

# DİJİTAL İMZA VE DİJİTAL İMZANIN BORÇLAR KANUNU HÜKÜMLERİ AÇISINDAN ELE ALINMASI

*Yrd. Doç. Dr. Zarife ŞENOCAK\**

## GİRİŞ

Günümüzde, kağıda dayalı geleneksel iletişim modelinden modern dijital iletişim modeline doğru hızlı bir gelişim yaşanmaktadır. Bilgi ve iletişim teknolojilerinin bu hızlı gelişimi, veri değiş-tokuşu ve iktisadi faaliyetler alanlarında yeni imkanlar yaratmaktadır. Mal ve hizmet siparişleri, bankalara verilen ödeme talimatları, tıp alanında özel bilgilerin iletilmesi, devlet makamları nezdinde yapılan başvurular ile geçmişte kağıda dayalı olarak yapılan ve hukuken önem taşıyan bir çok işlem, bugün dünyada büyük ölçüde elektronik yolla vuku bulmaktadır. Bu durum, özellikle, ülke sınırlarını aşan mal ve hizmet edimlerini içeren hukuki ilişkiler (elektronik ticaret) sahasında da geçerlidir. Elektronik ticaretin uluslararası iktisadi yaşamdaki önemi karşısında, ülkelerin bu konuyla ilgili iç hukuk kurallarının yeknesaklık taşıması önem arz etmektedir.

Modern bilgi ve iletişim tekniklerinin artan kullanımı ile birlikte, sahtecilik gibi riskler de ortaya çıkmaktadır. Elektronik olarak iletilen ya da kaydedilen veriler, üçüncü kişiler tarafından, gönderici veya alıcı farketmeksizin ve herhangi bir iz bırakmaksızın iletişim esnasında ya da sonradan değiştirilebilmektedir; verilerde değişiklik yapıldığının ispatlanması ise mümkün değildir. Diğer taraftan muhatap açısından, bir bilgi ya da veri dosyasını gönderen kişinin gerçekten gönderici olarak gözükmesi kişi olup olmadığı da kesin olarak belli değildir. Herkese açık global bir haberleşme ağı olan internetin, elektronik ticarete de yaygınlaşmasıyla, elektronik ticaretin önemi artarken, bu risklerin karşılanması ihtiyacı da kendisini daha fazla hissettirmeye başlamıştır. Bu sorunların çözümü hukukta değil, yine teknolojiye aranmaktadır. Nitekim endüstri, dijital imza olarak isimlendirilen asimetrik kriptografi (şifreleme)

---

\* Ankara Üniversitesi Hukuk Fakültesi Medeni Hukuk Anabilim Dalı Öğretim Üyesi

yöntemini ve buna bağlı olarak chip kartı, Trust Center gibi güvenlik hizmetlerine ilişkin teknolojileri geliştirmiştir.

Öte yandan hukuk da, hemen hemen eş zamanlı diyebileceğimiz kadar hızlı bir şekilde teknolojiyi takip etmektedir. Bu konuyla ilgili olarak, Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu'nun (UNCITRAL) hazırlamış olduğu 16 Aralık 1996 tarihli "*Elektronik Ticaret Model Kanunu*" ve aynı komisyonun Elektronik Ticaret Çalışma Grubunun hazırlamış olduğu "*Elektronik İmza Model Kanunu Tasarısı*" mevcuttur. Avrupa Birliği bünyesinde ise, 8 Haziran 2000 tarihli "*İç Pazarda Elektronik Ticaretin Hukukî Yönleri Hakkında Yönerge*" ve 13 Aralık 1999 tarihli "*Elektronik İmzaların Müşterek Çerçeve Şartları Hakkındaki Yönerge*" çıkarılmıştır. Yönergeler, Avrupa Birliği üyesi olan ülkeler için ulaşılması gereken amaçlar yönünden bağlayıcı olduğundan, üye ülkeler, bu yönergeleri iç hukuka uyarlama çalışmasına başlamışlardır.

Bu çalışmanın konusu, esas itibariyle dijital imza ile ilgili bazı hukuki problemlerin Borçlar Kanunu hükümleri açısından değerlendirilmesi olup, dijital imzanın Türk İspat Hukuku açısından değerlendirilmesi yapılmayacaktır.

