü kişinin nitelikli sertifika dolayısıyla bir mutlak hakkının ihlali söz konusu olmayacağından, burada hukuka aykırılık unsurunun tesisi için bir hukuk normuna aykırılık aranacaktır. İsviçre hukukunda hukuka aykırılık unsuru 59a hükmüne aykırılık dolayısıyla ortaya çıkmaktadır.

İsviçre hukukundaki düzenlemenin aksine, Türk hukukunda imza sahibinin nitelikli sertifika dolayısıyla uğradığı zararlardan dolayı sorumluluğunu düzenleyen özel bir hukuk normu bulunmamaktadır. Mevcut yasal düzenleme dikkate alındığında, imza sahibinin sorumluluğunun, Alman hukukundaki yaklaşıma paralel olarak, hukuki görünüşe güven prensibi esas alınarak incelenmesi daha isabetli gözükmektedir. Ancak böyle incelemenin yapılabilmesi, ilk olarak hukuki görünüşe güven prensibinin kapsamlı bir araştırmaya dayalı olarak irdelenmesini gerektirmektedir. Böyle bir araştırmaya burada yer verilmesi ise tezimizin sınırlarını aşmaktadır.

IV. HUKUKİ İŞLEMLERİN GEÇERLİLİK ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARI

Borçlar Kanunu'nun 14. maddesinin I. fıkrasında yapılan değişikle güvenli elektronik imzanın el yazısıyla imza ile aynı hukuki sonucu doğuracağı hükme bağlanmıştır. Bunun yanı sıra, EİK. 5 II hükmünde resmi şekle veya özel merasime tabi sözleşmelerin ve teminat sözleşmelerinin güvenli elektronik imza aracılığıyla yapılamayacağı düzenlenmektedir. Bu iki hüküm dikkate alındığında güvenli elektronik imzanın uygulama alanının belirlenmesi sorunu ortaya çıkmaktadır. Çalışmanın bu bölümünde, Borçlar Kanunu'nun geçerlilik şeklini düzenleyen

[341] Oğuzman / Öz, **a.g.e**., s.494 vd.; Fikret Eren, **Borçlar Hukuku Genel Hükümler**, 12. Bası, İstanbul, Beta, 2010, s.553 vd. Hukuka aykırı bir sonucu zarara uğrayan kimsenin haksız fiil hükümlerine göre tazminat isteyebilmesi için ihlal edilen kuralın amacının kapsamına o şahsın zarardan korunması da girmelidir (Oğuzman / Öz, **a.g.e**., s.494). İhlal edilen hukuk kuralının ihlal edilen menfaat ile arasında bulunması gereken ilişkiye hukuka aykırılık bağı denilmektedir. Hukuka aykırılık bağı kavramı hakkında bkz. Oğuzman / Öz, **a.g.e**., s.494 vd; Eren, **a.g.e**., s.556 vd; Selim Kaneti, **Haksız Fiilde Hukuka Aykırılık Unsuru**, İstanbul, Kazancı, 2007, s.227.

kurallarının (BK.11-16) güvenli elektronik imza ile birlikte nasıl yorumlanması gerektiği ve belirli hukuki işlemler bakımından geçerlilik şekli öngören kurallarının (örneğin BK. 163 I, BK. 213) güvenli elektronik imza ile ne ölçüde gerçekleştirileceği aydınlatılmaya çalışılacaktır.

A. BORÇLAR HUKUKU BAKIMINDAN ŞEKİL KAVRAMI

Bir irade beyanı kural olarak kendisini anlaşılabilir kılmaya elverişli her araç ile açıklanabilir. Bir irade beyanını açıklamak üzere kullanılan araca genel olarak *şekil* adı verilir. Bu anlamı esas alındığı takdirde, her irade beyanının bir şekli vardır[342]. Fakat teknik anlamı itibariyle şekil, kanun veya hukuki işlem ile bir irade beyanının hukuki sonuç doğurması için öngörülmüş belirli bir dış kalıbı, biçimi ifade etmektedir[343].

BK. 11 I hükmüne göre "*akdin sıhhati kanunda sarahat olmadıkça hiçbir şekle tabi değildir*". Buna göre, bir sözleşmeyi oluşturan irade beyanları için kural olarak belirli bir şekle uyma zorunluluğu bulunmamaktadır. Diğer bir ifadeyle sözleşmelerin geçerliliği açısından *şekil serbestisi ilkesi* hakimdir. Bu maddede yalnızca "akit"ten söz ediliyor olmasına rağmen, Borçlar Kanunu'nun sözleşmelerin şekillerine ilişkin kuralları, kıyasen bütün irade beyanlarına uygulanacağı kabul edilmektedir[344].

Buna göre taraflar kanunun açıkça belirli bir şekle uyma zorunluluğu öngörmediği hukuki işlemleri istenilen şekilde gerçekleştirebilirler. Diğer yandan kanunen bir şekil öngörülmemiş olmasına rağmen tarafların sözleşmenin geçerliliğini özel bir şekle tabi tutmaları da mümkündür.

Kanunun veya tarafların belirli bir hukuki işlemin geçerliliğini şekle bağlamasının çeşitli gerekçeleri bulunabilir. Öğretide şeklin faydaları hakkında şu

---

342 Kocayusufpaşaoğlu, **a.g.e**., s.270.

343 Tunçomağ, **a.g.e.**, s.215; İnan, **a.g.e.**, s.129.

344 Oğuzman / Öz, **a.g.e**., s.117; Eren, **a.g.e**., s.239.

gerekçeler ileri sürülmektedir: Şekil, bir hukuki işlemi meydana getirmeye yönelen iradenin ciddiyetini göstermektedir ve bu sayede bir hukuki işlemi bağlayıcılığı olmayan diğer beyanlardan ayırmak kolaylaşmaktadır[345]. Buna ilaveten, şekil, irade beyanına neleri kapsadığı konusunda açıklık ve kesinlik sağlar[346]. Ayrıca şekil taraflardan birini veya her ikisini korumak için de öngörülmüş olabilir. Çünkü şekil, irade beyanına bağlı olarak meydana gelecek hukuki sonuçlar hakkında tarafları düşünmeye sevkederek, onları geçici heveslerden veya arzulardan doğabilecek hafifliklere karşı koruyacak bir etki doğurur[347]. Bunların yanı sıra şekil, üçüncü kişilere yapılan hukuki işlemden haberdar olma imkanı vererek, aleniyeti ve hukuki emniyeti sağlamaktadır[348]. Nihayet şekil sayesinde belirli bir hukuki işlemin meydana getirildiğinin ispatı kolaylaştırılmış olmaktadır[349].

Aşağıda kanuni şekil başlığı altında Borçlar Kanunu'nda düzenlenen geçerlilik şekli türleri incelenecek, devamında iradi şeklin kanuni şekilden farklılaşan yönleri üzerinde durulacaktır.

1. Kanuna Dayanan (Yasal) Şekil

Kanunda bir şekil şartı öngörüldüğü takdirde, hukuki işlemin geçerli olması o şekle uyularak yapılmasına bağlıdır. Bir hukuki işlemin geçerli olması için hangi şekle riayet etmek gerektiğinin kanun tarafından belirlenmesi halinde *kanuna dayanan (yasal) şekil* söz konusudur. Kanuna dayanan şekil şartı gerçekleştirilmeksizin yapılan bir hukuki işlem şekle aykırılık sebebiyle kesin hükümsüz olacaktır. Ancak kanunda öngörülen şekillerin tamamı *geçerlilik şekli* değildir. Bazen ispat edilebilirliği için bir hukuki işlemin belirli bir şekilde yapılması gerekebilir. Örneğin HUMK. 288'de yazılı tutarı aşan değerdeki hukuki işlemlerin

---

345 Tunçomağ, **a.g.e**., s.216; Eren, **a.g.e**, s.237; Tunçomağ, **a.g.e**., s.216.

346 Tunçomağ, **a.g.e**., s.216; İnan, **a.g.e**., s.130; Feyzioğlu, **a.g.e**., s.303; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.,** s.99; Eren, **a.g.e**., s.238.

347 Tunçomağ, **a.g.e**., s.216; Feyzioğlu, **a.g.e**., s.303; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.99; Oğuzman / Öz, **a.g.e**., s.117.

348 Feyzioğlu, **a.g.e**., s.303; Oğuzman / Öz, **a.g.e**., s.117; İnan, **a.g.e**., s.130; Eren, **a.g.e**., s.238.

349 Eren, **a.g.e**., s.238; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.99; İnan, **a.g.e**., s.130.

senetle ispat olunması gerekmektedir. Bu durumda bir *ispat şekli* öngörülmüştür. İspat şekline uygun olarak yapılmamış olsa da sözleşme geçerli olarak hüküm ifade eder. BK. 11 II'e göre kanunun öngördüğü şekil, aksi belirtilmedikçe geçerlilik şeklidir.

Borçlar Kanunu geçerlilik şekli olarak iki şekil türünü düzenlemektedir: Adi yazılı şekil ve resmi yazılı şekil[350]. Aşağıda bu iki şekil türüne ilişkin açıklamalara yer verilecektir.

a. Adi Yazılı Şekil

Türk hukukunda alacağın temliki sözleşmesi (BK. 163 I), önalım (şuf'a) sözleşmesi (BK. 213), bağışlama vaadi (BK. 238 I), itibar emri (BK. 400 II), kefalet (BK. 484), kaydı hayat ile irad sözleşmesi (BK. 508), ölünceye kadar bakma sözleşmesi (BK. 512) geçerliliği adi yazılı şekle tabi tutulan sözleşmelerden bazılarıdır. Borçlar Kanunu 12-15. maddeleri arasında adi yazılı şekil türünü düzenlemektedir.

"*Adi yazılı şekil*" veya sadece "*yazılı şekil*" ile amaçlanan sözleşmenin niteliğini ve konusunu göstermeye yeterli olan ve borç altına girenlerin ya da bir hakkı devredenlerin imzalarını ihtiva eden herhangi bir yazıdır[351]. Buna göre hukuki sonuç doğurmaya yönelik irade beyanının yazılı bir metinde açıklanması ve beyanda bulunan tarafından imzalanması adi yazılı şekli gerçekleştirir[352]. Aslı borçlanan tarafından imzalanmış bir telgraf veya yine borçlanan tarafından imzalanan bir mektup yazılı şekli meydana getirir. BK. 13 II hükmü bu hususu açıkça ifade etmektedir: "*Hilafı kanunda yazılı olmadıkça imzalı bir mektup veya asli borcu*

---

[350] Bunların dışında kalan resmi tescil ve ilanın bir şekil türü olup olmadığı tartışmalı bir konudur. Bu konudaki tartışmalar için bkz. Kocayusufpaşaoğlu, **a.g.e**., s.219; Eren, **a.g.e**., s.251, Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.112.

[351] Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.113.

[352] Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.113; Kocayusufpaşaoğlu, **a.g.e**., s.279; Eren, **a.g.e**., s.246.

üzerine alanlar tarafından imza edilmiş olan telgrafname tahriri şekil makamına kaim olur".

Tarafların karşılıklı ve birbirine uygun irade beyanlarını açıkladıkları metnin kim tarafından, hangi araçla ve hangi madde üzerine yazıldığı önem taşımamaktadır[353]. Metnin elle, daktiloyla veya bilgisayarda yazılması mümkündür. Yalnızca metnin irade beyanlarının kapsamının belirlenmesine imkan verecek ölçüde tam ve açık olması gerekmektedir[354]. Bilgisayarda yazılan metnin adi yazılı şekil şartını gerçekleştirmesi için yazıcı (*printer)* vasıtasıyla yazılı biçime dönüştürülmesi ve beyan sahibinin el yazısıyla imzasının metnin sonuna eklenmesi gerekmektedir[355]. Aksi halde bilgisayarın sabit sürücüsüne kaydedilen elektronik veriler yazılı olma şartını yerine getirmeyecektir[356].

Adi yazılı şekilde önem taşıyan unsur el yazısıyla imzadır. İmza irade beyanında bulunan kişinin kimliğini belirlemeye ve irade beyanını açıklayan metnin imza sahibi tarafından kabul edildiğini tespite yarayan bir işarettir[357]. Bu işlevleriyle imza borçlunun borç altına girme iradesini kesin olarak açıklar ve tamamlayıp ortaya koyar[358].

Borçlar Kanunu'nda imza kavramı, hangi işlevleri yerine getirdiği esas alınarak tanımlanmış değildir. Yalnızca imzanın kural olarak beyan sahibinin eliyle yazılması gerektiği belirtilmektedir (BK. 14 I).

Bir sözleşmede, yazılı sözleşme metninin, o sözleşme ile borç altına giren taraf veya taraflarca imzalanması gerekmektedir (BK. 14 I). Buna göre, iki tarafa borç yükleyen sözleşmelerde her iki tarafın da imzasının bulunması zorunludur[359].

---

353 Esener, **a.g.e.,** s.173; Tunçomağ, **a.g.e**., s.222; İnan, **a.g.e**., s.137-138; Feyzioğlu, **a.g.e**., s.315-316; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.114, Kocayusufpaşaoğlu, **a.g.e**., s.279.

354 Tunçomağ, **a.g.e**., s.222; İnan, **a.g.e**., s.137.

355 Kocayusufpaşaoğlu, **a.g.e**., s.279.

356 Altınışık, **a.g.e**., s.76.

357 Tunçomağ, **a.g.e**., s.222, Oğuzman / Öz, **a.g.e**., s.122.

358 Esener, **a.g.e.,** s.246; Tunçomağ, **a.g.e**., s.227.

359 Tunçomağ, **a.g.e**., s.223; İnan, **a.g.e**., s.139; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.116; Kocayusufpaşaoğlu, **a.g.e**., s.280. Sözleşmede taraflardan yalnız birinin borç altına girmesi

Tek tarafa borç yükleyen sözleşmelerde, örneğin kefalet sözleşmesinde ve taşınır bağışlama vaadinde, borç altına giren tarafın -kefilin veya bağışlayanın- imzasının bulunması yeterlidir. Borçlandırıcı işlemlere yönelik olarak öngörülen BK. 14 I hükmü kıyasen tasarruf işlemlerinde de uygulanır ve hakkı üzerinde tasarrufta bulunanın, örneğin bir alacağın temliki işleminde sadece temlik edenin, imzasının bulunması yeterli kabul edilir[360].

İmzanın borç altına giren taraf veya tarafların temsilcileri tarafından da atılması kural olarak mümkündür[361]. İmzayı temsil yetkisi bulunmayan yardımcı kişiler atamazlar. Çünkü imza atmak bir irade açıklamak demektir. Bunu da yapmaya yetkili olan bizzat borç yüklenen kimse veya onun yetkili temsilcisidir[362].

İmzanın yapılan irade beyanının tamamını kapsaması gerekmektedir. Bu sebeple imzanın metnin sonuna, metnin tamamını kapsayacak şekilde atılması gerekmektedir[363]. Metin imzalandıktan sonra imzanın altına yazılan hususlar, hukuki işlemin şekle bağlanmak gereken içeriğine dahil ise geçerli sayılmazlar. Metinde sonradan yapılacak değişiklik, ilave ve çıkarmaların geçerli olması için bunların ayrıca imzalanması gerekmektedir[364].

El yazısı ile imza kuralının (BK. 14 I) bazı istisnaları vardır. BK. 14 II'ye göre iş hayatında yerleşmiş örf ve adetlere göre imzanın mekanik biçimde (kanunun ifadesi ile "bir alet vasıtasıyla") atılması veya kopya edilmesi uygun görüldüğü

---

ihtimali için "tek taraflı şekil", her iki tarafın da borç altına girdiği ihtimaller için de "iki taraflı şekil" terimleri kullanılmaktadır (Eren, **a.g.e**., s.246).

360 Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.116; Kocayusufpaşaoğlu, **a.g.e**., s.280; Eren, **a.g.e**., s.247.

361 Feyzioğlu, **a.g.e**., s.317; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.114. Temsilcinin kendi imzasını atması gerekir. Zira imza şahsa bağlı haklardandır ve başkası tarafından kullanılamaz. Bkz. Esener, **a.g.e**., s.175; İnan, **a.g.e**., s.139.

362 Esener, **a.g.e**., s.174; Tunçomağ, **a.g.e**., s.227.

363 İnan, **a.g.e**., s.138; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.117; Kocayusufpaşaoğlu, **a.g.e**., s.280; Oğuzman / Öz, **a.g.e**., s.123. Şu kadar ki, şayet metnin imzadan önce taraflarca görüldüğü ve kabul edildiği sabit olursa artık imzanın metinde bulunduğu yerin bir önemi kalmaz (Feyzioğlu, **a.g.e**., s.320)

364 Esener, **a.g.e**., s.174; Tunçomağ, **a.g.e**., s.228; Feyzioğlu, **a.g.e**., s.320; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.117; Kocayusufpaşaoğlu, **a.g.e**., s.280-281.

takdirde imzanın bu şekilde atılması yeterlidir[365]. Bu tür bir imza tekniği özellikle, BK. 14 II hükmünde de belirtildiği üzere, tedavüle çıkarılan çok sayıda kıymetli evrakın (örneğin anonim şirketin piyasaya sürülen binlerce pay senedinin) imzalanmasında kullanılır[366]. Fakat Ticaret Kanunu'na göre kambiyo senetlerinde (bono, poliçe, çek) mekanik yolla imza tekniğinin uygulanması imkanı bulunmamaktadır (TTK. 668, 690 ve 730).

Okuma yazma bilmemek, bedeni sakatlık vb. sebeplerden dolayı imza atma iktidarından yoksun kişilerin durumu ise BK. 15'te düzenlenmektedir. Bu durumdaki kişiler el yazısıyla imza yerine onaylanmış bir el işareti kullanabilirler veya resmi senetlemeye başvurabilirler[367].

Görme özürlülerin imzalarının geçerli sayılması için, imzalarının noter tarafından tasdik olunmasını veya tasdik olunmadığı takdirde imzaladıkları hukuki işlemin metnine vakıf olduklarının karşı tarafça ispat edilmesini öngören BK. 14 III hükmü, 5378 sayılı "Özürlüler ve Bazı Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun"un 50. maddesi ile yürürlükten kaldırılmıştır.

BK. 12'ye göre yazılı şekle tabi bir sözleşmenin hükümlerini sonradan değiştirmek isteyen tarafların (sözleşmeye aykırı olmayan veya onu değiştirmeyen tamamlayıcı ve yan şartlar hariç olmak üzere) bu değişiklikleri de yazılı şekilde yapması gerekmektedir[368].

Yazılı şekil şartı bir defa yerine getirildikten sonra, yazılı metnin kaybolması, çalınması, kısaca alacaklının rızası dışında elden çıkması halinde dahi sözleşme geçerli olarak kurulmuş sayılır[369].

---

[365] Bu hüküm yazı yazmayı bilen, imzasını koymaya muktedir kişilerle ilgilidir (Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.113.)

[366] TTK. 427'ye göre tahvillerde "imza, damga veya mühür şeklinde olabileceği gibi matbu dahi olabilir".

[367] İmza atma iktidarından yoksun kişilerin durumuyla ilgili detaylı inceleme ve değerlendirmeler için bkz. Kocayusufpaşaoğlu, **a.g.e**., s.285-290.

[368] Bu hüküm sadece kanunen şekle tabi tutulan sözleşmeler bakımından uygulanır. İradi yazılı şekle tabi bir sözleşmede yapılacak değişikliklerin yazılı olması zorunluluğu yoktur. Bkz. Esener, **a.g.e**., s.178; Feyzioğlu, **a.g.e**., s.314.

[369] Esener, **a.g.e**., s.173; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.120-121.

b. Resmi Yazılı Şekil

Resmi şekil, taraflara ait irade açıklamalarının doğrudan doğruya resmi makam veya kamu güveniyle donatılmış kişiler tarafından tespit edilerek kanunda öngörülen usullere uygun olarak resmi senede bağlanması suretiyle gerçekleştirilmektedir[370]. Resmi şeklin hangi usulde ve hangi makam tarafından gerçekleştirileceğine ilişkin hükümler Borçlar Kanunu'nda yer almamaktadır.

Kanunda başka bir makam gösterilmediği takdirde resmi şekli gerçekleştirme yetkisi kural olarak noterler aittir (Noterlik K. 60). Bununla beraber resmi şekle bağlı bazı işlemlerin başka makamlarca düzenlenmesini öngören hükümler de vardır. Örneğin, Tapu K. 26 hükmü uyarınca, resmi şeklin en önemli uygulama alanını oluşturan taşınmaz üzerindeki mülkiyeti veya sınırlı ayni hakların devrini hedef tutan sözleşmeler tapu memuru tarafından düzenlenir. Resmi vasiyetname ve miras sözleşmesi, noter yanında, sulh hakimi veya kanunla kendisine yetki verilmiş diğer bir görevli tarafından düzenlenebilir (MK. 532, 545 I). Dolayısıyla resmi şekil söz konusu olduğu takdirde kanunda bu şekli gerçekleştirecek özel bir makam veya mercinin gösterilmiş olup olmadığına bakılmalı, eğer böyle bir makam gösterilmemişse münhasıran noterlerin resmi şekli gerçekleştirmeye yetkili olduğu kabul edilmelidir.

Yetkili olduğu konularda noterlerin yalnızca düzenleme şekline uyarak re'sen düzenledikleri resmi senetler geçerlilik şeklini gerçekleştirir[371].Resmi şekil denildiğinde ilk akla gelen ve genellikle işaret edilen bu şekil türüdür. Düzenleme şeklindeki resmi senetler noter tarafından kaleme alınarak imzalanmaktadır[372].

Noter tarafından yalnızca senet altındaki imzaların tasdiki yapılan onaylama şeklindeki senetler ise geçerlilik şeklini yerine getirmeyecektir. Çünkü bu usulde

---

[370] Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.126.

[371] Feyzioğlu, **a.g.e**., s.335.

[372] Düzenleme şeklindeki senetlerin taşıması gereken unsurlar Noterlik K. 84 ve devamında yer almaktadır.

onaylanan senedin gerçeklik ve itibarı sadece tarih ve imzaya münhasır olup metnin içeriğini kapsamamaktadır[373].

BK. 12'de açıkça hükme bağlanmadığı halde, resmi şekle tabi bir sözleşmede yapılacak değişikliklerin yine resmi şekilde gerçekleştirilmesi gerekmektedir. Aksi halde bu değişiklikler geçerli olmaz[374].

2. Tarafların Anlaşmasına Dayanan (İradi) Şekil

Tarafların kanunun geçerliliğini belirli bir şekle bağlamadığı hukuki işlemleri, aralarında anlaşarak şekle bağlamaları mümkündür. Bu durumda, *iradi şekil* söz konusu olur. Taraflar kararlaştırdıkları şekli gerçekleştirmedikçe sözleşmeyle bağlanmış sayılmazlar (BK. 16 I). Taraflarca şekil anlaşmasında herhangi bir açıklama bulunmadığı takdirde, tereddüt halinde öngörülen şeklin bir geçerlilik şekli olduğu karine olarak kabul edilir. İspat şekli olduğunu iddia eden taraf bunu ispat ile yükümlüdür[375]. İradi şeklin geçerlilik şartı olarak düzenlenip düzenlenmediği irade beyanları yorumlanarak belirlenir[376].

Taraflar anlaşarak kanunen hiçbir şekle tabi olmayan bir sözleşmeyi şekle tabi kılabilecekleri gibi, kanuni şeklin şartlarını da ağırlaştırabilirler. Bununla birlikte, kanuni şeklin hukuki etkisinin anlaşma yoluyla zayıflatılması veya bertaraf edilmesi mümkün değildir[377].

---

[373] Esener, **a.g.e**., s.172; Feyzioğlu, **a.g.e**., s.334. Bu halde resmi yazılı şekil değil, resmi onamaya bağlı yazılı şeklin bir türünden söz edileceği görüşünde: Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.121-125. Onaylama şeklini düzenleyen Noterlik K. 90'a göre; hukuki işlemlerin altındaki imzanın onaylanması imzayı atan şahsa ait olduğunun bir şerhle belgelendirilmesi şeklinde yapılır. İmzası onaylanan iş kağıdının aslı ilgilisine verilir ve imzalı bir örneği dairede saklanır.

[374] Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.129.

[375] Tunçomağ, **a.g.e**., s.218; İnan, **a.g.e**., s.134; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.136; Eren, **a.g.e**., s.241.

[376] Eren, **a.g.e**., s.241.

[377] Esener, **a.g.e**., s.177; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.136; Eren, **a.g.e**., s.242.

Tarafların kendi kararlaştırdıkları sözleşme şeklini –herhangi bir şekle bağlı kalmadan- değiştirmeleri, hatta ortadan kaldırmaları mümkündür. Örneğin önce yazılı şekil kararlaştıran taraflar daha sonra resmi şekil tercih edebilir[378].

BK. 16 II'ye göre, "*İki taraf muayyen bir surette keyfiyeti izah etmiyerek tahriri şekilden bahsetmiş oldukları takdirde, kanun bu şekle riayet olunmasını emrediyorsa, iki tarafın ona riayet etmesi lazımdır*"[379]. Taraflar hiçbir açıklama yapmadan belirli bir şekilden bahsetmişlerse bu şekle nasıl uyulacağına ve uymamanın sonuçlarının ne olacağına ilişkin sorunlar kanunda öngörülen şekillere ait kullara göre çözümlenir. Buna göre, taraflar sözleşmenin yazılı şekilde yapılmasını kararlaştırmış olmakla birlikte, bunun nasıl gerçekleştirileceği hususunda bir açıklama getirmemişse, bu durumda Borçlar Kanunu'nun adi yazılı şekle ilişkin kuralları uygulama bulacaktır. Sözleşmede başka bir kayıt bulunmadığı takdirde, iradi şekil bakımından da kanunun öngördüğü adi yazılı şekil ve resmi şekil hükümlerine uyulması gerekmektedir. Bu husus adi yazılı şekil bakımından BK. 16 II hükmünde ifade edilmektedir. Aynı hükmün kıyasen resmi şekil için de uygulanması gerekmektedir[380].

Borçlar Kanunu burada bir karineye yer vermekte olup, tarafların irade özerkliği ilkesi çerçevesinde aksini kararlaştırmaları mümkündür. Aynı şekilde taraflar, yaptıkları şekil anlaşmasını hiçbir şekle uymaksızın, hatta çoğu zaman iradeyi açıklayan davranışlara ve örtülü biçimde de değiştirebilirler. Örneğin, yazılı şekil kararlaştırıldığı halde imza el yazısıyla değil başka bir araçla (daktilo makinesi, bilgisayar vb.) yazılmışsa ve taraflar herhangi bir çekince veya itiraz ileri

---

[378] Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.136.

[379] Yeni Borçlar Kanunu'nun 17. maddesine göre:

"Kanunda şekle bağlanmamış bir sözleşmenin taraflarca belirli bir şekilde yapılması kararlaştırılmışsa, belirlenen şekilde yapılmayan sözleşme tarafları bağlamaz.

Herhangi bir belirleme olmaksızın yazılı şekil kararlaştırılmışsa, yasal yazılı şekle ilişkin hükümler uygulanır".

[380] Oğuzman / Öz, **a.g.e**., s.131.

sürmeksizin sözleşmeyi ifa ederse, bu şekle ilişkin anlaşmanın daha sonradan yine karşılıklı anlaşma ile değiştirildiği anlamını taşıyacaktır[381].

BK. 12 hükmünün iradi şekil bakımından uygulanmayacağı kabul edilmektedir. Buna göre, taraflar kendi iradeleriyle belirledikleri şekle uygun olarak yaptıkları sözleşmenin içeriğini değiştirmek için aynı şekle uymak zorunda değildir[382].

B. GEÇERLİLİK ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARI

1. Kanuna Dayanan Şekil Açısından

EİK. 5 I hükmüne göre "*güvenli elektronik imza elle atılan imza ile aynı hukuki sonucu doğurur*".

Bu hükmün Borçlar hukuku açısından iki önemli sonucu vardır: Öncelikle geçerlilik şekli bakımından elektronik imzanın hukuki etkisi güvenli elektronik imzayla sınırlı olarak kabul edilmektedir. Basit elektronik imzaya ise bu bakımdan kural olarak hiçbir değer atfedilmemektedir[383].

---

[381] Kocayusufpaşaoğlu, **a.g.e**., s.330. Öğretide taraflarca öngörülen şekil zorunluluğunun ifa ile ortadan kalkacağı belirtilmektedir: Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.136. Bu durumda şeklin geçerlilik şartı olmadığının ortaya çıkacağı görüşünde: Tunçomağ, **a.g.e**., s.218; Eren, **a.g.e**., s.242.

[382] Tekinay / Akman / Burcuoğlu / Altop, **a.g.e.**, s.136; Oğuzman / Öz, **a.g.e**., s.136.

[383] Basit elektronik imzanın geçerlilik şeklini yerine getiremeyeceği kuralına ilişkin olarak yeni Hukuk Muhakameleri Kanunu'nun 412. maddesinin 3. fıkrası tartışma yaratabilecek bir ifade içermektedir:

> "*Tahkim sözleşmesi yazılı şekilde yapılır. Yazılı şekil şartının yerine getirilmiş sayılması için, tahkim sözleşmesinin taraflarca imzalanmış yazılı bir belgeye veya taraflar arasında teati edilen mektup, telgraf, teleks, faks gibi bir iletişim aracına veya elektronik ortama geçirilmiş olması ya da dava dilekçesinde yazılı bir tahkim sözleşmesinin varlığının iddia edilmesine davalının verdiği cevap dilekçesinde itiraz edilmemiş olması yeterlidir. Asıl sözleşmenin bir parçası hâline getirilmek amacıyla tahkim şartı içeren bir belgeye yollama yapılması hâlinde de tahkim sözleşmesi yapılmış sayılır*".

Hükmün ikinci cümlesinde yer alan "*elektronik ortama geçirilmiş olma*" ifadesiyle ne anlatılmak istediği pek açık değildir. Güvenli elektronik imzanın uygulanabilirliğine ilişkin olarak buna özel olarak yer verilmesine gerek yoktu. Yalnızca elektronik ortamda kaydedilmiş olmayı işaret eden

EİK. 5 I hükmünün ikinci sonucu ise -kanunda aksi öngörülmediği sürece- güvenli elektronik imzanın hukuki sonuçları itibariyle el yazısıyla imzaya eşdeğer sayılacağının kabul edilmiş olmasıdır[384]. Bunun için güvenli elektronik imzanın tüm yönleri ile mevzuatta belirtilen şartları yerine getirmesi gerekmektedir.

EİK. 5 I'e paralel olarak EİK. 22 hükmü ile Borçlar Kanunu'nun "*İmza*" başlıklı 14. maddesinin I. fıkrasında değişiklik yapılmıştır. Kanun'daki "*imza üzerine borç alan kimsenin el yazısı olmak lazımdır*" hükmü muhafaza edilmiş ve hükmün devamına "*Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir"* cümlesi eklenmiştir.

Güvenli elektronik imzanın hukuki etkisine Borçlar Kanunu'nun imza kavramını düzenleyen 14. maddesinde ayrıca yer verilmesi isabetli bir düzenlemedir[385]. Ancak burada el yazısıyla imzanın ispat gücünden söz edilmesi talihsizlik olmuştur[386].

Öğretide, böyle bir ifade kullanılmış olması dolayısıyla, bu düzenlemenin ispat hukukuna ilişkin olduğunu ve geçerlilik şekli bakımından bir farklılık yaratmadığı da ifade edilmektedir[387]. Bu düzenlemeye ilişkin madde gerekçesinde yer alan "*Borçlar Kanununun 14 üncü maddesinin birinci fıkrasına yapılan eklemeyle Hukuk Usulü Muhakemeleri Kanununun senetle ispat zorunluluğuna ilişkin hükümlerinin kaynağı olan Fransız Medenî Kanununun 1316-3 üncü maddesinde elektronik imzaya ilişkin yapılan düzenlemeye paralel bir düzenleme*

---

bu ifade basit elektronik imzanın da yazılı şekli gerçekleştirmek bakımından yeterli sayılacağı düşüncesini yaratmaktadır.

384 Aksoy, **a.g.e**., s.254.

385 Böylelikle Borçlar Kanunu ile Elektronik İmza Kanunu arasındaki çelişki giderilmiştir: Sağlam, **a.g.e**., s.174. Aksi görüşte: Keser Berber,**Tasarı**; Aksoy, **a.g.e**., s.255. Her iki yazar da EİK. 5 I hükmü varken, BK. 14 I hükmünde bu düzenlemeye yer verilmesinin bir anlamı olmadığını belirtmektedir. *Aksoy*, EİK. 5 I hükmünde yer alan düzenlemenin konuyla bağlantısı ve sistematik özelliği nedeniyle doğrudan doğruya BK.14 eklenebileceği ve Elektronik İmza Kanunu'nda böyle bir hükme hiç yer verilmeyebileceğini ifade etmektedir. Başka bir görüşe göre; EİK. 5 I hükmüne yalnızca BK. 14 I'de değişiklik yapan EİK. 22'de yer verilmesi gerekirdi: Ümit Gezder, **Mukayeseli Hukuk Açısından İnternet'te Aktedilen Sözleşmelerde Tüketicinin Korunması,** İstanbul, Beta, 2004, s.150.

386 Kocayusufpaşaoğlu, **a.g.e**., s.291; İnal, **a.g.e**., s.144.

387 Keser Berber, **Tasarı.**

yapılarak sözleşmelerle ilgili temel nitelikte kanun olan Borçlar Kanununda güvenli elektronik imzanın elle atılan imzayla eşdeğerliğinin sağlanması amaçlanmıştır" şeklindeki açıklama bu görüşü destekler niteliktedir.

Ancak Türk hukukunda BK. 14 I hükmü ispat şekline değil geçerlilik şekline ilişkindir. "İspat gücü" ifadesine ve bu ifadenin kaynağını belirterek bilinçli olarak kullanıldığını açıklayan gerekçe metnine rağmen, bu hüküm güvenli elektronik imzanın el yazısıyla imza ile hukuken eş değer olduğu, yani yazılı şekil şartının gerçekleşmesi için aranan imza unsurunun güvenli elektronik imzayla yerine getirilebileceği şeklinde anlaşılmalıdır. Bu sebeple de BK. 14 I hükmünün amacına uygun olarak şöyle bir ifade kullanılarak düzeltilmesi gerektiği öğretide ifade edilmiştir[388]: " *Güvenli elektronik imza elle atılan imza ile aynı hukuki sonuçları doğurur*".

Nitekim Yeni Borçlar Kanunu'nun 15. maddesinin 1.fıkrasının II. cümlesi de bu eleştirilere uygun olarak şu şekilde kaleme alınmıştır:

"*… Güvenli elektronik imza da, el yazısıyla atılmış imzanın bütün hukukî sonuçlarını doğurur*".

Ayrıca, Yeni Borçlar Kanunu'nun 14. maddesinin II. fıkrasında güvenli elektronik imzayla ilgili yeni bir hükme yer verilmektedir:

"Kanunda aksi öngörülmedikçe, imzalı bir mektup, asılları borç altına girenlerce imzalanmış telgraf, teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ya da güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil yerine geçer[389]".

---

[388] Kocayusufpaşaoğlu, **a.g.e**., s.291; İnal, **a.g.e**., s.144; Gezder, **a.g.e**., s.150. Bu hükmün "*güvenli elektronik imza aynı işlevi görür*" şeklinde değiştirilmesi gerektiği görüşünde: Falcıoğlu, **a.g.e.,** s.96.

[389] BK. 13 II'ye karşılık gelen, Yeni Borçlar Kanunu'nun 14. maddesinin II. fıkrası "teyit edilmiş olmaları kaydıyla faks veya buna benzer iletişim araçları ile gönderilip saklanabilen metinler"in de yazılı şekil yerine geçeceğini belirtmektedir. Ancak maddede bahsi geçen teyidin derhal yapılması şartının aranmamış olması büyük eksiklik olarak gösterilmektedir: Kocayusufpaşaoğlu, **a.g.e**., s.301. Diğer yandan maddede aranan teyidin ne şekilde gerçekleştirileceği de açık değildir.

Yeni Borçlar Kanunu'nun 15. maddesinde güvenli elektronik imzanın el yazıyla imzayla aynı hukuki sonucu doğuracağı açıkça öngörülmesine rağmen, hangi gerekçeyle, 14 II hükmünde güvenli elektronik imzalı belgenin yazılılık şartını yerine getireceğine dair böyle bir hükme ayrıca gerek duyulmuş olduğu hakkında bir açıklama bulmak güçtür. "İmza" başlıklı 15. maddenin I. fıkrasında, el yazısıyla imza ile aynı sonuçları doğuracağı düzenlenen, dolayısıyla da el yazısıyla imzaya denk kılınan bir tür güvenli elektronik imza kullanılarak imzalanan belgenin, yazılı şekil şartını yerine getirip getirmeyeceğine ilişkin açıklığa kavuşturulmayı bekleyen tartışmalı bir durum zaten mevcut değildir[390].

Yürürlükteki BK. 14 I hükmüne göre, geçerlilik şekli olarak bir metnin el yazısıyla imzalanmasının tek başına yeterli sayıldığı hukuki işlemler güvenli elektronik imza aracılığıyla da yapılabilir. El yazısıyla imzaya ek olarak, metnin el yazısıyla yazılmış olması veya resmi bir makamın katılımının gerekmesi gibi ilave bir şekil şartı öngörülen hukuki işlemlerse, kanunda aksi düzenlenmiş olmadığı takdirde, güvenli elektronik imza ile gerçekleştirilemez. Bu güvenli elektronik imzanın el yazısıyla imzaya denkliği ilkesinin bir sonucudur[391].

---

[390] Güvenli elektronik imzanın bulunduğu yerde yazılı şekil yerine geçen şekil değil, imza koşulunun gerçekleştiği yazılı şeklin kendisi mevcuttur: Ahmet M. Kılıçoğlu, **Türk Borçlar Kanunu Tasarısı'na Eleştiriler**, Türkiye Barolar Birliği, 2008, s.12.

[391] Bu yoruma paralel olarak, poliçe üzerindeki beyanların el yazısıyla olmasını şart kılan ve bono ve çek bakımından da kıyasen uygulanan TTK. 668 hükmü uyarınca, kambiyo senetlerinin elektronik imza kullanılarak düzenlenmesinin mümkün olmadığı öğretide ifade edilmektedir: Mine Erturgut, "Elektronik İmza Kanunu Bakımından E-belge ve E-imza**", Bankacılar Dergisi**, S. 48, 2003, s.66-79, s.71.

13.01.2011 tarihli ve 6102 sayılı Yeni Türk Ticaret Kanunu güvenli elektronik imza bakımından yeni bir istisna daha öngörmektedir. Kanun'un "*Güvenli elektronik imza*" başlıklı 1526. maddesinin 1. fıkrasına göre "*Poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetler güvenli elektronik imza ile düzenlenemez. Bu senetlere ilişkin kabul, aval ve ciro gibi senet üzerinde gerçekleştirilen işlemler güvenli elektronik imza ile yapılamaz*". Bu maddeye ilişkin gerekçede, kıymetli evrakta güvenli elektronik imzanın uygulanıp uygulanamayacağı hususunun açıklığa kavuşturulduğu ifade edilmektedir.

Kanun'un 1526. maddesinin 2. fıkrasına göre; "*konişmentonun, taşıma senedinin ve sigorta poliçesinin imzası elle, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla da atılabilir. Düzenlendikleri ülke kanunlarının izin verdiği ölçüde bu senetlerde yer alacak kayıtlar el yazısı, telgraf, teleks, faks ve elektronik diğer araçlarla yazılabilir, oluşturulabilir, gönderilebilir*". Maddenin 2. fıkrasına ilişkin olarak gerekçede, kıymetli evrakın güvenli elektronik imza ile düzenlenemeyeceği kuralına konişmento bakımından istisna getirilmesinde *Comite Maritime International*'ın düzenleme ve tavsiyelerinin rol oynadığı belirtilmektedir. Diğerlerinin ise kıymetli evrak niteliği bulunmadığından istisna edildiği ifade edilmektedir. Ancak, 1526. maddenin başlığı "*Güvenli Elektronik İmza*" olmasına rağmen bu

Bu bakımdan kanunen adi yazılı şekle tabi bir hukuki işlemin, güvenli elektronik imza kullanılarak da yapılmasının mümkün olduğu ifade edilmektedir[392]. Nitelikli (mevsuf) yazılı şekil öngörülen hukuki işlemler açısından ise el yazısıyla imzaya ek olarak aranan şekil şartının elektronik ortamda ikame edilebilir olup olmamasına bakılmalıdır[393]. Örneğin, 4077 sayılı Tüketicinin Korunması Hakkında Kanun'un[394] (TKHK.) uygulama alanına giren taksitli satış sözleşmelerine ilişkin olarak TKHK. 6A II hükmünde[395] öngörülen yazılı şekil nitelikli bir yazılı şekil türüdür. TKHK. 6A II hükmünde sözleşmenin geçerli olarak kurulabilmesi için sözleşme metninde yer alması gereken asgari unsurlar belirtilmektedir[396]. Bu unsurları ihtiva eden bir sözleşme metninin elektronik ortamda hazırlanması ve bu metnin güvenli elektronik imza ile imzalanması yoluyla taksitli satış sözleşmesinin geçerli olarak kurulması mümkündür.

---

madde hükmünde "elektronik herhangi bir araç" ifadesine yer verilmesi belirsizlik yaratmaktadır. Burada elektronik araç ifadesi, elektronik yolla atılabilen tüm imzalara (basit elektronik imza) karşılık gelecek şekilde geniş yorumlanabileceği gibi, sadece güvenli elektronik imzaya karşılık gelmek üzere dar da yorumlanabilecektir (Soysal, **a.g.e.**, s.729).

[392] Oğuzman / Öz, **a.g.e**., s.122; İnal, **a.g.e**., s.144.

[393] İsviçre hukukunda da, el yazısıyla imza ile denkliği öngörülen (OR. 14 II) güvenli elektronik imza kullanılarak, el yazısıyla kaleme alınması gereken başka unsurların elektronik ortamda yerine getirilemeyeceği ifade edilmektedir. Örneğin, sorumluluk sınırının el yazısıyla yazılması gerekli olan bir kefalet sözleşmesinin (OR. 493 II) güvenli elektronik imzayla yapılamayacağı belirtilmektedir. Bkz. Bot ZertES 2001, s.5687 ve 5707. Peter Gauch / Walter R. Schluep / Jörg Schmid / Susan Emmenegger, **Schweizerisches Obligationenrecht Allgemeiner Teil**, 9. Aufl., Zürich, Schultess, 2008; Alfred Koller, **Schweizerisches Obligationenrecht**, Allgemeiner Teil, 3. Aufl., 2009, §12 N.51.

[394] RG 08.03.1995, sayı 22221.

[395] TKHK. 6A II hükmü şu şekildedir:

> "*Taksitle satış sözleşmesinin yazılı şekilde yapılması zorunludur. Sözleşmede bulunması gereken asgari koşullar aşağıda gösterilmiştir:*
>
> *a) Tüketicinin ve satıcı veya sağlayıcının isim, unvan, açık adresleri ve varsa erişim bilgileri,*
>
> *b) Malın veya hizmetin Türk Lirası olarak vergiler dahil peşin satış fiyatı,*
>
> *c) Vadeye göre faiz ile birlikte ödenecek Türk Lirası olarak toplam satış fiyatı,*
>
> *d) Faiz miktarı, faizin hesaplandığı yıllık oran ve sözleşmede belirlenen faiz oranının yüzde otuz fazlasını geçmemek üzere gecikme faizi oranı,*
>
> *e) Peşinat tutarı,*
>
> *f) Ödeme planı,*
>
> *g) Borçlunun temerrüde düşmesinin hukuki sonuçları.*

[396] Bu özel şartlarda eksiklikliğinin sözleşmenin geçersizliğine yol açacağı, ancak bu şekil şartının tüketiciyi korumaya yönelik olması sebebiyle tüketicinin aleyhine olarak tüketiciye karşı ileri sürülemeyeceği görüşünde: Oğuzman / Öz, **a.g.e.,** s.120. Söz konusu eksikliklerin sözleşmenin geçerliliğini etkilemeyeceği görüşünde: Kocayusufpaşaoğlu, **a.g.e**., s.278.