## 1. DİJİTAL İMZA TEKNİĞİ

İnternet üzerinden sözleşmelerin kurulmasında hukuki güvenliğin sağlanması için, karşı tarafa iletilen bilgilerin (beyanın, mesajın) muhtevasının bütünlüğünün (İntegrität) sağlanması ve sözleşmenin diğer tarafının kimliğinin, kesin ve güvenilir şekilde tespit edilebilmesi gerekir. Ancak bu şekilde icap veya kabul beyanını şüpheye yer vermeyecek şekilde göndericiye izafe etmek mümkün olabilir. İşte bu güvenirliliği, günümüzde, açık anahtar kriptografisine dayalı dijital imza tekniği sağlayabilmektedir.

Dijital imza elektronik imza türlerinden biridir. Üst kavram olan elektronik imza, uluslararası ve ulusal hukukî düzenlemelerde verilen - hemen hemen- ortak bir tanıma göre<sup>1</sup>, "*diğer elektronik verilere eklenen veya bunlarla mantıksal bir bağlantı içerisinde olan, imzalayanın kimliğinin tespitini mümkün kılan ve elektronik verinin muhtevasını, imzalayanın kabul ettiğini gösteren elektronik şekildeki verilerdir*". Açık anahtar kriptografisine dayalı dijital imza yanında, bugün kullanılan ve el yazısı ile imzanın bir ya da daha fazla fonksiyonunu yerine getiren başka imzalar da mevcuttur.

<sup>1</sup> UNCITRAL Elektronik İmza Model Kanun Tasarısı'nda verilen tanım için bkz. II 1 B; Elektronik İmza Yönergesi'nde verilen tanım için bkz. II 2 B; Alman Elektronik İmza Kanunu ve Elektronik İmza Sahasında Sertifika Hizmetleri Hakkındaki İsviçre Federal Kanun Tasarısı'nda benimsenen imza türleri için bkz. II 3 A ve II 4.

Bunlara, (örneğin el yazısı ile imzayı esas alan) biyometrik yöntemle (biyometrik imza)<sup>2</sup> ya da PIN (Personal Identification Number- kişi tanımlama numarası) vasıtasıyla kimlik belirlemeye dayalı teknikler örnek olarak verilebilir<sup>3</sup>.

Dijital imzada, sahibinin isminin harflerinden oluşan bir paraf ya da el yazısı ile imzanın elektronik olarak kopyalanması söz konusu değildir; bilakis, dijital imza, elektronik olarak yaratılan ve gönderilen belgelerin şifrelenmesi esasına dayanmaktadır.

Dijital imza için herşeyden önce, aralarında matematiksel bir bağlantı olan ve fonksiyonel olarak bir birlik arz eden iki ayrı şifreye ihtiyaç vardır. Şifrelerden biri gizli olup (gizli anahtar), diğeri ise (açık anahtar) herkesçe bilinebilir, aleni olarak ulaşılabilir niteliktedir (örneğin yayınlanan açık anahtar listeleri aracılığıyla). Gizli anahtar dijital imzanın yaratılmasında, açık anahtar ise dijital imzanın tetkikinde kullanılmaktadır.

Bu anahtar çifti, ya sertifika hizmet sağlayıcıları (Zertifikatdiensteanbieter, Certification Service Provider, Certification Authority, Trust Center) tarafından üretilir ve sahibine teslim edilir; ya da kişiler tarafından bizzat off line şekilde bilgisayarda bir şifreleme programı aracılığıyla (örneğin PGP – pretty good privacy) elde edilir<sup>4</sup>. Üretilen şifrelerden gizli anahtar, ya bilgisayarın ana belleğine, diske veya diskete kopyalanır ve üçüncü kişilerin bu şifreyi okumasını engelleyici tedbirler alınır; ya da gizli anahtar akıllı kart olarak da adlandırılan chip karta yerleştirilir. Bu son durumda, şifreleme işleminin tamamı chip kartın mikro işlemcisinde (Mikroprozessor) gerçekleştiğinden, bu şifrenin kopyalanması bugünkü teknolojiyle mümkün değildir<sup>5</sup>. Chip kartların kullanımı hem şifrelerin kopyalanmasının mümkün olmaması, hem de sahibine farklı bilgisayarlarda çalışıp işlem yapabilme imkanını sağlaması açısından avantajlıdır<sup>6</sup>. Bununla beraber, bu kartın üçüncü kişilerin eline geçmesini engellemek için yeterli güvenlik tedbirleri alınmalıdır. Genellikle chip kartlar, PIN vasıtasıyla veya parmak izi, ses tahlili gibi biyometrik özellikli