El yazısıyla vasiyetnamenin ise güvenli elektronik imza kullanılarak gerçekleştirilmesine imkan bulunmamaktadır. Çünkü bir vasiyetnamenin geçerli olarak hüküm ifade edebilmesi için, yapıldığı yıl, ay ve gün gösterilerek başından sonuna kadar mirasbırakanın el yazısı ile yazılmış ve imzalanmış olması zorunludur (MK. 538 I). Güvenli elektronik imza, el yazısıyla imzanın hukuki sonuçlarını doğurmasına rağmen, vasiyetnamede el yazısıyla yazılması gerekli olan diğer unsurları elektronik ortamda karşılamak bakımından yeterli değildir[397]. Benzer şekilde özellikle hukuki işlemi yapan kişiyi korumak için, işlemle ilgili beyanın tamamının veya bir bölümünün el yazısı ile yazılmasının öngörüldüğü durumlarda bu beyanın elektronik ortamda yazılması ve güvenli elektronik imza ile imzalanması yeterli olmayacaktır[398].

2. İradi Şekil Açısından

Tarafların anlaşması sonucu geçerliliği iradi olarak adi yazılı şekle tabi tutulan hukuki işlemler güvenli elektronik imza ile yapılabilir[399]. Taraflar hiçbir açıklama yapmaksızın yalnızca yazılı şekilden bahsetmişlerse, BK. 16 II uyarınca kanunun öngördüğü adi yazılı şekil hükümlerine uyulması ve sözleşmenin güvenli elektronik imza ile imzalanması gerekmektedir. Şekil serbestisi ilkesi uyarınca

---

[397] El yazısıyla vasiyetname açısından görülen şekil şartının güvenli elektronik imzanın kullanılmasına engel olduğu görüşünde: Kocayusufpaşaoğlu, **a.g.e**., s.296; Rona Serozan / Baki İlkay Engin, **Miras Hukuku**, 2. Bası, Ankara, Seçkin, 2008, §4 N 88.

Öğretide, el yazısıyla vasiyetnamenin güvenli elektronik imza ile yapılamayacağına gerekçe olarak, bunun kanunun ruhuna aykırı düşeceği ve güvenli elektronik imzanın yerinin yalnızca borçlar hukuku bakımından netleştiği, miras hukuku alanında kıyasen uygulanmasının ise uygun düşmeyeceği ifade edilmektedir (Doruk Gönen, **El Yazılı Vasiyetname**, İstanbul, Legal, 2007, s.94). Bize göre burada sunulan iki gerekçe de isabetli değildir. Öncelikle borçlar hukukunun adi yazılı şekle ve imza unsuruna ilişkin 12-15.maddeleri, hakkında ayrı bir hüküm bulunmayan bütün hukuki işlemlerde kıyasen uygulanır (Oğuzman / Öz, **a.g.e**., s.117). Bu nedenle BK. 14 hükmünde düzenlenen güvenli elektronik imzanın yerinin yalnızca borçlar hukuku bakımından netleştiğini söylemek doğru değildir. El yazısıyla vasiyetnamede güvenli elektronik imzanın kullanılmasına engel olan, konunun miras hukukunda düzenlemiş olması değil, MK. 538 I hükmünde açıkça nitelikli bir şekil şartı olarak metnin de baştan sona el yazısıyla yazılmasının aranmış olmasıdır. Bu açık düzenleme karşısında "kanunun ruhu" kavramına başvurmaya da gerek bulunmamaktadır.

[398] Özdemir Kocasakal, **a.g.e**., s.102. Adi yazılı ve nitelikli yazılı şekle tabi sözleşmelerde güvenli elektronik imza kullanılıp kullanılamayacağı konusunda EİK. 5 hükmünde açıklık bulunmadığı görüşünde: Orta, **a.g.e**., s.140.

[399] Ahmet Kılıçoğlu, **Borçlar Hukuku Genel Hükümler**, 10. Bası, Ankara, Turhan Kitabevi, 2008, s.84.

tarafların, basit elektronik imza kullanılmasını öngörmek suretiyle de iradi şekil kararlaştırabilmeleri mümkündür[400].

İradi şekil söz konusu olan hallerde, BK. 16 I hükmü çerçevesinde, tarafların sözleşmenin geçerliliğini yalnızca el yazısıyla atılacak imza şartına bağlı tutmalarına, diğer bir ifadeyle tarafların güvenli elektronik imzanın adi yazılı şekil şartını gerçekleştirmeyeceğini kararlaştırmalarına ise şekil serbestisi gereği hiçbir engel bulunmamaktadır[401].

Bunun dışında tarafların iradi şekil kapsamında güvenli elektronik imzanın hukuki sonuç doğurmasını belirli bir teknik şartın yerine getirilmesine bağlamaları mümkün müdür? Örneğin, taraflar güvenli elektronik imzanın geçerliliğini yalnızca (A) Sertifika Sağlayıcısı tarafından üretilen veya (mevzuatta asgari olarak belirlenen standarttan daha gelişmiş) (X) standardını yerine getiren bir nitelikli sertifikaya dayanmasına bağlı tutabilir mi? Bu konu özellikle tarafların farklı ülkelerde bulunması ve yabancı sertifikaların kullanılması halinde önem kazanabilir. Elektronik İmza Kanunu'nun aradığı asgari şartları yerine getirmesi şartıyla taraflar arasında belirli tipte güvenli elektronik imzaların veya nitelikli sertifikaların kullanılmasına ilişkin böyle bir anlaşma yapılması, yine şekil serbestisi çerçevesinde, mümkün kabul edilmelidir.

---

[400] İnal, **a.g.e**., s.150. Bu konuda Alman hukukunda iradi olarak elektronik şekil kararlaştırılan hallerde, taraflarca açık veya örtülü olarak nitelikli elektronik imza kullanılması öngörülmediği takdirde, herhangi bir elektronik imzanın, bir basit elektronik imzanın dahi, iradi şekil bakımından yeterli sayılacağı kabul edilmektedir (BGB §127 III).

[401] Aksi görüş için bkz. Leyla Keser Berber, "Elektronik Ticaret Koordinasyon Kurulu'nun (ETKK) "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanunu Tasarısı Taslağı"na Yönelik Farklı Yaklaşımlar", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, S.1, 2002, s.165-195, s.174. ETKK tarafından hazırlanan taslakta, (güvenli elektronik imzaya karşılık gelen bir kavram olan) nitelikli elektronik imzanın el yazısıyla imzaya denkliğini "tarafların bunun aksini kararlaştırmamalarına" bağlı tutan bir düzenleme yer almaktaydı. Yazar, bu düzenlemenin, elektronik imza kanununu kabul etmekle çeliştiğini, bunun elektronik imzadan korktuğumuzu ve güvenmediğimizi sergileyen bir tutum olduğunu belirtmiştir.

C. GÜVENLİ ELEKTRONİK İMZA İLE YAPILAMAYACAK HUKUKİ İŞLEMLER

EİK. 5 II hükmüne göre "*kanunen resmi şekle veya özel bir merasime tabi tutulan hukuki işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez*"[402].

Bu hüküm ile ilk olarak resmi şekle veya özel bir merasime tabi hukuki işlemlerin hiçbir suretle güvenli elektronik imza ile yapılamayacağı açıklığa kavuşturulmaktadır. Ayrıca güvenli elektronik imzanın el yazısıyla imza ile aynı hukuki sonucu doğurmasını öngören EİK. 5 I hükmüne teminat sözleşmeleri bakımından istisna getirilmektedir. Teminat sözleşmeleri bakımından, madde gerekçesinde elektronik imzanın kullanımının kolaylığı nedeniyle doğması muhtemel zararların önüne geçilmesi amacı gözetilerek böyle bir istisna getirildiği belirtilmektedir.

Öğretide güvenli elektronik imzanın el yazısıyla imzayla denkliği kuralına Borçlar Kanunu'nda herhangi bir istisna öngörülmemiş olması nedeniyle, EİK. 5 II'de yer alan istisnaların yürürlüğünün tartışmalı hale gelebileceği ifade edilmiştir[403]. Bu hususta, Borçlar Kanunu'nda açıkça aksini öngören bir düzenleme olmaması nedeniyle, EİK. 5 II hükmünde yer alan istisnaların BK. 14 I hükmünün uygulama alanı bakımından da etki doğuracağını kabul etmek gerekmektedir. Bu düzenlemeye ne yürürlükteki Borçlar Kanunu'nda ne de 1.07.2012 tarihinde yürürlüğe girecek 6098 sayılı yeni Türk Borçlar Kanunu'nda yer verilmiş olması, bu hükümde yer alan istisnaların gelişen ekonomik ve sosyal koşullar neticesinde belirli bir süre sonra ortadan kalkabilecek bir nitelik taşıdığını ortaya koymaktadır. Özellikle teminat sözleşmeleri bakımından elektronik imzanın uyarı fonksiyonunun belirli bir bilincin gelişmesi neticesinde el yazısıyla imzayla eşit seviyeye gelebileceğinin öngörüldüğünü, bu nedenle temel kanun yerine özel nitelikli

---

[402] Bu hüküm AB Elektronik Ticaret Yönergesi'nin m.9/2 hükmünde üye devletlerce istisna edilebileceği belirtilen hukuki işlemlere işaret etmektedir (İnal, **a.g.e**., s.144).

[403] Aksoy, **a.g.e**., s.256.

Elektronik İmza Kanunu'nda muhafaza edilmek istenmiş olduğunu düşündürmektedir[404].

Aşağıda güvenli elektronik imzanın uygulanamayacağı hukuki işlemlere ilişkin EİK. 5 II hükmünde yer alan bu üç kategorinin nasıl anlaşılması gerektiği açıklanmaya çalışılacaktır[405].

1. Geçerliliği Resmi Şekle Tabi Tutulan Hukuki İşlemler

EİK. 5 II hükmüne göre "*kanunen geçerliliği resmi şekle veya özel bir merasime tabi tutulan hukuki işlemler… güvenli elektronik imza ile gerçekleştirilemez"*.

Bu hüküm, öncelikle resmi şekle tabi hukuki işlemlerin güvenli elektronik imza ile yapılamayacağını açıklığa kavuşturmaktadır. Aslında EİK. 5 I hükmü tek başına incelendiğinde güvenli elektronik imzanın resmi şekil şartını gerçekleştirmeye yeterli olmayacağı hükmün ifadesinden anlaşılmaktadır. Çünkü resmi şeklin tamamlanması için el yazısıyla imza unsuruna ek olarak resmi bir makamın katılımına da ihtiyaç bulunmaktadır. El yazısıyla imza zaten hukuki sonuçları itibariyle tek başına resmi şekli gerçekleştirmeye yeterli olmamaktadır. Bu açıdan, EİK. 5 II hükmü ile güvenli elektronik imzanın uygulama alanı bakımından bir istisna öngörüldüğünü söylemek yerine, resmi şekil bakımından ortaya çıkabilecek tereddütlerin giderildiğini ifade etmenin daha uygun olacağı kanaatindeyiz.

Resmi şekle tabi hukuki işlemeler bakımından, ileride noterlik hizmetlerinin elektronik ortamda verilmeye başlanması halinde durumun ne olacağı konusu önem kazanmaktadır. Örneğin, Avusturya hukukunda, 1 Ocak 2007 tarihi itibariyle yürürlüğe giren bir kanun değişikliğiyle, geçerliliği için noterin katılımı gerekli olan

---

[404] Dijital imzanın uyarı işlevi hakkındaki tartışmalar için bkz. s.24.

[405] EİK. 5 hükmü ile elektronik imzanın el yazısıyla imza ile aynı hukuki sonucu doğurmasının öngörüldüğü, ancak buna "kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler" ve "teminat sözleşmeleri" olmak üzere iki istisna tanındığı şeklinde: Kocayusufpaşaoğlu, **a.g.e**., s.295.

sözleşmelerin elektronik ortamda yapılması mümkün hale getirilmiştir[406]. Bunun için öncelikle tarafların sözleşme metnini güvenli elektronik imzaları ile noter önünde imzalamaları, daha sonrasında bu metni özel bir sertifikaya dayanan elektronik imzasını kullarak (*elektronische Beurkundungssignatur des Notars*) noterin de imzalaması gerekmektedir. Dolayısıyla, tarafların noter önünde bizzat bulunmaları bu belgelerin elektronik olarak meydana getirilmesi için zorunlu tutulmaktadır[407].

Türk hukukunda, e-devlet uygulamaları kapsamında noterlik işlemlerinin de elektronik ortamda yapılıp yapılamayacağı konusu tartışılmaktadır[408]. Bu bağlamda Noterlik Kanunu'nda değişikliğe gidilerek düzenleme veya onaylama şeklindeki işlemlerin noterler tarafından elektronik ortamda yapılabileceğinin kabul edilmesi gerektiği ileri sürülmektedir[409]. Hükümet tarafından 11.03.2010 tarihinde TBMM'ye sevk edilen "*Kamu Hizmetlerinin Hızlandırılması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı"*nın 11. maddesinde, noter huzurunda veya noter huzurunda olmadan yapılabilecek belirli noterlik işlemlerinin elektronik ortamda güvenli elektronik imza kullanılarak

---

406 Avusturya Elektronik İmza Kanunu (*Bundesgesetz über elektronische Signaturen*) §4 için bkz. BGBl. I Nr. 190/1999. 1 Ocak 2007 itibariyle yürürlüğe giren, 30 Aralık 2005 tarihli Kanun (*Berufsrechts-Änderungsgesetz für Notare, Rechtsanwälte und Ziviltechniker*) için bkz. BGBl. I Nr. 164/2005.

407 Daha sonra bu belgeler noterler tarafından özel bir arşivde (*Urkundenarchiv des österreichishen Notariats*) saklanacaktır. Avusturya hukukunda daha önceleri elektronik ortamda kurulamayacak sözleşmelere ilişkin AB Elektronik Ticaret Yönergesi'nde gösterilen istisnaların neredeyse tamamı kabul edilmekteyken, 1 Ocak 2007 tarihi itibariyle yürürlüğe giren değişikliklerle evlenme sözleşmesi ve vasiyetname gibi belirli işlemler dışında tüm hukuki işlemlerin elektronik ortamda yapılmasına izin verilmiş olmaktadır. Bkz. **The ELDOC Study: Legal Study on Legal and Administrative Practices Regarding the Validity and Mutual Recognition of Electronic Documents,** DG Enterprise & Industry, European Commission 2006, (Çevrimiçi) http://ec.europa.eu/enterprise/ sectors/ict/files/dumortier-final-report-draft_en.pdf, 10.06.2011.

408 Hukukumuzda elektronik noterlik konusunda henüz bir yasal düzenleme yapılmış değildir. Konuya genel bir bakış için bkz. İnci Biçkin, "Noterlik İşlemlerinin Elektronik Ortamda Yapılmasının Gerekliliği", **Türkiye Noterler Birliği**, S.126, Mayıs 2005, s.124.

409 Bir noterin, dijital imza esasına dayalı bir sistemde, aşağıdaki faaliyetleri ilke olarak elektronik ortamda yapabileceği düşünülmektedir:

a) Elektronik zaman damgası vurmak,

b) Elektronik olarak düzenleme şeklinde belge hazırlamak,

c) Elektronik olarak gönderilen dokümanlardaki elektronik imza ve tarihi onaylamak,

d) Elektronik dokümanları muhafaza etmek, bunların varlığını ve içeriğini istendiğinde elektronik olarak belgelendirmek (Biçkin, **a.g.e.**, s.124).

yapılabileceği düzenlenerek, söz konusu noterlik işlemlerinin neler olduğunun Adalet Bakanlığı'nın uygun görüşü alınarak Türkiye Noterler Birliği tarafından belirleneceği belirtilmektedir.[410]Ancak böyle bir değişikliğin yapılması halinde dahi, resmi şeklin elektronik ortamda gerçekleştirilmesine EİK. 5 II hükmünün varlığı halihazırdaki haliyle engel olacaktır[411].

---

[410] Tasarı'nın 11. maddesiyle 18.1.1972 tarihli ve 1512 sayılı Noterlik Kanunun 198'inci maddesinden sonra gelmek üzere aşağıdaki madde eklenmektedir.

"Elektronik işlemler:

MADDE 198/A- Bu Kanunun uygulanmasında, güvenli elektronik imza, elle atılan imza ile aynı ispat gücünü haiz olup, kanunlarda güvenli elektronik imza ile yapılamayacağı açıkça belirtilmiş olan işlemler dışında, elle atılan imza yerine kullanılabilir.

Elektronik ortamda güvenli elektronik imza kullanılarak noter huzurunda veya huzurda olmadan yapılabilecek noterlik işlemleri ile 15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu ve ilgili ikincil mevzuatta tanımlanan zaman damgası kullanılmasının zorunlu olduğu noterlik işlemleri, Adalet Bakanlığının uygun görüşü alınarak Türkiye Noterler Birliği tarafından belirlenir. Belirlenen bu noterlik işlemlerine ilişkin tüm belgeler güvenli elektronik imzayla elektronik ortamda düzenlenebilir, işlenebilir, saklanabilir ve gerektiğinde ilgili diğer kişi veya kurumlara elektronik ortamda gönderilebilir. Güvenli elektronik imza ile imzalanmış belgelerde kanunlarda belirtilen mühürleme işlemi uygulanmaz ve ayrıca suret aranmaz. Güvenli elektronik imza ile düzenlenen belge, özellikle talep edilmedikçe ayrıca fizikî olarak düzenlenmez. Elektronik ortamdan fizikî örnek çıkarılması gereken hâllerde, belgeye "Güvenli elektronik imzalı aslı ile aynıdır." ibaresi ile imzalayanın adı, soyadı, unvanı, çalıştığı birimin adı ve tarih eklenerek noter veya yetkili personel tarafından elle atılan imza ile imzalanır ve mühürlenir. Güvenli elektronik imza ile imzalanmış belgenin elle atılan imzalı suretiyle çelişmesi hâlinde, noterlerin kullandığı bilişim sisteminde kayıtlı olan güvenli elektronik imzalı nüsha esas alınır.

Bu Kanun kapsamında noterlik işlemlerinin elektronik ortamda yapılması için toplanması gerekli olan kişisel veriler, kişisel verilerin korunması ve bilgi güvenliğinin sağlanmasına ilişkin mevzuatta belirlenen tedbirler alınarak korunur.

Elektronik ortamda yapılacak noterlik işlemlerine ilişkin ücretler, Türkiye Noterler Birliğinin görüşü alınarak Adalet Bakanlığı tarafından düzenlenecek bir tarife ile belirlenir.

İkinci fıkra uyarınca elektronik ortamda yapılabilecek bir noterlik işleminin bir belgeye dayanması hâlinde; belge sureti, taraflar, vekilleri veya temsilcileri tarafından güvenli elektronik imza ile imzalanarak elektronik ortamda notere gönderilebilir. Ancak belge aslının fizikî olarak ibrazının zorunlu olduğu hâllerde, elektronik ortamda yapılan başvuru sonrasında belge aslı yönetmelikte belirlenen süre içinde notere ibraz edilir.

Elektronik ortamda noter huzurunda veya huzurda olmadan yürütülecek noterlik işlemlerine ve bu işlemleri yapabilecek noterlerin sağlaması gerekli olan asgarî teknik ve idarî şartlara dair usûl ve esaslar, Türkiye Noterler Birliğinin görüşü alınarak Adalet Bakanlığı tarafından yönetmelikle düzenlenir.

Yurt dışında yürütülen noterlik işlemlerinin elektronik ortamda yapılmasına ve bu işlemlerin yerine getirilmesi için sağlanması gerekli olan asgarî teknik ve idarî şartlara dair usûl ve esaslar, Türkiye Noterler Birliği ile Adalet Bakanlığının görüşleri alınarak Dışişleri Bakanlığı tarafından yönetmelikle düzenlenir."

[411] 31.12.2009 tarih ve 27449 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren ve 2918 sayılı Karayolları Trafik Kanunu'nun 20. maddesinin (d) ve (e) bentlerini değiştiren 5942 sayılı Kanun'un birinci maddesi gereğince, tescil edilmiş araçların her çeşit satış ve devirlerine ilişkin işlemler 01.05.2010 tarihinden itibaren noterler tarafından elektronik ortamda yapılmaya başlanmıştır. Satış ve devir sözleşmesi noter yetkilisi tarafından elektronik ortamdaki bilgiler esas alınarak hazırlanmakta ve taraflarca imzalanmaktadır. Daha sonra elektronik ortamda yeni sahipler

Bu açıklamalar çerçevesinde, örneğin resmi şekle tabi taşınmaz satış vaadinin veya ipotek sözleşmesinin güvenli elektronik imza yoluyla elektronik ortamda imzalanması söz konusu olamayacağı açıktır. Her ne kadar EİK. 5 II hükmü "*kanunların resmi şekle tabi tuttuğu işlemler*"in güvenli elektronik imza yoluyla gerçekleştirilemeyeceğini düzenliyor olsa da, aynı esasın (kanunen resmi şekil öngörülmediği halde) taraflarca iradi olarak bir sözleşmenin gerçerlilik şartı olarak resmi şeklin kararlaştırılması halinde de uygulanması gerekmektedir. Çünkü iradi olarak resmi şeklin geçerlilik şekli olarak kararlaştırıldığı hallerde de güvenli elektronik imza, resmi memur huzurunda gerçekleştirilmesi gereken resmi şekil şartını gerçekleştirmeye yeterli olmayacaktır[412].

2. Geçerliliği Özel Merasime Tabi Tutulan Hukuki İşlemler

EİK. 5 II hükmünde ikinci olarak, "*özel merasime tabi hukuki işlemler*"in güvenli elektronik imzayla gerçekleştirilemeyeceği belirtilmektedir. Merasimli şekil kavramı, ilk bakışta eski hukuk sistemlerinin kabul ettiği bir şekil tarzı olarak yorumlanmaya açıktır. Böyle bir merasim esnasında tarafların karşılıklı olarak bir takım sözleri sarf etmeleri gerekmektedir[413]. Medeni Hukuk açısından bu anlamdaki özel merasime tabi bir hukuki işleme örnek olarak evlenme sözleşmesi dışında bir örnek bulmak zordur[414]. Bir evlenme sözleşmesinin meydana gelebilmesi için de, tarafların karşılıklı ve birbirine uygun irade beyanlarını, yetkili evlenme memuru önünde sözlü şekilde açıklamaları gerekmektedir (MK. 142). Yani bu sözleşmede tarafların irade beyanlarını sözlü olarak açıklamak zorunda oluşu nedeniyle zaten el yazısıyla imza unsuru bulunmadığı gibi, bunun yanı sıra bir yetkili memurun

---

adına tescil işlemi yapılmaktadır. Ancak burada noterler tarafından elektronik ortamda yapılması kabul edilen işlemler usuli niteliktedir. Noterin hazırladığı satım sözleşmesini tarafların güvenli elektronik imza ile imzalaması gibi, tamamen elektronik ortamda (bilgisayar çıktısı alınmaksızın) noter aracılığıyla yapılabilmesi söz konusu değildir. Bu düzenleme güvenli elektronik imzanın resmi şekle tabi hukuki işlemler bakımından uygulanamayacağı kuralı bakımından bir değişiklik yaratmamaktadır.

412 Kılıçoğlu, **a.g.e.,** s.84; Kocayusufpaşaoğlu, **a.g.e**., s.291.

413 Bu nedenle bu tür sözleşmeleri "sözlü merasime tabi hukuki işlemler" olarak adlandırmak mümkündür: İnan, **a.g.e**., s.134.

414 Kocayusufpaşaoğlu, **a.g.e**., s.291.

bulunması zorunluluğu bu sözleşmenin güvenli elektronik imzaya elverişli olmadığını ortaya koymaktadır[415].

Diğer taraftan, EİK 5 II hükmündeki "özel merasime tabi hukuki işlemler" ifadesine, yazılı şeklin güvenli elektronik imza ile yerine getirilemeyen ilave unsurlarına karşılık gelecek şekilde, nitelikli yazılı şeklin öngörüldüğü hukuki işlemleri kapsayan, daha geniş bir anlam verilmesi de mümkün olabilir. Hükmün uygulama alanının bu şekilde belirlenmesi halinde, el yazısıyla vasiyetnamenin veya kefalet sözleşmesinin güvenli elektronik imza aracılığıyla yapılamayacağı, yukarıda el yazısıyla imza ile güvenli elektronik imzanın denkliği ilkesi çerçevesinde başvurduğumuz yoruma ihtiyaç olmaksızın[416], doğrudan yasal bir dayanağa kavuşturulmuş olacaktır.

3. Teminat Sözleşmeleri

a. Teminat Sözleşmesi Kavramı

Türk hukukunda teminat sözleşmesi kavramı, en geniş anlamıyla bir kimsenin bir başkasının karşı karşıya olduğu bir tehlikeyi (rizikoyu) kendi üzerine aldığı bütün sözleşmeler için kullanılmaktadır. Burada tehlike deyimi bir kimsenin malvarlığı ile ilgili bir zararın ortaya çıkması olasılığını ifade etmektedir[417].

Teminat sözleşmesi kavramının nasıl anlaşılması gerektiğini belirlerken, bağımsız bir sözleşme niteliği taşıyan teminat sözleşmeleri ile bir sözleşme içindeki bağımsız olmayan (fer'i) teminat yükümlülüklerinin birbirinden ayırt edilmesi gerekmektedir. Örneğin, satım sözleşmesinde satıcının ayıba ve zapta karşı tekeffül yükümlülüğü bizzat satıcı tarafından üstlenilen ve bağımsız nitelikte olmayan bir yükümlülüktür. Bir saat satışında iki yıl için bozulmayacağına veya bozulursa

---

[415] Aynı görüşte: Kocayusufpaşaoğlu, **a.g.e**., s.291.

[416] Bkz. s.112 vd.

[417] Halûk Tandoğan, **Borçlar Hukuku, Özel Borç İlişkileri,** C.II**,** 3. Bası, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü, 1987, s.685.

bedelsiz tamir edileceğine dair teminat verilmesi de bu niteliktedir[418]. Asıl borcun gereği gibi veya vaktinde yerine getirilmemesi tehlikesinden doğan zararı karşılamaya yönelik olarak kanun tarafından veya taraflarca öngörülen bu tür teminat yükümlülükleri teminat sözleşmesi kavramı içinde yer almamaktadır[419]. Bu tür yan yükümlülük niteliğinde bağımsız olmayan ve bizzat borçlu tarafından üstlenilen teminat yükümlülükleri içeren sözleşmelerin güvenli elektronik imza ile gerçekleştirilmesine engel bulunmamaktadır.

b. Teminat Sözleşmelerine İlişkin İstisnanın Anlamı

EİK. 5 II hükmüne göre "… *teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez*".

Bu hüküm ile güvenli elektronik imzanın el yazısıyla imza ile aynı hukuki sonucu doğuracağı kuralına (EİK. 5 I) istisna getirilmekte, güvenli elektronik imzanın uygulama alanı teminat sözleşmeleri bakımından daraltılmaktadır. EİK. 5 hükmüne ilişkin madde gerekçesinde, elektronik imzanın kullanımının kolaylığı nedeniyle doğması muhtemel zararların önüne geçilmesi amacıyla teminat sözleşmelerinin kapsam dışında bırakıldığı belirtilmektedir[420]. Burada el yazısıyla imzada bulunan uyarı işlevinin güvenli elektronik imza bakımından yeterli şekilde sağlanmadığı ifade edilmektir.

Güvenli elektronik imzanın uygulama alanı bakımından EİK. 5 II hükmünün nasıl yorumlanması gerektiğine ilişkin öğretideki hakim görüş, şekle tabi olup olmaması bakımından ayrım yapılmaksızın teminat sözleşmelerinin güvenli

---

[418] Türk hukukunda konunun özel bir düzenlemesi için bkz. 4077 sayılı Tüketicinin Korunması Hakkında Kanun'a dayalı olarak çıkarılan 14.06.2003 tarihli, 25138 sayılı Garanti Belgesi Uygulama Esaslarına Dair Yönetmelik.

[419] Tandoğan, **Özel Borç İlişkileri II**, s.686.

[420] Elektronik İmza Kanunu'nun genel gerekçesi ve madde gerekçeleri için bkz. (Çevrimiçi) http://www2. tbmm.gov.tr/d22/1/1-0613.pdf, 04.02.2011. Yazılı şeklin uyarı işlevi bakımından, ticari işlerde tacir kişilerin basiretli bir iş adamı gibi hareket etmesi kendilerinden beklendiğinden elektronik imzayı oluştururken de aynı özeni göstermeleri gerekmektedir; bu nedenle uyarı işlevinin tacirler açısından mevcut olduğu görüşü hakkında bkz. Karan, **a.g.e**., s.147.

elektronik imza yoluyla yapılamayacağı yönündedir. *Kocayusufpaşaoğlu*, teminat sözleşmeleri bakımından getirilen bu istisna neticesinde, kefalet ve garanti sözleşmeleri yanında, taşınır rehni kurmaya yönelik sözleşmelerde de elektronik imzanın kullanılamayacağını ifade etmektedir[421]. Aynı şekilde *Eren*, kefalet, rehin ve üçüncü kişinin fiilini taahhüt gibi teminat sözleşmelerinin elektronik imza ile yapılamayacağını belirtmektedir[422]. *Kılıçoğlu*'na göre, bu hüküm taşınır rehni bakımından önem taşımaktadır. Zira taşınmaz rehni MK. 856 gereğince kanunen resmi şekle bağlı bir sözleşme olduğundan zaten bu yasanın kapsamına girmez. Taşınır rehni ile ilgili MK. 939 hükmü bir şekil koşulu öngörmediği halde, EİK. 5 II karşısında buna ilişkin bir sözleşme elektronik imza yoluyla kurulamayacaktır[423]. Görüldüğü gibi bu görüşteki yazarlara göre, esasen geçerliliği bir şekle bağlı olmayan garanti ve taşınır rehni gibi sözleşmeler bir teminat sözleşmesi niteliği taşımaları nedeniyle, EİK. 5 II hükmünün kapsamına girmektedir, bu nedenle de güvenli elektronik imza yoluyla yapılmaları mümkün değildir[424].

Bu konuda *Oğuzman/Öz* daha farklı bir yaklaşımla, birer teminat sözleşmesi niteliğindeki kefalet, rehin, üçüncü kişinin fiilini taahhüt sözleşmelerinin sanal ortamda elektronik imza ile yapılamayacağını, ancak esasen taşınır rehni kurma ve üçüncü kişinin fiilini taahhüt sözleşmeleri kanunen hiçbir şekle tabi tutulmadığından bu hükmün sadece kefalet sözleşmesi bakımından pratikte önem arz edeceğini belirtmektedir[425].

Teminat sözleşmeleri açısından getirilen bu istisnanın kaynağı AB Elektronik Ticaret Yönergesi'nin 9. maddesinde yer almaktadır. AB Elektronik Ticaret Yönergesi m.9/1 (c) hükmüne göre üye devletler "*ticari, iş veya mesleki amaçları dışında hareket eden kişiler tarafından verilen teminatlara ilişkin sözleşmeler ve bu kişilerin borç altına girdiği kefalet sözleşmeleri*"nin elektronik ortamda kurulması

---

421 Kocayusufpaşaoğlu, **a.g.e**., s.296

422 Eren, **a.g.e.**, s.253.

423 Kılıçoğlu, **a.g.e**., s.84-85.

424 Aynı yönde: Haluk Nomer, **Borçlar Hukuku Genel Hükümler**, 9. Bası, İstanbul, Beta, 2011, s.60.

425 Oğuzman / Öz, **a.g.e**., s.122.

konusunda istisna öngörebilir. Bu hüküm tüketicinin koruması kaygısıyla ve bunun yanı sıra finans kurumlarının baskıları sonucu Yönerge metnine eklenmiş bir hükümdür. Bu baskıların temelinde, teminat sözleşmelerinin elektronik ortamda yapılması halinde, şeklin tarafları düşünmeye sevkederek bu sayede hukuki işlemin anlam ve sonuçlarını idrak etmelerini sağlayan uyarı işlevinin azalacağı kaygısı yer almaktadır[426].

AB Elektronik Ticaret Yönergesi m.9/2'deki dört bentte belirtilen sözleşmelerin, elektronik ortamda yapılmaları halinde, hukuki etki ve geçerlilik doğurmalarına üye devletlerin hukukunda engel olunabileceği, bu konuda m.9/1 hükmüne istisna getirilebileceği düzenlemektedir[427]. Yani bu hüküm, yalnızca güvenli elektronik imzayı değil, diğer tüm elektronik araçları da (e-posta, forum, video-konferans, sohbet odaları vb.) kapsamakta ve bu sayede belirtilen sözleşmeler bakımından elektronik ortamda açıklanan icap ve kabul beyanlarının hukuken etki doğurmayacağına ilişkin yapılacak düzenlemelere izin verilmektedir.

EİK. 5 II hükmü, AB Elektronik Ticaret Yönergesi m.9/2'ye paralel olarak, resmi şekle ve özel merasime tabi sözleşmeler yanında teminat sözleşmeleri bakımından da sınırlama öngörmekte, hatta Yönerge'nin bir adım ilerisine giderek teminatın mesleki amaç çerçevesinde verildiği durumları da kapsayacak daha geniş bir istisna öngörmektedir. Ayrıca EİK. 5 II hükmü teminat sözleşmelerinin güvenli elektronik imza ile yapılamayacağını hükme bağlamaktadır. Teminat sözleşmelerinin elektronik ortamda kuruluşuna ilişkin genel bir istisna öngörmemektedir.

Bununla birlikte, doktrindeki hakim görüş dikkate alındığında, EİK. 5 II hükmünün yorumu şekle tabi olmayan teminat sözleşmeleri bakımından önem taşımaktadır. Eğer bu istisnanın hukuki etkisi, EİK. 5 II hükmünün düzenlenmesinde örnek alınan AB Elektronik Ticaret Yönergesi m.9/2'ye paralel olarak yorumlanacak olursa, teminat sözleşmelerinin hiçbir şekilde elektronik olarak kurulamayacağı

---

[426] Andrew D. Murray, **Regulating Electronic Contracts: Comparing the European and North American Approaches**, (Çevrimiçi) http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=andrew_murray, 5.02.2011.

[427] AB Elektronik Ticaret Yönergesi m.9/2 hükmünün düzenleme şekli için bkz. s.31.

sonucuna varmak gerekir. Çünkü şekle tabi olmayan bir teminat sözleşmesi güvenli elektronik imza aracılığıyla yapılamıyorsa, basit elektronik imza kullanılarak da evleviyyetle yapılamayacaktır[428]. Bu durumda, şekle tabi olmayan örneğin bir garanti sözleşmesi elektronik yolla kurulamayacaktır.

Kanaatimizce teminat sözleşmelerine ilişkin olarak getirilen bu istisnanın yalnızca kanunen geçerliliği yazılı şekle tabi tutulan teminat sözleşmeleriyle sınırlı olarak dar yorumlanması isabetli olacaktır. Böyle bir yorumu tercih etmemizin gerekçelerinden ilki, BK.14 I hükmü ile yazılı şekil şartının güvenli elektronik imza yoluyla gerçekleştirileceğinin açıkça düzenlenmiş olmasıdır. Bu hüküm karşısında EİK. 5 II hükmü, yalnızca yazılı şekil şartının teminat sözleşmeleri bakımından güvenli elektronik imza ile yerine getirilemeyeceği yönelik olarak hukuki etki doğurabilir. Kanunun hiçbir şekle tabi tutmadığı, bu nedenle basit bir elektronik posta gönderilmesi yoluyla, hatta sözlü şekilde dahi kurulması mümkün olan teminat sözleşmelerinin, kanunen prensipte el yazısıyla imzaya denk kılınmış güvenli elektronik imza aracılığıyla yapılmasına hiçbir engel bulunmamaktadır.

Bunun yanı sıra, eğer şekle tabi olmayan teminat sözleşmelerinin elektronik ortamda kurulmasına engel olunması amaçlandıysa, diğer bir ifadeyle bu sözleşmelerin sözlü şekilde yapılması mümkün olmasına rağmen güvenli elektronik imza da dahil olmak üzere hiçbir suretle elektronik ortamda yapılamayacağı düzenlenlenmek istendiyse, o takdirde böyle bir istisnaya Elektronik İmza Kanunu yerine Borçlar Kanunu'nda yer verilmesi gerekirdi. Çünkü, Elektronik İmza Kanunu genel olarak elektronik imzanın teknik yapısı ve sertifikasyon hizmeti hakkında düzenlemeler getirmekte olup, elektronik ortamda sözleşmelerin kuruluşuna dair hiçbir düzenleme içermemektedir. Bu konu Borçlar hukukunun konusudur. Bu nedenle, şayet EİK. 5 II hükmü ile teminat sözleşmeleri gibi geniş bir kategoriye atıfta bulunularak bu kapsamda yer alan sözleşme türlerinin hiçbir şekilde elektronik yolla gerçekleştirilemeyeceğini düzenlemek amaçlanıyorsa, böyle bir sınırlamaya,

[428] Karşı görüş: İnal, **a.g.e**., s.144. Yazar, EİK. 5 II hükmü uyarınca, kanunen resmi şekle veya özel bir merasime tabi tutulmuş hukuki işlemlerin ve teminat sözleşmelerinin güvenli elektronik imza ile imzalanmış olsa dahi elektronik ortamda yapılamayacağını ifade etmektedir. Bu hükümle AB Elektronik Ticaret Yönergesi'nde üye devletlerce istisna edilebileceği düzenlenen hukuki işlemler, Türk hukukunda büyük ölçüde istisna edilmiş olmaktadır.

Borçlar Kanunu'nunda ve her sözleşmeye ilişkin maddede ayrı ayrı belirtmek suretiyle, yer verilmesi gerekmektedir[429]. Borçlar Kanunu'nun temel prensiplerinden biri olan şekil serbestisini büyük ölçüde sınırlandıran böyle bir düzenlemeye yalnızca Elektronik İmza Kanunu'nda yer verilmesi kanun koyucudan beklenemez.

Belirtilen gerekçelerle, yalnızca yasal olarak yazılı şekle tabi tutulan teminat sözleşmelerinin güvenli elektronik imzayla yapılamayacağı kabul edilerek, EİK. 5 II hükmünün güvenli elektronik imzanın el yazısıyla imzayla denkliği prensibine getirilen bir istisna hükmü olarak dar yorumlanması, bu hükmün yeri ve amacı dikkate alındığında daha isabetlidir. EİK. 5 II hükmündeki istisnanın, sözleşmelerin elektronik ortamda kuruluşu bakımdan etki doğurmayacağı tespit edildikten sonra, bu tespite paralel olarak, şekle tabi olmayan olmayan teminat sözleşmelerin güvenli elektronik imzayla yapılmasına EİK. 5 II hükmünün mani olmayacağını kabul etmek gerekmektedir.

Bu çerçevede aydınlatılmayı bekleyen başka bir konu EİK. 5 II'deki istisna hükmünün şekle tabi olmayan teminat sözleşmelerinin iradi olarak yazılı şekle tabi tutulmuş olması halinde uygulanıp uygulanmayacağıdır. Elektronik İmza Kanunu teminat sözleşmeleri bakımından yazılı şeklin imza unsurunun yalnızca el yazısıyla imza ile tamamlanacağını emretmektedir (EİK. 5 II). Böyle bir durumda, taraflarca yalnızca yazılı şekilden söz edilmiş ve sözleşme metninde bu konuda başka bir açıklamaya yer verilmediyse, bu durumda BK. 13-15 hükümleri ile birlikte EİK. 5 II hükmü de uygulama bulacak ve güvenli elektronik imzayla imzalanan sözleşme iradi şekle aykırılık dolayısıyla geçersiz olacaktır. Bununla birlikte, taraflar şeklin uyarı fonksiyonu bakımından sakınca duymayarak güvenli elektronik imza kullanmak konusunda anlaşmışsa, bu durumda iradi olarak kararlaştırılan yazılı şekil şartının güvenli elektronik imza ile gerçekleştirilmesine EİK. 5 II hükmü engel olmamalıdır.

---

[429] Örneğin, Alman hukukunda böyle bir yöntem benimsenmekte, elektronik şekilde yapılamayacak hukuki işlemler her ilgili maddede özel olarak belirtilmektedir. Alman hukukunda geçerliliği şekle tabi tutulan ancak elektronik şekilde yapılamayacağı düzenlenen hukuki işlemler şunlardır: Kefalet (§766 BGB), soyut borç ikrarı veya borç vaadi (§780-781 BGB), kaydı hayat ile irat sözleşmesi (§761 BGB).

c. Teminat Sözleşmelerine İlişkin İstisnanın Sonuçları

EİK. 5 II hükmü, el yazısıyla imza ile güvenli elektronik imzanın hukuki denkliğini öngören EİK. 5 I hükmü bakımından istisna getirmekte olup, bu hükmün kanunen hiçbir şekle tabi tutulmayan teminat sözleşmelerinin güvenli elektronik imza aracılığıyla yapılmasına engel teşkil etmemesi gerektiğini yukarıda belirtmiştik. Bu çerçevede güvenli elektronik imzanın hangi teminat sözleşmeleri bakımından uygulanabileceğinin açıklanmasına ihtiyaç bulunmaktadır.

Teminat sözleşmeleri ayni ve şahsi teminat sözleşmeleri olmak üzere ikiye ayrılmaktadır. Ayni teminat sözleşmeleri taşınmaz rehni sözleşmesi, taşınır rehni sözleşmesi, hak ve alacak rehni sözleşmeleri ve ticari işletme rehni sözleşmesi olmak üzere dört çeşittir[430]. Şahsi teminat sözleşmelerine, kefalet sözleşmesi, garanti sözleşmeleri, bir garanti sözleşmesi türü olduğu kabul edilen üçüncü kişinin fiilini taahhüt sözleşmesi[431] ve teminat amacıyla yapılan borca katılma sözleşmesi[432] örnek olarak gösterilebilir.

Ayni bir teminat sözleşmesi niteliğindeki taşınmaz rehninin kurulmasına ilişkin sözleşmelerin geçerliliği resmi şekilde yapılmalarına bağlıdır (MK. 856 II). Bu bakımdan teminat sözleşmeleri bakımından getirilen istisna hükmüne taşınmaz rehni sözleşmeleri açısından başvurmaya gerek bulunmamaktadır. Bununla birlikte resmi şekil zorunluluğuna ilişkin olarak Tapu Kanunu'nun 26. maddesinin son üç fıkrası uyarınca getirilen istisna hükmü bu konuda önem taşır. Bu hükmün ifadesi şöyledir:

---

[430] Tandoğan, **Özel Borç İlişkileri II**, s.688.

[431] Üçüncü kişinin fiilini taahhüt sözleşmesinin garanti sözleşmesi kavramıyla ilişkisi ve bu konudaki tartışmalar için bkz. Oğuzman / Öz, **a.g.e**., s.800-801 ve dn.11.; Tandoğan, **Özel Borç İlişkileri II**, s.848 vd.

[432] Borca katılma sözleşmesi esas itibariyle şahsi teminat niteliği taşıyan bir sözleşmedir. Ancak borca katılmanın istisnai olarak teminat dışında kalan başka amaçlarla da yapılmasının mümkün olduğu belirtilmekte ve buna en baştan ilk borçlunun borçtan ibrası şartıyla borcun üstlenilmesi ihtimali örnek olarak gösterilmektedir: Oruç Hami Şener, "Sözleşmeyle Yapılan Teminat Amaçlı Borca Katılma", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.11, Özel S., 2009 (Basım Y. 2010), s.1279-1322, s.1279 ve dn.1.