<sup>2</sup> El yazısı ile imzayı, ses tahlilini, retina taramasını, parmak izini vs. esas alan diğer biyometrik imzalar hakkında bilgi için bkz. Wirtz, B.: Biometrische Verfahren, DuD 1999, s. 129 vd.

<sup>3</sup> Draft Guide to Enactment of the Uncitral Model Law on Electronic Signatures (2001), Nr. 33 ([http://www.uncitral.org/english/workinggroups/wg\\_ec/wp-88e.pdf](http://www.uncitral.org/english/workinggroups/wg_ec/wp-88e.pdf))

<sup>4</sup> Deville R. /Kaltheneger R.: Wege zum Handelsverkehr mit elektronischer Unterschrift. NJW-CoR 1997, s.169. “PGP her türlü elektronik belgenin ve postanın şifrelenmesinde kullanılan bir yöntem olup, bununla belgeleri dijital imza ile imzalamak da mümkündür.” Bkz. Keser-Berber, L.: “İmzaforum O Halde Varım” Dijital İmza, Dijital İmza Hakkındaki Yasal Düzenlemeler, Dijital İmzalı Elektronik Belgelerin Hukuki Değeri, TBBD 2000, s.531.

<sup>5</sup> Kindl, J.: Elektronischer Rechtsverkehr und digitale Signatur, MittBayNot 1999, s. 32; Deville/Kaltheneger, s. 169.

<sup>6</sup> Deville/Kaltheneger, s.169.

yöntemlerle yetkisiz kullanımlara karşı emniyet altına alınmaktadır<sup>7</sup>. Gizli anahtarın chip karta kaydedilmesi durumunda, imza işlemi için bilgisayar yanında, kartın okunması için bir kart okuyucusuna da ihtiyaç vardır.

Dijital imza, şifreleme programı yardımıyla, elektronik bir metin üzerinde uygulanan iki aşamalı bir prosedürün sonucudur. İmzalayan bu prosedüre optik olarak vakıf olmadığı gibi, dijital imzanın özel bir program olmaksızın, muhteva itibarıyla (temsili bir şekilde) gözle görülmesi mümkün değildir.

Dijital imzalama için ilk önce, gönderilecek elektronik metnin tamamı seçilmekte ve şifreleme programı çağrılmaktadır. Program ilk aşamada, bu metne hash algoritmasını tatbik ederek, metni harf ve rakamlardan oluşan bir mesaj özetine, diğer bir deyimle hash değerine (Hashwert, Hash-Code) çevirmektedir<sup>8</sup>. Bilgisayar terminolojisinde "hash (öz)" yazılan bir metnin kısaltılmış şeklini ifade etmektedir<sup>9</sup>. Metnin bu şekilde kısaltılma sebeplerinden biri, asimetrik kriptografi (şifreleme) prosedürünün fazla zaman almasıdır<sup>10</sup>. Bu şekilde atılmış dijital imza, imzalanan belgenin özünü içerecektir<sup>11</sup>. Hash algoritmasının tatbiki esnasında program, metnin karakteristik özelliklerinin tümünü (işaretlerin türünü, sırasını ve sayısını) dikkate alarak metnin hash değerini elde etmektedir. Bu nedenle elde edilen değer, tamamen bilgisayarda seçilen ve işaretlenen metne özgü olup, bu metinde yapılacak bir değişiklik, elde edilen hash değerini değiştirecektir<sup>12</sup>.

İkinci aşamada, şifreleme programı, elde edilen bu hash değerini (mesaj özetini), göndericinin özel anahtarı ve asimetrik şifreleme sistemi vasıtasıyla şifrelemekte ve bu şekilde şifrelenen hash değeri (mesaj özeti), elektronik metne eklenerek muhataba gönderilmektedir. Sonuç olarak dijital imzanın, göndericinin gizli anahtarı ile şifrelenmiş mesaj özetinden ibaret olduğu söylenebilir. Bu şekilde elde edilen dijital imza, sadece imzalanan metne ve gizli anahtarın sahibine özgü bir imzadır; zira gerek metindeki, gerekse gizli anahtardaki bir değişiklik farklı bir dijital imza ortaya çıkaracaktır.

Muhatap ise, elektronik belgeyi kendisine gönderenin kimliğinin doğruluğunu ve belgenin metninde gönderme esnasında veya sonradan bir

<sup>7</sup> Kindl, s. 32; Keser-Berber, s.517.

<sup>8</sup> Hash algoritmasına, diğer tabirle hash fonksiyonuna tek yönlü fonksiyon da (one-way funktion) denilmektedir. Elde edilen hash değere bakılarak orjinal metnin elde edilmesi mümkün değildir. Thot, N. B.: Elektronischer Vertragsschluss, Frankfurt am Main 2000, s. 124, dph. 161; Runge, A. : "Elektronische Unterschriften", St.Gallen 1997, s.9.

<sup>9</sup> Keser-Berber, s. 524.

<sup>10</sup> Runge, s. 38; Jaburek, W.J./Wölf, N.: Cyber-Recht, Wien 1997, s. 144.

<sup>11</sup> Keser-Berber, s. 524.

<sup>12</sup> Deville/KaltheGener, s.169.

değişiklik yapıp yapılmadığını tespit için, bu metnin yine bir program aracılığıyla hash değerini hesaplayacaktır. Daha sonra, elektronik belgedeki dijital imzayı, gönderenin açık anahtarını kullanarak deşifre edecektir. Göndericinin gizli anahtarı ile şifrelenen metin, yine ancak bu gizli anahtarla matematiksel bağlantı içinde olan göndericinin açık anahtarı ile deşifre edilebilir. Açık anahtarı gönderici bizzat muhataba iletebilir veya muhatap bunu sertifika hizmet sağlayıcılarından temin edebilir. Dijital imzanın, açık anahtarlarla deşifre edilmesi sonucu orijinal metnin hash değeri (mesaj özeti) elde edilir. Muhatap bu şekilde elde ettiği hash değeri (mesaj özeti) ile, kendisine gönderilen elektronik belgenin metninin hash değerini (mesaj özetini) karşılaştıracaktır. Bu iki değer birbiriyle örtüşüyorsa, metnin göndericinin gizli anahtarı ile imzalanmış olduğundan ve elektronik belgenin metninin, gönderme esnasında veya sonradan üçüncü kişiler tarafından değiştirilmemiş olduğundan emin olacaktır<sup>13</sup>.

Doktrinde, “gizli anahtar, dijital imzanın atılmasında kullanılan yazı malzemesi, açık anahtar ise bu imzayı okuma aracıdır” şeklinde bir benzetme yapılmaktadır<sup>14</sup>.

Aşağıda dijital imza tekniğine bir örnek verilmiştir<sup>15</sup>. Aşağıdaki metnin dijital imza ile Ahmet Özdemir tarafından, Ali Özgüven’e gönderilmesi gerekmektedir.

---

<sup>13</sup> Dijital imza tekniği için bkz. **Thot**, s. 123 vd.; **Kuner, Chr.**: Rechtliche Aspekte der Datenverschlüsselung im Internet, NJW-CoR 1995, s. 413 vd.; **Tauschek, S.**: Rechtliche Problematik digitaler Signaturverfahren, BB 1997, s. 1544; **Malzer, H.M.**: Zivilrechtliche Form und prozessuale Qualität der digitalen Signatur nach dem Signaturgesetz, DNotZ 1998 s.97; **Ernst, S.**: Der Mausclick als Rechtsproblem-Willenserklärungen im Internet, NJW-CoR 1997, s.169 vd.; **Deville/Kaltheneger**, s.169 vd.; **Taupitz, J./Kritter, Th.**: Electronic Commerce- Probleme bei Rechtsgeschäften im Internet, JuS 1999, s. 845; **Kühn, U.**: Technische Grundlagen digitaler Signaturverfahren, Rechtsfragen der digitalen Signatur, Hrsg. Hoeren Th. / Schüngel, M. Berlin 1999, s.72 vd.