"*Konut yapanlara, ihracatçılara, turizm tesisi yapanlarla işletmecilerine, sanayicilere, esnaf ve sanatkârlara, konuları ile ilgili olarak bankalarca veya kamu kurum veya kuruluşlarınca (Ordu Yardımlaşma Kurumu dahil) açılacak kredilere karşılık teminat gösterilen gayrimenkullerin ipotek işlemleri, resmî senet tanzim edilmeksizin alacaklı ile borçlu ve varsa kefilleri arasında yapılan kredi veya borç sözleşmelerine istinaden, ilgililerin talebi üzerine, tapu sicil muhafızlıklarınca tapuya tescil edilir.*

Kamu kurum ve kuruluşları (Ordu Yardımlaşma Kurumu dahil), bankalar, Esnaf ve Sanatkarlar Kredi ve Kefalet Kooperatiflerince açılacak tüm kredilere karşılık teminat gösterilen gayrimenkullerin ipotek işlemleri, tarafların istemi halinde resmi senet tanzim edilmeksizin alacaklı ile borçlu ve varsa kefilleri arasında yapılan kredi veya borç sözleşmelerine istinaden, tapu sicil müdürlüklerince tapuya tescil edilir.

Tarımsal kredi sebebiyle bankalar veya kamu kurum ve kuruluşları lehine teminat olarak gösterilen gayrimenkullerin ipotek işlemlerinde de de bu usule uyulur".

Tapu K. 26'nın son üç fıkrasında belirtilen hallerde ipotek sözleşmesinin resmi şekilde yapılmasına gerek bulunmadığı belirtilmektedir[433]. Bu hüküm resmi senet kuralı bakımından istisna getirirken, geçerlilik şekli bakımından bir düzenleme öngörmemektedir. İpotek hakkının tapuya tescili bakımından, her halükarda bu sözleşmelerin asgari olarak yazılı şekilde yapılması gerekecektir. Güvenli elektronik imzalı bir belgenin, kağıda dayalı klasik sistemle işletilen tapu idaresine, elektronik yolla ibrazı söz konusu olamayacağından, bu sözleşmeler de güvenli elektronik imza yoluyla kurulamayacaktır[434].

---

[433] Bu hükümdeki istisnadan ipoteğin ancak bizzat kredi borçlusunun taşınmazı üzerinde tesis edildiği ihtimallerde yararlanılabileceği, ipoteğin bir üçüncü kişinin taşınmazı üzerinde tesis edildiği hallerde ipoteği tesis eden üçüncü kişi ile alacaklı arasında bir kredi veya borç sözleşmesi bulunmadığı için, bu durumda yine resmi şekilde bir ipotek sözleşmesinin gerekli olduğu görüşünde: İlhan Helvacı, **Eski Medenî Kanunumuzla Karşılaştırmalı Olarak Türk Medenî Kanunu'na Göre Sözleşmeden Doğan İpotek Hakkı**, İstanbul, On İki Levha Yayıncılık, 2008, s.115. Aynı görüşte; M. Kemal Oğuzman / Özer Seliçi / Saibe Oktay Özdemir, **Eşya Hukuku, İstanbul, 12. Bası, Filiz Kitabevi, 2009**, s.705.

[434] Tapu Sicil Tüzüğü'nün 6. maddesine 2004 yılında yapılan bir değişiklikle "*Genel müdürlük gerekli gördüğü yerlerde sicillerin bir kısmını ya da tamamını karteks şeklinde veya bilgisayar ortamında*

Taşınmaz rehni sözleşmeleri bakımından vardığımız sonuç ticari işletme rehni sözleşmeleri bakımından da geçerlidir. Çünkü, 1447 sayılı Ticari İşletme Rehni Kanunu'nun 4. maddesi uyarınca ticari işletmenin rehnine ilişkin sözleşmelerin ticari işletmenin kayıtlı bulunduğu sicil çevresindeki bir noter tarafından düzenlenmesi gerekmektedir.

Taşınır rehni kurma borcu doğuran bir sözleşmenin geçerliliği Medeni Kanun'da hiçbir şekle tabi tutulmamıştır. Bu nedenle de borç doğuran nitelikteki böyle bir sözleşmenin güvenli elektronik imza ile yapılması mümkün kabul edilmelidir. Teslime bağlı taşınır rehninin kurulabilmesi için rehin verenle rehin alanın anlaşmaları[435] ve rehin konusu malın dolaysız zilyetliğinin rehin alana geçirilmesi gerekmektedir (MK 939 I). Bu bakımdan rehin hakkının tesisi için, güvenli elektronik imza yoluyla imzalanmış bir sözleşme, taşınır fiilen rehnedenin hakimiyetinde kaldığı sürece yeterli olmayacaktır (MK. 939 III).

Aynı şekilde alacaklar ve diğer haklar üzerinde rehin kurma borcu doğuran sözleşmeler de herhangi bir şekle tabi olmadığından[436], bunların da güvenli elektronik imza ile yapılabileceğini kabul etmek gerekir.

---

tutturmaya ve uygulatmaya yetkilidir" hükmü eklenmiştir. Tapu ve Kadastro Genel Müdürlüğü bu hükme dayalı olarak TAKBİS (Tapu ve Kadastro Bilgi Sistemi) projesini uygulamaya başlamıştır. Bu proje ile mevcut taşınmaz kayıtlarının Türkiye genelinde bilgisayar ortamına aktarılarak tüm faaliyetlerin bilgisayar sistemi üzerinden yürütülmesi, böylece gerek özel, gerekse kamu taşınmaz mallarının etkin biçimde takip ve kontrolünün sağlanmasının amaçlandığı, bu bakımdan en temel devlet projelerinden biri olduğu ifade edilmektedir. TAKBIS projesi hakkında bilgi için bkz. http://www.tkgm.gov.tr/tkgm/index.php?page=projeler&pID=1. Öğretide, kişiliğin korunması, özel yaşamın gizliliği, mülkiyet hakkı bakımından önem taşıyan böyle bir konunun, tüzük aracılığıyla düzenlenmesi eleştirilmekte ve kanuni bir düzenlemeye başvurulmasının zorunlu olduğu belirtilmektedir. Ayrıca taşınmaz kayıtlarının bilgisayar ortamına aktarılmasında belirli bir standardın benimsenmemesi halinde, elektronik ortamda tutulan tapu sicilinin klasik tapu sicilinin üstlenmiş olduğu aleniyet fonksiyonunu yerine getirmeyeceği ifade edilmektedir. Bu sakıncaya Türk hukukunda benimsenen sisteminin kaynağını teşkil eden İsviçre'de de önemle işaret edilmektedir. Konunun karşılaştırmalı hukukta ve Türk hukukundaki gelişmeler çerçevesinde değerlendirmesi için bkz. Veysel Başpınar, "Elektronik Tapu Sicili Düzenlenirken, Tapu Sicilinin Aleniyeti ve Diğer Alanlarla İlgili Alınması Gereken Tedbirler", **AÜHFD**, C.57, S.53, 2008, s.97-131.

[435] Oğuzman / Seliçi / Oktay Özdemir, **Eşya Hukuku**, s.793. Bu anlaşma bir ayni sözleşme olarak adlandırılmaktadır: Bülent Köprülü / Selim Kaneti, **Sınırlı Aynî Haklar**, 2. Bası, İstanbul, 1982-1983, s.479.

[436] Köprülü / Kaneti, **a.g.e.**, s.583.

Kıymetli evrakın rehninde, borçlandırıcı bir işlem niteliğindeki rehin sözleşmesi şekle tabi değildir[437]. Bu nedenle güvenli elektronik imza yoluyla yapılabilir. Ancak rehnin kurulabilmesi için ise hamiline yazılı senetlerde, senedin rehin alana teslimi gerekmektedir (MK. 956 I). Diğer kıymetli evrakın rehninde, senedin ciro edilmiş veya yazılı devir beyanı yapılmış olarak teslim edilmesi şarttır (MK. 956 II).

Kıymetli evrak niteliğinde olmayan, adi senede bağlanmış alacakların rehninde, rehnin kurulmasını sağlayan tasarruf işlemi taraflar arasında yapılan yazılı rehin sözleşmesi ve senet üzerindeki zilyetliğin rehin alana geçirilmesi ile meydana gelmektedir[438]. Her iki unsur yerine getirilmediği müddetçe rehin tesis edilmiş olmamaktadır[439]. Tasarruf işleminin kurucu unsurlarından birini oluşturan rehin sözleşmesi yazılı şekle tabi tutulduğundan (MK. 955 I), bu unsurunun güvenli elektronik imza yoluyla yerine getirilmesi EİK.5 II hükmü gereği söz konusu olamaz.

Senede bağlanmamış alacakların[440] rehninde de rehin sözleşmesinin etkisinin kurucu olduğu kabul edilmektedir. Çünkü bu durumda ortada teslimi gereken bir senet bulunmadığından, alacak üzerindeki rehin hakkı, yalnızca rehin alan ile rehin veren arasında yapılan sözleşme yoluyla kurulmaktadır. Bu bakımdan buradaki tasarruf işlemi, ayni etkili bir rehin sözleşmesi olarak ifade edilmektedir[441]. Rehin sözleşmesinin geçerliliği için yazılı şekilde yapılması zorunludur. EİK. 5 II hükmü uyarınca bu şartın güvenli elektronik imza yoluyla yerine getirilmesi imkanı bulunmamaktadır.

---

[437] Lale Sirmen, **Alacak Rehni**, Ankara, Banka ve Ticaret Hukuku Enstitüsü, 1990, s.60.

[438] Sirmen, **a.g.e**., s.36. Yazılı rehin sözleşmesinin, teslime bağlı rehindeki ayni sözleşmenin yerini tuttuğu, eğer alacak için bir senet düzenlendiyse senedin devrinin de bir geçerlilik şartı olduğunu ifade edilmektedir. Bkz. Oğuzman / Seliçi / Oktay Özdemir, **Eşya Hukuku**, s.816. Tasarruf işleminin yalnızca senedin zilyetliğinin rehin alana geçirilmesinden ibaret olduğu, yazılı rehin sözleşmesinin borçlandırıcı işlem niteliğinde olduğu görüşünde: Ferit H. Saymen / Halid K. Elbir, **Türk Eşya Hukuku (Ayni Haklar)**, İstanbul, İsmail Akgün Matbaası, 1954. s.765.

[439] Rehin hakkının kurulma anı, senetli alacaklarda senedin rehin alana teslimi anıdır: Saymen / Elbir, **a.g.e**., s.765.

[440] Burada sözü edilen kıymetli evrak niteliği taşımayan adi senettir: Saymen / Elbir, **a.g.e**., s.765.

[441] Rehin hakkı senede bağlı olmayan alacaklarda yazılı rehin akdinin yapılmasıyla kurulur: Saymen / Elbir, **a.g.e**., s.765.

Bu durumda ortaya şöyle bir sonuç çıkmaktadır: Geçerliliği kanunen yazılı şekle tabi tutulan alacağın temliki sözleşmesi, bir teminat sözleşmesi karakteri bulunmadığı takdirde, güvenli elektronik imza ile yapılabilirken, alacak hakkı üzerinde daha sınırlı bir tasarruf etkisi doğuran alacak rehni sözleşmesi bir ayni teminat kurması nedeniyle güvenli elektronik imza ile yapılamayacaktır.

Uyarı işlevinin tam olarak gerçekleşmediği ve teminat vereni korumak amacıyla böyle bir istisna getirilmiş olduğu gerekçesi burada tatmin edici gözükmemektedir. Alacağın temlikinde uyarı işlevi bakımında sakınca görmeyen kanunu koyucunun aynı yaklaşımı *a fortiori* alacak rehni bakımından benimsemiş olması beklenirdi.

Diğer taraftan, alacağın temlikinin teminat amacıyla yapılması halinde güvenli elektronik imza kullanımının mümkün olup olmadığı açıklığa kavuşturulması gereken başka bir konudur. Alacağın teminat amacıyla temlikinde, teminat sebebini oluşturan borçlandırıcı işlem bakımından yazılı şekil şartı aranmamaktadır. Bu nedenle teminat sebebinin yazılı olduğu metnin güvenli elektronik imza ile imzalanarak geçerli bir şekilde meydana getirilmesine engel yoktur[442].

Bununla birlikte, alacağın teminat amacıyla temlik edildiği hallerde çoğu zaman borçlandırıcı işlem ve tasarruf işlemi aynı metin içinde yer almaktadır. Tarafların kendi aralarında anlaşarak temlikin sebebini oluşturan hukuki ilişkiyi temlik sözleşmesinin metnine dahil ettiği böyle bir durumlarda, alacağın temliki sebebe bağlı kılınmakta ve borçlandırıcı işlemin herhangi bir sebeple geçersiz olması temlik işlemini de geçersiz hale getirmektedir[443]. Böyle bir durumda, teminat

---

[442] Şekle tabi olmayan teminat sözleşmelerinin de güvenli elektronik imza ile yapılamayacağı kabul edildiği takdirde (bu görüşteki yazarlar için bkz. s.126), alacağın temlikinin sebebe bağlı olduğu görüşünün kabul edilmesi, alacağın teminat amacıyla temlikinin elektronik imza ile yapılamayacağı sonucuna varmayı gerektirir. Sebepten soyut olduğu kabul edilirse, teminat sebebi geçersiz olsa bile temlik işlemi geçerli olarak hüküm ifade edecektir. Alacağın temliki işleminin sebepten soyut olduğu görüşünde: Oğuzman / Öz, **a.g.e**., s.923; Tunçomağ, **a.g.e**., s.1091; İnan, **a.g.e**., s.387. Alacağın temlikinin sebebe bağlı olduğu görüşünde: Eren, **a.g.e.**, s.1181 vd.; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.241 vd.

[443] Alacağın temliki sözleşmesinde, temlikin daha önceki temlik vaadinin ifası amacıyla yapıldığının açıklanması, alacağın temlikinin iki tarafa borç yükleyen bir sözleşmede bir tarafın borcunun ifası

sözleşmesi, esasen yazılı şekil şartına tabi olmadığı halde, yazılı olarak ve ifasını oluşturan tasarruf işlemiyle birlikte karşımıza çıkmaktadır. O halde, halen daha alacağın teminat amacıyla temliki işleminin güvenli elektronik imza ile yapılabileceğini savunmak mümkün müdür?

Öncelikle, böyle bir metinde, geçerliliği şekle tabi tutulan işlem bir tasarruf işlemi niteliğindeki alacağın temliki işlemidir. Teminat karakterini veren borçlandırıcı işlem, alacağın temliki işleminin şekliyle meydana getirilmiş olmasına rağmen, bu yasal olarak öngörülen bir geçerlilik şartı değildir. Geçerliliği için hiçbir şekil şartı aranmayan ve alacağın temliki işlemiyle aynı metinde yer alması zorunluluğu olmaksızın sözle dahi geçerli olarak yapılabilen teminat sözleşmesinin, alacağın temlikiyle birlikte aynı metinde yer aldığı ihtimallerde de, güvenli elektronik imzayla bu metnin imzalanması suretiyle, geçerli bir şekilde yapılabileceğini kabul etmek daha uygun gözükmektedir.

Şahsi teminat sözleşmeleri bakımından geçerliliği kanunen hiçbir şekle tabi olmayan garanti sözleşmesinin veya üçüncü kişinin fiili taahhüt sözleşmesinin güvenli elektronik imza aracılığıyla yapılmasına bir engel bulunmamaktadır[444]. Ancak geçerli olması için yazılı şekilde yapılması gereken kefalet sözleşmesi (BK. 484) ise güvenli elektronik imza aracılığıyla elektronik ortamda geçerli olarak kurulamayacaktır.

Yeni Borçlar Kanunu'nun kefalet sözleşmesinin şeklini düzenleyen 583. maddesinin I. fıkrası şu şekildedir:

"Kefalet sözleşmesi, yazılı şekilde yapılmadıkça ve kefilin sorumlu olacağı azamî miktar ile kefalet tarihi belirtilmedikçe geçerli olmaz. Kefilin, sorumlu olduğu azamî miktarı, kefalet tarihini ve müteselsil kefil olması durumunda, bu sıfatla veya bu anlama gelen herhangi bir ifadeyle yükümlülük altına girdiğini kefalet sözleşmesinde kendi el yazısıyla belirtmesi şarttır".

---

olarak yer alması, teminat sebebinin ve temlik işleminin aynı metinde yer alması hallerinde alacağın temliki sebebe bağlanmış olmaktadır: Oğuzman / Öz, **a.g.e**., s.925.

444 Yeni Borçlar Kanunu'nun bu konuda yarattığı değişiklikler için bkz. aşağıda s.136.

Yeni Borçlar Kanunu'nda artık kefilin sorumlu olduğu azami miktarın, kefalet tarihinin ve müteselsil kefil olmaya yönündeki taahhüdün de el yazısıyla kaleme alınması şartı aranmaktadır. Yeni Borçlar Kanunu yürürlüğe girdikten sonra, kefalet sözleşmesinin geçerliliğine ilişkin olarak öngörülen bu nitelikli yazılı şekil karşısında, kefalet sözleşmesinin güvenli elektronik imza aracılığıyla gerçekleştirilmesine EİK. 5 I hükmü engel olacaktır. Zira yukarıda el yazısıyla yazılması gerekli olduğu belirtilen unsurların elektronik ortamda gerçekleştirilmesi mümkün değildir. Bu durumda güvenli elektronik imzanın uygulama alanı bakımından teminat sözleşmeleri açısından istisna getiren EİK. 5 II hükmüne başvurulmasına gerek olmayacaktır.

Yeni Borçlar Kanunu'nun 603. maddesi, kefalet sözleşmesinin şeklinin uygulama alanı bakımından Eski Borçlar Kanunu'nda yer almayan yeni bir düzenleme getirmektedir:

"Kefaletin şekline, kefil olma ehliyetine ve eşin rızasına ilişkin hükümler, gerçek kişilerce, kişisel güvence verilmesine ilişkin olarak başka ad altında yapılan diğer sözleşmelere de uygulanır".

Bu hüküm ile birlikte kefalet sözleşmesinin şekline, kefil olma ehliyetine ve eşin rızasına ilişkin hükümlerinin uygulama alanı genişletilmiş olmaktadır[445]. Bu durumda, kefalet sözleşmesinin yanı sıra, gerçek kişiler tarafından yapıldığı hallerde sınırlı olmak üzere, birer şahsi teminat sözleşmesi niteliğindeki garanti, üçüncü kişinin fiilini taahhüt veya teminat amacıyla yapılan borca katılma sözleşmeleri de kefalet sözleşmesi açısından öngörülen geçerlilik şekline tabi tutulmaktadır[446]. Yeni Borçlar Kanunu'nun yürürlüğe girmesinden itibaren, bu sözleşmelerin güvenli elektronik imza aracılığıyla yapılması imkanı ortadan kalkacak ve güvenli elektronik imzanın uygulama alanı da önemli ölçüde sınırlandırılmış olacaktır.

---

[445] Maddeye ilişkin gerekçede, bu hüküm gereğince, artık başka ad altında yapılan şahsi teminat sözleşmeleri bakımından da kefalet hükümlerinin uygulanacağı belitilmektedir. Gerekçede bu sayede, kefili koruyucu hükümlerden kurtulmanın, bu hükümlerin dolanılmasının önlenmek istendiği ifade edilmektedir. Yeni Borçlar Kanunu'nu gerekçe metni için bkz. (Çevrimiçi) http://www2. tbmm.gov.tr/d23/1/1-0499.pdf, 17.05.2011.

[446] Turgut Öz, **Yeni Borçlar Kanununun Getirdiği Başlıca Değişiklikler ve Yenilikler**, İstanbul, Vedat Kitapçılık, 2011, s.19 ve s.25.

Yeni Borçlar Kanunu'nun 603. maddesinin yürürlüğe girmesiyle, yalnızca gerçek kişilerin imza sahibi olabileceğini öngören EİK. 3 (c) hükmünü varlığı karşısında, garanti, üçüncü kişinin fiilini taahhüt veya borca katılma sözleşmelerinin tüzel kişiler tarafından güvenli elektronik imza kullanılarak yapılıp yapılamayacağı meselesi ortya çıkar. Aslında bu konuda varılacak sonuç, daha geniş çerçevede tüzel kişilerin borç altına girdiği tüm teminat sözleşmeleri açısından önem taşımakta olup, yürürlükteki hukuku da ilgilendirmektedir. Bu hususta Elektronik İmza Kanunu'ndaki imza sahibi kavramı ile borç altına giren kavramı birbirinden ayırt edilmeli, teminat sözleşmelerine ilişkin bu istisnanın yorumlanmasında kimin borç altına girdiği esas alınmalıdır. Tüzel kişiler tarafından verilen teminatlarda, tüzel kişi adına imza atan kişinin EİK 3 (c) uyarınca gerçek kişi olması zorunluluğu, bu teminatların geçerli olarak yapılmasına engel teşkil etmemelidir[447].

D. İSPAT ŞEKLİ BAKIMINDAN GÜVENLİ ELEKTRONİK İMZANIN SONUÇLARINA GENEL BAKIŞ

12.1.2011 tarihli ve 6100 sayılı yeni Hukuk Muhakemeleri Kanunu (HMK.) 4.02.2011 tarihli ve 27836 sayılı Resmi Gazete yayımlanarak yürürlüğe girmiştir[448]. Güvenli elektronik imzanın hukuki etkileri "*Adi senetlerin ispat gücü*" başlıklı HMK. 205 hükmünde aşağıdaki şekilde düzenlenmektedir:

> ***"*** *(1) Mahkeme huzurunda ikrar olunan veya mahkemece inkâr edenden sadır olduğu kabul edilen adi senetler, aksi ispat edilmedikçe kesin delil sayılırlar.*
>
> *(2) Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir.*

---

[447] Güvenli elektronik imza kullanımında imza sahibi sıfatının borç altına giren kişi kavramından ayırt edilmesi hakkında bkz. 94.

[448] Kanun'un, zaman yönünden uygulanmasına ilişkin olarak 448. maddesinde, tamamlanmış işlemleri etkilememek kaydıyla derhal uygulanacağı ifade edilmektedir.

(3) Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin[449], güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler".

Bu hüküm ile elektronik belgelerin senet değeri ve kesin delil etkisi, güvenli elektronik imza ile imza edilmiş olmaları şartıyla kabul edilmekte, basit elektronik imzalı belgeler bu hükmün dışında bırakılmaktadır[450]. Bu sınırlamanın hüküm ifade edebilmesi için, hakim belgenin hangi tür elektronik imza ile imzalandığını res'en incelemekle yükümlü kılınmıştır (HMK. 205 b.3)[451]. Kanun koyucunun böyle bir yükümlülük öngörmesi isabetli olmuştur. Aksi halde, taraflar itiraz etmediği takdirde, basit elektronik imza ile imzalanmış elektronik belgelerin de senet olarak kabul edilmesi ve kesin delil etkisi doğurması durumu söz konusu olacaktı[452].

HMK. 210 hükmüne göre, **"***güvenli elektronik imzayla oluşturulmuş verinin inkârı[453] hâlinde, hâkim tarafından veriyi inkâr eden taraf dinlendikten sonra bir kanaate varılamamışsa, bilirkişi incelemesine başvurulur*".

El yazısıyla imzalanmış belgenin, adi yazılı senet niteliği gözle yapılacak bir inceleme ile hakim tarafından tespit edilebilirken, güvenli elektronik imzanın varlığı ve nitelikli sertifikanın kontrolü yapılarak geçerliliğinin tespit edilebilmesi özel bir

---

[449] Elektronik imzalı belgeyle "imzalanmış verinin teknik durumu" anlatılmak istenir. Elektronik imzalı belgeler, sesler ve resimler de içerebilir. Bir elektronik imzalı belgede teknik olarak bir veya daha fazla veri söz konusu olabilir: Erturgut, **E-belge ve E-imza**, s.71. Elektronik belge veya elektronik kayıt gibi terimler, elektronik ortamda yaratılan bir bilgiyi ifade etmek üzere kullanılmaktadır: Yaltı Soydan, **E-İmza I**, s.131.

[450] EİK. 23 hükmü ile 18.06.1927 tarihli ve 1086 sayılı eski Hukuk Usulü Muhakemeleri Kanunu'na 295/A maddesi eklenmişti:

"*Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar.*

Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkâr ederse, bu Kanunun 308 inci maddesi kıyas yoluyla uygulanır".

[451] Bu hükme karşılık gelen eski HUMK. 295/A'da ise mahkeme bakımından böyle bir yükümlülük hükme bağlanmış değildi. Bu durum öğretide eleştirilere maruz kalmaktaydı. Bkz. Erturgut, **a.g.e**., s.187-188.

[452] Erturgut, **a.g.e**., s.187-188.

[453] Hukuk Muhakemeleri Kanunu'nun 210. maddesinin başlığı "*Güvenli elektronik imzalı belgenin inkârı*" olmasına rağmen maddede "*güvenli elektronik imzayla oluşturulmuş verinin inkârı"*ndan söz edilmektedir. HMK. 205 hükmünde de hem veri hem belge deyimi kullanılmaktadır. Bunların arasında bir fark bulunmamaktadır. Elektronik imzalı belgenin bir veri olarak da ifade edilmesi teknik olarak mümkündür. Ancak burada terim birliği sağlanması ve daha hukuki bir deyim olan "güvenli elektronik imzalı belge"de karar kılınması gerekirdi.

teknik incelemeyi gerektirmektedir. Hakimin bu inceleme yükümlülüğünü yerine getirebilmesi için yine bir bilirkişiye başvurması gerekebilir[454]. Zira belirtilen ölçüde bir teknik incelemenin hakim tarafından kağıda dayalı belgeler üzerinde yapılması imkanı bulunmamaktadır. Güvenli elektronik imzalı belgenin mevzuatta aranan şartları taşıyıp taşımadığı yanlızca elektronik ortamda denetlenebilir. Güvenli elektronik imzalı belgenin kağıda aktarılması söz konusu olamaz.

Güvenli elektronik imza niteliği taşımayan bir basit elektronik imza kullanılarak imzalanan belgeler senet olarak kabul edilmemektedir. Bunun dışında, yazılı delil başlangıcı[455] olarak veya keşif[456], bilirkişi[457] veya özel hüküm sebebi[458] delilleri arasında değerlendirilebileceği öğretide ifade edilmektedir. Bunun için, elektronik imzanın kimden sadır olduğunun bilinmesi, bu belgenin sonradan değiştirilip değiştirilmediğinin incelenmesi ve son olarak hukuki işlemle bağlanma iradesinin varlığı hususlarında hakimin kanaate varması gerekmektedir[459].

11.03.2010 tarihli "*Kamu Hizmetlerinin Hızlandırılması Amacıyla Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun Tasarısı"*nın 24. maddesinin I. fıkrasıyla Elektronik İmza Kanunu'nun 21. madde metni tamamen değiştirilerek "Diğer Elektronik İmzalar" başlıklı şu düzenlemenin yapılması öngörülmüştür: *"Güvenli elektronik imza dışındaki elektronik imzalar ile oluşturulan elektronik veriler, takdirî delil sayılır".*

---

[454] Erturgut, **a.g.e**., s.187-188. Eski HUMK. 295/A güvenli elektronik imzanın inkarı halinde HUMK. 308 vd. hükümlerinin kıyasen uygulanacağını belirtmekteydi. HUMK. 308 vd. hükümleri ise, adi senette yer alan imzanın borçlu tarafından inkar edilmesi halinde, mahkemenin yapacağı imza inceleme prosedürüne ilişkindir. Bu hükümler incelendiğinde; hakimin imza incelemesi yaparken imzayı inkar eden tarafa kendi önünde yazı yazdıracağı veya imza attıracağı (istiktap edeceği), o borçlu tarafından imzalandığı muhakkak olan diğer belgelerle (uygulamaya elverişli belgeler), adi senet altındaki imzasını karşılaştıracağı, bunlardan kanaat edinemiyorsa bilirkişiye müracaat edebileceği şeklinde bir yol çizilmektedir. HUMK. 308 vd. hükümlerinin bu niteliği itibariyle, elektronik bir belgede yer alan dijital imzanın inkarı halinde aynen uygulanabilmesi mümkün değildir (Keser Berber, **Tasarı**). Bu açıdan bakıldığında HMK. 210 hükmünde bilirkişi incelemesinin ayrı olarak düzenlenmesi isabetli olmuştur.

[455] Keser Berber, **Dijital İmza**, s.548; Erturgut, **a.g.e**., s.256-257.

[456] Erturgut, **a.g.e**., s.261-262.

[457] Erturgut, **a.g.e**., s.264-266.

[458] Keser Berber, **Dijital İmza**, s.548; Erturgut, **a.g.e**., s.267-268.

[459] Basit elektronik imzalı belgelerin delil olarak değerlendirilmesi konusu, öncelikle delil türlerinin unsurlarının belirlenmesini ve bunların elektronik ortamda ne şekilde ikame olunabileceğinin araştırılmasını gerekli kılmaktadır. Medeni usul hukuku bakımından kapsamlı bir araştırmayı gerektiren bu konuda tezin sınırlarını aşmamak bakımından genel bir bilgi vermekle yetiniyoruz.

ÜÇÜNCÜ BÖLÜM

SERTİFİKA SAĞLAYICININ ELEKTRONİK İMZA KANUNU'NDAN DOĞAN YÜKÜMLÜLÜKLERİ VE ÜÇÜNCÜ KİŞİLERE KARŞI HUKUKİ SORUMLULUĞU

I. SERTİFİKA SAĞLAYICI KAVRAMI VE SERTİFİKA SAĞLAYICININ ELEKTRONİK İMZA KANUNU'NDAN DOĞAN YÜKÜMLÜLÜKLERİ

Elektronik imza kullanılarak meydana getirilen hukuki ilişkilerde sertifika sağlayıcıları, hukuki ilişkinin tarafları arasında güvenin tesis edilmesi görevini üstlenmektedir. Böyle bir güvenin yaratılması en temelde nitelikli sertifika düzenlemek suretiyle elektronik imza kullanıcılarının kimliğini elektronik ortamda belirlenebilir kılmaları sayesinde mümkün olmaktadır. Sertifika sağlayıcıları kimlik bilgilerinin yer aldığı nitelikli bir sertifika düzenlerken, bu bilgilerin güvenilir bir şekilde tespit edilmiş olduğunu ve gerçeği yansıttığını, söz konusu nitelikli sertifikaya dayanarak hukuki işlemde bulunan üçüncü kişilere garanti etmektedir.

Nitelikli sertifikanın düzenlenmesi dışında, güvenli elektronik imzanın EİK.4'te belirtilen geçerlilik şartlarının tamamının yerine getirilmesi sertifika sağlayıcıları tarafından üstlenilmektedir. Diğer bir ifadeyle, başta Borçlar Kanunu olmak üzere, hukukumuzda el yazısıyla imzayla aynı sonucu doğuracağı öngörülen güvenli elektronik imza, sertifika sağlayıcının Kanun'da belirtilen yükümlülüklerini eksiksiz bir şekilde yerine getirmesi şartıyla varlık kazanmakta ve öngörülen hukuki sonuçları meydana getirmektedir. Dolayısıyla, güvenli elektronik imzanın geçerlilik şartlarının belirlenmesi, sertifika sağlayıcıların bu şartların yerine getirilmesine yönelik yükümlülüklerinin ayrı olarak incelenmesini zorunlu kılmaktadır. Yükümlülüklerin incelenmesi ise devamında bu yükümlülüklerin ihlali halinde doğacak sorumluluğun türü ve kapsamının ne şekilde belirleneceği sorusunu beraberinde getirmektedir.

Elektronik İmza Kanunu, sertifika sağlayıcının yükümlülüklerini ve bu yükümlülükleri yerine getirmemesinden ötürü nitelikli sertifikaya güvenen üçüncü kişilere karşı sorumluluğunu özel olarak düzenlemektedir. Bu çerçevede, aşağıda ilk olarak güvenli elektronik imzanın geçerlilik şartlarının sağlanması temelinde, sertifika sağlayıcılar tarafından yerine getirilmesi gereken yükümlülükler incelenecek, devamında ise bu yükümlülüklerin ihlali dolayısıyla sertifika sağlayıcının üçüncü kişilere karşı sorumluluğu konusuna yer verilecektir.

A. SERTİFİKA SAĞLAYICI KAVRAMI

Sertifika sağlayıcıları EİK. 8 hükmünde tanımlandığı üzere elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişileridir.

Sertifika sağlayıcı bir gerçek kişi ya da kamu hukuku veya özel hukuk tüzel kişisi olabilir. Elektronik İmza Kanunu'nda sertifika sağlayıcı olarak faaliyet gösterecek özel hukuk tüzel kişilerinin hangi ticaret şirketi tipinde kurulacağı konusunda sınırlayıcı bir hükme yer verilmemiştir[460]. Gerçek kişiler bakımından, sertifika sağlayıcı olma imkanının tanınması sertifika sağlayıcının yükümlülükleri ve sorumluluğu açısından öngörülen ağırlaştırılmış kusursuz sorumluluk sistemi göz önüne alındığında, yerinde olmadığı ifade edilmektedir[461].

Kamu kurum ve kuruluşlarının sertifika sağlayıcı olma imkanı, Kamu Sertifikasyon Merkezi Oluşturulması Hakkında 06.09.2004 tarihli 2004/21 sayılı Başbakanlık Genelgesi ile sınırlandırılmıştır. Genelgede, tüm kamu kurum ve kuruluşlarının, kurumsal sertifika (kamu çalışanlarınca kurum içi ve kurumlar arası işlemlerde kullanılacak sertifika)[462] ihtiyaçlarının karşılanması amacıyla, Kamu Sertifikasyon Yapısı'nın oluşturulması[463] ve bu yapı içerisinde, en üst seviyede bir

---

460 Orta, **a.g.e.**, s.119.

461 Çiğdem Çamurdan, **Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme**, (Çevrimiçi) http://www e-imza.gen.tr, 28.11.2010.

462 Kamu çalışanları, kurumsal sertifikalarını kamu dışı bireysel işlemlerinde de kullanabilecektir (Genelge, s.2).

463 Böyle bir yapıya başvurulması Genelge'de şu şekilde gerçekçelendirilmektedir: "… Kamu kurum ve kuruluşlarının iş ve işlemlerini elektronik ortama dönüştürme sürecinde elektronik imza ve

"*Kök Sertifika Hizmet Sağlayıcısı*" ile buna bağlı olarak "*Kamu Sertifika Hizmet Sağlayıcısı*" kurulması kararlaştırılmaktadır[464]. Genelge'de belirtilen istisnalar dışında, kamu kurum ve kuruluşları, kurumsal sertifikalarını, Kamu Sertifika Hizmet Sağlayıcısı'ndan temin edecekler, kendileri sertifika sağlayıcı olarak faaliyette bulunamayacaklardır[465].

EİK. 8 II hükmünde, sertifika sağlayıcının faaliyete başlaması için idareye bildirimde bulunulmasının yeterli olduğu düzenlenmektedir. Bildirim şartı öngörülürken AB Elektronik İmza Yönergesi'nin esas alındığı anlaşılmaktadır. Bununla birlikte bildirim sürecinin tamamı ve hukuki sonuçları incelendiğinde sertifika sağlayıcının faaliyetinin Yönerge'den farklı olarak idarenin iznine tabi tutulduğu tespit edilmektedir.

Sertifika sağlayıcı olarak faaliyet vermek isteyen gerçek kişiler ile kamu hukuku veya özel hukuk tüzel kişilerinin Bilgi Teknolojileri ve İletişim Kurumu'na (Kurum) "bildirim"de bulunması gerekmektedir (EİK. 8 I).

Sertifika sağlayıcı Kurum'a yapacağı bildirimde,

a) güvenli ürün ve sistemleri kullanmak,

b) hizmeti güvenilir bir biçimde yürütmek,

c) sertifikaların taklit ve tahrif edilmesini önlemekle ilgili her türlü tedbiri almak ile ilgili şartların sağlandığı ayrıntılı bir biçimde gösterir (EİK. 8 II)[466].

---

sertifikasyon işlemlerini yürütecek yapıları kendi bünyelerinde ve münferit olarak sağlamaya çalıştıkları gözlenmektedir. Bu münferit çalışmaların, bir yandan sistemin kendi işleyişi içerisinde karmaşaya yol açması, diğer yandan da mükerrerliklere ve dolayısıyla emek ve kaynak israfına neden olması kaçınılmazdır".

[464] Bu yapının kuruluş işlemlerinin gerçekleştirilmesi ve işletilmesi görevi ve sorumluluğu TÜBİTAK'a bağlı Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Müdürlüğü'ne (UEKAE) verilmiştir. Söz konusu yapının gözden geçirilmesi ve uygunluğunun izlenmesi görev ve sorumluluğu ise Telekomünikasyon Kurumu'na verilmiştir (Genelge, s.2).

[465] Yürüttükleri görevler açısından özel niteliği haiz belirli kamu kurum ve kuruluşları açısından istisna öngörülmektedir. Buna göre; Türk Silahlı Kuvvetleri, Emniyet Genel Müdürlüğü, MİT Müsteşarlığı, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Dışişleri Bakanlığı kök sertifika ihtiyaçlarını kurulacak Kök Sertifika Hizmet Sağlayıcısından karşılayacaklar, kamu sertifika hizmet sağlayıcısı sistemlerini kendi bünyelerinde oluşturabileceklerdir (Genelge, s.2).

[466] Bu amaçla, EİY. 6 hükmüne göre sertifika sağlayıcı olma talebini içeren dilekçenin ve Ek-1'de yer alan bilgi ve belgelerin eksiksiz olarak ibraz edilmesi gerekmektedir. Ek-1'de belirtilen bilgi ve belgeler şunlardr:

Sertifika sağlayıcı faaliyete başlayabilmek için bildirimde bulunduğu tarihten itibaren iki ay beklemek zorundadır (EİK. 8 I). "*Faaliyette bulunmak*" ifadesi ile EİK. 8'de sertifika sağlayıcı tanımında yer alan "*elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetlerin sağlanması*" anlaşılmalıdır. Bu kapsamda değerlendirme görecek faaliyetlerde bulunulması EİK. 8 I hükmü uyarınca bildirimi takip eden iki aylık süre için yasaklanmıştır.

Kurum bildirimi derhal incelemeye alır ve incelemeyi iki ay içinde sonuçlandırır (EİY. 7 I). Yönetmelik'in ifadesinden idarenin incelemeyi tamamlaması için öngörülen iki aylık sürenin bildirimin yapıldığı tarihten itibaren başladığı, bu sürenin sertifika sağlayıcının faaliyete başlamak için beklemek zorunda olduğu iki aylık süreye paralel olarak işlediği anlaşılmaktadır.

Kurum yaptığı inceleme sonucunda bildirim şartlarının tam olarak yerine getirilmediğini tespit ederse, bu eksikliklerin yerine getirilmesi için sertifika sağlayıcıya bir ayı geçmemek üzere bir süre verir (EİK. 8 III). Sertifika sağlayıcı bu sürenin sonuna kadar faaliyette bulunamaz (EİK. 8 III).

Sertifika sağlayıcı verilen süre zarfında eksikliklerini giderdiğini ispatlayan bilgi ve belgeleri Kurum'a sunar. Gerekli şartları sağladığı tespit edilen sertifika sağlayıcı bildirim yaptığı tarihten itibaren iki aylık sürenin tamamlanmış olması

---

1. İletişim Bilgileri: Adı/unvanı ve tüm birimlerine ait iletişim bilgileri (adres, telefon, faks, e-posta adresi, internet adresi),
2. Şirket ile İlgili Belgeler: Ticari şirket ise; şirketin kuruluş Ticaret Sicil Gazetesi, vergi levhası, şirketin imza sirküleri, ticaret sicil belgesi ve şirketi temsile yetkili kişi/kişilerin adli sicil kayıtları ve iletişim bilgileri,
3. Personel: Organizasyon şeması, istihdam ettiği kişilerin ESHS personeli olduğunu gösterir sosyal güvenlik kuruluşundan alınmış belge, istihdam ettiği ve ettirdiği tüm personelin adli sicil kayıtları ile teknik personelin özgeçmişi ve uzmanlığını ispatlayan belgeleri,
4. Sertifika İlkeleri ve Sertifika Uygulama Esasları,
5. Zaman Damgası İlkeleri ve Zaman Damgası Uygulama Esasları,
6. Kendi Sertifikasının Örneği,
7. Sertifika Mali Sorumluluk Sigortası: Sertifika mali sorumluluk sigortası için sigorta şirketi ile yaptığı sözleşmenin bir örneği,
8. Sözleşme ve/veya Taahhütnameler Örneği: Taahhütnamelerin ve/veya nitelikli elektronik sertifika sahipleri ile yapacağı sözleşmenin birer örneği,
9. Hizmet Sözleşmesi: Hizmet alması durumunda, hizmet aldığı taraf ile imzaladığı sözleşmenin bir örneği,
10. Tebliğ ile İstenilen Bilgi ve Belgeler.

halinde faaliyete başlar (EİY. 7 II). Eksiklikler verilen bir aylık sürede giderilmezse, Kurum sertifika sağlayıcının faaliyetine son verir (EİK. 8 III).

Sertifika sağlayıcının faaliyetine başlaması, EİK'nın "bildirim" lafzına rağmen, gerçekte Kurum tarafından verilen izne tabi tutulmaktadır[467]. Zira Kurum'a yapılan bildirimi takiben hemen faaliyete başlayamamakta ve faaliyete başlamadan önce ve faaliyeti süresince güvenlik şartları konusunda Kurum tarafından gerçekleştirilen bir denetime tabi olmaktadır (EİK. 15)[468]. Söz konusu şartlara uyulduğunun tespiti konusunda Kurum'a geniş bir takdir yetkisi tanınmaktadır[469]. Sertifika sağlayıcının mevzuatta aranan şartları taşımaması halinde faaliyete başlamasının engellenmesi mümkündür. Ayrıca sertifika sağlayıcının bu şartları sonradan kaybetmesi halinde Kurum kapatma kararı vermeye yetkili kılınmıştır (EİY. 29).

AB Elektronik İmza Yönergesi m.3/1 düzenlemesinden[470] farklı olarak sertifika hizmetlerinin sağlanmasının önceden alınacak bir izne bağlı tutulması Kanun'un kapsamına uyan ve isabetli bir düzenlemedir. Çünkü Kanun'da ve Yönetmelik'te yer alan hükümler nitelikli sertifika verilmesi ve nitelikli sertifika dayalı elektronik imza uygulamalarının sağlanmasına ilişkindir. Nitelik sertifikaya dayalı elektronik imzanın meydana getireceği hukuki etkiler dikkate alındığında sertifika sağlayıcıların faaliyetleri açısından idare tarafından verilen izne tabi tutulan etkin bir denetim sisteminin öngörülmesi yerindedir[471].

---

[467] Sarıakçalı, **a.g.e**., s.81. Sertifika hizmetlerinin verilmesinin izne tabi tutulmadığına ilişkin aksi yönde değerlendirmeler için bkz. Orta, **a.g.e**., s.119; **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu,** s.43. Raporda, hukukumuzda AB Elektronik İmza Yönergesi m.3/1 düzenlemesi ile uyumlu olarak sertifika sağlayıcıların kurulması ve faaliyete geçmesinin önceden alınacak bir izne bağlı tutulmadığı belirtilmektedir.

[468] Bu anlamda sertifika sağlayıcının kurumsal güvenliğe sahip olup olmadığı Kurum'un denetimi altındadır: Erturgut, **a.g.e**., s.98. Kanun'da denetimin gerekli görülen zamanlarda Kurum tarafından gerçekleştirileceği belirtilmektedir (EİK. 15).

[469] Kanun'da güvenlik şartları düzenlenirken soyut ifadelerin kullanıldığı tespit edilmektedir. Bu kriterlerin yerine getirildiğinin tespiti konusunda Kurum'a geniş bir takdir yetkisi verilmiş olmaktadır, bkz. Sarıakçalı, **a.g.e**., s.80.

[470] AB Elektronik İmza Yönergesi'nde kabul edilen izne tabi olmama ilkesi, Avrupa Birliği'nin serbest dolaşımın önündeki engellerin kaldırılması ilkesine dayanmaktadır (Dumortier / Kelm / Nilsson / Skouma / Van Ecke**, a.g.e.,** s.40)

[471] Aynı görüşte Sarıakçalı, **a.g.e**., s.81. Nitekim, bu anlayışa paralel olarak, sertifika hizmetlerinin sunulması önceden izin alma şartına bağlanmamakla birlikte, her üye devletin "nitelikli sertifika"

B. SERTİFİKA SAĞLAYICININ YÜKÜMLÜLÜKLERİ

1. Nitelikli Sertifika Talep Eden Kişilerin Kimliğini Tespit Etme Yükümlülüğü

El yazısıyla imzada, imza şeklinin karakteristik olması sayesinde imzalayanın kimliği tespit edilebilirken, elektronik imzada böyle bir özellik (karakteristik kişiselleştirme özelliği) bulunmamaktadır[472]. Bunun yerine imza sahibinin kimliği, kimlik bilgilerini içeren nitelikli sertifika aracılığıyla belirlenebilmektedir. Sertifika sağlayıcının asli yükümlülüğü, nitelikli sertifika aracılığıyla, imza sahibi ile gizli anahtar arasındaki bağlantının güvenilir bir şekilde kurulmasıdır[473]. Bunun için ilk olarak nitelikli sertifika başvurusunda bulunan kişinin kimlik bilgilerinin güvenilir biçimde tespit edilmesi gerekmektedir. Kimlik tespitinin yerine getirilmesi, gizli anahtarın sertifikada adı belirtilen kişiye gerçekten özgülenmesi için zorunludur[474].

Kimlik tespitinin yapılması nitelikli sertifika hizmetinin sağlanması kapsamında sertifika sağlayıcının en önemli yükümlülüğüdür[475]. Bu yükümlülük EİK. 10 I (b) hükmünde ayrı olarak düzenlenmiş olmasına rağmen, nitelikli sertifika düzenleme yükümlülüğü ile birlikte değerlendirilmesi gerekmektedir[476]. Çünkü, nitelikli sertifika kimlik tespiti sırasında edinilen bilgilere dayalı olarak ve bu bilgileri kapsayacak şekilde üretilecektir. Kimlik tespiti yapılarak kimlik bilgilerinin sertifikaya kaydedilmesi ile imza sahibi, her seferinde kimlik doğrulaması için ek bir çaba sarf etmesine gerek olmaksızın, elektronik ortamda hukuki işlemlerde bulunabilme imkanına sahip olmaktadır[477].

---

düzenleyen sertifika sağlayıcılarını denetlemek için uygun bir sistem oluşturması gereği AB Elektronik İmza Yönergesi m.3/3'te düzenlenmektedir.

472 Erturgut, **a.g.e.**, s.108. Bu yönüyle gizli anahtarın kişiye özgü biyometrik verilerden farklı olduğu, kişiyle bağlantılı bir işaret niteliğinde olduğu ifade edilmektedir: Hansen, **a.g.e**, s.47;

473 Hansen, **a.g.e**., s.47.

474 Thomale, **a.g.e**., s.143.

475 von Seck, **a.g.e**., s.96; Spiegelhalder, **a.g.e**., s.59.

476 aus der Fünften, **a.g.e**., s.14. Nitelikli sertifika düzenlenmesi yükümlülüğü hakkında inceleme için bkz. s.154.

477 Albrecht von Harnier, **Organisationsmöglichkeiten für Zertifizierungsstellen nach dem Signaturgesetz**, Baden-Baden, Nomos, 2000, s.76.

AB Elektronik İmza Yönergesi (m.8 III), Alman Elektronik İmza Kanunu (SigG §7 I ve §14 II), İsviçre Elektronik İmza Kanunu (ZertES 7 I c) kişisel verilerin korunması temelinde, sertifikada takma adın belirtilebileceğini kabul etmektedir. Hatta Avrupa Birliği Yönergesi m.8 III'te üye devletlerin sertifikada takma adın kullanılması imkanını engelleyemeyeceği ifade edilmektedir. Sertifika talebinde bulunan kişinin, kimliğini açıklayan kişisel verileri kamu erişimine açık elektronik dizinde paylaşmaktan kaçınması mümkündür. Bu durumda sertifikada adı ve soyadının yerine kendi belirlediği bir takma adın yer almasını talep edebilir. Takma adın değişmeyen ve başka bir gerçek kişi tarafından kullanılmayan bir ad olması gerekmektedir. Takma ad diğerlerinden ayırt edilebilir olmalı ve sertifikaya kimliği belirlemeye yardımcı başka bilgiler de eklenmelidir. Sertifika sahibi takma adını ticari ilişkileri olan kimselerle paylaşarak başkaları tarafından bilinebilir kılmaktadır. Bununla birlikte, takma adı altında hukuki işlemlerde bulunan kişi bu hukuki işlemlerden doğan borçlarını yerine getirmediği takdirde (veya nitelikli sertifikanın kötüye kullanılması halinde), sertifika sağlayıcı talep halinde sertifika sahibinin gerçek kimliğini açıklamakla yükümlüdür[478].

Türk hukukunda takma adın sertifikada belirtilebileceğini açıkça öngören bir düzenleme bulunmamaktadır. Bununla birlikte, EİK 9 (c) hükmünde nitelikli sertifikada "*imza sahibinin teşhis edilebileceği kimlik bilgilerinin yer alması*" gerektiği belirtilmektedir. Bu ifade nitelikli sertifikada belirtilen kimlik bilgilerinin imza sahibi belirlemeye imkan verdiği ölçüde yeterli kabul edileceği şeklinde yorumlanmaya müsaittir. Takma adın belirtilmesi usulünün de imza sahibinin kimliğinin üçüncü kişiler tarafından belirlenmesini mümkün kılması şartıyla, nitelikli sertifikada yalnızca takma adın belirtilmesine herhangi bir hukuki engel bulunmamaktadır.

EİK. 10 I (b)'ye göre sertifika sağlayıcı nitelikli sertifika verdiği kişilerin kimliğini resmi belgelere göre güvenilir bir biçimde tespit etmekle yükümlüdür. EİY. 9 I'e göre sertifika sağlayıcı nitelikli elektronik sertifika vereceği kişilerin kimliğini nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli resmi belgelere göre tespit edecektir. Nüfus cüzdanı, pasaport gibi resmi belgelerde yer alan bilgiler

[478] Thomale, **a.g.e**., s.144-145.

sertifikada bulunması gereken bilgilerin sadece bir bölümünü içermektedir[479]. Bunlar çoğunlukla ad, soyadı, doğum yeri ve doğum tarihidir. Sertifika sahibinin kimlik bilgileri dışındaki diğer bilgilerin, örneğin sertifika sahibi üçüncü bir kişi adına hareket ediyorsa (bir şirketin avukatına temsil yetkisi vermesi örneğinde olduğu gibi) bu yetkisine ilişkin bilginin, mesleki veya diğer kişisel bilgilerinin, gerekli belgelere dayanılarak eksiksiz, doğru ve güvenilir biçimde tespit edilmesi gerekmektedir (EİK. 10 I (c), EİY. 9 III). Özellikle temsil olunan kişinin verdiği temsil yetkisinin belgelendirilmesi konusu önem taşımaktadır[480]. Gerçekte üçüncü kişiyi temsil yetkisi bulunmamasına rağmen sertifikada temsile yetkili görünen elektronik imza sahibi ile işlemde bulunan üçüncü kişinin sertifikada yer alan gerçeğe aykırı bilgi sebebiyle zarara uğraması mümkündür[481]. Bu sebeplerle sertifika sağlayıcının sertifikaya ekleyeceği bilgilerin doğruluğunu yeterli seviyede araştırması ve değerlendirmesi gerekmektedir[482].

Nitelikli elektronik sertifika verilecek kişinin kimlik tespiti esnasında bizzat hazır bulunması gerekmektedir. Nitelikli elektronik sertifika verilecek kişinin kimliğinin önceden tespit edilmiş olduğu hallerde (örneğin nitelikli sertifikanın yenilenmesi durumunda) veya kurumsal başvurularda kimlik tespiti için sertifika sağlayıcı bizzat hazır bulunma şartını aramayabilir (EİY. 9 II).

Kurumsal başvuru bir tüzel kişiliğin çalışanları, müşterileri, üyeleri veya hissedarları adına yaptığı nitelikli elektronik sertifika başvurusunu ifade etmektedir (EİY. 4). Kanun'da yer almayan bu düzenlemeye göre, kurumsal başvuru sahibinin, adına başvuruda bulunduğu kişilerin nitelikli elektronik sertifika taleplerini yazılı olarak belgelendirmesi yeterlidir (EİY. 9 II). Kurumsal başvuru sırasında bizzat hazır bulunma şartının kaldırılmasının, sertifika sağlayıcının sertifika başvurusunda

---

479 Hansen, **a.g.e**., s.129.

480 Thomale, **a.g.e**., s.145; aus der Fünften, **a.g.e**., s.14-15. Sertifikanın iptali temsil olunan kişilere sertifika sağlayıcı tarafından ihbar edilmelidir. Böyle bir ihbarda bulunulmasının amacı ileride çıkması muhtemel ihtilafların önüne geçmektir (Hansen, **a.g.e**., s.47, dn.615). Yoksa bu kişiler EİK. 13'ün koruma kapsamındaki üçüncü kişi kavramına dahil değildir. Üçüncü kişiye ek olarak mesleki yeterlilik belgesi veren veya diğer bilgilerle ilişkilendirilen başka bir kişi veya kurumun da sertifikada yer alan bilgiler ve sertifikanın iptali hakkında bilgilendirilmesi gerekmektedir (Thomale, **a.g.e**., s.145).

481 Thomale, **a.g.e**., s.145.

482 Thomale, **a.g.e**., s.145; Kimlik tespiti yükümlülüğü ile sertifika sağlayıcıları, noterlere benzer bir görev üstlenmektedir: von Harnier, **a.g.e**, s.76.

bulunan kişilerin kimliğini güvenilir bir şekilde tespit etme yükümlülüğünü etkilemediği kabul edilmelidir. Kanun'la belirlenen bu yükümlülüğün Yönetmelik hükümleriyle kapsamı daraltılamaz. Kurumsal başvuruda adına nitelikli sertifika başvurusu yapılan kişinin kimliğinin doğru olarak belirlenememesi halinde yine sorumluluk sertifika sağlayıcıya aittir.

2. İmza Oluşturma ve Doğrulama Verilerinin Üretilmesi Yükümlülüğü

Elektronik imzayı meydana getirebilmek için imza sahibinin imza oluşturma ve doğrulama verilerine sahip olması gerekmektedir. Dijital imza tekniğinde, bu verilere karşılık gelen gizli anahtar ve açık anahtarın sağlaması gereken üç temel kriter bulunmaktadır: i) anahtar çifti tek olmalıdır[483]; ii) anahtar çifti birbiriyle uyumlu olarak kullanılabilmelidir[484]; iii) gizli anahtarın açık anahtardan tekrar hesaplanması matematiksel olarak mümkün olmamalıdır[485].

İmza oluşturma ve doğrulama verilerinin, sertifika talep eden kişinin seçimine göre sertifika sağlayıcı tarafından veya sertifika talep eden kişi tarafından üretilmesi mümkündür[486]. Günümüzde sertifika sağlayıcı tarafından üretilmesi genellikle tercih edilmektedir[487]. Bunun sebebi, sertifika talep eden kişinin hakimiyetindeki bilgisayarın çoğu zaman dışarıdan gelebilecek saldırılar açısından zayıf korumaya sahip olmasıdır[488]. Ayrıca, imza oluşturma ve doğrulama verilerinin imza sahibi tarafından üretilmesi halinde teknik ve güvenlik kriterlerin yerine getirildiğinin ispatı güçlük arz etmektedir[489]. Söz konusu veriler uygulamada, sertifika sağlayıcı tarafından üretilmekte ve sertifika talep eden kişiye güvenli elektronik imza

---

[483] Dörr, **a.g.e**., s.80. Sertifika sağlayıcı ürettiği gizli anahtarın bir kopyasını saklamamalıdır: Hansen, **a.g.e**., s.46.

[484] İmza oluşturma ve doğrulama verilerinin birbiriyle uyumlu olarak kullanılabilmesi kriterinin yerine getirilmemesi, AB Elektronik İmza Yönergesi'nde sertifika sağlayıcı açısından bir sorumluluk dayanağı olarak gösterilmektedir.

[485] Dörr, **a.g.e**., s.80; Hansen, **a.g.e**., s.46.

[486] Dörr, **a.g.e.**, s.80; Hansen, **a.g.e.**, s.127; Erturgut **a.g.e.**, s.314; Şenocak, **a.g.e**., s.99, Keser Berber, **Dijital İmza**, s.531.

[487] Hansen, **a.g.e**., s.46; Thomale, **a.g.e**., s.147; Erturgut, **a.g.e**., s.94.

[488] Hansen, **a.g.e**., s.46.

[489] Hansen, **a.g.e**., s.46, dn.220.

oluşturma aracında kayıtlı olarak teslim edilmektedir[490]. Diğer taraftan imza oluşturma verisinin, imza sahibi tarafından ve güvenli elektronik imza oluşturma aracı kullanılarak üretilmesi imkanının güvenlik yönünden güçlü olduğu ve yakın gelecekte uygulamada kabul göreceği ifade edilmektedir[491].

EİK. 10 I (d) hükmüne göre sertifika sağlayıcı: *"İmza oluşturma verisinin elektronik sertifika hizmet sağlayıcısı tarafından veya sertifika talep eden kişi tarafından elektronik sertifika hizmet sağlayıcıya ait yerlerde üretilmesi durumunda bu işlemin gizliliğini sağlamakla veya elektronik sertifika hizmet sağlayıcısının sağladığı araçlarla üretilmesi durumunda, bu işleyişin güvenliğini sağlamakla yükümlüdür".* Kanun, sertifika sağlayıcının yükümlülüklerini belirlemeye yönelik olarak, imza oluşturma verisinin sertifika sağlayıcı tarafından veya sertifika talep eden kişi tarafından üretildiği temelde iki ayrı ihtimali düzenlemektedir[492].

a. İmza Oluşturma Verisinin Sertifika Sağlayıcı Tarafından Üretilmesi

Bu ihtimalde sertifika sağlayıcı imza oluşturma verisinin mevzuatta aranan teknik ve güvenlik kriterlerine uygun olarak üretilmesini ve bu işleminin gizliliğini (EİK. 10 I d) sağlamakla yükümlüdür. İmza oluşturma verisinin üretimi esnasında gizliliğin sağlanması, diğer bir ifadeyle imza oluşturma verisine başkaları tarafından erişilememesi ve bu verinin kopyalanamaması imza oluşturma verisinin teklik özelliği bakımından şarttır[493]. Belirtilen iki halde sertifika sağlayıcı imza oluşturma verisinin başkaları tarafından kopyalanması riskini ortadan kaldırmak için gerekli önlemleri almakla ve mevzuatta belirtilen teknik ve güvenlik kriterlerini yerine getirmekle yükümlüdür.

06.01.2005 tarihli ve 25692 sayılı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 5. maddesinde sertifika sağlayıcının işleyişinin

---

[490] Hansen, **a.g.e.**, s.127; Thomale, **a.g.e**., s.147

[491] Thomale, **a.g.e**., s.146 Erturgut, **a.g.e**., s.94.

[492] Erturgut, **a.g.e**., s.314.

[493] Erturgut, **a.g.e.**, s.315; Hansen, **a.g.e**., s.147.

bütün aşamalarında uyması gereken standartlar[494] belirtilmekte, 6. maddesinde imza oluşturma ve doğrulama verilerinin üretilmesinde hangi algoritmaların ve parametrelerin kullanılması gerektiği gösterilmektedir[495].

EİK 10 II'ye göre; "*elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz"*. Bu hükümde sözü edilen, dijital imzada gizli anahtarın kurtarılması (*key recovery*) işlemidir. Bu işlemde imza sahibi gizli anahtarını kaybettiği takdirde veya başka özel durumlarda sertifika sağlayıcıda bulunan kopyası sayesinde aynı anahtarı kullanmaya devam edebilmesi mümkün olmaktadır. Hukukumuzda, doğabilecek riskler dikkate alınarak sertifika sağlayıcı tarafından imza oluşturma verisinin yedeklenmesi işlemi bu hüküm ile yasaklanmıştır[496].

b. İmza Oluşturma Verisinin İmza Sahibi Tarafından Üretilmesi

(1) İmza Oluşturma Verisinin İmza Sahibi Tarafından Sertifika Sağlayıcıya Ait Yerlerde Üretilmesi

İmza oluşturma verisinin imza sahibi tarafından sertifika sağlayıcıya ait yerlerde üretilmesi halinde sertifika sağlayıcı bu işlemin gizliliğini ve güvenliğini sağlamakla yükümlüdür (EİK. 10 I d). Bu seçenekte imza sahibi sertifika sağlayıcı tarafından temin edilen araçlarla ve sertifika sağlayıcıya ait yerlerde imza anahtarı üretimini gerçekleştirmektedir. Bunun gerçekte imza oluşturma verisinin sertifika sağlayıcı tarafından üretildiği durumdan pek bir farkı bulunmamaktadır. Çünkü gizliliğin ve güvenliğin yine sertifika sağlayıcı tarafından temin edilmesi

---

[494] Bu standartların sertifika sağlayıcının Elektronik İmza Kanunu'nda düzenlenen yükümlülüklerini yerine getirip getirmediğinin değerlendirmesinde ne şekilde etki doğuracağı konusunda bkz. s.190 vd.

[495] İmza oluşturma ve doğrulama verilerinin üretilmesinde kullanılan, 06.01.2005 tarihli ve 25692 sayılı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen algoritma ve parametrelerin geçerlilik süresi son olarak 31.12.2011 tarihine kadar uzatılmıştır (bkz. 18.12.2010 tarihli ve 27789 sayılı "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"de Değişiklik Yapılmasına Dair Tebliğ m.1).

[496] Böyle bir durumda imza oluşturma verisinin aynısından bir tane daha üretilmiş olmaktadır. İmza oluşturma verisinin yedeklenmesine ilişkin bu yasağın, Kanun'un lafzı dikkate alındığında, yalnızca sertifika sağlayıcıya yönelik olarak öngörüldüğü, imza sahibi açısından herhangi bir yasağın bulunmadığı ifade edilmektedir; detaylı bilgi için bkz. **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu,** s.43.

gerekmektedir. Tek farkı imza oluşturma verisinin üretilmesi esnasına imza sahibinin bu süreci yakından izleme imkanına sahip olmasıdır.

(2) İmza Oluşturma Verisinin İmza Sahibi Tarafından ve Sertifika Sağlayıcının Sağladığı Güvenli Elektronik İmza Oluşturma Araçlarıyla Üretilmesi

İmza oluşturma verisinin, imza sahibi tarafından güvenli imza oluşturma aracı kullanılarak üretilmesi mümkündür[497]. Üretilen imza oluşturma verisine karşılık gelen imza doğrulama verisi daha sonra sertifika sağlayıcı tarafından düzenlenen nitelikli sertifikaya bağlanacaktır[498].

İmza oluşturma verisinin imza sahibi tarafından ve sertifika sağlayıcının sağladığı araçlarla üretilmesi durumunda, sertifika sağlayıcı bu işlemin güvenliğini sağlamakla yükümlüdür (EİK. 10 I d). "*Elektronik sertifika hizmet sağlayıcısının sağladığı araçlar*" ile anlaşılması gereken Kanun'da düzenlenen güvenli imza oluşturma aracıdır. Bu halde sertifika sağlayıcı güvenli imza oluşturma aracını (EİK. 6) imza sahibine teslim etmekte ve imza oluşturma verisi bu araç kullanılarak imza sahibi tarafından üretilmektedir. Dolayısıyla, sertifika sağlayıcı, imza oluşturma verisinin kendisinin verdiği imza oluşturma aracı vasıtasıyla üretilmesi durumunda, bu imza oluşturma aracının EİK. 6'da belirtilen güvenli elektronik imza aracı niteliğinde olmasını sağlamakla yükümlüdür. EİK. 6 (a) hükmüne göre; güvenli elektronik imza oluşturma aracının ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamalıdır. Bu hüküm gereği imza oluşturma verisinin başka bir eşinin bulunmaması şartı, sertifika sağlayıcı tarafından üstlenilmiş olmaktadır.

Sertifika sağlayıcının, imza oluşturma verisinin kendisinin sağladığı araçlarla üretildiği durumlarda, bu işleyişin güvenliğini sağlamakla yükümlü olduğu belirtilmiş ancak gizliliğini sağlama yükümlülüğü öngörülmemiştir. Bunun sebebi, imza oluşturma verisinin üretildiği ortamdaki işleyişi sertifika sağlayıcının denetleme

---

[497] EİK. 6 I'e göre imza oluşturma verisinin güvenli elektronik imza oluşturma aracı ile üretilmesi mümkündür.

[498] Thomale, **a.g.e**., s.148.

imkanının çoğu zaman olmamasıdır. Zaten imza sahibi sertifika sağlayıcıya güvenmemesi sebebiyle imza oluşturma verisini kendisi üretmek istemektedir[499]. Bu sebeple, imza oluşturma verisinin ürettiği esnada sertifika sağlayıcının işlemin gizliliğini denetlemesini istemeyecektir. Bu durumda sertifika sağlayıcının yükümlülüğü imza oluşturma aracının gereken güvenlik şartlarını taşımasını sağlamaktan ibarettir. Üretilen imza oluşturma verisinin gizliliğinin korunması imza sahibine düşmektedir.

İmza verisinin üretimi imza sahibi tarafından gerçekleştirildikten sonra, sertifika sağlayıcının, imza oluşturma verisine karşılık gelen imza doğrulama verisinin kendisinin düzenlemiş olduğu sertifika ile bağlantısını kurması gerekmektedir[500].

(3) İmza Oluşturma Verilerinin İmza Sahibi Tarafından Sertifika Sağlayıcıya Ait Olmayan Yerlerde ve Araçlarla Üretilmesi

Bu ihtimalde kişi kendi bilgisayarında imza anahtarını üretmekte ve sadece sertifikasyon amacıyla sertifika sağlayıcıya başvurmaktadır. Sertifika sağlayıcı kimlik denetimini yaptıktan sonra imza anahtarının belirli bir kişiye özgülendiğini açıklamak amacıyla bir nitelikli sertifika hazırlamaktadır[501].

Elektronik İmza Kanunu'nda hiç yer verilmemiş olmasına rağmen, sertifika talep eden kişi tarafından imza oluşturma ve doğrulama verilerinin sertifika sağlayıcıya ait olmayan yerlerde ve araçlarla üretmesi imkanı "*Nitelikli Elektronik Sertifika Sahibinin Yükümlülükleri*" başlıklı Elektronik İmza Yönetmeliği'nin 15. maddesinin I. fıkrasında düzenlenmektedir. EİY. 15 I (c) hükmüne göre, nitelikli elektronik sertifika sahibinin "*İmza oluşturma verisini kendisi üretmesi durumunda Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ ile belirlenen algoritmaları ve parametreleri kullanmakla*" ve aynı maddenin (h) bendinde "*İmza oluşturma ve doğrulama verilerinin sertifika hizmet sağlayıcıya ait olmayan yerlerde*

---

[499] Erturgut, **a.g.e**., s.315.

[500] Thomale, **a.g.e**., s.150.

[501] Mine Erturgut, "Elektronik Sertifika Hizmet Sağlayıcısı", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.6, S.2, 2004, s.97-130, s.104.

ve araçlarla üretilmesi durumunda gerekli güvenliği sağlamakla" yükümlü olduğu belirtilmektedir. Yönetmelik'te böyle bir imkan öngörülmekle birlikte, bu imkanın tercih edilmesi halinde belirtilen algoritmaların ve parametrelerin kullanıldığının ve gerekli güvenliğin sağlandığının ne şekilde denetleneceği düzenlenmemektedir.

İmza oluşturma verisinin imza sahibi tarafından ve kendi sağladığı araçlarla üretilmesi imkanın Kanun yerine Yönetmelik'te düzenlenmiş olması, böyle bir imkanın hukuken var olup olmadığının belirlenmesi bakımından soru işareti yaratmaktadır. Üstelik, uygulamada, güvenlik açısından dışarıdan gelen müdahalelere açık olması ve imza sahibinin sorumluluğunu ağırlaştırması sebebiyle bu imkanın genelde tercih edilmediği ifade edilmektedir[502].

İmza oluşturma verisinin doğrudan imza sahibi tarafından üretilmesi halinde, ilk olarak tespit edilmesi gereken husus bu ihtimalde güvenli bir elektronik imzanın varlığından söz edilip edilemeyeceğidir. Elektronik imza uygulamasının güvenliği açısından riskler taşıyan ve meydana gelecek zararlardan sorumluluğun belirlenebilmesi açısından önem arz eden böyle bir imkanın varlığının ve bu yolla oluşturulan elektronik imzanın güvenli bir elektronik imza olduğunun kabul edilmesi için, bu konudaki düzenlemelere Kanun'da açıkça yer verilmesi gerekmektedir. Ayrıca imza sahibi tarafından üretilen imza oluşturma verisine karşılık gelen imza doğrulama verisinin nitelikli sertifika ile bağlantısı kurulmadan önce, sertifika sağlayıcı açısından bunların mevzuatta aranan teknik ve güvenlik kriterleri taşıyıp taşımadığını denetleme yükümlülüğü öngörülmelidir. Denetim yükümlülüğü Kanun'da düzenlenmeli, kapsamı ve niteliği açıklığa kavuşturulmalıdır.

Diğer yandan, sertifika sağlayıcının sertifika verdiği imza oluşturma verilerinin mevzuatta aranan kriterlerini yerine getirmemesi halinde, bunların kullanımından ötürü meydana gelecek zararlardan kendi ürettiği imza oluşturma verileri gibi sorumlu olup olmadığı meselesi yine Kanun'da açıkça düzenlenmelidir. İmza sahibinin ürettiği imza oluşturma verisinin gerekli kriterleri taşımaması sebebiyle meydana gelen zararlardan tek başına sorumlu olduğunun kabul edilmesi, Elektronik İmza Kanunu'nun benimsediği, üçüncü kişinin nitelikli sertifikaya

[502] Thomale, **a.g.e**., s.148.

güvenini koruyan sorumluluk sistemiyle bağdaşmamaktadır. Burada sorumluluğun sertifika sağlayıcı tarafından üstlenilmesine yönelik yasal tedbirler alınmalıdır.

Belirttiğimiz bu hususlara ilişkin gerekli düzenlemeler yapılmadığı takdirde, imza oluşturma verilerinin imza sahibi tarafından sertifika sağlayıcıya ait olmayan yerlerde ve araçlarda üretilmesi imkanı hukuki dayanaktan yoksundur, bu nedenle de böyle bir imkanın kabul edilmesi mümkün değildir.

3. Nitelikli Sertifika Düzenleme Yükümlülüğü

İmza oluşturma verisinin üretiminin gerçekleştirilmesinden sonraki aşama, iç ilişkide gerçekleştirilmiş olan imza doğrulama verisinin imza sahibine özgülenmesi işleminin nitelikli sertifika ile kamuya açıklanmasıdır[503]. Nitelikli sertifikanın düzenlenmesi sertifika sağlayıcının asli yükümlülüğünü oluşturmaktadır[504]. Diğer yükümlülükler, özellikle kimlik tespiti ve imza doğrulama verisinin özgülenmesi yükümlülükleri, nitelikli sertifika düzenleme yükümlülüğünü tamamlayıcı niteliktedir[505]. Elektronik ortamda gerçekleştirilen işlemlerin hukuki güvenliği imza doğrulama verisinin belirli bir gerçek kişiye nitelikli sertifika ile özgülenmesi sayesinde sağlanmaktadır[506].

Dijital imza tekniğinde gizli anahtar hangi kullanıcıya ait olduğunu, kendisi ile uyumlu çalışan açık anahtar ile açıklar. Ancak açık anahtar ve gizli anahtar çiftinin tamamlayıcı işlerliği tek başına kimlik tespitini gerçekleştirmeye yaramamaktadır[507]. Gizli anahtar ile açık anahtar arasında güvenli bir matematiksel bağlantı bulunmasına rağmen, açık anahtar ile kullanıcı arasındaki bağ dışarıdan gelebilecek müdahalelere açıktır. Gizli anahtarı elinde bulunduran herkesin imza sahibi gibi hareket etmesi mümkündür. Nitelikli sertifikanın amacı gizli anahtar ile

---

503 Hansen, **a.g.e**., s.47

504 Hansen, **a.g.e**., s.128.

505 aus de Fünften, **a.g.e**., s.145. Kimlik tespitinin nitelikli sertifika düzenleme yükümlülüğü ile ilişkisi hakkında bkz. s.147. İmza oluşturma verilerinin imza sahibine özgülenmesinin nitelikli sertifika düzenleme yükümlülüğü ile ilişkisi hakkında bkz. s.158.

506 Thomale, **a.g.e**., s.151; Erturgut, **a.g.e**., s.83; Sözer, **a.g.e.**, s.1014. Sertifikaya bağlanan ve imza sahibine özgülenen her zaman yalnızca imza doğrulama verisidir, bkz. Jungermann, **a.g.e**., s.55.

507 Erturgut, **a.g.e**., s.83.

imza sahibi arasındaki ilişkinin güvenilir bir şekilde kurulmasıdır[508]. Bunu gerçekleştirmek için gizli anahtara karşılık gelen açık anahtar nitelikli sertifika aracılığıyla imza sahibine özgülenmektedir.

Nitelikli sertifika, imza sahibinin kimlik bilgilerinin hızlı ve kendiliğinden çalışan bir sistemle belirlenebilmesine imkan vermektedir. Sertifika sayesinde, güvenli elektronik imza ile imzalanan bir irade beyanının kimden sadır olduğu belirlenebilmektedir[509].

Nitelikli sertifikada bulunması gereken bilgiler EİK. 9 hükmünde yer almaktadır. Nitelikli sertifikada belirtilmesi gereken bilgiler arasında, sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilginin (EİK. 9 g), sertifika sahibi talep ederse mesleki veya diğer kişisel bilgilerinin (EİK. 9 h) [510], sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddi sınırlamalara ilişkin bilgilerin (EİK. 9 ı) bulunması zorunlu değildir[511]. EİK. 9'da sayılan diğer bilgiler eksiksiz olarak belirtilmediği takdirde, düzenlenen sertifika nitelikli sertifika olma özelliğini yerine getirmeyecektir[512].

Nitelikli sertifikanın kullanılacağı işlemlere ilişkin getirilecek olan sınırlamalar, bu işlemlerin türü ve maddi kapsamı bakımından getirilecek sınırlamalar olmak üzere iki türlü olabilir[513]. Elektronik İmza Kanunu'nda açıkça hükme bağlanmış olmamakla birlikte, işlemin türü bakımından sınırlamaya gidilebileceği EİY. 15 (d) hükmünün ifadesinden anlaşılmaktadır. Nitelikli sertifikanın kullanılacağı işlemlerin türü ve değeri hakkında öngörülen sınırlamalar, imza sahibini imza oluşturma verisinin çalınması, kaybolması, güvenlik açısından başka bir riskin ortaya çıkması durumlarında zarara uğraması ihtimaline karşı

---

[508] Hansen, **a.g.e**., s.47; von Harnier, **a.g.e**., s.78.

[509] Thomale, **a.g.e**., s.151. Güvenli elektronik imzada kimlik tespiti işlevinin kesin bir şekilde gerçekleştiğinden hiçbir zaman söz edilemez. Bu konudaki değerlendirmeler için bkz. s.18 vd.

[510] İmza sahibinin üçüncü bir kişiyi temsil yetkisi veya imza sahibinin mesleki bilgileri gibi kimlik bilgileri dışında kalan benzeri ek bilgilerin nitelikli sertifikaya bağlı, görev sertifikası olarak nitelendirilen ayrı bir sertifikaya kaydedilmesi imkanı hakkında bkz. yukarıda s.86, dn.300.

[511] Sertifika esas itibariyle imza doğrulama verisi ile imza sahibinin "adı" arasında bağlantı kurmaktadır. Temsil yetkisi, mesleki yeterlilik belgesi, sertifikanın kullanımına ilişkin maddi sınırlamalar benzeri bilgilerin sertifikada bulunması zorunlu değildir: Hansen, **a.g.e**., s.47.

[512] EİK. 4 (c) hükmünde nitelikli sertifika güvenli elektronik imzanın bir geçerlilik şartı olarak düzenlenmektedir.

[513] Fischer-Dieskau / Hornung, **a.g.e**., s.2897.

korumayı amaçlamaktadır[514]. Elektronik imzalı metnin alıcısı üçüncü kişi tarafından imza doğrulaması yapılırken, nitelikli sertifika görüntülenerek, sertifikanın kapsamına ilişkin maddi bir sınırlama bulunup bulunmadığı belirlenebilmektedir[515].

Sertifika sağlayıcı tarafından düzenlenen nitelikli sertifikanın geçerliliği belirli bir süre ile sınırlıdır[516]. EİK. 9 (e) hükmüne göre, nitelikli elektronik sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihlerinin sertifika üzerinde gösterilmesi zorunludur (EİK 9 e). Sertifikanın geçerlilik süresi taraflar arasındaki sözleşmeye göre belirlenmektedir (EİY. 10). Nitelikli elektronik sertifikanın, geçerlilik süresinin sona ermesinden önce imza sahibinin talebi ile sertifika sağlayıcı tarafından yenilenmesi mümkündür (EİY. 12). Elektronik İmza Kanunu'nda nitelikli elektronik sertifikanın geçerliliğine ilişkin azami bir süre öngörülmemektedir[517]. Ancak her halükarda nitelikli sertifikanın geçerlilik süresinin, nitelikli sertifikaya dayalı imza oluşturma ve doğrulama verilerinin oluşturulmasında kullanılan algoritmaların ve parametrelerin geçerlilik süresi ile sınırlı olduğunun kabul edilmesi gerekir[518]. Algoritmaların ve parametrelerin geçerlilik süresinin ne zaman sona erdiği sertifika sağlayıcı tarafından ilgili mevzuat takip edilerek bilinebilir. Geçerlilik süresi sona erdiğinde, bunlara dayalı olarak üretilen nitelikli sertifikalar sertifika sağlayıcı tarafından iptal edilecektir.

Nitelikli sertifika bir tür elektronik belgedir. İnternet üzerinden transfer edilen diğer elektronik belgeler gibi içeriksel bütünlüğü dışarıdan gelen müdahalelere açıktır ve düzenleyen sertifika sağlayıcının kimliğinin güvenilir biçimde belirlenmesi

---

514 Thomale, **a.g.e**., s.152; Fischer-Dieskau / Hornung, **a.g.e**., s.2897.

515 Fischer-Dieskau / Hornung, **a.g.e**., s.2897. Nitelikli sertifikadaki gerçeği yansıtmayan sınırlamalar sebebiyle üçüncü kişinin zarara uğraması mümkündür (Thomale, **a.g.e**., s.152). Bu sınırlamaların sertifika sağlayıcının üçüncü kişilere karşı sorumluluğu bakımından etkisi hakkında bkz. s.204.

516 Geçerlilik süresinin uzunluğu, dijital imzada, kriptografik güvenliğe göre yapılan tahminler ve hesaplanan anahtar uzunluklarına göre kararlaştırılır. Kriptografik güvenlik, kriptoanalitik gelişmeler ve sürekli devam eden hesaplamalara uygun olarak tanımlanmaktadır (Hansen, **a.g.e**., s.51, dn.247).

517 Alman Elektronik İmza Yönetmeliği'nde nitelikli elektronik sertifikanın geçerlilik süresinin uygulanan algoritmaların ve ilgili parametrelerin geçerli olduğu süreyi aşamayacağı, her halükarda en fazla beş yıl olarak kararlaştırılabileceği belirtilmektedir (§14 III SigV).

518 İmza oluşturma ve doğrulama verilerinin üretilmesinde kullanılan, 06.01.2005 tarihli ve 25692 sayılı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen algoritma ve parametrelerin geçerlilik süresi son olarak 31.12.2010 tarihine kadar uzatılmıştır (bkz. 30.12.2009 tarihli ve 30209 sayılı "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"de Değişiklik Yapılmasına Dair Tebliğ m.1).

gerekmektedir. Bunun için sertifika sağlayıcının nitelikli sertifikanın tamamını, herkes tarafından görülebilir biçimde, kendi güvenli elektronik imzasını kullanarak imzalaması gerekmektedir[519]. Buna paralel olarak, EİK. 9 (j) hükmünde, nitelikli sertifikada yer alan bilgiler arasında sertifika sağlayıcının güvenli elektronik imzasının bulunması zorunlu olduğu belirtilmektedir.

Nitelikli sertifika elektronik imza ile imzalandığı takdirde, içerdiği bilgilerin sertifika sağlayıcı dışında başka bir kişi tarafından değiştirilmesi engellenmektedir. Bu şekilde nitelikli sertifikanın üretimi tamamlanmış olmaktadır[520]. Sertifika sağlayıcı nitelikli sertifikada yer alan bilgilerin tahrif edilmesini, sahtesinin üretilmesini önlemek için gereken tedbirleri almalı, özellikle sertifikayı imzalamak için kullandığı kendi imza oluşturma verisinin gizliliğini ve güvenliğini temin etmelidir[521].

4. İmza Doğrulama Verisini İmza Sahibine Özgüleme Yükümlülüğü

Güvenli elektronik imzanın şartlarından biri münhasıran imza sahibine bağlı olmasıdır (EİK. 4 a). Bu şartın gerçekleştirilmesi için sertifika sağlayıcı tarafından üretilen imza oluşturma verisinin imza sahibinin tasarrufuna sunulması ve buna karşılık gelen imza doğrulama verisi ile imza sahibi arasında nitelikli sertifika aracılığıyla bağlantı kurulması gerekmektedir[522]. Aksi takdirde, elektronik imzanın nitelikli sertifikaya dayanmasının hiçbir değeri bulunmamaktadır[523].

İmza oluşturma verisinin üretilmesini takip eden, imza doğrulama verisinin nitelikli sertifikayla bağlantısının kurulması, imza oluşturma verisinin nitelikli sertifika ile birlikte imza sahibine teslimi, ilk kullanımda imza sahibinin kimlik

---

519 Jungermann, **a.g.e**., s.55; Thomale, **a.g.e**., s.151; Hansen, **a.g.e**., s.48.

520 Hansen, **a.g.e**., s.48.

521 Hansen, **a.g.e**., 129.

522 Nitelikli sertifika imza oluşturma verisinin imza sahibine özgülendiğini garanti eder: Erturgut, **a.g.e**., s.311. Bir kereye mahsus olmak üzere, bir anahtar çifti, sertifika işlemi sayesinde bir gerçek kişiye özgülenir. Sertifika ile özgüleme belgelendirilir: Erturgut, **Elektronik Sertifika Hizmet Sağlayıcısı**, s.105.

523 Hansen, **a.g.e.**, s.129.

doğrulamasının gerçekleştirilmesi fiillerinin tamamı imza doğrulama verisinin imza sahibinine özgülenmesi yükümlülüğü kapsamındadır[524].

Bu yükümlülüğün yerine getirilmesinde sertifika sağlayıcıları tarafından verilen güvenli elektronik imza oluşturma araçları belirleyici rol oynamaktadır[525]. Güvenli elektronik imza oluşturma araçları, imza oluşturma verisinin üzerinde kayıtlı olduğu disket veya akıllı kart gibi veri taşıyıcı yapısına sahip donanımı ve ayrıca imzalama programının çalışması için gerekli yazılımı kapsamaktadır[526]. Nitelikli sertifikaya dayanan imza oluşturma verisinin münhasıran imza sahibinin kontrolünde olması için imza oluşturma verisinin güvenli imza oluşturma aracına kaydedilmesi ve imza sahibi dışında kalan kişiler tarafından kullanımının engellenmesi gerekmektedir[527]. EİK. 6'ya göre, güvenli elektronik imza oluşturma araçları, üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini sağlayan araçlardır (EİK. 6 b). Bu araçlar, üzerinde kayıtlı imza oluşturma verilerinin üçüncü kişilerce elde edilemesini ve kullanılamasını engelleyen teknik nitelikleri haiz olmalıdır (EİK. 6 c).

Sertifika sağlayıcının imza oluşturma verisinin kayıtlı olduğu güvenli elektronik imza oluşturma aracını imza sahibinin şahsına teslim etmesi gerekmektedir[528]. Tarafların teslim şeklini istedikleri şekilde kararlaştırmaları mümkündür[529]. Ancak imza oluşturma verisinin yetkisiz kullanımı sebebiyle oluşabilecek zararlardan imza oluşturma verisi imza sahibinin tasarrufuna erişinceye dek sertifika sağlayıcı sorumludur[530]. Bu durumda sertifika sağlayıcının imza oluşturma verisinin imza sahibi dışındaki başka bir kişiye teslim edilmesi halinde meydana gelecek zararları engellemek için gerekli tedbirleri alması gerekmektedir[531]. Bunun için önerilen yöntem; imza oluşturma verisi ilk defa olarak kullanılmadan

---

[524] Hansen, **a.g.e**., s.49.

[525] Hansen, **a.g.e.**, s.129.

[526] Erturgut, **a.g.e.**, s.313.

[527] Hansen, **a.g.e**., s.129.

[528] Hansen, **a.g.e**., s.129.

[529] Uygulamada imza oluşturma verisi taşıyıcı araçta (güvenli elektronik imza oluşturma aracı) kaydedilmekte ve posta yoluyla imza sahibine gönderilmektedir: Hansen, **a.g.e**., s.49.

[530] Hansen, **a.g.e**., s.129.

[531] Hansen, **a.g.e**., s.130.

önce, güvenli elektronik imza oluşturma aracına giriş kontrolü kurulmasıdır. Giriş kontrolleri, bilgiye dayalı (PIN, şifre) veya biyometrik yöntemler (parmak izi, retina tarama vb.) vasıtasıyla, kullanıcının sertifikada kimlik bilgileri belirtilen imza sahibi olduğunu kanıtlamaya yaramaktadır. Giriş kontrollerine bu işleme özgü olarak üretilen erişim verisi (PIN, parmak izi) girilmektedir. Bu şekilde imza sahibinin kimlik doğrulamasının ilk defa olarak gerçekleştirilmesiyle imza doğrulama verisinin özgülenmesi işlemi tamamlanmış olmaktadır[532]. Bundan sonra, imza oluşturma verisinin yetkisiz kişiler tarafından kullanılmasını engelleme yükümlülüğü imza sahibine aittir (EİY. 15 e).

İmza sahibi imza oluşturma verisini kendisi ürettiği takdirde, sertifika sağlayıcının imza oluşturma verisini imza sahibinin tasarrufuna sunma yükümlülüğü bulunmamaktadır[533]. Bu durumda imza oluşturma verisi zaten imza sahibinin hakimiyetindedir. Ancak sertifika sağlayıcının imza oluşturma verisinin kaydedildiği imza oluşturma aracının gereken nitelikleri taşıyıp taşımadığını kontrol etmelidir[534]. İmza doğrulama verisinin sertifika aracılığıyla imza sahibine özgülenmesi işleminin ise sertifika sağlayıcı tarafından gerçekleştirilmesi gerekmektedir[535].