<sup>14</sup> **Taupitz/Kritter**, s.845.

<sup>15</sup> Örnek için bkz. **Jaburek/Wölf**, s.144-145.

Sayın Dr. Özgüven,  
 30.05.2001 tarihli mektubunu aldım  
 Sayfa 1 .....  
 .....  
 Sayfa 2 .....  
 .....

Saygılarımla  
 Ahmet Özdemir

**I. Hash algoritması yardımıyla şekil 1'deki metinden, şekil 2'deki hash değeri (mesaj özeti) elde edilir.**

**Ş E K İ L: 1 (Metin)**

Sayın Dr. Özgüven,  
 30.05.2001 tarihli mektubunu aldım  
 Sayfa 1 .....  
 .....  
 Sayfa 2 .....  
 .....

Saygılarımla  
 Ahmet Özdemir

**Ş E K İ L: 2 (Hash Değeri-Mesaj Özeti)**

0000 0001 00012 1976 8844 1374 BB31 A 976

**II. Hash değeri (mesaj özeti) göndericinin özel anahtarı ile şifrelenir ve böylece şekil 1'deki hash değerinden, şekil 2'deki dijital imza elde edilir.**

**Ş E K İ L 1 (Hash Değeri-Mesaj Özeti)**

0000 0001 00012 1976 8844 1374 BB31 A 976

**Ş E K İ L 2 (Dijital İmza)**

43AB 8cb7 5A67 4C3A 87D1 22A5 5678 F91A

**III. Metin imza ile gönderilir:****M E T İ N**

Sayın Dr. Özgüven,

30.05.2001 tarihli mektubunu aldım

Sayfa 1 .....

Sayfa 2 .....

Saygılarımla  
Ahmet Özdemir

**D İ J İ T A L İ M Z A**

43AB 8cb7 5A67 4C3A 87D1 22A5 5678 F91A

**IV. Muhatap yukarıdaki (Nr. III) dijital imzalı metni alır.**

**V. Muhatap hash algoritması yardımıyla metinden (şekil 1), hash değerini (şekil 2) elde eder.**

**Ş E K İ L 1 ( Metin)**

Sayın Dr. Özgüven,

30.05.2001 tarihli mektubunu aldım

Sayfa 1 .....

Sayfa 2 .....

Saygılarımla  
Ahmet Özdemir

**Ş E K İ L 2 ( Hash Değeri-Mesaj Özeti)**

0000 0001 00012 1976 8844 1374 BB31 A 976

**VI. Muhatap gönderilen dijital imzayı (şekil 1), göndericinin açık anahtarı ile deşifre eder (sonuç: şekil 2).**

**Ş E K İ L 1 (Dijital İmza)**

43AB 8CB7 5A67 4C3A 8701 22AB 5678 591A

**Ş E K İ L 2 ( Deşifre Edilmiş İmza)**

0000 0001 00012 1976 8844 1374 BB31 A 976

**VII. Muhatap deşifre edilen imza ile (Nr. VI, şekil 2) gönderilen metnin hash değerini (Nr. V, şekil 2) karşılaştırır. Eğer bu değerler (şekil 1 ve şekil 2) birbirine uyuyorsa, gerçekten metin gönderici tarafından imzalanmış ve gönderilen metin başkaları tarafından değiştirilmemiştir.**

**Ş E K İ L 1 (Deşifre Edilen İmza)**

0000 0001 00012 1976 8844 1374 BB31 A 976

**UYUMLU =**

**Ş E K İ L 2 (Gönderilen Metnin Hash Değeri-Mesaj Özeti)**

0000 0001 00012 1976 8844 1374 BB31 A 976

Elektronik ticarete dijital imzanın kullanımı, hukukî ilişkilerde güvenliğin sağlanmasına ilişkin altyapı çalışmalarını da gerektirmektedir. Kendisine dijital olarak imzalanmış bir belge gönderilen kişinin, anahtar çiftinin (gizli ve açık anahtarın) gerçekten imzada ismi gözükken kişiye izafe edilebileceğine güvenebilmesi gerekir. Bu nedenle anahtar çiftinin üretimi ve göndericinin kimliğini belirleme konularında güvenilir üçüncü bir kişiye, sertifika hizmet sağlayıcılarına ihtiyaç duyulmuştur. Sertifika hizmet sağlayıcıları, kullanılan ve aleni olan açık anahtarın belirli bir kişiye ait olduğunu sertifika hizmetleri sayesinde üçüncü kişilere temin ederler. Böylece *açık ve gizli anahtar, sertifika hizmet sağlayıcıları ile sertifikalar,*