5. Elektronik İmza Araçlarını Sağlama Yükümlülüğü

Elektronik imza araçları; güvenli elektronik imza oluşturma aracı (EİK. 6)[536] ve güvenli elektronik imza doğrulama aracıdır (EİK. 7)[537]. Sertifika sağlayıcı

---

[532] Hansen, **a.g.e**., s.49.

[533] von Harnier, **a.g.e**., s.77.

[534] von Harnier, **a.g.e**., s.77.

[535] Thomale, **a.g.e**., s.150.

[536] Güvenli elektronik imza oluşturma aracının şartları hakkında inceleme için bkz. s.80.

[537] İmza doğrulama aracı elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracı olarak tanımlanmaktadır (EİK. 2).

Güvenli elektronik imza doğrulama araçlarının sahip olması gereken özellikler EİK. 7 hükmünde sayılmıştır. Bu hükme göre güvenli elektronik imza doğrulama araçları;

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

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

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

tarafından imza sahibine teslim edilen bu araçların, Kanun'da aranılan özellikleri taşıması ve Kurum tarafından düzenlenen tebliğlerde aranılan standartlara uygun olarak üretilmesi gerekmektedir.

Güvenli elektronik imza oluşturma aracı kullanılması el yazısıyla imza ile aynı hukuki etki doğuran bir güvenli elektronik imzanın meydana getirilmesi için zorunludur. Güvenli elektronik imza doğrulama aracı ise imza sahibinin, kendisine gönderilen belgeler üzerinde yer alan güvenli elektronik imzanın geçerliliğini doğrulamak amacıyla kullanacağı bir araçtır. Bu nedenle, imza sahibinin aynı zamanda üçüncü kişi konumunda yer aldığı durumlarda, kullandığı güvenli elektronik imza doğrulama aracının kendisinden beklenen işlevleri yerine getirmesi önem taşımaktadır.

EİY. 16 (b) hükmünde üçüncü kişinin "*Nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla*" yükümlü olduğu belirtilmektedir. Bu hükümden anlaşıldığı kadarıyla, güvenli elektronik imza doğrulama aracının kullanılması zorunlu olmayıp, bu araç vasıtasıyla yapılacak kontrollerin doğrudan sertifika sağlayıcı tarafından elektronik ortamda yayınlanan iptal listesi üzerinden gerçekleştirilmesi de mümkündür[538].

---

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

e) imza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,

f) imzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan,

İmza doğrulama araçlarıdır.

Güvenli elektronik imza doğrulama araçlarına ilişkin bu şartlar AB Elektronik İmza Yönergesi Ek IV'ten alınmıştır.

[538] Güvenli elektronik imza doğrulama aracı nitelikli sertifikanın iptal ve geçerlilik durumunun kontrolünün yanı sıra açık anahtar ve gizli anahtar arasındaki doğrulama işleminin gerçekleştirerek belgenin değiştirilmediğini tespite yaramaktadır. Bu durum karşısında üçüncü kişinin nitelikli sertifikaya güveni bakımından ortaya çıkan çelişkili durum hakkında bkz. s.185 vd.

6. İmza Sahibini Bilgilendirme Yükümlülüğü

İmza sahibinin güvenlik gerekliliklerine uygun davranışlarda bulunabilmesi için elektronik imzanın teknik yapısı, elektronik imza kullanımına ilişkin özellikler ve elektronik imza kullanımının meydana getireceği hukuki sonuçlar hakkında sertifika sağlayıcı tarafından bilgilendirilmesi gerekmektedir. Bu yükümlülüğün yerine getirilmesi elektronik imzanın güvenlik altyapısının tam olarak inşa edilebilmesi için gereken temel unsurlardan biridir[539]. Böyle bir bilgilendirme yapılmadığı takdirde, imza sahibinin kusurlu davranışlarda bulunması mümkündür ve uzun vadede bu tür davranışlar elektronik imza kullanımının güvenliği ve geçerliliğine olan güvenin sarsılmasına yol açabilir[540]. Bundan kaçınmak amacıyla, EİK. 10 (e) ve EİY. 14 nitelikli sertifika düzenleyen sertifika sağlayıcıların imza sahibini bilgilendirme yükümlülüğünü düzenlemektedir. Bilgilendirme yükümlülüğünün elektronik imza sahibi kişilere karşı yerine getirilmesi öngörülmüş olup, nitelikli sertifikaya güvenen üçüncü kişilere karşı sertifika sağlayıcının böyle bir yükümlüğü bulunmamaktadır[541].

EİK. 10 I e'ye göre sertifika sağlayıcı; "*sertifikanın kullanımına ilişkin özellikler ve uyuşmazlıkların çözüm yolları ile ilgili şartlar hakkında ve kanunlarda öngörülen sınırlamalar saklı kalmak üzere güvenli elektronik imzanın el yazısıyla imza ile eşdeğer olduğu hakkında sertifika talep eden kişiyi sertifikanın tesliminden önce yazılı olarak bilgilendirmekle yükümlüdür*". EİY. 14 bilgilendirme yükümlülüğünün kapsamını daha da somutlaştırmaktadır. Buna göre, sertifika sağlayıcı nitelikli elektronik sertifika verilecek kişiyi nitelikli elektronik sertifika vermeden önce asgari olarak; "*a) Kanun'da öngörülen sınırlamalar saklı kalmak üzere, güvenli elektronik imzanın el yazısıyla imza ile eşdeğer olduğuna, b) imza oluşturma verisini ve aracını başkasına kullandırmamasına, c) nitelikli elektronik sertifikanın kullanımı ile ilgili usul ve sınırlamaların kapsamına, d) nitelikli elektronik sertifikanın iptal durumuna, e) nitelikli elektronik sertifika sahibi ile*

---

[539] Stefanie Fischer-Dieskau, **Das elektronisch signierte Dokument als Mittel zur Beweissicherung,** Baden-Baden, Nomos, 2006, s.260.

[540] Fischer-Dieskau, **a.g.e**., s.260.

[541] AB Elektronik İmza Yönergesi Ek II'deki düzenlemelere paralel olarak üçüncü kişi elektronik imza altyapısına ilişkin temel bilgileri kendi başına edinmek durumundadır. Detaylı inceleme için bkz. Fischer-Dieskau, **a.g.e**., s.260.

arasında çıkacak uyuşmazlıklarda başvurulabilecek alternatif uyuşmazlık çözüm yollarına, f) sözleşmenin hüküm ve şartlarında meydana gelecek değişikliklere ilişkin yazılı olarak bilgilendirir".

Bilgilendirme yükümlülüğü kapsamında öncelikle imza oluşturma verisi kullanılarak oluşturulan elektronik imzanın el yazısı ile imza ile aynı hukuki sonuçları meydana getireceğinin imza sahibine açıklanması gerekmektedir (EİK. 10 I e, EİY. 14)[542]. Yazılı şeklin en önemli işlevlerinden biri olan uyarı işlevinin elektronik ortamda sağlanması, güvenli elektronik imzaya atfedilen hukuki değerin imza sahibine yeterli şekilde açıklanmış olmasına bağlıdır[543]. Diğer taraftan, imza sahibinin, böyle bir hukuki değeri haiz güvenli elektronik imzanın hangi teknik şartları sağlaması gerektiği, aksi halde ortaya çıkabilecek sonuçların neler olduğu hakkında bilgilendirilmesi gerekmektedir[544]. İmza sahibine, imza oluşturma verisinin gizliliğin temin edilmesi, sertifika kullanımına ilişkin özellikler ve elektronik imza kullanımındaki teknik araçlar hakkında bilgi verilmelidir[545]. Bu açıdan bilgilendirme yükümlülüğünün yerine getirilmesi, imza sahibine elektronik imza kullanımı hakkında bir tür eğitim verilmesi niteliğindedir[546]. EİK. 10 I (e) hükmünde yer alan "*sertifikanın kullanımına ilişkin özellikler*" ifadesini bu içerikte anlamlandırmak gerekmektedir.

Elektronik imza hakkında, sertifika sağlayıcı tarafından mevzuata uygun olarak geliştirilen teknik özelliklere ilişkin bilgisi bakımından, imza sahibi sertifika sağlayıcıya göre zayıf konumdadır[547]. İmza sahibi, sertifika sağlayıcının kendisinin tecrübesizliğini ve buna bağlı olarak ortaya çıkabilecek riskleri öngördüğünü kabul ederek, elektronik imza kullanımına ilişkin temel konularda onu aydınlatacağına

---

542 Dörr, **a.g.e**., s.82; Thomale, **a.g.e**., s.147.

543 Thomale, **a.g.e**., s.147.

544 Fischer-Dieskau, **a.g.e**., s.260.

545 von Harnier, **a.g.e**., s.78.

546 von Harnier, **a.g.e**., s.78.

547 Dörr, **a.g.e**., s.108.

güvenmektedir[548]. Bu açıdan bakıldığında sertifika sağlayıcının bu yükümlülüğü bir tür aydınlatma yükümlülüğü niteliği taşımaktadır[549].

İmza sahibinin, imza oluşturma verisinin ve imza oluşturma verisine erişimek için kullanılan kimlik doğrulama verilerini saklaması, imza oluşturma verisi ve aracına başkasına kullandırmaması gerektiği konusunda aydınlatılması gerekmektedir (EİY. 14). İmza sahibine imza oluşturma verisinin yalnızca kendi tasarrufu altında bulunduğu ve bunun gizliliğini temin etme yükümlülüğünün ona ait olduğu açıklanmalıdır. İmza oluşturma verisinin gizliliğinden şüphe etmesi halinde sertifikanın iptalini talep etmesi gerektiği belirtilmelidir[550]. İmza sahibine sertifikanın kullanılacağı işlemlerin değeri ve türleri hakkında maddi sınırlamalara (EİK. 9 (1) hükmündeki sınırlamalar) başvurabileceği hakkında bilgi verilmelidir[551].

Kendisine gönderilen elektronik imzalı belgeler bakımından, imza doğrulamasının güvenli bir şekilde gerçekleştirilmesi için sertifika sağlayıcı gerekli tüm güvenlik kriterleri hakkında imza sahibini bilgilendirmelidir. İmza doğrulama araçları hakkında bilgi verilmesi yanında, nitelikli sertifikaya dayalı bir elektronik imzanın geçerliliğinin ve nitelikli sertifikadaki maddi sınırlamaların ne şekilde denetleneceği imza sahibine açıklanmalıdır.

İmza sahibinin kullandığı elektronik imza verilerine ve araçlarına ilişkin mevcut bilgilerinin teknolojideki gelişmelere bağlı olarak güncellenmesi gerektiği ifade edilmektedir[552]. Bunlar arasında imza oluşturma verilerinin güncellenmesi güvenlik açısından önem taşımaktadır. İmza oluşturma verilerinin dayalı olduğu parametre ve algoritmaların geçerliliği belirli bir süre ile sınırlıdır. Elektronik imzalı bir belgenin uzun bir süre saklanması gerekmesi halinde, buna dayalı olarak ortaya çıkabilecek riskler hakkında imza sahibinin bilinçlendirilmesi gerekmektedir[553]. İmza sahibi, kendisine verilen elektronik imza oluşturma verilerinin güvenlik değerinin

---

548 Dörr, **a.g.e**., s.108.

549 Dörr, **a.g.e**., s.81.

550 von Harnier, **a.g.e**., s.78; Thomale, **a.g.e**., s.146.

551 Thomale, **a.g.e**., s.147.

552 Fischer-Dieskau, **a.g.e**., 261. İmza sahibi her yıl düzenli olarak veya belirli aralıklarla ilan yoluyla (örneğin e-posta ile) güvenlik açısından ortaya çıkan riskler konusunda bilgilendirilebilir.

553 Bu konuda Alman hukukunda yer alan düzenleme için bkz. SigG §6.1.2 ve SigV §6.5.

belirli bir süre geçtikten sonra azalacağı, bu nedenle yenilenmesi gerektiği konularında aydınlatılmalıdır[554].

Sertifika sağlayıcının bilgilendirme yükümlülüğü kapsamında, imza sahibini sertifikanın (dolayısıyla sertifikada belirtilen kimlik bilgilerinin) kamuya açık bir dizinde yayınlanması ve buna bağlı olarak doğabilecek tehlikeler konusunda bilgilendirilmesi konusu da bulunmaktadır[555]. Nitelikli sertifikanın kamuya açık bir dizinde yayınlanması EİK. 12 (b) ve EİY. 11 II hükümleri uyarınca imza sahibinin rızasına bağlıdır. Sertifika sağlayıcının, imza sahibini bu konuya ilişkin olarak da bilgilendirmesi ve iradesinin ne yönde olduğu tespit etmesi gerekmektedir[556].

Nitelikli sertifikaya dayanan elektronik imza uygulamalarının tümünün güvenliğinin sağlanmasında bilgilendirme yükümlülüğü önemli bir yere sahiptir. Elektronik imza güvenliğinin mutlak biçimde sağlanabilmesi için, her kullanıcının bilgilendirilmesi, mevzuatta kapsamı belirtilen bilgiye her kullanıcının sahip olması gerekmektedir[557]. Elektronik İmza Kanunu'na göre sertifika sağlayıcı tarafından gerçekleştirilen bilgilendirme yükümlülüğü yalnızca imza sahibine yönelik olarak öngörülmüş olup, elektronik imzalı belgenin muhatabı konumundaki üçüncü kişiyi kapsamamaktadır. AB Elektronik İmza Yönergesi Ek II'ye paralel olarak getirilen bu düzenlemeye göre, sertifika sağlayıcı tarafından üçüncü kişiye sunulan bilgiler elektronik imzanın doğrulaması için gerekli nitelikli sertifikada yer alan bilgiler ile sınırlıdır[558]. Nitelikli sertifikada belirtilen bu bilgiler ise elektronik imza kullanımında üçüncü kişinin sertifikaya güvenini tesis etmeye yöneliktir[559]. Bu durumda, örneğin elektronik imza doğrulamasını gerçekleştiren üçüncü kişi bu işleme ilişkin olarak sertifika sağlayıcıya, elektronik imza teknolojisine ilişkin temel bilgilere (nitelikli sertifikanın tespiti, bu sertifikada yer alan bilgilerin elektronik

---

554 Fischer-Dieskau, **a.g.e**., 261; Thomale, **a.g.e**., s.146.

555 **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu,** s.68.

556 Sertifika sağlayıcının nitelikli sertifikayı kamuya açık bir dizinde yayınlama yükümlülüğü hakkında bkz. s.180.

557 Fischer-Dieskau, **a.g.e**., 260.

558 Üçüncü kişiye nitelikli sertifikaya güvenerek belirli bir işlemde bulunma kararı vermesi aşamasında sertifikada yer alan bilgilerin doğruluğu garanti edilmektedir.

559 Fischer-Dieskau, **a.g.e**., 260.

ortamda görüntülebilir oluşu, bu bilgilerin özellikle nitelikli sertifikadaki sınırlamaların hukuki etkileri, açık ve gizli anahtarın işlerliği vb.) sahip olduğu takdirde başvurabilecek, aksi takdirde sertifika sağlayıcıya başvurmayı düşünmesi dahi söz konusu olamayacaktır[560]. Diğer taraftan Elektronik İmza Yönetmeliği'nin 16. maddesinde üçüncü kişinin bu tür teknik konularda yeterli bilgiye sahip olup olmadığı konusunda herhangi bir ayrım yapılmaksızın, "*nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla*" yükümlü olduğu, nitelikli sertifikaya olan güveninin koruma görebilmesi için zorunlu tutulmaktadır.

Nitelikli elektronik imza ile imzalanmış belgenin alıcısı üçüncü kişinin imza sahibi gibi eşit kapsamda bilgilendirildiği varsayıldığı takdirde, tüm elektronik imza kullanıcılarının mevzuatta öngörülen bilgiye sahip olduğu ve elektronik imzanın güvenliğin genel olarak sağlandığı kabul edilebilir. Ancak, böyle bir varsayımın günümüzde gerçekleştirilmesi mümkün değildir[561]. Eksik bilgilendirmenin yaratabileceği olumsuz sonuçların etkisinin ortadan kaldırılması için, kendisi imza sahibi konumunda olmayan (başka bir sertifika sağlayıcı tarafından kendisine elektronik imza araçları sağlanmamış olan) her elektronik imzalı belgenin alıcısının, elektronik imza doğrulamasını gerçekleştiremediği zaman, belgeyi geri çevirmesi ve kağıt üzerindeki çıktısını talep etmesi gerekir. Uygulamada ise çoğu zaman elektronik imzalı belgenin alıcısı, kendisine gönderilen belgeyi kabul etmekte ve saklamaktadır[562]. Bu durum karşısında eksik bilgilendirmeye dayalı olarak örneğin şu sonuç ortaya çıkmaktadır: Elektronik imza doğrulamasını güvenli şekilde gerçekleştirmiş ve nitelikli sertifikanın iptal durumunu kontrol etmiş olsaydı, elektronik imzanın geçerliliğine ilişkin şüphe duyacak olan üçüncü kişi, yeterli bilgiye sahip olmaması halinde, bu tür denetimleri gerçekleştirmeksizin elektronik imzalı belgeyi geçerli olarak kabul etmekte ve buna dayalı olarak hukuki işlemlerde bulunmaktadır[563].

---

[560] Fischer-Dieskau, **a.g.e**., 260.
[561] Fischer-Dieskau, **a.g.e**., 261.
[562] Fischer-Dieskau, **a.g.e**., 261.
[563] Fischer-Dieskau, **a.g.e**., 261.

Bu çelişkili durum Elektronik İmza Kanunu'nda çözüme kavuşturulmuş değildir. EİK. 10 I (e), imza sahibinin elektronik imza kullanımının yaratabileceği sonuçları öngörebilmesi açısından yerinde olarak, sertifika sağlayıcının imza sahibini elektronik imzanın hukuki sonuçları, kullanımına ilişkin özellikler hakkında bilgilendirmesi yükümlülüğünü düzenlenmektedir. Bunun dışında, Elektronik İmza Kanunu'na göre elektronik ortamda (ticari veya ticari olmayan nitelikte) faaliyet gösteren tüm kullanıcıların elektronik imza konusunda bilinçlendirilmesi sertifika sağlayıcılar tarafından yerine getirilmesi gereken bir yükümlülük olarak düzenlenmemektedir. Bu durumda da, elektronik imzanın geçerli olarak hukuki sonuç doğurmasından menfaati olan üçüncü kişilerin, böyle bir yükümlülüğün düzenlenmemiş olması dolayısıyla ortaya nitelikli sertifikaya güven temelinde ortaya çıkan riskleri kendi başına üstlenmesi gerektiği sonucu ortaya çıkmaktadır.

EİK. 10 I (e) hükmü bilgilendirme yükümlülüğünün nitelikli sertifikanın tesliminden önce ve yazılı bir şekilde yerine getirilmesini öngörmektedir. Bu şekilde imza sahibinin sertifikaya dayalı olarak işlemde bulunmadan önce bilgilendirilmesi ve böylelikle elektronik imzayı bilinçli olarak kullanması amaçlanmaktadır. Sertifika sağlayıcının bilgilendirme yükümlülüğünü, imza sahibine elektronik posta yoluyla ve kendi güvenli elektronik imzası ile imzaladığı bir belgeyle yerine getirmesi mümkündür[564].

7. Nitelikli Elektronik Sertifikayı İptal Etme Yükümlülüğü

Sertifika sağlayıcı tarafından düzenlenen nitelikli sertifikanın geçerliliği belirli bir süre ile sınırlıdır[565]. Bu süre zarfında imza oluşturma ve doğrulama verilerinin gizliliği veya güvenliği tehlikeye düştüğü takdirde veya sertifikada yer alan bilgilerin artık gerçeği yansıtmaması halinde, sertifika sağlayıcı tarafından

---

[564] **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu,** s.42.

[565] Hansen, **a.g.e**., s.51, dn.247.

nitelikli sertifika derhal iptal edilerek, imza oluşturma verisi ile imza sahibi arasındaki bağlantının kesilmesi gerekmektedir[566].

Dijital imzada, kimlik tespitini gerçekleştirmek üzere, gizli anahtar (imza oluşturma verisi) ile imza sahibi arasında kurulan bağlantı iki temele dayanmaktadır: Açık anahtar (imza doğrulama verisi) ve sertifika. Gizli anahtar ile açık anahtar arasındaki bağlantının ortadan kaldırılması matematiksel olarak mümkün değildir. Ayrıca, sertifika dayalı olmaları sebebiyle, sertifika iptal edilmeksizin gizli ve açık anahtarların yenilenmesi imkanı da bulunmamaktadır. Bu sebeple, gerekli olduğu takdirde, gizli anahtar ile imza sahibi arasındaki bağlantı doğrudan sertifikanın iptali gerçekleştirilmek suretiyle sona erdirilmelidir[567].

a. Nitelikli Sertifikanın İptalini Gerektiren Sebepler

Nitelikli elektronik sertifikanın geçerlilik süresi sona ermeden önce, belirli sebeplerin gerçekleşmesi halinde, sertifika sağlayıcı sertifikayı iptal etmekle yükümlüdür. Elektronik İmza Kanunu'nun ve Elektronik İmza Yönetmeliği'nin çeşitli hükümlerinde belirtilen başlıca sebepler aşağıda ayrı ayrı incelenecektir.

(1) Nitelikli Sertifika Sahibinin Talebi

Elektronik İmza Kanunu'nda nitelikli sertifika sahibi olarak ifade edilen kişi, güvenli elektronik imza oluşturma aracını elinde bulunduran imza sahibidir (EİK. 3 c). İmza sahibinin, imza oluşturma verisinin gizliliğinden veya güvenliğinden şüphe duyması halinde nitelikli sertifikanın iptalini talep etmesi mümkündür. Bunun dışında, nitelikli sertifikaya dayalı elektronik imza hizmetinden artık yararlanmak istememesi halinde de geçerlilik süresi sona ermeksizin, sertifikanın iptalini talep edebilir. Dolayısıyla iptal talebinde bulunan kişinin imza sahibi olması halinde, herhangi bir sebep gösterilmesi zorunluluğu bulunmamaktadır. EİK. 11 (a) hükmü, sertifikanın iptalinin gerçekleştirilmesi için imza sahibinin bu hususstaki iradesini tek başına yeterli görmektedir.

---

[566] Hansen, **a.g.e**., s.51.

[567] Hansen, **a.g.e**., s.51.

Kurumsal başvuru halinde, yalnızca çalışan değil, aynı zamanda çalışanı adına nitelikli sertifika düzenlettiren kurum, nitelikli sertifika sahibi sıfatını taşımamasına rağmen, sertifika sağlayıcı ile kurulan sertifika sözleşmesinin tarafı konumunda olması dolayısıyla iptal talebinde bulunma hakkına sahiptir[568]. EİK. 3 (c) hükmü uyarınca imza sahibi sıfatını taşıyan çalışanın da iptal talebinde bulunması mümkündür. Bunun yanında EİY. 13 I hükmü sözleşmeyle belirlenen başka kişilerin de iptal talebinde bulunabileceğini ifade etmektedir.

(2) Nitelikli Elektronik Sertifikada Yer Alan Bilgilerin Sahteliğinin veya Yanlışlığının Ortaya Çıkması veya Bilgilerin Değişmesi

Nitelikli sertifikada yer alan bilgilerin sahteliğinin veya yanlışlığının ortaya çıkması veya bilgilerin değişmesi sebebiyle nitelikli sertifikanın artık gerçeği yansıtmaması halinde sertifikanın iptal edilmesi gerekmektedir (EİK. 11 b).

Nitelikli sertifikadaki gerçeği yansıtmayan bilgiler, imza sahibinin kimlik bilgileri, mesleki bilgileri veya üçüncü bir kişiyi temsil yetkisine ilişkin olabileceği gibi, sertifikanın kullanılacağı işlemler için belirlenen maddi sınırlamalara ilişkin de olabilir. Sertifika başvurusunda bulunan kişinin kimliğinin sahte belgelere dayalı olarak tespit edilmesi halinde sertifikaya kaydedilen kimlik bilgilerinin sahteliği söz konusu olur. İmza sahibi tarafından belirlenen 1000 liralık sertifikanın kullanıma ilişkin maddi sınırlamanın, sertifika sağlayıcı tarafından hatalı olarak 10.000 lira olarak sertifikaya kaydedilmesi halinde sertifikadaki bilginin yanlışlığı söz konusu olacaktır. Nitelikli sertifikada yer alan bilgilerin değişmesine, imza sahibinin üçüncü kişiyi temsil yetkisinin sertifikada belirtilmiş olması halinde bu yetkisinin sona ermesi örnek olarak verilebilir[569]. Bu durumda, imza sahibi yanında temsil olunan üçüncü kişinin de nitelikli sertifikanın iptalini talep etmesi mümkündür[570].

---

[568] Kurumsal başvuru halinde taraflar arasında kurulan sözleşmenin niteliği konusunda bkz. s.94.

[569] Hansen, **a.g.e**., s.131, dn.625.

[570] Sertifikanın iptali talebinin yalnızca imza sahibi tarafından yapılması zorunluluğu bulunmamaktadır: Jungermann, **a.g.e**., s.56, dn.56.

(3) İmza Oluşturma Verisinin Çalınması, Kaybolması veya Başka Bir Şekilde İmza Sahibinin İradesi Dışında Elinden Çıkması Sonucu Gizliliğinin Ortadan Kalkması

Sertifikanın derhal iptalini gerektiren en önemli sebeplerden biri imza oluşturma verisinin çalınması, kaybolması veya benzeri bir nedenle imza oluşturma verisinin gizliliğinin ortadan kalkması hallerinde söz konusu olur[571]. Örneğin, güvenli imza oluşturma aracının (bugünkü teknolojiye göre akıllı kartın veya USB çubuğun) kaybolması veya çalınması halinde imza oluşturma verisinin yetkisiz kişilerce kullanılması tehlikesi meydana gelmektedir. İmza oluşturma verisini ele geçiren kişi, imza sahibine yöneltilen gizli mesajları okuyabilir, onun adına hukuken bağlayıcı işlemlerde bulunabilir veya yalnızca imza sahibine sunulan hizmetlerden (örn. zaman damgası) yararlanabilir[572]. İmza oluşturma verisinin gizliliğine ilişkin şüphe yaratan söz konusu tehlikelerin gerçekleşmesi halinde sertifikanın iptal edilebileceği EİY. 13 III hükmünde düzenlenmektedir.

İmza oluşturma verisi, imza sahibinin fiili hakimiyetinde bulunduğundan, herhangi bir nedenle iradesi dışında elinden çıkması halinde, sertifikanın iptali talebinin imza sahibi tarafından gerçekleştirilmesi gerekmektedir. Bu konuda, EİY.15 (i) hükmünde imza sahibinin imza oluşturma aracının veya erişim verisinin kaybolması, çalınması, güvenilirliğinden şüphe edilmesi durumunda sertifika sağlayıcıyı derhal bilgilendirmekle yükümlü olduğu açıkça belirtilmektedir.

(4) İmza Oluşturma Verisinin Güvenliğinin Ortadan Kalkması

İmza oluşturma verisinin güvenliğinin ortadan kalkması, imza oluşturma verisinin kayıtlı olduğu imza oluşturma aracının teknik donanımında veya imza oluşturma verisinin üretildiği algoritma ve parametrelerde güvenlik açıklarının tespit edilmesi hallerinde söz konusu olur[573]. İmza oluşturma aracının güvenliğinin

---

[571] Jungermann, **a.g.e**., s.56; Hansen, **a.g.e**., s.131.

[572] Hansen, **a.g.e**., s.51.

[573] Jungermann, **a.g.e**., s.56

teknolojideki gelişmelere bağlı olarak geçen süre zarfında azalması mümkündür[574]. Ayrıca, yukarıda belirtildiği gibi, nitelikli sertifikaya dayalı imza oluşturma ve doğrulama verilerinin oluşturulmasında kullanılan algoritmaların ve parametrelerin geçerliliği belirli bir süre ile sınırlıdır[575]. Bu sürenin sonunda, imza oluşturma verilerinin güvenliğine ilişkin riskler ortaya çıkabilir. Bu hallerde elektronik imzanın imza sahibi dışında başka bir kişi tarafından oluşturulması veya elektronik imzalı metnin deşifre edilerek başkaları tarafından okunması, değiştirilmesi tehlikeleri oluştuğundan, imza oluşturma verisinin bağlantılı olduğu nitelikli sertifikanın, sertifika sağlayıcı tarafından iptal edilmesi gerekmektedir (EİY. 13 III).

Sertifika sağlayıcı, imza oluşturma verisine ilişkin güvenlik açıklarını en iyi şekilde öngörebilecek konumda olduğundan[576], bu halde (imza sahibini bilgilendirmek şartıyla) sertifikanın iptalini resen gerçekleştirmesi mümkündür.

(5) Nitelikli Sertifika Sahibinin Fiil Ehliyetinin Sınırlandığının, İflasının veya Gaipliğinin ya da Ölümünün Öğrenilmesi

EİK. 11 (c) hükmü uyarınca nitelikli sertifika sahibinin fiil ehliyetinin sınırlandığının, iflasının veya gaipliğinin ya da ölümünün öğrenilmesi durumunda nitelikli sertifikanın sertifika sağlayıcı tarafından derhal iptal edilmesi gerekmektedir.

(6) Elektronik İmzanın İmza Oluşturma ve Doğrulama Amacı Dışında Kötüye Kullanıldığının Tespit Edilmesi

İmza sahibi, imza oluşturma ve doğrulama verilerini sadece elektronik imza oluşturma ve doğrulama amaçlı olarak kullanmakla yükümlüdür (EİY. 15 d). İmza

---

574 Fischer-Dieskau, **a.g.e**., s.261.

575 İmza oluşturma ve doğrulama verilerinin üretilmesinde kullanılan, 06.01.2005 tarihli ve 25692 sayılı Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'de belirtilen algoritma ve parametrelerin geçerlilik süresi son olarak 31.12.2011 tarihine kadar uzatılmıştır (bkz. 18.12.2010 tarihli ve 27789 sayılı "Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ"de Değişiklik Yapılmasına Dair Tebliğ m.1).

576 Fischer-Dieskau, **a.g.e**., s.260.

sahibinin bu yükümlülüğe aykırı olarak hareket etmesi ve elektronik imzayı kötüye kullanması halinde nitelikli sertifikanın iptaline başvurulabilir. Kötüye kullanma, elektronik imzanın imza oluşturma ve doğrulama amacı dışında başka bir amaçla kullanılması halinde ortaya çıkar. Örneğin, dijital imzanın gizli anahtar kullanılarak metnin şifrelenmesi esasına dayalı olması ve bu şekilde çapraz şifreleme yöntemi kullanılarak[577] metnin içeriğinin üçüncü kişiler tarafından öğrenilmesini engelleyen özelliğinin, belirli bir suçun işlendiğini gizlemek amacıyla kullanılması halinde, elektronik imzanın kötüye kullanılması söz konusu olur. Buna benzer kötüye kullanımların sertifika hizmet sağlayısı tarafından tespit edilmesi halinde nitelikli sertifikanın iptal edilmesi gerekmektedir[578].

(7) Sertifika İlkelerinin Değişmesi

Sertifika sağlayıcılar tarafından düzenlenen nitelikli sertifikaların birbiriyle uyumlu olması ve birlikte çalışabilirliğinin sağlanması için mevzuatımızda sertifika ilkeleri düzenlenmektedir. Yürürlükteki sertifika ilkeleri Bilgi ve İletişim Teknolojileri Kurumu tarafından hazırlanan 18.04.2007 tarihli ve 2007/DK-77/207 sayılı Kurul Kararı'nda yer almaktadır. EİY. 13 III hükmüne göre, sertifika

---

[577] Çapraz şifreleme yöntemi hakkında bkz. dn 30.

[578] Suç faaliyetlerinin izlenmesinde istihbarat amaçlı olarak, bazı yetkili devlet birimlerinin belirli olay ve süre ile sınırlı olarak ve yargısal denetime tabi bir şekilde kullanıcıların gizli anahtarlarına ulaşmalarını sağlayan bir imkan öngörülebilir. Ancak böyle bir imkanın ve bunun sınırlarının kanun yoluyla belirlenmesi gerekmektedir.

10.11.2008 tarihli ve 27050 sayılı Elektronik Haberleşme Kanunu'nun "kodlu ve kriptolu haberleşme" hakkındaki 39. maddesine dayalı olarak Bilgi ve İletişim Teknolojileri Kurumu tarafından hazırlanan, 23.10.2010 tarihli ve 27738 sayılı Yönetmelik kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin elektronik haberleşme hizmeti içinde kodlu veya kriptolu haberleşme yapma usul ve esaslarını düzenlemektedir. Yönetmelik'in 5. maddesi kodlu veya kriptolu haberleşme cihazı veya sistemi ithal veya imal eden üreticinin, bunlara ilişkin izin alabilmesi için "kripto algoritması ve anahtarı, anahtar üretme, dağıtma ve yükleme modülü/cihazı, bu amaçla kullanılan tüm yazılım/donanım, gerektiğinde şifrenin çözülmesine imkân tanıyan yazılım ve/veya donanım"ın Kurum'a teslim edilmesi gerekmektedir (m.5 ç). Bu şekilde CMK m.135'de öngörülen telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri kapsamında, kriptografiye dayalı olarak şifrelenen elektronik imzalı belgelerin, bir suçun kovuşturmasına yönelik olarak gizliliğinin yetkili devlet birimleri tarafından ortadan kaldırılarak, taraflar arasındaki iletişimin kayıt altına alınması mümkündür.

ilkelerinin değişmesi halinde bu ilkelere dayalı olarak üretilen nitelikli sertifikaların iptal edilmesi (ve ücret talep edilmeksizin yenilenmesi) gerekmektedir[579].

(8) Sertifika Sağlayıcının Faaliyetinin Sona Ermesi

Sertifika sağlayıcı tarafından sertifikanın iptal edilmesi konusu, EİK. 11 III hükmünde sertifika sağlayıcının faaliyetinin sona ermesi haline özgü olarak ayrıca düzenlenmektedir. Sertifika sağlayıcı, faaliyetine son vermesi ve düzenlediği nitelikli sertifikaların başka bir sertifika sağlayıcı tarafından kullanımının sağlanamaması durumunda, bu sertifikaları derhal iptal etmekle yükümlüdür (EİK. 11 III). Prensip olarak, sertifika hizmet sağlayısı faaliyetine son vermesi halinde dahi vermiş olduğu sertifikaların geçerliliğini ayakta tutmak yükümlülüğü altındadır[580]. EİK. 11 III hükmü sertifika sağlayıcının bu yükümlülüğünü vermiş olduğu sertifikaları başka bir sertifika sağlayıcıya devrederek yerine getirmesini öngörmektedir. Ancak bunun teknik olarak mümkün olmaması halinde vermiş olduğu sertifikaları iptal etmesi gerekmektedir.

Sertifika sağlayıcının faaliyetine Bilgi Teknolojileri ve İletişim Kurumu tarafından son verilmesi halinde, Kurum faaliyetine son verilen sertifika sağlayıcının vermiş olduğu nitelikli elektronik sertifikaların başka bir sertifika sağlayıcıya devredilmesine karar verir ve durumu ilgililere duyurur (EİK. 11 IV). Bu düzenleme ile sertifika sağlayıcının faaliyetinin sona erdirilmesinin nitelikli sertifikaların geçerliliğini etkilememesi amaçlanmaktadır. Nitelikli sertifikaların başka bir sertifika sağlayıcı tarafından üstlenilememesi halinde ise, son çare olarak sertifikaların Kurum tarafından iptal edilmesi yoluna başvurulacaktır.

b. Nitelikli Sertifikanın İptaline İlişkin Taleplerin Yapılması

Nitelikli sertifikanın iptalinin, imza (sertifika) sahibi (EİK. 11 a), sözleşme ile belirlenen başka kişiler (EİY. 13 I) veya kurumsal başvuru söz konusu olan

[579] EİY. 13 III'te sertifika ilkelerinin değişmesi durumunda imza sahibinin kusuru bulunmadığından sertifikanın yenilenmesi için ücret talep edilemeyeceği belirtilmektedir.

[580] Spiegelhalder, **a.g.e**., s.63.

hallerde, imza sahibi yanında kurumsal başvuru sahibi tarafından da yapılabileceğini yukarıda belirtmiştik[581]. Bunun dışında, Yönetmelik, iptal talebinde bulunabilecek kişiler arasında sertifika sağlayıcıya da yer vermektedir (EİY. 13 II). Sertifika sağlayıcının kendi kendisine talepte bulunması söz konusu olamayacağından, bu ifade Kanun'da ve Yönetmelik'te belirlenen sebeplerin gerçekleştiğine dair kesin kanıya varmış olması halinde, sertifika sağlayıcının resen sertifikanın iptalini gerçekleştirmeye yetkili olduğu şeklinde yorumlanmalıdır.

Öğretide, nitelikli sertifikanın iptaline ilişkin sertifika sağlayıcıya yapılacak taleplerin, imza sahibinin yanı sıra üçüncü bir kişi tarafından da yapılmasının mümkün olduğu ifade edilmektedir[582]. Bu konuda, nitelikli sertifikada üçüncü bir kişiyi temsil yetkisinin yer alması halinde, temsil olunan üçüncü kişinin de iptal talebinde bulunabilmesi örnek olarak gösterilmektedir[583]. Gerçekten de nitelikli sertifikada bir üçüncü kişiyi temsil yetkisine yer verilmiş olması halinde, temsil olunan üçüncü kişi imza sahibi konumunda olmadığı gibi, her zaman kurumsal başvuru sahibi veya sözleşmede kendisine iptal yetkisi tanınan bir kişi konumunda da olmayabilir. Bu durumda, söz konusu üçüncü kişinin, temsil yetkisinin sona ermesi halinde nitelikli sertifikanın artık gerçeği yansıtmadığı gerekçesiyle iptalini talep etmekte hukuken korunmaya değer bir menfaati bulunmaktadır. Çünkü nitelikli sertifikanın iptal edilmemesi ve temsil yetkisinin nitelikli sertifikada görüntülenebilir olmaya devam etmesi halinde, temsilcinin bu elektronik imzayı kullanarak yapacağı işlemlerden ötürü meydana gelecek hukuki sonuçlardan temsil olunan olarak görünen üçüncü kişi sorumlu olacaktır.

Hukukumuzda üçüncü kişilerin sertifikayı iptal için talepte bulunmaya yetkili olup olmadığı konusu düzenlenmemektedir. Bununla birlikte, yukarıda belirttiğimiz sertifikada belirtilen temsil yetkisinin sona ermesine konusuna ilişkin olarak, sertifikada yer alan bilgilerin değişmesi halini nitelikli sertifikanın iptal sebebi olarak düzenleyen EİK. 11 (b) hükmünü esas almak suretiyle, temsil olunan olarak görünen

---

[581] Bkz. s. 168.

[582] Thomale, **a.g.e**., s.156; aus der Fünften, **a.g.e**., s.16.

[583] Spiegelhalder, **a.g.e**., s.63.

üçüncü kişinin de sertifikanın iptalini talep edebileceğini kabul etmek isabetli olacaktır.

Bunun dışında, örneğin imza sahibinin ölümü, kısıtlanması, sertifikanın imza oluşturma amacı dışında kalan amaçlarla kötüye kullanıldığının tespit edilmesi hallerinde, sertifikanın iptalini gerektiren bu sebeplerin gerçekleştiğinin üçüncü kişiler tarafından sertifika sağlayıcıya bildirilmesi imkanı vardır. Ancak bu tür bildirimlerin yapılması, sertifikanın iptalini talep etme yetkisine sahip olmaktan ayrı bir nitelik taşımaktadır.

Nitelikli sertifikanın iptalini talep eden kişinin, imza sahibi olduğunu iddia etmesi halinde, bu kişinin gerçekte imza sahibi olup olmadığının güvenli bir şekilde tespit edilmesi gerekmektedir[584]. Buna paralel olarak, sözleşme ile kendisine iptal talebinde bulunma yetkisi tanınmış kişilerin de iptal talebi yürürlüğe konulmadan önce kimlik bilgileri doğrulanmalıdır.

Sertifikanın iptalinin ancak mevzuatta öngörülen nitelikteki sebeplerin gerçekleşmesi halinde yürürlüğe konulabileceğinden hareketle, iptal talebinin sertifika sağlayıcıya gerekçesi belirtilerek iletilmesi gerekmektedir[585]. Aynı şekilde sertifika sağlayıcı tarafından resen gerçekleştirilecek iptal işleminin yeterli şekilde gerekçelendirilmesi gerekmektedir. İptal talebinde bulunan kişinin imza sahibi olması halinde, herhangi bir sebep gösterilmesi zorunluluğu bulunmamaktadır. Zira EİK. 11 (a) hükmünün ifadesinden, sertifikanın iptalinin gerçekleştirilmesi için imza sahibinin bu hususstaki iradesini tek başına yeterli gördüğü anlaşılmaktadır.

Sertifika sağlayıcı tarafından iptal yükümlülüğünün gerektiği şekilde yerine getirilebilmesi, sertifika sağlayıcının her zaman ulaşılabilir olmasına bağlıdır[586]. Sertifika sağlayıcı iptal taleplerinin yapılabilmesini, asgari olarak telefonla ve kesintisiz sağlamakla yükümlüdür (EİY. 13 I).

---

[584] von Harnier, **a.g.e**., s.80.

[585] von Harnier, **a.g.e**., s.80; aus der Fünften, **a.g.e**., s.16.

[586] Hansen, **a.g.e**., s.51; aus der Fünften, **a.g.e**., s.16.

c. Nitelik Sertifikanın İptal Edilmesi ve İptal Kararının Sertifika Sağlayıcı Tarafından Oluşturulan İptal Listesinde Yayınlanması

Nitelikli elektronik sertifika, iptal talebinin alınmasından sonra sertifika sağlayıcı tarafından derhal iptal edilir (EİK. 11 I). İptalinin derhal gerçekleştirilmesinde ihmal edilmesi sertifika sağlayıcının sorumluluğuna yol açabilir[587]. Talebin varlığına rağmen iptalin gerçekleştirilmemiş olması halinde veya geçerli bir talep bulunmamasına rağmen (örneğin iptal talebinde bulunan kişinin kimlik doğrulamasının gerçekleştirilmemiş olması veya sertifikanın iptalini gerektiren bir sebebin bulunmaması halinde) sertifika iptal edilirse, imza sahibinin önemli zararlara uğraması mümkündür[588]. Bu zararaların, sertifika sağlayıcı tarafından tazmin edilmesi gerekmektedir.

Sertifika sağlayıcı, nitelikli sertifikaların iptal edildiği zamanın tam olarak belirlenmesini sağlayan ve üçüncü kişilerin hızlı ve güvenli bir biçimde ulaşabileceği bir iptal listesi[589] oluşturmakla yükümlüdür (EİK. 11 II). Bu şekilde sertifikanın, iptal edilerek geçerliliğine son verilmiş olduğu kamuya açıklanacaktır[590].

Sertifikanın iptal edildiği zamanın iptal listesinde belirtilmesi gerekmektedir[591]. İptalin gerçekleştirildiği zamanın kesin olarak tespit edilebilmesi için sertifika sağlayıcı tarafından nitelikli zaman damgası oluşturulmalıdır[592]. Nitelikli sertifikanın geçerliliği iptal listesinde belirtilen iptal zamanından itibaren ileriye etkili olarak sona ermektedir. Bu zamana kadar nitelikli sertifikaya dayalı olarak oluşturulan elektronik imzaların geçerliliği iptal kararından etkilenmeyecektir[593]. Sertifika sağlayıcı geçmişe yönelik olarak sertifikayı iptal edemez (EİK. 11 V, EİY. 13 II).

---

587 Thomale, **a.g.e**., s.157.

588 von Harnier, **a.g.e**., s.79.

589 Elektronik İmza Kanunu'nun "iptal durum kaydı" ifadesi yerine, uygulamada da benimsenen daha sade ve anlaşılır nitelikteki "iptal listesi" ifadesini kulllanmayı tercih ediyoruz.

590 von Harnier, **a.g.e**., s.78.

591 Spiegelhalder, **a.g.e**., s.63; aus der Fünften, **a.g.e**., s.16. Görev sertifikasının iptali ile nitelikli sertifikanın iptali aynı zamanda meydana gelmektedir: Thomale, **a.g.e**., s.155.

592 Spiegelhalder, **a.g.e**., s.63; von Seck, **a.g.e**., s.112.

593 Spiegelhalder, **a.g.e**., s.63; von Seck, **a.g.e**., s.112.

İptal edilen nitelikli sertifika, geçerlilik süresinin bitimine kadar iptal listesinde yer alır (EİY. 13 II). İptal listesinin, herhangi bir kimlik doğrulamasına gerek olmaksızın, ücretsiz ve kesintisiz olarak sertifika sağlayıcı tarafından kamu erişimine açık tutulması gerekmektedir (EİY. 13 II). İptal listesinin bir sonraki güncelleme zamanı halihazır listede açıkça gösterilmelidir. (EİY. 13 II). İptal listesinin sertifika sağlayıcı tarafından elektronik imza ile imzalanması gerekmektedir[594].

İptal listesine kayıt düşülmesine ek olarak, nitelikli sertifika bilgilerinin yayımlandığı kamuya açık dizinden iptal edilen sertifikanın kaldırılması gerekmektedir[595]. Bu gereklilik, Kanun'da veya Yönetmelik'te belirtilmiş olmamasına rağmen, nitelikli sertifikanın iptalinin kamuya açıklanması kapsamındadır[596].

İptal işlemi, nitelikli sertifikaya dayalı olarak karar alacak olan üçüncü kişiyi etkileyen bir işlemdir. Sertifika iptal listesi, üçüncü kişiye elektronik imzanın uygulandığı anda sertifikanın geçerli olup olmadığını kontrol etme imkanı vermektedir[597]. İptal işlemi gerçekleştirildikten ve iptal kaydı düşüldükten sonra, üçüncü kişi elektronik imzanın geçerli bir sertikaya dayanmadığını bilmediğini ileri sürerek iyiniyet iddiasında bulunamaz[598]. Bununla birlikte, üçüncü kişinin iptal kaydı düşülmeden önce durumdan haberdar olduğunun ispatlanması mümkündür. Örneğin, imza sahibi iptali gerekli kılan bir sebebin gerçekleştiğini veya iptal talebinde bulunulduğunu ancak iptal kaydının henüz sertifikaya işlenmediğini üçüncü kişiye bizzat iletmiş olabilir. Böyle bir durumda hukuken korunmaya değer bir güveni bulunmamaktadır.

8. Nitelikli Sertifikayı Kamuya Açık Bir Dizinde Yayımlama Yükümlülüğü

---

[594] Spiegelhalder, **a.g.e**., s.63.

[595] von Harnier, **a.g.e**., s.78.

[596] Thomale**, a.g.e**., s.155; von Harnier, **a.g.e**., s.78.

[597] Thomale, **a.g.e.**, s.155; Hansen, **a.g.e.**, s.131.

[598] Bu dizinler yüksek kapasiteli sunucular (*server*) tarafından işletilmekte ve devamlı güncellenmektedir: Hansen, **a.g.e**., s.49.

Nitelikli sertifikanın kamuya açık bir dizinde yayınlanması konusu "Bilgilerin Korunması" başlıklı EİK. 12'nin (b) fıkrasında örtülü bir ifadeyle düzenlenmektedir: "*Elektronik sertifika hizmet sağlayıcısı sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz"*. EİY. 11 hükmüne göre, "*elektronik sertifika hizmet sağlayıcısı imza sahibinin onayını almak kaydıyla nitelikli sertifikayı kamuya açık bir dizinde yayımlamakla yükümlüdür. Sertifika hizmet sağlayıcı, dizin hizmetinin kesintisiz olarak verilmesini sağlar"*.

Güvenli elektronik imza oluşturma aracı niteliğindeki taşınır araçların hafıza ve işlem kapasitesi sınırlı olduğundan, dijital imzanın dayalı olduğu açık anahtar alt yapısının işletilmesi için gerekli olan birçok bilgi kamu erişimine açık bir dizinde depolanmaktadır[599]. Bu bilgilerin kaynağını oluşturan en önemli iki belge, sertifika sağlayıcının imza sahipleri için düzenlediği kullanıcı sertifikaları ve kendisi için düzenlediği kök sertifikasıdır.

İlk olarak, kullanıcı sertifikalarının kamuya açık bir dizinde yayınlanmasıyla sertifikanın taşıdığı bilgilerin doğruluğu ve sertifikanın geçerliliğinin denetlenmesi imkanı sağlanmaktadır. Ayrıca açık anahtarın belirli bir kişiye özgülenmiş olduğu kamuya açıklanmaktadır[600]. Bu sayede, üçüncü kişi, kendisine ulaşan bir metnin kaynağının doğruluğunu, imza sahibinin açık anahtarına hızlı ve güvenli bir biçimde erişerek teyit edebilir[601]. Açık anahtar ve sertifika bilgilerinin üçüncü kişilere bir web sitesi veya elektronik posta aracılığıyla elektronik olarak açıklanması mümkündür[602].

Bununla birlikte, nitelikli sertifikanın kamuya açık bir dizinde kesintisiz olarak yayınlanmasının teknik olarak zorunlu olmadığı ifade edilmektedir[603]. İmza sahibinin kendi kullanıcı sertifikasının bir kopyasını ve açık anahtar bilgisini eklemek suretiyle transfer edilen elektronik verilerin doğruluğunu ve bütünlüğünü garanti etmesi mümkündür[604]. Ancak, imza sahibinin kullanıcı sertifikasının

---

599 Hansen, **a.g.e**., s.49.

600 Thomale, **a.g.e**., s.153; von Harnier, **a.g.e.**, s.79.

601 Jungermann; **a.g.e**., s.55; Hansen, **a.g.e**., s.50; Spiegelhalder, **a.g.e**., s.62.

602 von Harnier, **a.g.e.**, s.79; Hansen, **a.g.e**., s.50.

603 Hansen, **a.g.e**., s.50 ve s.130.

604 Nitekim, elektronik ortamda hukuki ilişkinin kurulmasına yönelik olarak ilk defa iletişim eylemini gerçekleştiren kişi, üçüncü kişi değil, imza sahibidir: Hansen, **a.g.e**., s.49.

bağlayıcılığının üçüncü kişi tarafından denetlenebilmesi için, günümüzdeki gelişmelere göre, sertifika sağlayıcının kök sertifikasını ve açık anahtarını kamuya açık dizinde yayınlaması gerekmektedir[605]. Diğer taraftan, nitelikli sertifikanın kamuya açık bir dizinde yayınlanması, imza sahibinin sertifikada yer alan bilgilerini herkes tarafından erişilebilir kılması nedeniyle, kişisel verilerin korunması yönünden önemli riskler barındırmaktadır. Sertifikada yer alan bilgiler sayesinde sertifika sahibinin kişiliği internet ortamında herkes tarafından belirlenebilir olmaktadır[606]. Bu risklerin varlığı göz önünde bulundurularak, EİK. 12 (b) ve EİY. 11 II hükümleri uyarınca nitelikli sertifikanın kamuya açık dizinde yayınlanması için (iptal listesinde nitelikli sertifikaya ilişkin iptal kaydının açıkça yayınlanmasının aksine) imza sahibinin rızasının bulunması zorunlu tutulmuştur[607].

Kamuya açık dizinlerde yayınlanması gereken en önemli belgelerden biri, sertifika sağlayıcının kendisi için düzenlemiş olduğu kök sertifikasıdır. Kök sertifikası, sertifika sağlayıcının kimliği ile kullanıcı sertifikalarını imzaladığı imza oluşturma verisi arasında bağlantı kurmaktadır. Bir üçüncü kişi, sertifika sağlayıcının imza oluşturma verisine karşılık gelen (kök sertifikasında belirtilen) imza doğrulama verisi aracılığıyla, kullanıcı sertifikasının doğruluğunu ve bütünlüğünü denetleyebilir[608]. Dolayısıyla, imza sahibinin üçüncü kişiye yalnızca açık anahtarı göndermesi yeterli olmayıp, ayrıca sahip olduğu nitelikli sertifikayı da göndermesi gerekmektedir. Aksi takdirde, üçüncü kişi elektronik imzanın nitelikli bir sertifikaya dayanıp dayanmadığını, hangi sertifika sağlayıcı tarafından düzenlendiğini ve sertifikanın geçerliliğini denetleme imkanına sahip olmayacaktır[609].

Nitelikli sertifika, sertifika sağlayıcının güvenli elektronik imzası ile imzalanmış bir elektronik belgedir. Bu niteliği gereği, sertifika sağlayıcının, kamuya açık dizinde yayınlamakta olduğu sertifikaların yetkisiz kişilerce değiştirilmesini engellemekle yükümlü olduğu kabul edilmelidir.

---

605 Hansen, **a.g.e**., s.50.

606 Hansen, **a.g.e**., s.130.

607 Aynı gerekçeyle, Alman Elektronik İmza Kanunu'nda nitelikli sertifikaların kamuya açık dizinde yayınlanması zorunlu olmaktan çıkarılarak, imza sahibinin rızasına bağlı kılınmıştır (SigG §5 I 2). Detaylı bilgi için bkz. Hansen, **a.g.e**., s.130.

608 Hansen, **a.g.e**., s.50; Erturgut, **Elektronik Sertifika Hizmet Sağlayıcısı**, s.116, dn.62.

609 Hansen, **a.g.e**., s.50.

Uygulamada dizin hizmeti, sertifika iptal listelerini, sözleşmeleri, sertifika uygulama esaslarını da kapsayan bilgi deposu şeklinde geniş bir şekilde tanımlanmaktadır[610].

9. Zaman Damgası Hizmetini Sağlama Yükümlülüğü

Sertifika sağlayıcının, imza oluşturma verisi ve dayandığı sertifikanın yönetimi yanında, üstlendiği hizmetler arasında en önemlisi zaman damgası hizmetidir.

Sertifika sağlayıcı, nitelikli sertifikanın düzenlenmesinde ve iptalinde zaman damgasını kullanmaktadır[611]. Nitelikli sertifikanın iptal edildiği anın kesin olarak belirlenmesi zaman damgası sayesinde mümkün olmaktadır. Böylece, zaman damgası esas alınarak, bir elektronik imzanın nitelikli sertifikanın iptalinden önce mi sonra uygulandığı tespit edilebilmektedir[612]. Ayrıca, nitelikli sertifikanın geçerlilik süresinin ne zaman sona erdiğinin belirlenmesinde de zaman damgasından yararlanılmaktadır[613].

Elektronik ortamda kurulan bir hukuki işlemin hükümlerini doğurduğu anın kesin olarak belirlenebilmesi için bazen tarafsız bir üçüncü kişi tarafından oluşturulan zaman damgasına ihtiyaç duyulabilir[614]. Böyle bir durumda, taraflar değiştirilebilir olması nedeniyle bilgisayarın zamanını esas almak istememektedir. Ayrıca, irade açıklamasında bulunan kişi tarafından eklenen zaman bilgisi, sonradan taraflar arası çekişme konusu olabileceğinden, yeterli görülmeyebilir[615]. Bu hallerde, sertifika sağlayıcıdan zaman damgası hizmetinin talep edilmesi imkanı bulunmaktadır. Belirtmek gerekir ki, zaman damgası elektronik belgenin hangi tarihte ve zamanda imzalandığını belirlemeye yaramaktadır. Bunun dışında

---

[610] **Kamu SM Nitelikli Sertifika Uygulama Esasları**, TÜBİTAK UEKA, 2008, s.13, (Çevrimiçi) http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SUE/KSM_NES_SUEv5.pdf, 10.06.2011.

[611] Hansen, **a.g.e**., s.52.

[612] Jungermann, **a.g.e**., s.56.

[613] Jungermann, **a.g.e**., s.56.

[614] von Harnier, **a.g.e**., s.80.

[615] von Harnier, **a.g.e**., s.80.

elektronik belgenin (örneğin elektronik ortamda hazırlanan bir icap veya kabulün) ne zaman gönderildiğini belirlemek için kullanılamamaktadır[616]

EİK. 3 (h) hükmüne 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 kaydı"* ifade etmektedir. Bu amaçla talep edilen zaman damgası, sertifika sağlayıcı tarafından düzenlenen bir tür elektronik belge olup, bir elektronik verinin var olduğu zamanı kesin olarak tespit etme amacına hizmet etmektedir[617]. Bu hizmeti talep eden kullanıcı, elektronik verileri (örneğin elektronik formattaki bir sözleşme metnini) sertifika sağlayıcıya göndermektedir ve sertifika sağlayıcı tarafından bu veriler *hash* değerine dönüştürülmektedir. Sertifika sağlayıcı meydana gelen *hash* değerine güvenli bir zaman bilgisi eklemektedir ve meydana gelen zaman damgasını kendi gizli anahtarını kullanarak güvenli elektronik imzası ile imzalamaktadır[618]. Bu şekilde zaman damgasının başkaları tarafından değiştirilmesi engellenmiş olmaktadır[619].

EİK. 8 hükmüne göre zaman damgası hizmetin verilmesi sertifika sağlayıcıları tarafından üstlenilecektir. Ancak zaman damgası hizmetinin yerine getirilmesinde uygulanacak esaslar Elektronik İmza Kanunu'nda düzenlenmemektedir. Zaman damgası ilkeleri[620] ve zaman damgası uygulama esaslarının[621] oluşturulması sırasında uyulması gereken standartlar Bilgi Teknolojileri ve İletişim Kurumu tarafından hazırlanan Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ'in 10. maddesinde düzenlenmektedir.

EİY. 31 hükmünde, sertifika sağlayıcının, zaman damgası hizmetini imza sahibinin talep etmesi halinde sağlamakla yükümlü olduğu ifade edilmektedir. Bu

---

[616] Belgenin ne zaman gönderildiğinin ve ulaştığının tespit edilmesi için elektronik fatura kullanılmaktadır. Detaylı inceleme için bkz. Dumortier, **E-imza**, s.163-165.

[617] Hansen, **a.g.e**., s.52.

[618] von Harnier, **a.g.e**., s.80; Hansen, **a.g.e**., s.52.

[619] Jungermann, **a.g.e**., s.56.

[620] EİY. 4 hükmüne göre; zaman damgası ilkeleri, "*zaman damgası ve hizmetleri ile ilgili genel kuralları içeren belgeyi*" ifade eder.

[621] EİY. 4 hükmüne göre; zaman damgası uygulama esasları, "*zaman damgası ilkelerinde yer alan hususların nasıl uygulanacağını detaylı olarak anlatan belgeyi"* ifade eder.

nedenle, imza sahibinin böyle bir talebi bulunmadığı takdirde, sertifika hizmetinin kapsamında olduğu ileri sürülerek, sertifika sağlayıcı tarafından zaman damgası hizmetinin verilmesine karşılık olarak imza sahibinden ayrıca bir bedel talep edilemez.

10. Sertifika Sağlayıcının Diğer Yükümlülükleri

EİK. 10 (a) hükmüne göre; "*sertifika hizmet sağlayıcı hizmetin gerektirdiği nitelikte personel istihdam etmekle yükümlüdür"*. Bu yükümlülüğün yerine getirilmesi sertifika hizmet sağlacılarının kurumsal güvenliğinin sağlanmasında önemli bir yere sahiptir[622]. Diğer taraftan, personelin seçiminde gereken özenin gösterilmemesi, sonrasında elektronik imza ve sertifika hizmetinin verilmesine ilişkin olarak öngörülen yükümlülüklerin ihlaline ve bu yüzden meydana gelecek zararlardan ötürü sertifika sağlayıcının sorumluluğuna yol açabilecektir[623]. EİY. 19 II bu yükümlülüğün yerine getirilmesine ilişkin olarak daha somut bir düzenleme getirmektedir. Buna göre, sertifika sağlayıcı, bilgi güvenliği, elektronik imza teknolojileri ve veri tabanı yönetimi alanlarında yeteri kadar teknik personel istihdam etmeli veya ettirmelidir. Teknik personel, konusunda yeterli mesleki deneyime sahip ya da ilgili alanlarda eğitim almış olmalıdır. Sertifika sağlayıcı organizasyon şemasında istihdam ettiği veya ettirdiği tüm personelinin görev tanımını ve dağılımını belirler.

Sertifika sağlayıcı, EİK. 10 (g) hükmü uyarınca, "*verdiği hizmetlere ilişkin tüm kayıtları yönetmelikle belirlenen süreyle saklamakla yükümlüdür"*. Bu sayede, yapılan bütün işlemlerin her zaman kontrol edilmesi imkanı sağlanmış olacaktır[624]. EİY. 14 II bu süreyi en az yirmi yıl olarak öngörmektedir. Sertifika sağlayıcının saklamakla yükümlü olduğu kayıtlar şunlardır (EİK. 14 II):

a) Geçerlilik süresi sona eren nitelikli elektronik sertifikalar,

---

[622] Kurumsal güvenlikle kastedilen, sertifika sağlayıcılarının güvenlik altyapısına ilişkin organizasyonunun güvenilir olmasıdır. Detaylı bilgi için bkz. Erturgut, **a.g.e**., s.97.

[623] Gizli anahtarın üretildiği çevrede çalışan personelin güvenilirliği daha fazla önem taşımaktadır: Jungermann, **a.g.e**., s.58.

[624] Jungermann, **a.g.e**., s.58.

b) Nitelikli elektronik sertifika başvurusunda talep edilen bilgi, belge ve elektronik veriler,

c) Sertifika ilkelerini ve sertifika uygulama esasları,

d) Zaman damgası ilkelerini ve zaman damgası uygulama esasları,

e) Geçerlilik süresinin sona ermesinden itibaren kendi sertifikası,

f) Nitelikli elektronik sertifika yönetimine ilişkin tüm işlemlere, bu işlemlerin yapıldığı zamana ve işlemleri yapan kişiye veya kişilere ait bilgileri içeren kayıtlar.

Kişisel verilerin korunması konusu EİK. 12 hükmünde özel olarak düzenlenmektedir. Bu düzenlemeye göre, sertifika sağlayıcı sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez (EİK. 12 a). İmza sahibinin rızası bulunmadığı takdirde, sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz[625] (EİK. 12 b) ve sertifikanın hazırlanmasına ilişkin olarak sunulan imza sahibine ait kişisel verileri üçüncü kişilerle iletemez (EİK. 12 c). Sertifika sağlayıcı, imza sahibine ait kişisel verileri yalnızca sertifika hizmetinin sağlanması amacıyla sınırlı olarak kullanmakla yükümlüdür (EİK. 12 c).

II. SERTİFİKA SAĞLAYICININ ÜÇÜNCÜ KİŞİLERE KARŞI SORUMLULUĞU

Bir elektronik imzanın güvenli elektronik imza niteliği taşıması sertifika sağlayıcının Kanun'da ve Yönetmelik'te öngörülen yükümlülüklerini eksiksiz bir şekilde yerine getirmesine bağlıdır. Sertifika sağlayıcıları Bilgi ve İletişim Teknojileri Kurumu'ndan gerekli güvenlik kriterlerini sağladıklarına ilişkin olarak izin aldıktan sonra faaliyete başlayabilmekte ve faaliyetleri süresince belirli

[625] Bu düzenlemenin kamuya açık dizin hizmeti açısından uygulanması için bkz. s.177.

aralıklarla Kurum'un denetimine tabi olmaktadırlar. Bu denetimlerin tek başına yeterli olmayacağı öngörülerek, ikinci bir araca daha başvurulmuş ve sertifika sağlayıcının üçüncü kişiye karşı sorumluluğu konusunda, borçlar hukukunun genel hükümlerinden ayrılarak, EİK. 13 hükmünde özel bir sorumluluk düzenlemesine yer verilmiştir. EİK. 13 II ve III hükümlerinde düzenlenen sorumluluk sistemiyle, sertifikasyon sistemlerinin ve güvenli elektronik imza teknolojilerinin güvenliği ve altyapısının mevzuata uygunluğunu temin etmek amaçlanmaktadır.

EİK. 13 II hükmüne göre, "*elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz"*. EİK. 13 III hükmüne göre, "*elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması halinde de zarardan sorumlu olup, elektronik sertifika sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz*".

EİK. 13 II ve III hükümlerinde sertifika sağlayıcının üçüncü kişilere karşı sorumluluğu düzenlenirken, üçüncü kişinin kim olduğuna ilişkin bir tanım verilmemektedir. Kanunun 13. maddesine ilişkin gerekçede ise üçüncü kişinin "*nitelikli elektronik sertifikaya güvenen üçüncü kişi*" olduğu ifade edilmektedir[626]. Gerekçede yer alan bu üçüncü kişi tanımının sorumluluğun kapsamı belirlenirken esas alınması karşılaştırmalı hukuktaki düzenlemelere de uygun düşmektedir[627].

Sorumluluğun kapsamı bakımından aydınlatılması gereken ikinci bir husus sertifika hizmetinin türü bakımından ortaya çıkmaktadır. Elektronik İmza

---

[626] Aynı yönde: Orer, **a.g.e**., s.148. Ayrıca bkz. **Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu,** 44. Sertifika sağlayıcı ile arasında sözleşme ilişkisi bulunmayan herkesin üçüncü kişi kavramına dahil olduğu görüşünde: Yıldırım, "Nitelikli Elektronik Sertifika Hizmet Sağlayıcısının Hukuki Sorumluluğu", **Bilişim Hukuku**, der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s.27-43, s.36.

[627] Karş: AB Elektronik İmza Yönergesi m.6 I, UNCITRAL Elektronik İmza Model Kanunu m. 2 (f). UNCITRAL düzenlemesinde üçüncü kişi yerine doğrudan güvenen taraf (*relying party*) deyimine yer verilmektedir. Üçüncü kişiye ilişkin Alman hukukunda verilen tanım için bkz. SigG §11 I.

Kanunu'nda adi sertifika düzenleyen ve nitelikli sertifika düzenleyen sertifika sağlayıcıları arasında bir ayrım yapılmamaktadır. Kanun'un tamamı incelendiğinde, nitelikli sertifika veya adi sertifika düzenleyen tüm sağlayıcılara yönelik düzenlemeler getiren genel nitelikli ifadelerin kullanıldığı görülmektedir. Bu durum adi sertifika düzenleyen sağlayıcıların da Kanun'da belirtilen yükümlülüklere ve özellikle üçüncü kişilere karşı kabul edilen ağırlaştırılmış sorumluluk rejimine tabi olup olmayacağı konusunda soru işareti yaratmaktadır.

EİK. 5 I hükmünde yalnızca nitelikli sertifikaya dayanan güvenli elektronik imza türünün el yazısıyla imza ile aynı hukuki sonucu doğuracağı düzenlenmektedir. Bunun dışında kalan basit elektronik imza türlerinin ise ad ve soyadın yazılı olduğu basit bir elektronik posta gönderilmesi işleminden hukuki etkileri bakımından bir farkı bulunmamakta, kural olarak bunların el yazısıyla imzanın işlevlerini gerçekleştirmeye yeterli olmadıkları kabul edilmektedir. Bu nedenle de adi sertifika düzenleyen sertifika sağlayıcılar açısından bu kadar ağır yükümlülüklerin ve sorumluluk sisteminin öngörülmesinin bir anlamı bulunmamaktadır.

Bunun yanı sıra, tekrar üçüncü kişi bakımından konuya yaklaşıldığında, böyle bir düzenlemenin anlamsız olacağı şu şekilde ortaya çıkmaktadır. Üçüncü kişinin sertifikaya güveninin hukuken koruma görebilmesi için bu sertifikanın nitelikli sertifika olması gerekmektedir. Bu hususun EİK. 13 hükmüne ilişkin madde gerekçesinde de belirtildiğini yukarıda da ifade etmiştik[628]. Ayrıca üçüncü kişinin yükümlülüklerini düzenleyen EİY. 16 hükmüne göre, üçüncü kişiler sertifikanın *"nitelikli elektronik sertifika" olup olmadığını kontrol etmekle"* yükümlüdür. Yani bir kimsenin nitelikli olmadığını fark ettiği bir sertifikaya dayanan elektronik imzanın geçerliliğine güvenmesi koruma görmeyecektir. Bu nedenle sertifika sağlayıcı açısından öngörülen sorumluluk sisteminin adi sertifika düzenleyen sertifika sağlayıcılarını da kapsayacak şekilde genişletilmesinin pratikte bir sonucu bulunmamaktadır.

---

[628] Bkz. s.186.

Belirtilen gerekçelerle, Kanun'da açıklık bulunmamasına rağmen sertifika sağlayıcı açısından öngörülen yükümlülüklerin ve sorumlulukların yalnızca nitelikli sertifika düzenleyen sertifika sağlayıcıları bakımından uygulanacağını kabul etmek daha isabetli olacaktır[629]. Kanun'un sistematiği de bu yorumu destekler niteliktedir[630]. Ayrıca Kanun'un ne şekilde uygulanacağını açıklamak üzere hazırlanan Elektronik İmza Yönetmeliği'ndeki düzenlemelerin tamamı nitelikli sertifika konusuna ilişkindir[631].

A. SORUMLULUĞUN NİTELİĞİ VE ŞARTLARI

EİK. 13 II hükmüne göre*: "Elektronik sertifika hizmet sağlayıcısı, bu Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli suretiyle üçüncü kişilere verdiği zararları tazminle yükümlüdür. Elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz".*

EİK. 13 II hükmünde sertifika sağlayıcının nitelikli sertifikaya güvenen üçüncü kişilere karşı sorumluluğu kusura dayanan bir haksız fiil sorumluluğu olarak düzenlenmiştir. Sertifika sağlayıcının bu sorumluluktan kurtulabilmesi için söz konusu yükümlülüklere aykırı davranmakta kusurunun bulunmadığını ispat etmesi gerekmektedir[632]. Öğretide, böyle bir düzenleniş tarzının benimsenmiş olması

---

629 İnal, **a.g.e**., s.148.

630 İkinci bölümün başlığı "*Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar*" olup, EİK. 9 vd. hükümlerinde sırasıyla, "*Nitelikli Elektronik Sertifika*", "*Elektronik Sertifika Hizmet Sağlayıcısının Yükümlülükleri", "Nitelikli Elektronik Sertifikaların İptal Edilmesi", "Bilgilerin Korunması", "Hukukî Sorumluluk", "Yabancı Elektronik Sertifikalar"* başlıklarına yer verilmektedir. Burada öncelikle nitelikli sertifika kavramı düzenlenerek daha sonra yükümlülükler ve sorumluluk konusuna yer verilmiş olması nedeniyle, bu düzenlemelerin nitelikli elektronik sertifika düzenleyen sertifika sağlayıcılara yönelik olduğu kabul edilmelidir.

631 İnal, **a.g.e**., s.148 ve dn.212. Yazar, Kanun'da sertifika sağlayıcılara ilişkin ayrımın açıkça vurgulanmamış olmasını, bilinçli bir tercihten çok kanunun kaleme alınmasındaki bir ihmal olarak değerlendirilebileceğini ifade etmektedir.

632 Alman Elektronik İmza Kanunu'nda da aynı şekilde ispat yükü ters çevrilmiş kusur sorumluluğu öngörülmüştür. Bkz. SigG §11 Abs. 2. İsviçre Elektronik İmza Kanunu'nda ise bir tür kusursuz sorumluluk benimsenmektedir. Hukuka aykırılık şartının üçüncü kişi tarafından ispat edilmesi

dolayısıyla, sertifika sağlayıcıların sorumluluğu ispat yükü tersine çevrilmiş bir kusur sorumluluğu olarak nitelendirilmektedir[633]. Buna göre, EİK. 13 II hükmünde ispat yükü yalnızca kusurun ispatı bakımından tersine çevrilmiş olup bunun dışında kalan unsurların genel hükümler çerçevesinde üçüncü kişi tarafından ispat edilmesi gerekmektedir.

Üçüncü kişi yalnızca nitelikli sertifikada yer alan bilgilerin doğruluğuna güvenmesi yüzünden meydana gelen zararlardan ötürü sertifika sağlayıcının sorumluluğuna başvurabilir. Nitelikli sertifikada yer alan ve üçüncü kişinin nitelikli sertifikaya güveninin sağlanmasında rolü bulunan bilgiler EİK. 9 hükmüne göre şunlardır:

> "a) *Sertifikanın "nitelikli elektronik sertifika" olduğuna dair bir ibare,*
> *b) Sertifika hizmet sağlayıcısının kimlik bilgileri ve kurulduğu ülke adı,*
> *c) İmza sahibinin teşhis edilebileceği kimlik bilgileri,*
> *d) Elektronik imza oluşturma verisine karşılık gelen imza doğrulama verisi*
> *e) Sertifikanın geçerlilik süresinin başlangıç ve bitiş tarihleri,*
> *f) Sertifikanın seri numarası,*
> *g) Sertifika sahibi diğer bir kişi adına hareket ediyorsa bu yetkisine ilişkin bilgi*
> *h) Sertifika sahibi talep ederse meslekî veya diğer kişisel bilgileri,*
> *ı) Varsa sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgiler*
> *j) Sertifika hizmet sağlayıcısının sertifikada yer alan bilgileri doğrulayan güvenli elektronik imzası".*

Nitelikli sertifikaya güven şartının gerçekleştirilmesi için üçüncü kişinin nitelikli sertifikada yer alan bilgileri kontrol etmesi, bunun için kendisinden beklenen özeni göstermesi gerekmektedir. Buradaki özen külfetinin kapsamının ne şekilde tayin edileceği Elektronik İmza Yönetmeliği'nin "*Üçüncü Kişilerin Yükümlülükleri*"

---

gerekli olmayıp, sertifika sağlayıcının sorumluluktan kurtulmak için hukuka aykırılık şartının gerçekleşmediğini ispat etmesi gerekmektedir. Bkz. ZertES §16 II.

633 İnal, **a.g.e**., s.149.

başlıklı 16. maddesinde açıklığa kavuşturulmaktadır. Bu maddeye göre üçüncü kişiler;

> *"a) Sertifikanın "nitelikli elektronik sertifika" olup olmadığını kontrol etmekle,*
> *b) Nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli elektronik imza doğrulama aracı kullanmakla,*
> *c) Nitelikli elektronik sertifikanın kullanımına yönelik herhangi bir kısıtlamanın olup olmadığını kontrol etmekle yükümlüdür".*

EİK. 16 hükmünde düzenlenen husus bir yükümlülük değil bir külfet niteliğindedir. Üçüncü kişi bu maddede gösterilen fiilleri gerçekleştirmek suretiyle nitelikli sertifikanın geçerliliğinin kontrol etmediği takdirde uğradığı zararlardan ötürü sertifika sağlayıcının sorumluluğuna başvuramayacaktır[634].

Üçüncü kişi yalnızca nitelikli sertifikada görünen bilgileri kontrol etme külfeti altındadır. Bunun dışında meydana gelebilecek güvenlik yönünden risk teşkil eden konuları üçüncü kişi bilebilecek durumda değildir. Örneğin, sertifika sağlayıcının temin ettiği güvenli elektronik imza araçları gereken nitelikleri taşımadığından üçüncü kişi zarara uğramış olabilir. Bunlar nitelikli sertifikadan anlaşılabilecek, sertifikadaki bilgilerin gerçeği yansıtmaması kapsamında değerlendirme görecek hususlar değildir. Buna rağmen, üçüncü kişinin uğradığı zarar sertifika sağlayıcının yükümlülüklerine aykırı davranmasından kaynaklanmaktadır. Bu nedenle sertifikadan anlaşılamayacak hususlara ilişkin olarak da sertifika sağlayıcının sorumluluğu söz konusudur.

Bununla birlikte üçüncü kişinin nitelikli sertifikada görünen bilgileri kontrol etme külfetinin kapsamını tayin eden EİY. 16 hükmünün yeterli bir düzenleme olmadığını belirtmek gerekir. EİY. 16 (b) hükmünde üçüncü kişinin *"nitelikli elektronik sertifikanın iptal ve geçerlilik durumunu kontrol etmekle veya güvenli*

---

[634] Külfet (yüküm, gerekli davranış) bir kimseye herhangi bir hak sağlamayıp, bir kimsenin belirli hakları kazanabilmek veya kaybetmemek için belirli bir davranışta bulunması gerekliliğini ifade etmektedir: Oğuzman / Öz, **a.g.e**., s.15. Yükümlülük ve külfet ayrımına ilişkin başka örnekler için bkz. Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.32.

elektronik imza doğrulama aracı kullanmakla" yükümlü olduğu ifade edilmektedir. Öncelikle, bir güvenli elektronik imza doğrulama aracının kullanılması sonucu elde edilecek ve üçüncü kişinin nitelikli sertifikaya güveninde rol oynayacak bilgiler, nitelikli sertifikanın iptal ve geçerlilik durumunun kontrolünden çok daha geniş kapsamlıdır. Şöyle ki, EİK. 8 hükmünde belirtildiği üzere bir güvenli elektronik imza doğrulama aracı;

> *"a) İmzanın doğrulanması için kullanılan verileri, değiştirmeksizin doğrulama yapan kişiye gösteren,*
> *b) İmza doğrulama işlemini güvenilir ve kesin bir biçimde çalıştıran ve doğrulama sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,*
> *c) Gerektiğinde, imzalanmış verinin güvenilir bir biçimde gösterilmesini sağlayan,*
> *d) İmzanın doğrulanması için kullanılan elektronik sertifikanın doğruluğunu ve geçerliliğini güvenilir bir biçimde tespit ederek sonuçlarını değiştirmeksizin doğrulama yapan kişiye gösteren,*
> *e) İmza sahibinin kimliğini değiştirmeksizin doğrulama yapan kişiye gösteren,*
> *f) İmzanın doğrulanması ile ilgili şartlara etki edecek değişikliklerin tespit edilebilmesini sağlayan, imza doğrulama araçlarıdır".*

EİK. 8 hükmünün detaylı bir şekilde düzenlenen bu kapsamı dolayısıyla nitelikli sertifikaya güvenin unsurlarının belirlenmesi sorunu ortaya çıkmaktadır. Üçüncü kişinin yalnızca nitelikli sertifikanın geçerlilik durumunu ve sertifika sağlayıcının internet sayfasına girerek iptal listesini kontrol etmesi, EİK. 13 II kapsamında koruma görebilmesi için yeterli midir? Dikkat edilirse, bu soruya olumlu cevap verilmesi halinde açık anahtar ve kapalı anahtarın uyumluluğun tespit eden imza doğrulaması işlemi güven şartının dışında bırakılmaktadır. Oysa ki, güvenli elektronik imzanın el yazısıyla imzaya paralel olarak sağlaması gereken işlevlerin kimlik tespiti işlevi ve sonuçlandırma işlevi olmak üzere iki türlü olduğunu daha önce belirtmiştik. Seçimlik olarak gösterilen şekilde, yalnızca nitelikli sertifikanın geçerlilik durumunun ve iptal listesinin kontrolü külfetinin yerine getirilmesi,

elektronik imzanın sonuçlandırma işlevini göz ardı etmekte, belgede herhangi bir değişiklik yapılıp yapılmadığına, diğer bir ifadeyle belgede yer alan irade açıklamasının imza sahibi tarafından kabul edilip edilmediğine dair yapılacak bir denetimi, nitelikli sertifikaya güven bakımından gerekli görmemektedir. Güvenli elektronik imza doğrulama aracı ise esas itibariyle sonuçlandırma işlevinin yerine getirilip getirilmediğinin kontrolünü esas alan, bununla birlikte nitelikli sertifikanın geçerlilik ve iptal durumunu kontrol etmeye imkan veren fonksiyonları da taşımaktadır.

Yalnızca sertifikanın geçerlilik durumunun ve iptal listesinin kontrolünün yeterli sayılması halinde üçüncü kişinin belgede herhangi bir değişiklik yapılıp yapılmadığını araştırmaksızın elektronik imzanın metnin tamamına ilişkin olduğuna güvendiği bir durum ortaya çıkar. Bu durumda el yazısıyla imzayla güvenli elektronik imzanın işlevleri itibariyle denk olmasından söz edilemez. Çünkü kağıda dayalı ortamda el yazısıyla imzanın metnin tamamına mı yoksa bir bölümüne mi ilişkin olduğu tespit edilebilirken, güvenli elektronik imza doğrulama aracı kullanılmadığı takdirde böyle bir sonuca varılamamaktadır.

Ancak yürürlükte düzenleme gereğince, bir üçüncü kişinin nitelikli sertifikanın geçerlilik durumunu ve iptal listesini kontrol etmiş olması nitelikli sertifikaya güveni sebebiyle EİK. 13 II'e dayanarak koruma görmesi bakımından yeterli kabul edilecektir. Bunun dışında kalan ve güvenli elektronik imza doğrulama aracının sağladığı diğer fonksiyonların üçüncü kişinin güvenini tesis etmekteki rolü sertifika sağlayıcı tarafından üstlenilmiş olmaktadır. Bu durumda şöyle bir sonuç ortaya çıkmaktadır: Bir üçüncü kişi güvenli elektronik imza doğrulama aracı kullanmadığı ve bu yüzden (bu aracı kullansaydı uğramayacağı) bir zarara uğradığı takdirde koruma görecek, güvenli elektronik imza doğrulama aracı kullanan bir üçüncü kişi ise bu araç sayesinde anlayabildiği hususlarda nitelikli sertifikaya güveninin bulunduğundan söz edilemeyeceğinden koruma görmeyecektir.

AB Elektronik İmza Yönergesi'nde nitelikli sertifikaya güvenen kişinin bu güveninin haklı olması gerektiği ifade edilmektedir (m.6 I). Burada nitelikli sertifikaya güvenin haklı kabul edilmesi ile anlatılmak istenen, üçüncü kişinin

nitelikli sertifikada yer alan bilgilerin gerçeği yansıtmadığını bilmemesi veya kendisinden beklenen özeni gösterdiği takdirde dahi bilemeyecek durumda olmasıdır.

Hukukumuz açısından da, üçüncü kişinin sertifikada yer alan bilgilerin gerçeği yansıtmadığını bildiği hallerde korunacak sertifikaya güveni yoktur. Bu ihtimalde, zararın sertifika sağlayıcının hukuka aykırı davranışında kaynaklandığı da söylenemez. Üçüncü kişinin bu davranışı zarar ile sertifika sağlayıcının davranışı arasındaki illiyet bağını kesecek yoğunluktadır. Üçüncü kişinin nitelikli sertifikadaki bilgilerin gerçeği yansıtmadığını bilmesi gereken durumlarda da, tazminatın kapsamının belirlenmesi bakımından, kusurun ağırlığına göre bir değerlendirme yapılmalıdır.

Aşağıda, sertifika sağlayıcının nitelikli sertifikaya güvenen üçüncü kişilere karşı haksız fiile dayalı sorumluluğunun şartları ayrı ayrı incelenecektir.

1. Hukuka Aykırı Fiil

Kusura dayanan haksız fiil sorumluluğun temel şartı, sorumlu tutulacak kişinin hukuka aykırı bir fiilinin bulunmasıdır[635]. Hukuka aykırılık, bir fiilin genel davranış kurallarını ihlal etmesi demektir. Bir kimsenin başka birinin mutlak hakkını ihlale yönelik fiili hukuka aykırıdır. Bununla birlikte, davranış kuralları her zaman kişilerin mutlak hakkını koruma amacı gütmez. Bazı davranış kuralları, kişilerin mutlak haklar dışında kalan menfaatlerini koruma amacı güderler. Bu menfaatleri koruyan davranış kurallarına özel koruma normları denilir. Özel koruma normlarının da ihlali bazen BK. 41/1 anlamında hukuka aykırılık teşkil eder. Ancak, bunun için

[635] Oğuzman / Öz, **a.g.e**., s.492, Eren, a**.g.e**., s.544, Kılıçoğlu, **a.g.e**., s.198. Hukuka aykırılık, sorumluluğun objektif şartıdır: Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.855. Aynı yönde: Feyzioğlu, **a.g.e**., s.483.

özel koruma normunun, kişilerin hukuki bir varlığını ve özellikle de malvarlığına ilişkin bir menfaatini koruma amacı gütmesi gerekir[636].

Sertifika sağlayıcının sorumluluğunda, hukuka aykırılık unsuru, özel bir koruma normunun ihlali dolayısıyla ortaya çıkmaktadır. EİK. 13 II hükmüne dayalı olarak sertifika sağlayıcının sorumluluğuna başvurulabilmesi için, sertifika sağlayıcının Elektronik İmza Kanunu ve Yönetmeliği hükümlerinin ihlaline sebep olan, yapma veya yapmama tarzında hukuka aykırı bir fiilinin bulunması gerekmektedir.

EİK. 13 II'de "*Kanun veya bu Kanuna dayanılarak çıkarılan yönetmelik hükümlerinin ihlâli"* şeklinde hukuka aykırılık unsurunun yorumu bakımından önem arz eden geniş bir ifadeye yer verilmektedir. Kanun'da ve Yönetmelik'te yer alan hükümlerin neredeyse tamamında, bir nitelikli sertifikanın oluşturulması, idaresi ve güvenli elektronik imza araçlarının temini konularında sertifika sağlayıcı bakımından çeşitli yükümlülükler öngörülmektedir. Bu nedenle hükmün bu ifadesinin sertifika sağlayıcının Kanun'dan ve Yönetmelik'ten doğan yükümlülüklerine aykırılık şeklinde anlaşılması isabetli olacaktır[637].

Bu yükümlülüklerin hiç veya gereği gibi yerine getirilmemesi halinde hukuka aykırı bir fiil söz konusu olur. Örneğin, sahte kimlik bilgilerine dayalı olarak bir nitelikli sertifika üretilmiş olması veya imza sahibinin talebine rağmen nitelikli sertifikayı derhal iptal etmekte veya iptal listesine iptal kaydını eklemekte gecikilmiş olması ya da imza sahibine karşı öngörülen bilgilendirme yükümlülüğü yerine getirilmediğinden imza sahibi tarafından güvenli elektronik imza aracının özensizce kullanılması dolayısıyla üçüncü kişinin zarara uğraması hallerinde, meydana gelen zarar sertifika sağlayıcının Kanun'da yer alan yükümlülüklerin tam olarak yerine getirmemiş olmasından kaynaklanmaktadır. Ancak, söz konusu hükümlerin koruma

---

[636] Eren, **a.g.e**., s.544 vd, Oğuzman / Öz, **a.g.e**., s.494 vd. BK. 41 anlamında hukuka aykırılık zararlı neticeyi yasak edici ya da önleyici davranış normlarına aykırılıktır: Kaneti, **a.g.e**., s.153.

[637] İsviçre Elektronik İmza Kanunu'nda (ZertES Art.16 I) sertifika sağlayıcının Kanun'da ve Yönetmelik'te düzenlenen yükümlülüklerine aykırılığı halinde sorumluluğunun ortaya çıkacağı belirtilmektedir. Alman Elektronik İmza Kanunu'da (SigG §11) ise bizdeki ifadeye paralel olarak Kanun'da ve Yönetmelik'teki düzenlemelere aykırılık şartı aranmaktadır.

amacının[638] kapsamına, nitelikli sertifikaya güvenen kişileri zarardan korumak ve uğrayacakları zararı tazmin etmek girmiyorsa, ortada hukuka aykırılık bağı yoktur[639]. Sorumluluk dayanağı normun koruma amacı ile zarar arasında bulunması gereken ilişkiye "hukuka aykırık bağı" denilmektedir. Nitelikli sertifikaya güvenen üçüncü kişiyi koruma amacının dışında kalan, özellikle idare hukukunu ilgilendiren diğer hükümlerin ihlali, hukuka aykırılık bağının eksikliği dolayısıyla hukuka aykırılık unsurunun gerçekleşmesinde hiçbir etki doğurmayabilir.

Hukuka aykırılığın belirlenmesinde sertifikasyon hizmetinin verilmesi ve elektronik imza araçlarının sağlanmasına ilişkin olarak mevzuatta belirlenen teknik kriterlerin tamamının yerine getirilip getirilmediği esas alınacaktır[640]. "*Teknik Hususlara İlişkin Tebliğ*" başlıklı EİY. 34 hükmüne göre, *"nitelikli elektronik sertifika başvurusu, sertifikanın oluşturulması, yayımlanması, yenilenmesi, iptali ve arşivleme süreçleri dahil olmak üzere ESHS'nin işleyişine, imza oluşturma ve doğrulama verilerine, sertifika ilkelerine ve sertifika uygulama esaslarına, imza oluşturma ve doğrulama araçlarına, ESHS'nin faaliyetleri için kullandığı sistem, cihaz ile fiziki güvenliğine, personeline, zaman damgasına ve hizmetlerine ilişkin uyulması gereken teknik kriterler tebliğ ile belirlenir".*

Gerçekten de sertifika sağlayıcı tarafından verilen araçların birer güvenli elektronik imza oluşturma ve doğrulama aracı olup olmadığı, üretilen sertifikaların

---

[638] Bu ifade Alman hukukunda geliştirilen normun koruma amacı teorisine (*normzwecktheorie*) ilişkindir. Bu teori bir kimsenin hukuka aykırı davranışının hangi sonuçlarından sorumlu olacağını belirlemede uygun illiyet bağı teorisinin yetersiz kaldığı düşüncesiyle geliştirilmiştir. Bu görüş çerçevesinde ihlal edilen normun koruyucu etki alanına giren bir zarardan söz edebilmek için üç unsurun yerine getirilmesi gerekmektedir:

a) Zarar gören, ihlal edilen normun korumayı hedef tuttuğu şahıs çevresine girmelidir;

b) Zarar bu normun koruduğu bir hukuk objesi üzerinde gerçekleşmelidir;

c) Zararın oluş biçimi, ihlal edilen normun önlemeyi hedef tuttuğu biçime uygun olmalıdır.

Bu teori hakkında detaylı bilgi için bkz. Teoman Akünal, **Haksız Fiilden Doğan Zararlarda Denkleştirme Sorunu**, Sulhi Garan Matbaası, 1977, s.105.

[639] Hukuka aykırılık bağı hakkındaki görüşler için bkz. Akünal, **a.g.e**., s.103 vd; Eren, **a.g.e**., s.566 vd; Oğuzman / Öz, **a.g.e**., s.494; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.476; Kaneti, **a.g.e**., s.228.

[640] Hangi fiillerin hukuka aykırı olduğu konusu genellikle kanunla belirlenir. Fakat bu zorunlu olmayıp, bir fiilin tüzüklere, yönetmeliklere, hatta bir kurumun çıkardığı genelgelere aykılığı halinde, hukuka aykırılık unsuru gerçekleşmiş olacaktır: Kılıçoğlu, **a.g.e**., s.198. Kanun dışı normlara aykırılığın da hukuka aykırılığı gerçekleştireceği görüşünde: Kaneti, **a.g.e**., s.88.

bir nitelikli sertifika taşıyıp taşımadığının belirlenmesinde hangi kriterlerin esas alınacağına söz konusu tebliğler ışık tutacaktır. Örneğin, EİK. 6 (c) hükmüne göre bir güvenli elektronik imza oluşturma aracının üzerinde kayıtlı olan elektronik imza oluşturma verilerinin üçüncü kişilerce elde edilememesini sağlaması gerekmektedir. Bu şartın yerine getirilmesi bakımından hangi teknik unsurların arandığı konusu ise tebliğler aracılığıyla düzenlenmektedir. Ancak, bu tespitin bir adım ilerisinde çözümü bekleyen problem şudur: Sertifika sağlayıcının söz konusu teknik kriterlere uygun olarak mevzuatta düzenlenen yükümlülüklerini yerine getirmiş olması hukuka uygun davrandığını kabul etmek bakımından yeterli midir?

Elektronik imza araçlarının prensip olarak teknolojinin ulaştığı en ileri güvenlik kriterleri esas alınarak üretilmesi beklenir. Ancak bu standardın her zaman objektif olarak en üst seviyede tutulması, teknolojinin devamlı olarak gelişen tabiatı dolayısıyla mümkün değildir. Gelişen teknolojinin yarattığı imkanlar yürürlükteki teknolojiye dayalı olarak üretilen araçların manipülasyonuna yol açabilecek riskleri beraberinde getirmektedir[641]. Örneğin, daha ileri bir teknolojiye erişme imkanına sahip bir *hacker* (şifre kırıcı) tarafından güvenli elektronik imza aracında kayıtlı veriye ulaşılarak elektronik imzalı belgenin içeriğine müdahale edilmesi veya yine elektronik imzalı bir belge niteliği taşıyan nitelikli sertifkada yer alan bilgilerin değiştirilmesi tehlikesi her zaman mevcuttur.

Bir sertifika sağlayıcının mevzuatta belirlenen asgari kriterlerin tamamını yerine getirmesine rağmen, bu kriterlerin teminat altına alamadığı bir güvenlik açığının ortaya çıkması halinde, sertifika sağlayıcının Kanun'da ve Yönetmelik'teki yükümlülüklerine aykırı davrandığını kabul etmek ve buna göre bir üçüncü kişinin uğradığı zarardan ötürü sertifika sağlayıcıyı sorumlu tutmak yürürlükteki EİK. 13 II düzenlemesi çerçevesinde uygun gözükmemektedir. Elbette ki, varılan bu sonuç, güvenlik riskleri dolayısıyla oluşabilecek zarara üçüncü kişinin katlanacağı anlamına gelir, bunun adalet hisleri bakımından tatmin edici bir sonuç olmadığı şüphesizdir.

[641] Örneğin 10 yıl sonra üretilmesi beklenen kuantum bilgisayarların dijital imza şifrelerini kolaylıkla kırabildiği daha şimdiden ifade edilmekte ve kuantum tekniğine dayalı olarak yapılan bu tür saldırılara dayanıklı dijital imzalar üzerinde çalışılmaktadır. Monica Heger, **Cryptographers Take On Quantum Computers,** (Çevrimiçi) http://spectrum.ieee.org/computing/software/cryptographers-take-on-quantum-computers, 14.06.2011.

Sertifika faaliyetinin verilmesine ilişkin olarak burada bir riskin üstlenilmesi meselesi ortaya çıkmaktadır ve böyle bir riskin varlığı aslında *de lege feranda* bir tehlike sorumluluğu düzenlemesi gerekli kılmaktadır. Ancak, Kanun'un kusur sorumluluğu şeklinde yapmış olduğu açık tercihe rağmen burada tehlike sorumluluğunun esaslarını işleterek sertifika sağlayıcıyı sorumlu tutmak amaca uygun yorumun sınırlarını zorlayan bir yöntem olarak gözükmektedir. Kanaatimizce, sertifika sağlayıcıların üçüncü kişilere karşı sorumluluğunun, yukarıda da belirtilen kaygılar dikkate alınarak bir tehlike sorumluluğu olarak düzenlenmesi isabetli olacaktır.

2. Zarar

Sertifika sağlayıcının Kanun ve Yönetmelik hükümlerine aykırılık oluşturan davranışı, ancak nitelikli sertifikaya güvenen bir üçüncü kişinin zarara uğramasına sebep olursa tazminat yükümlülüğü doğar. Sertifika sağlayıcının hukuka aykırı bir davranışı olmasına rağmen bu yüzden bir zarar meydana gelmediği takdirde, haksız fiil sorumluluğu yoktur. Örneğin, imza sahibine teslim ettiği imza oluşturma verisinin bir kopyasını daha üretmiş ve saklamış olabilir. Sertifika sağlayıcının böyle bir davranışı EİK. 10 II hükmüne aykırılık teşkil eder. Ancak, kopyalanan imza oluşturma verisi hiç kullanılmamışsa veya kullanıldığı halde bir üçüncü kişi zarara uğramamışsa, bu durumda sertifika sağlayıcının tazminat ödeme yükümlülüğü doğmamaktadır. Diğer taraftan, sertifika sağlayıcının haksız fiil sorumluluğu bulunmasa bile, sertifika sağlayıcının bu davranışı EİK. 16 hükmü uyarınca cezai sorumluluğunu ve EİK. 18 hükmü uyarınca da idari sorumluluğunu ortaya çıkaracaktır.

Sertifika sağlayıcının üçüncü kişilere karşı sorumluluğu kapsamında tazmini talep edilecek olan zararlar arasında, ilk sırada bir üçüncü kişinin nitelikli sertifika güveni dolayısıyla uğradığı maddi zararlar yer almaktadır. Maddi zarar, bir kimsenin

malvarlığında rızası dışında meydana gelen azalmadır[642]. Bunun dışında, nitelikli sertifikaya güven dolayısıyla üçüncü kişinin manevi zarara uğradığı bir örnek bulmak güç olmakla birlikte, manevi zararların da EİK. 13 II'ye göre tazmininin talep edilebilmesine teorik olarak bir engel bulunmamaktadır[643].

Üçüncü kişinin nitelikli sertifikayı veya iptal listesini bilgisayarına yüklemesi sırasında, bu elektronik belgelerin bilgisayarının işletim sistemde yol açtığı ve birer mutlak hak ihlali niteliği taşıyan zararların, amaca uygun sınırlama yoluyla, EİK. 13 II hükmünün dışında kalan ayrı bir tazminat talebine konu olması gerektiği savunulabilir. EİK. 13 II hükmündeki sorumluluk düzenlemesinin amacı nitelikli sertifikaya güvenen üçüncü kişileri bu yüzden uğradıkları zararlara karşı korumaktadır. Nitelikli sertifikaya güven dolayısıyla uğranan zararlar dışında meydana gelen zararlar hükmün koruma amacının dışında kalmaktadır.

2. Uygun İlliyet Bağı

Hayat tecrübelerine göre, bir fiilin, olayların normal akışında meydana getireceği zararlarla olan mantıksal illiyet bağına uygun illiyet bağı denilmektedir. Haksız fiil sorumluluğunun gündeme gelebilmesi için, mantıki illiyet zinciri içinde bir sebebin zararı meydana getirmeye uygun bir sebep olup olmadığı araştırılmalıdır[644].

Nitelikli sertifikaya güveni dolayısıyla zarara uğrayan üçüncü kişinin, uğramış olduğu zararın sertifika sağlayıcının Kanun'dan ve Yönetmelik'ten doğan yükümlülüklerine aykırı davranması sonucu meydana geldiğini, yani zarar ile hukuka aykırı fiil arasındaki uygun illiyet bağını ispat etmesi gerekmektedir.

---

642 Oğuzman / Öz, **a.g.e**., s.338; Tunçomağ, **a.g.e**., s.806; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.855.

643 Orer, **a.g.e**.,s .143.

644 Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.573 vd.; Oğuzman / Öz, **a.g.e**., s.519 vd.; Eren, **a.g.e**., s.492 vd.; Tunçomağ, **a.g.e**., s.450.

Üçüncü kişi, sertifika sağlayıcının hukuka aykırı fiili yüzünden zarara uğramış olabileceği gibi, bunun yanı sıra imza sahibinden kaynaklanan başka bir sebeple de zarara uğrayabilir. Örneğin, sertifika sağlayıcının imza sahibine teslim ettiği akıllı kart mevzuatta öngörülen asgari nitelikleri taşıyan bir güvenli elektronik imza aracı niteliğinde olmayabilir. Böyle bir araç kullanılarak üretilen elektronik imza EİK. 4 hükmünde aranan şartları yerine getirmeyeceğinden güvenli elektronik imzanın hukuki sonuçlarını doğurmayacaktır. Bu yüzden uğranılan zararlar bakımından sertifika sağlayıcının sorumluluğuna başvurulabileceği konusunda tereddüt bulunmamaktadır. Ancak, başka bir kimse bu aracı imza sahibinin iradesi dışında ele geçirerek ve imza sahibinin ortada bıraktığı PIN kodunu kullanarak bir elektronik imza meydana getirmiş, bu yüzden de üçüncü kişi zarara uğramış olabilir. Böyle bir durumda üçüncü kişinin uğramış olduğu zarar ile sertifika sağlayıcının hukuka aykırı fiili arasında illiyet bağı bulunmamaktadır. Verilen bu örnekte, üçüncü kişinin uğradığı zarar imza sahibinin imza aracını saklamakta gereken özeni göstermemiş olmasından kaynaklanmaktadır. İmza sahibi bu hususta kendisinden beklenen özeni göstermiş olmasına rağmen, imza aracının asgari güvenlik kriterlerini taşımaması nedeniyle şifre kırılmış ve bu şekilde elektronik imza üretilmiş olsaydı, bu durumda üçüncü kişinin uğradığı zararın sertifika sağlayıcının hukuka aykırı fiili dolayısıyla meydana geldiğini kabul etmek gerekecekti.

Yukarıda verdiğimiz örnekle de ilişkili olarak, sertifika sağlayıcının sorumluluğu belirlenirken hukuka aykırılık şartı ile illiyet bağı kavramlarının birbirine karıştırılmaması gerekir. Örneğin, sertifika sağlayıcının nitelikli sertifikayı derhal iptal etmemesi yüzünden bir üçüncü kişinin zarara uğraması mümkündür. Ancak bu durum sertifika sağlayıcıdan kaynaklanabileceği gibi, imza sahibinin iptali gerektiren sebepler ortaya çıkmış olmasına rağmen iptal talebinde bulunmamış olmasından da kaynaklanabilir. Birinci ihtimalde, sertifika sağlayıcının sorumluluğu bakımından aranan hukuka aykırılık unsuru gerçekleşmektedir. İkinci örnekte ise

sertifika sağlayıcının sorumluluğuna gidilmesine engel olan illiyet bağının kesilmesi değil, hukuka aykırılık unsurunun bulunmamasıdır[645].

4. Kusur

Öğretide haksız fiilin kusur unsuru, bir kimsenin hukuka aykırı sonucu istemesi (kast) veya bu sonucu istemiş olmamakla beraber hukuka aykırı davranıştan kaçınmak için iradesini yeterli ölçüde kullanmaması (ihmal) olarak tarif edilmektedir[646].

EİK. 13 II hükmüne göre "*elektronik sertifika hizmet sağlayıcısı kusursuzluğunu ispat ettiği takdirde tazminat ödeme yükümlülüğü doğmaz"*. Bu hükümde sertifika sağlayıcı bakımından bir kusur karinesine yer verilmektedir. Buna göre, hukuka aykırı bir fiili ile nitelikli sertifikaya güvenen bir üçüncü kişiye zarar veren sertifika sağlayıcının kendisine yükletilen sorumluluktan kurtulması için kusurunun bulunmadığını ispat etmesi gerekir[647]. Böyle bir düzenlemeye başvurulmasının sebebi, zarara uğrayan üçüncü kişinin sertifika sağlayıcının kusurlu davrandığını ispat edebilme imkanının çoğu zaman olmayışıdır[648].

Kanun'da ve Yönetmelik'te öngörülen yükümlülüklere aykırı davranarak bir üçüncü kişinin zarara uğramasına sebep olan sertifika sağlayıcının söz konusu yükümlülükleri yerine getirmemekte kusuru bulunmadığını ispat etmesi gerekmektedir. Aksi takdirde üçüncü kişinin zararının tazminle yükümlüdür (EİK. 13 II). Sertifika sağlayıcının kusurunun tespitinde, sertifika sağlayıcının davranışı bakımından objektif bir ölçütün kullanılması gerekir. Kusurun objektifleştirilmesi,

---

645 Zararın ihlal edilen normun koruma alanı dışına çıkması, bir illiyet bağı meselesi değil bir hukuka aykırılık meselesidir: Kaneti, **a.g.e**., s.228. Bu konuda bkz. Thomale, **a.g.e**., s.191-192. Oysa, yazar bu örneği illiyet bağı unsurunu incelerken esas almaktadır.

646 Oğuzman / Öz, **a.g.e**., s.526; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., 492 vd.; Tunçomağ, **a.g.e**., s.439; Eren, **a.g.e**., s.529 vd.

647 Bu konuda belgelendirme yükümlülüğünü eksiksiz yerine getirmiş olması sertifika sağlayıcının menfaatine olacaktır: Hans-Christoph Thomale, "Die Haftungsregelung nach §11 SigG", **MMR**, Heft 2, 2004, s.80-86, s. 82; Hansen, **a.g.e**., s.134.

648 Thomale, **§11 SigG**, s.80-86, s. 82.

haksız fiilin kusur unsuru ile hukuka aykırılık unsuru arasındaki farkın tespit edilmesini zorlaştırmaktadır[649]. Bununla birlikte hukuka aykırlık kusura oranla tamamen objektif bir niteliği haizdir. Bu iki unsuru birbirinden ayırt ederken, sertifika sağlayıcının ürettiği imza oluşturma verilerinin, araçlarının, nitelikli sertifikaların mevzuatta aranan kriterleri taşıyıp taşımadığı konusunun hukuka aykırılık unsuruyla ilgili olduğunu gözden kaçırmamak gerekir.

EİK. 13 II hükmü hazırlanırken AB Elektronik İmza Yönergesi'nin 6. maddesinde yer alan ispat yükü tersine çevrilmiş kusur sorumluluğu düzenlemesinin esas alındığı anlaşılmaktadır. Aslında, Yönerge'nin ilk taslağında sertifika sağlayıcıların sorumluluğu tehlike sorumluluğu olarak düzenlenmiştir. Böyle bir düzenleme iki açıdan eleştirilere konu olmuştur. Bu konudaki eleştirilerden biri, tehlike sorumluluğu düzenlemesiyle Yönerge'nin amacını aşmış olacağı, çünkü bunun (asgari uyumlaştırma amacını aşarak) genel olarak üye devletlerin sorumluluk kurallarının uyumlaştırması sonucunu doğuracağıdır. İkinci olarak, böyle bir düzenlemenin Avrupa Birliği üyesi devletlerde yerleşik sertifika sağlayıcılarının Asya ülkelerinde ve ABD'de yerleşik sertifika sağlayıcılarına kıyasla aleyhine bir durum yaratacağı, rekabet edebilirliklerini azaltacağı ifade edilmiştir[650]. Türk hukuku bakımından, tehlike sorumluluğunun gerekli olduğu üçüncü kişinin menfaatleri dikkate alındığında açıkça görülebilir olduğu halde, hangi gerekçeyle kusur sorumluluğuna başvurulduğu EİK. 13 hükmüne ilişkin gerekçe metninden anlaşılmamaktadır.

Üçüncü kişi, nitelikli bir sertifikayı EİY. 16 hükmünde kapsamı gösterilen şekilde kontrol etmeyerek, bu sertifikaya dayalı bir hukuki işlemde bulunması ve zarara uğraması halinde, özen külfetini yerine getirmediğinden sertifika sağlayıcının sorumluluğuna başvuramayacaktır. Böyle bir ihtimalde, zarar gören üçüncü kişinin

---

[649] Eren, **a.g.e**., s.572. Kusurun objektifleştirilmesinde esas alınan "*örnek (model) davranış teorisi*" hakkında bkz. Eren, a.g.e., s.530-531. Ayrıca bkz. Oğuzman / Öz, **a.g.e**., s.531. Yazarlar, kusurun objektifleştirilmesinin kusur kavramı ile bağdaşmayacağını prensip olarak ifade etmekte, ancak bir mesleği icra eden kişinin bu mesleği icra ederken göstermesi gereken özenin belirlenmesinde örnek davranış teorisine yakın bir ölçüt kullanılabileceğini belirtmektedir.

[650] Christopher Kuner, **Remarks of the German Government on the EU Draft Directive concerning Electronic and Digital Signatures**, 1998, (Çevrimiçi) http://www.kuner.com/data/sig/gov_ger_eu-draft.htm, 1 Şubat 2011. Aynı yönde yukarıda bkz. s.46, dn.197.

kusuru zararın meydana gelmesinde başlıca etkendir. Bu durumda, sertifika sağlayıcının hukuka aykırı fiili ile zarar arasında illiyet bağının bulunmadığı veya kesildiği kabul edilebilir[651].

Örneğin, imza oluşturma aracı çalınan imza sahibi sertifika sağlayıcıya nitelikli sertifikayı iptal talebinde bulunmuş, ancak sertifika sağlayıcı nitelikli sertifikayı derhal iptal etmekte geç kalmıştır. İptal kaydının ilan olunmadığı bu süre zarfında, imza aracı yetkisiz bir kişi tarafından ele geçirilerek, bir üçüncü kişiye nitelikli sertifikada yer alan bilgilere aykırı içerikte (nitelikli sertifikadaki sınırlamaları aşan, sertifikadaki kimlik bilgileriyle örtüşmeyen vb.) bir teklif gönderilmiş ve bu teklif bir üçüncü kişi tarafından nitelikli sertifika kontrol edilmeksizin kabul edilmiş olabilir. Bu olayda, sertifika sağlayıcının iptal yükümlülüğünü gereken şekilde yerine getirmemiş olması (bunun yanı sıra, belki de verdiği imza aracının gereken güvenlik tedbirlerine sahip olmayışı) dolayısıyla hukuka aykırı bir eylemi bulunmaktadır. Ancak, meydana gelen zarar sertifika sağlayıcının nitelikli sertifikayı derhal iptal etmemiş olmasından değil, üçüncü kişinin nitelikli sertifikada yer alan bilgileri kontrol etmek hususunda gereken özeni göstermemiş olmasından kaynaklanmaktadır. Üçüncü kişi nitelikli sertifikayı kontrol etseydi, irade beyanı ile nitelikli sertifika arasındaki uyumsuzluğu kendi başına tespit edecek ve kendisine gönderilen elektronik imzalı belgeye güvenerek bir işlemde bulunmayacaktı. Diğer bir ifadeyle, böyle bir olayda, sertifika sağlayıcının hukuka aykırı fiili ile üçüncü kişinin uğradığı zarar arasında illiyet bağı bulunmamaktadır.

Üçüncü kişinin sertifikanın kontrolü dışında kalan, daha hafif kusurlu bir fiille başka bir zararın meydana gelmesine veya zararın artmasına sebep olması halinde, bu husus sertifika sağlayıcının sorumlu olduğu tazminat miktarının indirilmesinde etki doğuracaktır[652].

---

[651] Eren, **a.g.e**., s.732.

[652] Thomale, **§11 SigG**, s.82.

B. SERTİFİKA SAĞLAYICININ ÇALIŞTIRDIĞI KİŞİLERİN DAVRANIŞLARINDAN SORUMLULUĞU

a. Sorumluluğun Anlamı

EİK. 13 III hükmüne göre "*elektronik sertifika hizmet sağlayıcısı, söz konusu yükümlülük ihlâlinin istihdam ettiği kişilerin davranışına dayanması hâlinde de zarardan sorumlu olup, elektronik sertifika hizmet sağlayıcısı, bu sorumluluğundan, Borçlar Kanununun 55 inci maddesinde öngörülen türden bir kurtuluş kanıtı getirerek kurtulamaz".*

EİK. 13 III sertifika sağlayıcının söz konusu yükümlülüklerinin ihlalinin çalıştırdığı personelin davranışından kaynaklanması halinde, haksız fiile dayalı bir kusursuz sorumluluk türü olan adam çalıştıranın sorumluluğu konusunda BK. 55 hükmünden farklı bir düzenleme öngörmektedir. EİK. 13 III hükmüne göre, sertifika sağlayıcı adam çalıştıran sıfatına dayanılarak kendisine yükletilen sorumluluktan BK. 55 hükmünde gösterilen kurtuluş kanıtlarını ileri sürmek suretiyle kurtulamayacaktır. Kanun'un ilgili maddesine ilişkin gerekçe metninde, böyle bir düzenleme yoluyla sertifika sağlayıcıların personel seçiminde daha dikkatli davranmalarının amaçlandığı belirtilmektedir[653].

---

[653] EİK. 13 III hükmüne paralel bir hüküm İsviçre Elektronik İmza Kanunu'nda yer almaktadır (ZerES Art. 16 III). Alman hukukunda da sertifika sağlayıcıların sorumluluğu konusunda SigG §11 IV hükmünde benzer bir düzenleme yer almaktadır. Bu hükümde sertifika sağlayıcının bir sözleşmeye dayalı olarak yükümlülüklerini devrettiği üçüncü kişilerin fiillerinden ötürü veya garanti ettiği yabancı sertifikalar sebebiyle üçüncü kişilerin uğradığı zararlardan kendi fiilerinde olduğu gibi sorumlu olacağı ve BGB §831 1/II'de öngörülen kurtuluş kanıtlarını ileri sürerek bu sorumluluktan kurtulamayacağı düzenlenmektedir (Hansen, **a.g.e**., s.135 **;** Thomale, **§11 SigG,** s.84**)**. Sertifika sağlayıcının bir sözleşmeye dayalı olarak yükümlülüklerini devrettiği üçüncü kişilerin kapsamına sertifika sağlayıcının çalıştırdığı personelin de dahil olup olmadığı tartışma konusu olmuştur. Kanun'un gerekçesi de dikkate alınarak bu hükümde belirtilen kişilerin sosyal ve ekonomik bakımdan, ticari işletmesi, yönetimi itibariyle sertifika sağlayıcıdan ayrı bir varlık oluşturması gerektiği, bu nedenle sertifika sağlayıcının çalıştırdığı personelin bu hükmün kapsamına girmeyeceği ifade edilmektedir. Dolayısıyla sertifika sağlayıcının çalıştırdığı

b. Sorumluluğunun Şartları

BK. 55 hükmüne göre adam çalıştıranın sorumluluğunun olumlu şartları hukuka aykırı bir fiil bulunması ve hukuka aykırı bu fiil dolayısıyla bir kişinin zarara uğramış olmasıdır. Bu bir tür kusura dayanmayan haksız fiil sorumluluğu olup, adam çalıştıranın kendisine yükletilmiş özen yükümlülüğünü yerine getirmemiş olduğu esasına dayanmaktadır[654]. Sertifka sağlayıcının sorumluluğunu için kendisinin kusuru aranmadığı gibi, çalıştırdığı kişilerin de kusurunun bulunması şart değildir[655].

BK. 55 hükmü çerçevesinde sertifika sağlayıcının adam çalıştıran sıfatıyla sorumluluğunun doğabilmesi için Kanun'da ve Yönetmelik hükümlerinde öngörülen yükümlülüklerine aykırılığı dolayısıyla ortaya çıkan hukuka aykırı bir fiilinin bulunması gerekmektedir. Hemen belirtelim ki, EİK. 13 III hükmünün varlığı hukuka aykırılık şartının tespitine ilişkin olarak yukarıda belirtmiş olduğumuz sakıncayı ortadan kaldıran bir değişiklik yaratmamaktadır[656]. Sertifika sağlayıcının mevzuatta öngörülen teknik kriterleri yerine getirdiği ispat ederek sorumluluktan kurtulması halen daha mümkündür.

Sertifika sağlayıcının adam çalıştıranın sorumluluğu esasına dayalı olarak sorumlu tutulmasında önem taşıyan husus zarar verici fiil ile adam çalıştıranın görülen işi arasında aranan fonksiyonel bağlılıktır. Diğer bir ifadeyle, haksız fiil çalışan tarafından işin görülmesi sırasında ve hizmet dolayısıyla işlenmiş olmalıdır[657]. Sertifika sağlayıcının çalıştırdığı personelin işin görülmesi amacının

---

personelin vermiş olduğu zararlardan ötürü SigG §11 1 hükmünde düzenlenen kusur sorumluluğu uygulama bulacaktır (Hansen, **a.g.e.,** s.135).

654 Oğuzman / Öz, **a.g.e**., s.590; Tandoğan, **a.g.e**., s.54; Eren, **a.g.e**., s.575; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.503.

655 Yarg. İBK. 27.03.1957, 1/3 (YKD., S.3, 1975, s.42-43); ayrıca bkz. Tandoğan, **a.g.e**., s.55.

656 Bkz. s.192 vd.

657 Tandoğan, **a.g.e**., s.62; Eren, **a.g.e**., s. 582; Oğuzman / Öz, **a.g.e**., s.596; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.506-507.

dışında kalan bir saikle, örneğin sertifika başvurusunda bulunan kişiyle arasındaki hususi bir sebebe dayalı olarak, onun adına oluşturulan imza oluşturma verisini, nitelikli sertifikasını ve diğer kişisel verilerini ele geçirmesi ve bunları kullanarak bir üçüncü kişiye kasten zarar vermesi halinde sertifika sağlayıcının sorumluluğu gündeme gelecek midir? Bu konuda fonksiyonel bağlılık kavramının geniş yorumlanması sertifika hizmetinin niteliği gereğidir[658]. Sertifika hizmetine ilişkin en büyük risklerden biri çalışan personelin bu tür konulardaki dürüstlüğü konusunda ortaya çıkmaktadır.

Adam çalıştıranın sorumluluğunun olumsuz şartları BK. 55'teki kurtuluş kanıtlarını getirerek sorumluluk karinesini çürütmemiş olmasıdır. Buna göre, adam çalıştıranın ileri sürebileceği kurtuluş kanıtları kendisinin sorumluluğuna yol açan fiil karinesinin veya illiyet karinesinin çürütülmesi şeklinde iki türlüdür. Fiil karinesinin çürütülmesi çalışanın seçiminde, çalışana talimat vermede ve nezaret etmede özen gösterildiğini ispat etmek suretiyle mümkündür[659]. Adam çalıştıranın sorumluluktan kurtulması için başvurabileceği ikinci imkan ise Kanun'un ifadesiyle çalışanın "*dikkat ve itinada bulunmuş olsa bile zararın vukuuna mâni olamayacağını*" ispat etmek suretiyle illiyet karinesini çürütmesidir. Burada bulunmadığı ispat edilecek illiyetin, çalışanın fiiliyle zarar arasındaki illiyet değil, adam çalıştıranın özen göstermemesi şeklinde ortaya çıkan fiili ile zarar arasındaki illiyet olduğu belirtilmektedir[660].

---

658 "…sorumluluğun önemli koşullarından birisi de çalıştırılan kişinin zararlı eylemi ile hizmetin yürütülmesi arasında sıkı bir ilginin varlığıdır. Şayet, çalıştırılanın zarar verici eylemi ile hizmeti arasında gaye ve görev bakımından sıkı bir ilgi yoksa adam çalıştıran tazminatla sorumlu tutulamayacaktır. Ancak bu ilke uygulanırken madde hükmünün gayesinin, çalıştırılan kişinin, yerinde olmayan, zarar verici eylemleri dolayısıyla adam çalıştıranı sorumlu kılmak olduğu da gözden uzak tutulmamalıdır. Zira, 55. madde hükmünün uygulama alanını yalnızca çalıştırılan kişinin görevi uyarınca isabetli olarak yapması gereken ve kendisine verilen talimata uygun eylemlerinden doğan zararların tazminiyle sınırlamak, adam çalıştıranın sorumluluğunu lüzumundan fazla daraltıcı sonuca götürür". Yarg. 4.HD. 20.11.1984 E. 1984/7770 K. 1984/8597, Hukuktürk Mevzuat ve İçtihat Bankası.

659 Oğuzman / Öz, **a.g.e**., s.598; Eren, **a.g.e**., s.585 vd.; Tandoğan, **a.g.e**., s.66 vd.; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., 508 vd.

660 Oğuzman / Öz, **a.g.e**., s.599; Eren, **a.g.e**., s.586. Öğretide, kanun koyucunun BK. 55 I'in ikinci fıkrasındaki kurtuluş kanıtına ayrıca yer verilmesine gerek olmadığı, bu hallerde zaten adam çalıştıranın illiyet bağı hakkındaki genel ilkelere göre sorumlu tutulamayacağı belirtilmektedir. Bkz. Tandoğan, **a.g.e**., s.70-71; Tekinay / Akman / Burcuoğlu / Altop, **a.g.e**., s.510.

Yeni Borçlar Kanunu'nun adam çalıştıranın sorumluluğu hükmüne karşılık gelen "*Adam Çalıştıranın Sorumluluğu*" başlıklı 66. maddesinde[661] fiil karinesinin çürütülmesi konusunda, adam çalıştıranın yukarıda belirtilen özen yükümlülüğünün kapsamına ek olarak, "*işletmenin çalışma düzeninin zararın doğmasını önlemeye elverişli olduğunu ispat etmedikçe, o işletmenin faaliyetleri dolayısıyla sebep olunan zararı gidermekle yükümlü*" olduğu hükmü eklenmiştir[662]. Bu değişikliğin yanı sıra 66. maddede getirilen başka bir değişiklik illiyet bağının çürütülmesi konusundadır. BK 55'te öngörülen illiyet bağının kesildiğine ilişkin olarak istihdam edenin kurtuluş kanıtı getirebileceği yönündeki düzenlemeye Yeni Borçlar Kanunu'un 66. maddesinde yer verilmemektedir.

EİK. 13 III hükmünde sertifika sağlayıcının BK. 55'teki kurtuluş kanıtlarını ileri süremeyeceği düzenlenerek, ağırlaştırılmış bir kusursuz sorumluluk esası benimsenmiş olmaktadır. Bu düzenlemeyle sertifika sağlayıcının istihdam ettiği kişilerin verdiği zararlardan ötürü sorumluluğu konusuna özel bir önem atfedildiği ve Türk hukukunda noterlerin hukuki sorumluluğu bakımından öngörülen kusursuz sorumluluk sistemine benzetildiği sonucuna varılmaktadır[663].

Nitelikli sertifikaya güvenen üçüncü kişinin EİK. 13 II'ye göre sertifika sağlayıcının kusura dayalı haksız fiil sorumluluğuna başvurabilmesi için uğradığı

---

[661] Yeni Borçlar Kanunu'nun yürürlüğe girmesiyle birlikte EİK. 13 III hükmünde yer alan BK. 55 şeklindeki madde atfının BK. 66 olarak değişitirilmesi gerekecektir. Böyle bir değişikliğin olması ihtimali göz önünde bulundurularak, doğrudan madde numarasını belirtmek yerine adam çalıştıranın sorumluluğu şeklinde hukuki müessesenin adı belitilerek yapılacak daha isabetli olurdu.

[662] İsviçre Federal Mahkemesi bazı kararlarında istihdam edenin ayrıca iyi bir organizasyonu gerçekleştirdiğini ispat etmesi gerektiğinden söz edilmektedir. Ancak belirtilen üç aşamada istihdam eden gereken özeni gösterdiyse, zaten iyi bir organizasyon var demektir. Bu nedenle iyi bir organizasyonun ispatı ayrıca söz konusu olamaz: Oğuzman / Öz, **a.g.e**., s.599.

[663] 1512 sayılı Noterlik K. 162 I hükmüne göre *"Stajyer, katip ve katip adayları tarafından yapılmış olsa bile noterler, bir işin yapılmamasından veya hatalı yahut eksik yapılmasından dolayı zarar görmüş olanlara karşı sorumludurlar"*. Bu hüküm ile noterlere çalıştırdıkları kişilerin sebep olduğu zararlar dolayısıyla kurtuluş kanıtı getirme olanağı tanınmamaktadır: Tandoğan, **a.g.e.**, s.84; Hasan Pulaşlı, "Türk ve Alman Hukuklarında Noterlerin Hukuki Sorumluluğu", **Türkiye Noterler Birliği Hukuk Dergisi**, S.39, 1983, s.10-16, s.11. Noterlerin böyle ağır bir sorumluluğa tabi tutulması, noterlerin yaptıkları işlemlerdeki yanlışlık sebebiyle büyük zararların doğması tehlikesi bulunduğu dikkate alındığında, iş sahiplerine bir teminat sunmaları gerektiği düşünülerek haklı sayılabilir (Tandoğan, **a.g.e.**, s.84). Aksi yöndeki bir düzenlemeyle, adalet hizmeti ifa eden bir notere istihdam ettiği kişilerin verdiği zarardan ötürü sorumluluktan kurtuluş kanıtı ileri sürülerek kurtulma imkanının tanınması hukuki güvenliği zedeleyecektir (Pulaşlı, **a.g.e.**, s.12).

zararı ve bu zararın sertifika sağlayıcının Kanun'da ve Yönetmelik'te belirlenen yükümlülüklerine aykırı davranması nedeniyle meydana geldiğini ispat etmesi gerekir. Bunun dışında sertifika sağlayıcının kusurunu ispat etmesine ihtiyaç bulunmamaktadır. Kusursuzluğunu ispat yükü EİK. 13 II uyarınca sertifika sağlayıcı üzerindedir. BK. 55'ye dayalı olarak adam çalıştıranın sorumluluğuna gidilmesi halinde de, bir kusursuz sorumluluk hali söz konusu olduğundan, haksız fiilin kusur dışındaki diğer unsurlarının gerçekleştiği üçüncü kişi tarafından ispat edilmelidir.

C. NİTELİKLİ SERTİFİKANIN KULLANIM ALANI VE MADDİ KAPSAMINA İLİŞKİN SINIRLAMALARIN SERTİFİKA SAĞLAYICININ SORUMLULUĞUNA ETKİSİ

Nitelikli sertifikada öngörülebilecek sınırlamalar sertifikanın kullanım alanı ve maddi kapsamına yönelik olmak üzere iki çeşittir. Nitelikli sertifikanın kullanım alanına ilişkin olarak belirli türdeki borçlandırıcı işlemlerin veya tasarruf işlemlerinin nitelikli sertifika ile yapılamayacağı kararlaştırılabilir. Böyle bir sınırlama nitelikli sertifika kullanımının yalnızca belirli bir amaca veya belirli bir konuya özgülenmesi şeklinde ortaya çıkabilir. Örneğin, bir elektronik imzanın yalnızca UYAP üzerinden gerçekleştirilecek hukuki işlemlerde kullanılacağının nitelikli sertifikada öngörülmesi durumunda böyle bir sınırlama söz konusu olur.

Nitelikli sertifikanın kullanılacağı işlemlere ilişkin olarak maddi bir sınırın kararlaştırılması da mümkündür. Nitelikli sertifikanın kullanılacağı hukuki işlemin değerinin 1000 lirayı geçmeyeceğinin kararlaştırılması buna örnektir. EİK. 9 (ı) hükmünün ifadesinden sertifikadaki maddi sınırlamaların yalnızca her hukuki işlem bakımından mı belirleneceği, yoksa nitelikli sertifikanın kullanılacağı hukuki işlemlerin tamamını kapsayacak şekilde (kredi kartlarına benzer olarak) genel bir sınırlamaya gidilmesinin mümkün olup olmadığı anlaşılamamaktadır. Her hukuki işlemin değeri bakımından münferit bir sınırın kararlaştırılmasının daha uygun gözüktüğü, çünkü nitelikli sertifikaya ilişkin genel bir sınırlamaya gidilmesi halinde

bunun nitelikli sertifikaya güvenerek hukuki işlemde bulunan üçüncü kişi tarafından tespit edilebilmesinin mümkün olmayacağı ifade edilmektedir[664].

EİK. 13 IV hükmüne göre; "*nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere, elektronik sertifika hizmet sağlayıcısının üçüncü kişilere ve nitelikli elektronik imza sahibine karşı sorumluluğunu ortadan kaldıran veya sınırlandıran her türlü şart geçersizdir*".

Bu hükümde kural olarak sertifika sağlayıcının hafif kusurları bakımından dahi sorumsuzluk kaydı öngöremeyeceği düzenlenmektedir[665]. Bununla birlikte, hükmün "*nitelikli elektronik sertifikanın içerdiği kullanım ve maddî kapsamına ilişkin sınırlamalar hariç olmak üzere"* şeklindeki ifadesi[666], imza sahibinin iradesine uygun olarak sertifika sağlayıcı tarafından öngörülen nitelikli sertifikanın kullanım alanı ve maddi kapsamına ilişkin sınırlamaların, sertifika sağlayıcının sorumluluğunun sınırlandırılması şeklinde bir etki doğurup doğurmayacağı konusunda tereddüt oluşturmaktadır.

Nitelikli sertifikadaki bilgileri görüntüleyen üçüncü kişi, bu tür sınırlamaların mevcut olduğunu sertifikadan tespit edebilmesi rağmen, buna uygun davranmadığı takdirde uğradığı zarardan ötürü sertifika sağlayıcının sorumluluğuna başvuramaz[667]. Örneğin, 1.000 lirayla sınırlandırılmış bir nitelikli sertifikanın iptali için imza sahibi tarafından talepte bulunulmasına rağmen, sertifika sağlayıcı iptali derhal

---

[664] Thomale, **§11 SigG**, s.85. Teknolojideki gelişmelerin, kredi kartlarında olduğu gibi, toplam limitin gerçekleştirilen her hukuki işlemde üçüncü kişi tarafından belirlenebilmesini mümkün kılması halinde böyle bir sakınca ortadan kalkacaktır.

[665] Öğretide, sorumluluğun dayanağının sözleşme olmadığı, sorumluluğun doğrudan doğruya kanundan doğduğu hallerde sorumsuzluk anlaşması yapmadan, sertifika sağlayıcının imza sahibi ile arasındaki sözleşmede üçüncü kişilere karşı sorumlu olmayacağının düzenlenmesinin zaten mümkün olmadığı ifade edilmiştir. Bu çerçevede, hükmün üçüncü kişiyi koruyucu sözleşme kuramı çerçevesinde sertifika sağlayıcı ile imza sahibi arasındaki sözleşme ilişkisine göre zararlarını tazmini talep eden kişilere karşı sorumsuzluk kayıtlarının ileri sürülmesi mümkün olmadığı şeklinde okunması gerektiği belirtilmektedir (Orer, **a.g.e**., s.151).

[666] EİK. 9 (ı) hükmünde "sertifikanın kullanım şartları" ve "sertifikanın kullanılacağı işlemlerdeki maddi sınırlamalar" şeklinde iki tür ifade olunmasına rağmen, EİK. 13 IV hükmünde "nitelikli sertifikanın kullanımına ilişkin sınırlamalar" ve "nitelikli sertifikanın maddi kapsamına ilişkin sınırlamalar" şeklinde daha farklı bir ifade kullanılmaktadır. Bu farklı ifade ediliş şekline rağmen, iki hükmün birbirine paralel şekilde anlaşılması gerekmektedir.

[667] Thomale, **§11 SigG**, s.85.

gerçekleştirmekte ihmal göstermiş olabilir. Üçüncü kişi bu süre zarfında yetkisiz bir kullanıcı tarafından kendisine gönderilen sertifikayı aşan 2.000 lira değerindeki bir sözleşme teklifini kabul ettiyse ve bu yüzden zarara uğradıysa, uğramış olduğu zararlardan ötürü EİK. 13 II dayanan bir korumadan yararlanamaz. Çünkü, böyle bir olayda imza sahibinin iradesiyle nitelikli sertifikada yer alan sınırlama kaydı arasındaki uyumsuzluk üçüncü kişi tarafından açıkça tespit edilebilir niteliktedir[668]. Bu uyumsuzluğun varlığı üçüncü kişinin nitelikli sertifikaya güveni şartını ortadan kaldırır ve sertifika sağlayıcının sorumluluğunun doğmasına engel olur. Sertifika sağlayıcının sorumluluğu hiç doğmayacağından, 1.000 liralık sınır esas alınarak tazminat ödemesi gerektiği de burada savunulamayacaktır.

Elbette ki, bu sınırlamalar nitelikli sertifikada görüntülenebilir olmadığı takdirde sorumluluk yine sertifika sağlayıcıya ait olacaktır[669]. Çünkü nitelikli sertifikada gösterilmiş olmaları şartıyla üçüncü kişi tarafından tespit edilmeleri mümkündür. Aksi takdirde imza sahibinin söz konusu sınırlamaları aşan bir hukuki işlemde bulunup bulunmadığı bir üçüncü kişi tarafından görülemez. Nitekim, nitelikli sertifikanın şartlarını belirleyen EİK. 9 (ı) hükmünde "*sertifikanın kullanım şartları ve kullanılacağı işlemlerdeki maddî sınırlamalara ilişkin bilgilerin*" nitelikli sertifikada bulunması gerektiği belirtilmektedir.

Sonuç itibariyle, nitelikli sertifikadaki sınırlamaların aşılması esas itibariyle üçüncü kişinin nitelikli sertifikaya güveni şartını ortadan kaldıran, dolayısıyla sertifika sağlayıcının sorumluluğunun doğmasını engelleyen bir hukuki etki

---

[668] Böyle bir ihtimalde güvenli elektronik imzanın sonuçlandırma işlevini yerine getirmeyeceği yönündeki tespitimiz ve buna ilişkin gerekçe hakkında bkz. s.87 vd.

[669] Bu sınırlamaların başka bir koruyucu etkisi imza sahibi bakımındandır. İmza sahibinin bunları ihlal eden ölçüde borç altına girmesi ve tasarruflarda bulunması ihtimaline karşı korunması amaçlanmaktadır. Bu koruma söz konusu ihlallerin yetkisiz kişiler tarafından meydana getirilmesi halinde önem taşımaktadır. Böyle bir durumda nitelikli sertifikadaki sınırı gören üçüncü kişi bu sınırı aşan bir sözleşme teklifini kabul etmeyecek, bu sayede imza sahibinin iradesi dışında kullanılan güvenli elektronik imza sebebiyle üçüncü kişi zarara uğramayacaktır.

yaratmakta, bunun dışında sertifika sağlayıcının sorumluluğunun sınırlandırılması bakımından herhangi bir etkisi bulunmamaktadır[670].

Örneğin, nitelikli sertifikaya kimlik bilgilerinin yanlış işlenmesi veya güvenli elektronik imza araçlarının teknik kriterleri yerine getirmemesi nedeniyle üçüncü kişi bir zarara uğradıysa, nitelikli sertifikadaki sınırlamalar sertifika sağlayıcının tazminat borcunun bakımından bir sınır teşkil etmemelidir. Üçüncü kişi nitelikli sertifikadaki sınırlamalarla bağlı olmaksızın uğradığı zararın tazminini talep edebilmelidir. Aksi yönde bir yorum, sertifika sağlayıcı tarafından üçüncü kişiye karşı sorumluluğunu ortadan kaldıran veya sınırlandıran hiçbir sorumsuzluk kaydı öngörülemeyeceğini düzenleyen EİK. 13 IV hükmünde yer alan prensibi etkisiz hale getirir ve hatta ağırlaştırılmış sorumluluk düzenlemesinin (EİK. 13 II ve EİK. 13 III) amacına aykırılık teşkil ederek nitelikli sertifikaya güvenen üçüncü kişiyi korumasız bırakır.

D. ZORUNLU SERTİFİKA MALİ SORUMLULUK SİGORTASI

EİK. 13 V ve devamı hükümlerinde sertifika sağlayıcının mali sorumluluk sigortası yaptırma yükümlülüğü aşağıdaki şekilde düzenlenmektedir:

"Elektronik sertifika hizmet sağlayıcısı, bu Kanundan doğan yükümlülüklerini yerine getirmemesi sonucu doğan zararların karşılanması amacıyla sertifika malî sorumluluk sigortası yaptırmak zorundadır. Sigortaya ilişkin usul ve esaslar Hazine Müsteşarlığının görüşü alınarak Kurum tarafından çıkarılacak yönetmelikle belirlenir.

Bu maddede öngörülen sertifika malî sorumluluk sigortası Türkiye'de ilgili branşta çalışmaya yetkili olan sigorta şirketleri tarafından yapılır. Bu sigorta şirketleri sertifika malî sorumluluk sigortasını yapmakla yükümlüdürler. Bu yükümlülüğe uymayan sigorta şirketlerine Hazine Müsteşarlığınca sekizmilyar lira

[670] Ayni yönde: Orer, **a.g.e**., s.146; Yıldırım, **a.g.e**., s.39. Her iki yazar da, sertifikadaki sınırlamaları aşan işlemlerde güvenli elektronik imza kullanılmış ve bundan bir zarar doğmuş ise, bu zararlardan sertifika sağlayıcının ve imza sahibinin sorumlu olmayacağını belirtmektedir.

idarî para cezası verilir. Bu para cezasının tahsilinde ve cezaya itiraz usulünde 18 inci madde hükümleri uygulanır.

Elektronik sertifika hizmet sağlayıcısı, nitelikli elektronik sertifikayı elektronik imza sahibine sigorta ettirerek teslim etmekle yükümlüdür".

Bilgi ve İletişim Teknolojileri tarafından EİK 13 hükmünde yer alan düzenlemeye dayanılarak hazırlanan Sertifika Mali Sorumluluk Sigortası Yönetmeliği'nin[671] 6. maddesinde sertifika mali sorumluluk sigortasının kapsamı daha detaylı olarak şu şekilde belirtilmektedir:

"Sertifika mali sorumluluk sigortası, elektronik sertifika hizmet sağlayıcısının güvenli ürün ve sistemleri kullanma, hizmeti güvenilir bir biçimde yürütme ve sertifikaların taklit ve tahrif edilmesini önlemekle ilgili yükümlülüklerini yerine getirmemesi dolayısıyla zarar görecek olanlara karşı doğacak hukuki sorumlulukların teminat altına alınmasını kapsar".

Bir mali sorumluluk sigortası ile malvarlığının pasifinde meydana gelebilecek artış şeklinde ortaya çıkan zararlara karşı güvence verilmektedir. Malvarlığının aktifinde meydana gelebilecek azalmalar mali sorumluluk sigortası teminatının dışında kalmaktadır[672]. Mali sorumluluk sigortası sözleşmesi uyarınca menfaati güvence altına alınan ve sigortalı sıfatını taşıyan kişiler, malvarlığının pasifinde artış meydana gelmesi rizikosu bulunan kişiler[673]. EİK. 13 V hükmüne göre sertifika sağlayıcının kendi menfaatini güvence altına almak için bir mali sorumluluk sigortası sözleşmesi yapması zorunlu tutulmakta, bunun yanında EİK. 13 VII hükmünde imza sahibi lehine mali sorumluluk sigortası yapma yükümlülüğü öngörülmektedir. Bu durumda sigortalı sıfatını taşıyan kişiler sertifika sağlayıcı ve imza sahibi olarak ortaya çıkmaktadır.

---

671 RG 26.08.2004, Sayı 25565.

672 Malvarlığının aktifinde meydana gelecek azalmalar mal sigortası sözleşmeleri ile teminat altına alınmaktadır: Kerim Atamer, "Yeni Türk Ticaret Kanunu Uyarınca "Zarar Sigortaları"na Giriş", **BATİDER,** C. XXVII, S.1, 2011, (Ayrı Bası), s.48.

673 Atamer, **a.g.e**., s.53.

İmza sahibi, sertifika sağlayıcının, Kanun'dan ve Yönetmelik'ten doğan yükümlülüklerini yerine getirmemesi sonucu uğradığı zararların karşılanması amacıyla doğrudan sigortacıya başvurabilir. Nitelikli sertifikaya güveni sebebiyle zarar gören üçüncü kişi ise sigortalı sıfatını taşımamaktadır. Yürürlükteki mevzuatımızda zarar gören kişiye yalnızca bazı sorumluluk sigortalarıyla sınırlı olarak (örneğin 13.10.1983 tarihli ve 2918 sayılı Karayolları Trafik Kanunu 97 ve 98 I) doğrudan sigortacıya başvurma imkanı tanınmaktadır[674]. Elektronik İmza Kanunu'nda ise nitelikli sertifikaya güvenen üçüncü kişiye böyle bir hak tanıyan bir hüküm bulunmamaktadır.

Yeni Ticaret Kanunu'nun 1478. maddesinin I. fıkrası ile zarar görenin sigortacıya doğrudan başvuru hakkını genel hüküm haline getirilmiştir. Buna göre, Yeni Ticaret Kanunu'nun yürürlüğe girmesinden itibaren, zarar gören üçüncü kişiler- bu kapsamda nitelikli sertifikaya güveni sebebiyle zarara uğrayan üçüncü kişi- uğradığı zararın sigorta bedeline kadar olan kısmının tazminini, sigorta sözleşmesi için geçerli zamanaşımı süresi içinde kalmak şartıyla, doğrudan sigortacıdan isteyebilecektir[675].

---

[674] Yangın dolayısıyla sorumluluk sigortası bakımından yürürlükteki Türk Ticaret Kanunu'nun 1310. maddesinde de zarar gören kişinin doğrudan doğruya dava hakkına ve bunun sonuçlarına yer verilmektedir. Bu madde hükmüne göre zarara maruz kalan üçüncü kişiler, doğrudan doğruya sigortacıya başvurabilmektedir. Yargıtay Hukuk Genel Kurulu 31.01.1996 tarihli kararında yangın dolayısıyla sorumluluk sigortasını düzenleyen TTK. 1309 ve 1310 hükümlerini mali sorumluluk sigortaları bakımından bir genel hüküm niteliğinde değil ise de, bu hükümlerin diğer sorumluluk sigortası türlerinden ileri gelen uyuşmazlıklarda kıyas yolu ile uygulanabileceği kabul etmiştir. Yarg. HGK. E. 1995/11-980, K. 1996/18, T. 31.1.1996 (Kazancı Mevzuat İçtihat Bilgi Bankası).

[675] Zehra Şeker Öğüz / Aslıhan Sevinç Kuyucu, **Yeni Türk Ticaret Kanununda Sigorta Hukuku,** İstanbul, Filiz Kitabevi, 2011, s.106.

SONUÇ

Türk hukukunda elektronik imza bakımından getirilen düzenlemeler karşılaştırmalı hukukta bu konuda benimsenen yaklaşımlarla uyumluluk arz etmektedir. Prensip itibariyle el yazısıyla imzanın işlevlerinden hareketle güvenli elektronik imzanın taşıması gereken teknik şartlar belirlenmiş, bu çerçevede getirilen düzenlemelerin belirli bir teknolojinin diliyle kaleme alınmamasına özen gösterilmiştir. Bununla birlikte, uygulamada güvenli elektronik imza tekniği olarak dijital imzanın benimsenmiş olması dolayısıyla, teknolojiden bağımsız bu yaklaşımın pratikte bir önemi bulunmamaktadır.

Güvenli elektronik imza kural olarak el yazısıyla imzaya denk kılınmış, bu sayede yasal olarak geçerliliği şekle tabi tutulan hukuki işlemlerin güvenli elektronik imza yoluyla geçerli olarak meydana getirilmesi mümkün hale getirilmiştir (BK. 14 I).

Güvenli elektronik imzanın uygulama alanı teminat sözleşmeleri bakımından EİK. 5 II hükmü uyarınca sınırlandırılmaktadır. Uyarı işlevinin eksikliği gerekçesi esas alınarak getirilen bu istisnanın yeniden gözden geçirilmesinin isabetli olacağı kanaatindeyiz. Öncelikle, teminat sözleşmeleri şeklinde, belirli bir kanun maddesine atıf yapmayan, bir sözleşme kategorisine karşılık gelen bir ifade benimsemek yerine, özel olarak hangi türdeki teminat sözleşmelerinin güvenli elektronik imza yoluyla yapılmasına engel olunmak istendiği açıklığa kavuşturulmalıdır. Diğer taraftan, teminat sözleşmeleri bakımından bu tür istisnalar öngörülürken, günümüzdeki elektronik imza uygulamalarının karmaşık yapısı ve toplumun bilinç seviyesi dikkate alınarak, halen daha uyarı işlevinin bu tür istisnaların varlığını haklı gösterip göstermediği incelenmelidir.

Güvenli elektronik imza kavramının temelinde nitelikli sertifika unsuru yer almakta ve elektronik ortamın en önemli sakıncasını oluşturan elektronik imzanın belirli bir kişiye kesin olarak atfedilebilirliği sorunu nitelikli sertifika sayesinde çözüme kavuşturulmaktadır. Nitelikli sertifika, elektronik ortamda kurulan hukuki ilişkilerde, kişilerin kimlik bilgilerini sergilemeye yarayarak, güvenin tesisinde en

büyük rolü oynamaktadır. Nitelikli sertifikanın bu işlevi, taşıdığı bilgilerin gerçeği yansıttığının sertifika sağlayıcıları tarafından garanti edilmiş olmasından kaynaklanmaktadır. Sertifika sağlayıcıları bir taraftan nitelikli sertifika aracılığıyla kişilerinin kimlik bilgilerini tespit ederken, diğer taraftan dijital imza alt yapısına dayalı imza oluşturma ve doğrulama verilerini üretmektedir. Bu verilerin birbiriyle uyumlu çalışabilirliği, elektronik imzalı belgelerin değiştirilmediğini, yani belgede yer alan beyanın imza sahibinin iradesini yansıttığını belirlemeye yaramaktadır. Bu sayede, el yazısıyla imzanın iki temel işlevini oluşturan kimlik tespiti ve sonuçlandırma işlevi güvenli elektronik imza bakımından da sağlanmış olmaktadır.

Diğer taraftan, sertifika sağlayıcıları yalnızca nitelikli sertifika yoluyla kişilerin kimlik bilgilerinin belirlenmesi görevini üstlenmemekte, bunun yanı sıra kişilerin mesleki bilgileri, bir üçüncü kişiyi temsil yetkisi, nitelikli sertifikanın kullanım alanı ve maddi kapsamına ilişkin sınırlamalar gibi başka bilgileri de nitelikli sertifiya kaydederek, elektronik ortamda sağlanması hedeflenen güvenin kapsamını bir adım daha ileriye taşımaktadır. Bu bilgilerin de doğruluğunun ve geçerliliğinin sertifika sağlayıcı tarafından garanti edilmesi sayesindedir ki, güvenli elektronik imza, aslında bir bakıma, el yazısıyla imzayı işlevleri itibariyle ikame etme amacının ötesine geçmekte, imza sahipleri tarafından açıklanan irade beyanlarının içeriğinin belirlenmesinde de rol oynamaktadır.

Bu çerçevede, sertifika sağlayıcının Elektronik İmza Kanunu ve Elektronik İmza Yönetmeliği'nde düzenlenen yükümlülüklerini gereği gibi yerine getirmesiyle güvenli elektronik imzanın geçerli hukuki sonuç doğurması birbiriyle bağlantılı şekilde ortaya çıkmaktadır. Bu yapı dikkate alınarak Kanun'daki ve Yönetmelik'teki sistematiğin yeniden ele alınması gerekmektedir. Bu çerçevede yapılması gereken, sağlayıcının yükümlülüklerinin madde aralarında serpiştirilmiş olmaktan kurtarılarak, tek bir başlık altında ve güvenli elektronik imzanın şartlarının anlaşılmasına hizmet edecek şekilde daha sistematik bir üslupla düzenlenmesidir. Ayrıca, bu yükümlülüklerin yalnızca güvenli elektronik imzanın yaratılması amacına mı yöneldiği, bu bağlamda sertifika sağlayıcının sorumluluğunun yalnızca güvenli

elektronik imza kullanımı dolayısıyla mı ortaya çıkacağının Kanun'da açıklığa kavuşturulması gerekmektedir.

EİK. 13 hükmünde sertifika sağlayıcının üçüncü kişilere karşı sorumluluğu kusuru ispat yükü tersine çevrilmiş bir haksız fiil sorumluluğu olarak düzenlenmektedir. Bu düzenlemeyle koruma gören kişiler, nitelik sertifikaya güvenen ve bu yüzden zarara uğrayan üçüncü kişilerdir. Türk hukukunda elektronik imza düzenlemesinin en önemli eksikliklerinden biri, üçüncü kişinin nitelikli sertifikaya güveninin belirlenmesi konusunda ortaya çıkmaktadır. EİK. 13 hükmünün koruma amacını oluşturan bu konuya ilişkin bir düzenleme Elektronik İmza Kanun'nunda yer almamaktadır. Üçüncü kişinin özen külfetinin belirlenmesinde tek hukuki dayanağı oluşturan Elektronik İmza Yönetmeliği'nin 16. maddesi güven unsurunun varlığının kabul edilmesinde ayrı esaslardan hareket eden ve üçüncü kişinin tercih edeceği iki ayrı imkana yer vermektedir. Birincisine göre, üçüncü kişi tarafından, nitelikli sertifikanın geçerlilik durumu ve iptal listesinin kontrolü yoluyla yalnızca nitelikli sertifikadaki bilgilerin araştırılmasını yeterlidir. İkinci olarak gösterilen güvenli elektronik imza doğrulama aracı kullanılması imkanı güven unsurunun kapsamını genişletmektedir. Bu araç sayesinde edinilen bilgiler belgenin değiştirilip değiştirilmediğinin kontrolünü de güven unsurunun kapsamına dahil etmektedir. Kanaatimizce, mevcut düzenleme çerçevesinde birinci imkan dahilinde yer alan asgari unsurların kontrolü bir kişinin nitelikli sertifikaya güveninden söz edebilmek için yeterlidir.

EİK. 13 II hükmünde gelişmekte olan teknolojiyi doğrudan ilgilendiren böyle bir alanda kusur sorumluluğuna başvurulmuş olması nitelikli sertifikaya güvenen üçüncü kişileri hukuki korumadan yoksun bırakacak bir nitelik taşımaktadır. Bu düzenleme benimsenirken, AB Elektronik İmza Yönergesi'nin esas alındığı anlaşılmaktadır. Yönerge'de kusur sorumluluğu yerine tehlike sorumluluğuna başvurulmamış olmasının gerekçesi sertifika sağlayıcıların faaliyete başlaması bakımından caydırıcı nitelikte bir hukuki engel yaratmamak ve bu sayede elektronik imzanın yaygınlaşmasını teşvik etmek olarak ifade edilmektedir. Ancak, Yönerge bununla birlikte elektronik imzanın güvenliğini artırmaya yönelik ihtiyari

akreditasyon sistemlerini de düzenlemektedir. Bu şekilde AB ülkelerinde akredite edilmiş elektronik imzalar üçüncü kişinin güvenini pekiştirici bir rol oynayabilirken, akreditasyon düzenlemesi bulunmayan Türk hukukunda üçüncü kişinin güvenini sağlamlaştırmaya yönelik ek bir imkan bulunmamaktadır.

Sonuç olarak, nitelikli sertifikaya güvenen üçüncü kişinin teknolojiden kaynaklanan risklere katlanması adil bir çözüm olarak gözükmediğinden yürürlükteki mevzuatımıza göre sertifika sağlayıcının üçüncü kişilere karşı sorumluluğunun bir tehlike sorumluluğu olarak düzenlenmesi yerinde olacaktır. Böyle bir düzenlemeye başvurulması halinde, sertifika sağlayıcıların üçüncü kişilere nitelikli sertifika aracılığıyla imza sahibinin kimlik bilgilerinin doğruluğunu ve imzalanan metnin değiştirilmediğini garanti ettiğini kesin bir şekilde kabul etmek mümkün olabilecektir.

KAYNAKÇA

Aalberts, Babette / van der Hof, Simone: **Digital Signature Blindness: Analysis of legislative approaches toward electronic authentication,** (Çevrimiçi) http://cwis.kub.nl/~ frw/people/hof/ds-fr.htm, 03.11.2009.

Acır, Birsen: **Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi**, Sermaye Piyasası Kurulu Yeterlilik Etüdü, Ankara, 2000.

Akipek, Şebnem: **Özel Hukuk ve İnternet**, Ankara Üniversitesi'nde İNET-TR'99 Programı çerçevesinde düzenlenen "Internet ve Hukuk" konulu panelde sunulan Tebliğ, 19-21 Kasım 1999, (Çevrimiçi) http://inet-tr.org.tr/inetconf5/tammetin/hukuk.html,12.02.2011.

Aksoy, Sanem: "Borçlar Hukukunda Güvenli Elektronik İmza", **HPD**, S.5, 2005, s.252-256.

Akünal, Teoman: **Haksız Fiilden Doğan Zararlarda Denkleştirme Sorunu**, İstanbul, Sulhi Garan Matbaası, 1977.

Altınışık, Ulvi: **Elektronik Sözleşmeler**, Ankara, Seçkin, 2003.

Arıkan, Ayşe Saadet: "Bilgisayar Programlarının Korunması: AB ve Türkiye (1. Bölüm)", **TBBD,** S.3, 1996, s.309-382.

Atamer, Kerim: "Yeni Türk Ticaret Kanunu Uyarınca "Zarar Sigortaları"na Giriş", **BATİDER,** C. XXVII, S.1,

2011 (Ayrı Bası).

aus der Fünften, Jörg: **Die Haftung der Zertifizierungsstellen nach dem Signaturgesetz**, Münster, LIT Verlag, 2000.

Başpınar, Veysel: "Elektronik Tapu Sicili Düzenlenirken, Tapu Sicilinin Aleniyeti ve Diğer Alanlarla İlgili Alınması Gereken Tedbirler", **AÜHFD**, C.57, S.53, 2008, s.97-131.

Bell, Josh / Gomez, Ruben / Hodge, Paul / Mayer-Schönberger, Viktor: "Elektronic Signature Regulation: An Early Scorecard – Comparing Electronic Signatures Legislation in the US and the European Union", **Computer Law and Security Report**, Vol.17, Issue 6, 2001, s.399-402.

Bergfelder, Martin: **Der Beweis im elektronischen Rechtsverkehr,** Hamburg, Verlag Dr. Kovač, 2006.

Biçkin, İnci: "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler", **TBBD**, S.63, Mart-Nisan 2006, s.109-125. (Kısaltma: Elektronik İmza)

Biçkin, İnci: "Noterlik İşlemlerinin Elektronik Ortamda Yapılmasının Gerekliliği", **Türkiye Noterler Birliği Dergisi**, S.126, Mayıs 2005.

Bilgili, Fatih: "Özel Hukukta Elektronik İmza ve Elektronik Ticaret", **Prof.Dr. Ömer Teoman'a Armağan**, C.II, İstanbul, Beta, 2002, s.991-1012.

Bösing, Sebastian: **Authentifizierung und Autorisierung im elektronischen Rechtsverkehr,** Baden-Baden, Nomos, 2005.

Brazell, Lorna: **Electronic Signatures Law and Regulation,** London, Sweet & Maxwell, 2004.

Brehm, Roland: **Berner Kommentar, Band IV: Das Obligationenrecht, 1. Abt, 3. Teilband, 1. Urteilband Art.41-61 OR,** 3. Aufl., Bern, 2006.

Bromby, Michael: "Identification, trust and privacy: How biometrics can aid certification of digital signatures", **International Review of Law, Computers & Technology**, Vol.24, Issue 1, March 2010, s.133-141.

Çamurdan, Çiğdem: **Elektronik İmza Kanunu Tasarısı Üzerine Bir Değerlendirme**, (Çevrimiçi) http://www.e-imza.gen.tr/index.php?Page=KoseYazisi&YaziNo=21&YazarNo=22, 28.11.2010.

Çelebi Başçi, Gülen: **Sertifika Geçerlilik Kontrolündeki Sorunların Giderilmesi**, Tübitak UEKAE Kamu Sertifikasyon Merkezi (Çevrimiçi) http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/Makaleler/Sertifika%20Gecerlilik%20Kontrolundeki%20Sorunlarin%20Giderilmesi.pdf, 28.05.2011.

Dörner, Heinrich: **Rechtsgeschäfte im Internet,** AcP 202, 2002.

Dörr, Bianka Sofie: **Elektronische Signaturen unnd Haftung der Anbieter von Zertifizierungsdiensten,** Zürich, 2002.

Dumortier, Jos: "The European Regulatory Framework for Electronic Signatures: A Critical Evaluation", **EU Electronic Commerce Law**, edit. Ruth Nielsen/ Søren Sandfeld Jacobsen/ Jan Trzaskowski, Djøf Publishing, Copenhagen, 2004, s. 69-93.

Dumortier, Jos: "E-imza, E-fatura ve E-ticaret", **Ankara Barosu Hukuk Kurultayı 03-07 Ocak 2006, C.IV: Bilişim Hukuku**, Ankara, Ankara Barosu Yayınları, 2006, s.159-167. (Kısaltma: E-imza)

Dumortier, Jos / Kelm, Stefan / Nilsson, Hans / Skouma, Georgia / Van Ecke, Patrick: **The Legal and Market Aspects of Electronic Signatures, Study for the European Commission – DG Information Society**, (Çevrimiçi) http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf, 04.08.2010.

Ekşi, Nuray: "Elektronik İmzalara İlişkin UNCITRAL Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme", **Yasa Hukuk Dergisi**, S.03, 2001, s.333-340.

Eren, Fikret: **Borçlar Hukuku Genel Hükümler**, 12. Bası, İstanbul, Beta, 2010.

Erturgut, Mine: **Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi**, Ankara, Yetkin Yayınları, 2004.

Erturgut, Mine: "Elektronik Sertifika Hizmet Sağlayıcısı", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.6, S.2, 2004, s.97-130.

Erturgut, Mine: "Elektronik İmza Kanunu Bakımından E-belge ve E-imza", **Bankacılar Dergisi**, Sayı 48, 2003, s.66-79. (Kısaltma: E-belge ve E-imza)

Esener, Turhan: **Borçlar Hukuku C.1: Akitlerin Kuruluşu ve Geçerliliği,** Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1969.

Falcıoğlu, Mete Özgür: **Türk Hukukunda Elektronik Satım Sözleşmesi ve Kuruluşu,** Ankara, Yetkin Yayınları, 2004.

Feyzioğlu, Feyzi Necmettin: **Borçlar Hukuku C.I: Genel Hükümler**, 2. Bası, İstanbul, Fakülteler Matbaası, 1976.

Fischer-Dieskau, Stefanie: **Das elektronisch signierte Dokument als Mittel zur Beweissicherung,** Baden-Baden, Nomos, 2006.

Fischer-Dieskau, Stefanie / Hornung, Gerrit: "Erste höchstrichterliche Entscheidung zur elektronischen Signatur", **NJW,** Heft 40, 2007, s. 2897 – 2899.

Forder, Jay: "The inadequate legislative response to e-signatures", **CLSR**, Vol. 26, 2010, s.418-426.

Furrer, Andreas / Müller-Chen, Markus: **Obligationenrecht Allgemeiner Teil**, 1. Aufl., Zurich, Schulthess, 2008.

Gauch, Peter / Schluep, Walter R. / Jörg Schmid / Emmenegger, Susan: **Schweizerisches Obligationenrecht Allgemeiner Teil**, 9. Aufl., Zürich, Schultess, 2008.

Geis, Ivo: "Die elektronische Signatur: Eine internationale Architektur der Identifizierung im E-Commerce", **MMR**, Heft 11, 2000, 667-674.

Gezder, Ümit: **Mukayeseli Hukuk Açısından İnternet'te Aktedilen Sözleşmelerde Tüketicinin Korunması**, İstanbul, Beta, 2004.

Gönen, Doruk: **El Yazılı Vasiyetname**, İstanbul, Legal, 2007.

Hansen, Mathias: **Die ausservertragliche Haftung von Zertifizierungsdiensteanbietern,** Hamburg, Verlag Dr. Kovač, 2008.

Heger, Monica: **Cryptographers Take On Quantum Computers,** (Çevrimiçi) http://spectrum.ieee.org/computing/software/cryptographers-take-on-quantumcomputers, 14.06.2011.

Helvacı, İlhan: **Eski Medenî Kanunumuzla Karşılaştırmalı Olarak Türk Medenî Kanunu'na Göre Sözleşmeden Doğan İpotek Hakkı**, İstanbul, On İki Levha Yayıncılık, 2008.

Henniger, Olaf / Schneider, Björn / Struif, Bruno / Waldmann, Ulrich: "Improving the Binding of Electronic Signatures to the Signer by Biometric Authentication", **Advances in Biometrics**, edit. David Zhang / Anil K. Jain, Springer Berlin, Heidelberg, 2006, s.523-530.

İnal, Emrehan: **E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması**, İstanbul, Vedat Kitapçılık, 2005.

İnan, Ali Naim: **Borçlar Hukuku Genel Hükümler**, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, Sevinç Matbaası, 1979.

Schlauri, Simon: **Elektronische Signaturen,** Zürich-Basel-Genf, Schulthess Juristische Medien AG, 2002, s.746.

Schwenzer, Ingeborg: **Schweizerisches Obligationenrecht Allgemeiner Teil,** 5. Aufl., Bern, 2009.

Serozan, Rona / Engin, Baki İlkay: **Miras Hukuku**, 2. Bası, Ankara, Seçkin, 2008.

Jungermann, Sebastian: **Der Beweiswert elektronischer Signaturen,** Frankfurt am Main, Peter Lang, 2002.

Karan, Hakan: **Elektronik Konişmento**, Ankara, Turhan Kitabevi, 2004.

Kennedy, Gwen: "Thumbs Up for Biometric Authentication", **Computer L. Rev. & Tech.,** Vol.VIII, 2004, s.379-407.

Keser Berber, Leyla: "İmzalıyorum, O Halde Varım! Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri", **TBBD**, S.2, 2000, s. 503-556. (Kısaltma: Dijital İmza)

Keser Berber, Leyla: "Şekil ve Dijital İmza", **Elektronikteki Gelişmeler ve Hukuk, Noterlik Hukuku Sempozyumu,** Ankara, NOTEV Yayını, 2001. (Kısaltma: Şekil ve Dijital İmza)

Keser Berber, Leyla: "Elektronik Ticaret Koordinasyon Kurulu'nun (ETKK) "Elektronik Veri, Elektronik Sözleşme ve Elektronik İmza Kanunu Tasarısı Taslağı"na Yönelik Farklı Yaklaşımlar", **Maltepe Üniversitesi Hukuk Fakültesi Dergisi**, S.1, 2002, s.165-195. (Kısaltma: ETKK Taslağı)

Keser Berber, Leyla: **İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza,** Ankara, Yetkin Yayınları, 2002.

Keser Berber, Leyla: "E-Sözleşme Bağlamında Dijital İmza ve ETKK Yasa Taslağı Açısından Türkiye'de Durum", **Internet ve Hukuk** (der. Yeşim Atamer), Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.780. (Kısaltma: E-Sözleşme Bağlamında Dijital İmza)

Keser Berber, Leyla: **Elektronik İmzanın Düzenlenmesi Hakkında Kanun Tasarısı Hükümlerinin Değerlendirilmesi**, (Çevrimiçi) http://www.hukukcu.com/bilimsel/ kitaplar/e_imza_ tasari elestiri.htm, 14.02.2011.

(Kısaltma: Tasarı)

Keser Berber, Leyla / Lostar Murat: **Bilişimde Biyometrik Yöntemler**, Yetkin Yayınları, Ankara, 2006. (Kısaltma: Biyometrik Yöntemler)

Kılıçoğlu, Ahmet M: **Borçlar Hukuku Genel Hükümler**, 10. Bası, Ankara, Turhan Kitabevi, 2008.

Kılıçoğlu, Ahmet M: **Türk Borçlar Kanunu Tasarısı'na Eleştiriler**, Türkiye Barolar Birliği, 2008. (Tasarı)

Kırçova, İbrahim / Öztürk, Pınar: **İnternette Ticaret ve Hukuksal Sorunlar**, İstanbul, İstanbul Ticaret Odası Yayını, 2000.

Kilian, Wolfgang: "Dijital Communication and Contract Law", **Uluslararası İnternet Hukuku Sempozyumu**, İzmir, Dokuz Eylül Üniversitesi Yayını, 2002, s.145-161.

Kocayusufpaşaoğlu, Necip: **Borçlar Hukuku Genel Bölüm,** C.I, 4. Bası, İstanbul, Filiz Kitabevi, İstanbul, 2008.

Koller, Alfred: **Schweizerisches Obligationenrecht**, Allgemeiner Teil, 3. Aufl., 2009.

Koops, Bert Jaap: "Should ICT Reguation be Technology-Neutral", **IT & Law Series,** Vol.9, The Hague: T.M.C. Asser Press 2006, s.77-108.

Köprülü, Bülent / Kaneti, Selim: **Sınırlı Aynî Haklar**, 2. Bası, İstanbul, 1982-1983.

Kubilay, Huriye / Akıntürk, Esen: "Elektronik Konişmento", **Prof.Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı**, İstanbul, Beta, 2001, s.333-354.

Kuner, Christopher: **Remarks of the German Government on the EU Draft Directive concerning Electronic and Digital Signatures**, 1998, http://www.kuner.com/data/sig/gov_ger_eudraft.htm, 1.02.2011.

Larenz, Karl / Wolf, Manfred: **Allgemeiner Teil des deutschen bürgerlichen Rechts,** 9. Aufl. , München, Beck, 2004.

Liu, Yue: Identifying Legal Concerns in the Biometric Context, **JILT,** Vol.3, Issue 1, 2008, s.45-54.

Martínez Nadal, Apol·lónia / Ferrer Gomila, Josep Lluís: "Critical Comments on the European Directive on a Common Framework for Electronic Signatures and Certification Service Providers", **LNCS: Financial Cryptography,** Vol.1962, 2001, Springerlink, s.225-244. (Kısaltma: European Directive)

Martínez Nadal, Apol·lónia / Ferrer Gomila, Josep Lluís: "Comments to the UNCITRAL Model Law on Electronic Signatures", **LNCS: Information Security,** Vol.2433, 2002, Springerlink, s.229-243. (Kısaltma: UNCITRAL Model Law)

Martínez Nadal, Apol·lónia / Ferrer Gomila, Josep Lluís: "Liability of Certification Authorities: A Juridical Point of View", **LNCS: Information Security**, 2001/2200, Springerlink, s.204-219.

Murray, Andrew D.: **Regulating Electronic Contracts: Comparing the European and North American Approaches**, (Çevrimiçi) http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=andrew_murray, 5.02. 2011.

Noack, Ulrich: "Elektronische Form und Text Form", **Das Neue Schuldrecht**, Barbara Dauner-Lieb, Thomas Heidel, Gerhard Ring (Hrsg.), Heidelberg, C.F.Müller, 2002.

Oğuzman, Kemal M. / Öz, Turgut M.: **Borçlar Hukuku Genel Hükümler,** 8. Bası, İstanbul, Vedat Kitapçılık, 2010.

Oğuzman, Kemal M. / Seliçi, Özer / Özdemir, Sahibe Oktay: **Eşya Hukuku, İstanbul,** 12. Bası, Filiz Kitabevi, 2009. (Kısaltma: Eşya Hukuku)

Orer, Gürsel: **Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu**, Ankara, Adalet Yayınevi, 2011.

Orta, Mesut: **Elektronik İmza ve Uygulaması**, Ankara, Seçkin, 2005.

Öz, Turgut: **Yeni Borçlar Kanununun Getirdiği Başlıca Değişiklikler ve Yenilikler**, İstanbul, Vedat Kitapçılık, 2011.

Özdemir Kocasakal, Hatice: **Elektronik Sözleşmelerden Doğan Uyuşmazlıkların Çözümünde Uygulanacak Hukukun ve Yetkili Mahkemenin Tespiti**, İstanbul, Vedat Kitapçılık, 2003.

Özdemir Kocasakal, Hatice: "Elektronik İmzanın Geçerliliği ve İspat Gücü Açısından Uluslararası Planda Yaşanan Gelişmeler", **Prof. Dr. Ergun Önen'e Armağan**, İstanbul, Alkım, 2003, s.217-251. (Kısaltma: Elektronik İmza)

Özdemir Kocasakal, Hatice: "Elektronik Sözleşmeler", **GSÜHFD**, S.1, 2006, s.49-53. (Kısaltma: Elektronik Sözleşmeler)

Özsunay, Ergun: "Elektronik Ticaret ve E-Sözleşmelerin Temel Sorunları", **Uluslararası İnternet Hukuku Sempozyumu**, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002, s.121-145.

Pauliac, Lucien: **The Hiddden Truth About Electronic Signatures**, çev. Nicholas Allen, (Çevrimiçi) http://www.mega preuve.org/cariboost_files/Hidden_20Truth_20Abou t_20Electronic_20Signatures.pdf, 27 Eylül 2010, Erişim Tarihi:11.03.2011.

Pulaşlı, Hasan: **"Türk ve Alman Hukuklarında Noterlerin Hukuki Sorumluluğu",** Türkiye Noterler Birliği Hukuk Dergisi, S.39, 1983, s.10-16.

Rado, Türkan: **Roma Hukuku Dersleri: Borçlar Hukuku,** İstanbul, Filiz Kitabevi, 1997.

Reed, Chris: "Taking Sides on Technology Neutrality", **SCRIPT-ed,** Vol.4, Issue 3, September 2007, s.264-284.

Sağlam, İpek: **Elektronik Sözleşmeler**, İstanbul, Legal, 2007.

Sarıakçalı, Turgay: **İnternet Üzerinden Akdedilen Sözleşmeler,** Ankara, Seçkin, 2008.

Saymen, Ferit H. / Elbir, Halid K.: **Türk Eşya Hukuku (Ayni Haklar),** İstanbul, İsmail Akgün Matbaası, 1954.

Schaub, Martien: **European Legal Aspects of E-Commerce**, Groningen, Europa Law Publishing, 2004.

Schnell, Daniel: **Signaturmissbrauch und Rechtssheinhaftung,** Berlin, Dunker & Humblot, 2007.

Scoville, Adam White: "Clear Signature, Obscure Signs", **Cardozo Arts Ent. L.J.**, 1999/17, s.346-412.

Selçuk, Gonca Hülya: **E-Devlet Uygulamaları için Elektronik İmza Formatları**, Tübitak UEKAE Kamu Sertifikasyon Merkezi, (Çevrimiçi) http://www.kamusm.gov.tr/tr/Bilgideposu/Belgeler/Makaleler/EDevletUygulamalariIcinElektronikImzaFormatlari.pdf, 08.03.2011.

Sirmen, Lale: **Alacak Rehni,** Ankara, Banka ve Ticaret Hukuku Enstitüsü, 1990.

Smedinghoff, Thomas J. / Bro, Ruth Hill: **Electronic Signature Legislation**, (Çevrimiçi) http://library.findlaw.com/1999/Jan/1/241481.html, 12.03.2010.

Soysal, Tamer: "Teknik ve Hukuki Açıdan Elektronik İmza", **Legal Hukuk Dergisi**, Mart 2006, s.697-733.

Sözer, Bülent: **Elektronik Sözleşmeler**, İstanbul, Beta, 2002.

Sözer, Bülent: "Elektronik İmza Kanunu'na Göre Digital İmza", **Prof.Dr. Ergon A. Çetingil ve Prof. Dr. Rayegân Kender'e 50. Birlikte Çalışma Yılı Armağanı**, Ankara, Çizgi Basım, 2007.

Spiegelhalder, Torsten: **Rechtsscheinhaftung im Stellvertretungsrecht bei der Verwendung elektronischer Signaturen**, Hamburg, Verlag Dr. Kovač, 2007.

Spindler, Gerald / Anton, Katharina: "BGB §126a: Elektronische Form", **Recht der elektronischen Medien**, Gerald Spindler, Fabian Schuster (Hrsg.), 2. Aufl., München, C.H. Beck, 2011.

Srivastava, Aashish: "Electronic signatures and security issues: An emprical study", **Computer Law & Security Review**, 2009/25, s.432-446.

Şeker Öğüz, Zehra / Sevinç Kuyucu, Aslıhan: **Yeni Türk Ticaret Kanununda Sigorta Hukuku,** İstanbul, Filiz Kitabevi, 2011.

Şener, Oruç Hami: "Sözleşmeyle Yapılan Teminat Amaçlı Borca Katılma", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.11, Özel S.2009 (Basım Y. 2010), s.1279-1322, s.1279 ve dn.1.

Şenocak, Zarife: "Dijital İmza ve Dijital İmzalı Belgelerin Borçlar Kanunu Hükümleri Açısından Ele Alınması"**,** **AÜHD**, C.50, S.2, 2001, s.98-135.

Tandoğan, Halûk: **Kusura Dayanmayan Sözleşme Dışı Sorumluluk Hukuku,** Ankara, Turhan Kitabevi, 1981.

Tandoğan, Halûk: **Borçlar Hukuku: Özel Borç İlişkileri**, C.II, 3. Bası, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü, 1987. (Kısaltma: Özel Borç İlişkileri II)

Tekinay, Selahattin Sulhi / Akman, Sermet / Burcuoğlu, Haluk / Altop, Atilla: **Borçlar Hukuku Genel Hükümler**, 7. Baskı, İstanbul, Filiz Kitabevi, 1993.

Thomale, Hans-Christoph: **Haftung und Prävention nach dem Signaturgesetz,** Baden-Baden, Nomos, 2003.

Thomale, Hans-Christoph: "Die Haftungsregelung nach §11 SigG", **MMR**, Heft 2, 2004, s.80-86. (Kısaltma: §11 SigG)

Tunçomağ, Kenan: **Türk Borçlar Hukuku C.1: Genel Hükümler,** 6. Bası, İstanbul, Sermet Matbaası, 1976.

von Harnier, Albrecht: **Organisationsmöglichkeiten für Zertifizierungs-stellen nach dem Signaturgesetz,** Baden-Baden, Nomos, 2000.

von Seck, Claudia: **Die elektronische Signatur im Hinblick auf die Haftung der Zertifizierungsdiensteanbieter**, Marburg, 2003.

Wang, Minyan: "The Impact of Information Technology Development on the Legal Concept- A Particular Examination on the Legal Concept of "Signatures"", **International Journal of Law and Information Technology**, Vol. 15, No:3, Oxford University Press, 2006, s.253-274.

Wang, Minyan: "A Review of Electronic Signatures Regulations: Do They Faciliate of Impede International Electronic Commerce?", **ICEC'06**, Fredericton Canada, ACM, s.548-552. (Kısaltma: Electronic Commerce)

Yardım, Mehmet Ertan: **Elektronik İmza ve Elektronik İmzanın Medeni Usul Hukukumuza Etkileri**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2006.

Yaltı Soydan, Billur: "E-imza ve E-belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk – I", **Vergi Sorunları Dergisi**, S.151, 2001, s.127-135. (Kısaltma: E-imza I)

Yaltı Soydan, Billur: "E-imza ve E-belge: Kağıtsız ve Mürekkepsiz Dünyada Hukuk – II", **Vergi Sorunları Dergisi**, S.152, 2001, s.156-165. (Kısaltma: E-imza II)

Yıldırım, Mustafa Fadıl: "Nitelikli Elektronik Sertifika Hizmet Sağlayıcısının Hukuki Sorumluluğu", **Bilişim Hukuku**, der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s.27-43.

YARARLANILAN DİĞER KAYNAKLAR

Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, çalışma grubu: Leyla Keser, Yasin Beceni, Tugrul Sevim, Temmuz 2004, İstanbul, (Çevrimiçi) http://www.tk.gov.tr/eimza/doc/diger/e-imza%20hukuk%20calisma%20grubu%20raporu.pdf, 10.06.2011.

The ELDOC Study: Legal Study on Legal and Administrative Practices Regarding the Validity and Mutual Recognition of Electronic Documents, DG Enterprise & Industry, European Commission 2006, (Çevrimiçi) http://ec.europa.eu/enterprise/sectors/ict/files/dumortier-final-report-draft_en.pdf, 10.06.2011.

Kamu SM Nitelikli Sertifika Uygulama Esasları, TÜBİTAK UEKA, 2008, (Çevrimiçi) http://www.kamusm.gov.tr/BilgiDeposu/KSM_NES_SUE/KSM_NES_SUEv5.pdf, 10.06.2011.

UNCITRAL Elektronik İmza Model Kanunu Türkçe Çevirisi, "Internet ve Hukuk" (der. Yeşim Atamer), Bilgi Üniversitesi Yayınları, İstanbul, 2004, s.780.