elektronik ticarete güvenliğin sağlanması için gerekli alt yapıyı oluşturmaktadır<sup>16</sup>. Dijital imzaya ilişkin hukuki düzenlemelerde, sertifika hizmet sağlayıcılarının görevleri ana hatları ile, -zorunlu olmamakla beraber- anahtar çiftinin üretilmesi, anahtar çiftinin sahibinin kimliğinin güvenilir şekilde tespiti, gizli anahtarın teslimi, açık anahtarın sahibine izafesinin sağlanması ve bu izafenin, herkesin her zaman telekomünikasyon bağlantıları vasıtasıyla tetkik edebileceği bir imza anahtarı sertifikası ile teyid edilmesi olarak sayılmaktadır<sup>17</sup>.

## II. DİJİTAL İMZA İLE İLGİLİ HUKUKİ DÜZENLEMELER VE ÇALIŞMALAR

### 1. UNCITRAL Elektronik Ticaret Model Kanunu ve UNCITRAL Elektronik İmza Model Kanunu Tasarısı

#### A . Uncitral Elektronik Ticaret Model Kanunu<sup>18</sup>

Birleşmiş Milletler Uluslararası Ticaret Hukuku Komisyonu'nun (UNCITRAL) hazırlamış olduğu Elektronik Ticaret Model Kanunu Tasarısı, 16 Aralık 1996 tarihinde Birleşmiş Milletler Genel Kurulu'nda kabul edilmiştir. Model Kanun iki tespitten hareket etmektedir. Bunlardan birincisi, modern iletişim araçlarının (e-posta, elektronik veri değişimi-elektronik data interchange-EDI)<sup>19</sup> kullanımının arttığı ve internetin artan kullanım imkanları dolayısıyla bu alanda büyük bir gelişimin beklendiğidir. İkinci tespit ise, hukuken önem arz eden bilgilerin elektronik olarak iletilmesinin, bu tür mesajların kullanımındaki hukukî engeller ve bunların hukuki etki ve geçerlilikleri konusundaki belirsizlikler nedeniyle güçlük arz ettiğidir. Model Kanun'un amacı bu hukukî engelleri kaldırmak ve elektronik ticaret alanında güvenli bir hukukî ortam sağlamaktır<sup>20</sup>. Model Kanun her ülke tarafından aynen veya değiştirilerek ulusal hukuka aktarılabilir<sup>21</sup>.

<sup>16</sup> Taupitz/Kritter, s.845.

<sup>17</sup> Kindt, s.33. Sertifika, sertifika hizmet sağlayıcılarının imzasıyla donatılmış dijital bir kimlik belgesidir.

<sup>18</sup>UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 (<http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm>)

<sup>19</sup> "Elektronik veri değişimi (EDI), bir bilginin, üzerinde mutabakata varılan standartlara uygun olarak, bir bilgisayardan diğerine elektronik olarak transferidir." Model Kanun mad.1 (b). Daha fazla bilgi için bkz. Guide Nr. 33-34.

<sup>20</sup> Guide, Nr.2.

<sup>21</sup> Nitekim 1999'un ortalarında ilk olarak Güney Kore, Singapur ve ABD'de Illionis eyaletinde, bu Model Kanun, ulusal Kanun olarak kabul edilmiştir. Bernstorff, v. Ch. G.: Ausgewählte Rechtsprobleme im Electronic Commerce, RIW 2000, s.15.

Model Kanun iki bölümden oluşmaktadır. Birinci bölümde genel olarak elektronik ticaret, daha az kapsamlı olan ikinci bölümde ise mal taşımacılığına ilişkin özel hükümler yer almaktadır. İkinci bölümde yer alan hükümler, şimdiye kadar kâğıda dayalı olarak yapılan bir takım işlemlerin (malın nitelik ve değerinin bildirilmesi, fatura ibrazı, sözleşme şartlarının bildirilmesi, hasar bildirimini gibi) veri mesajı ile yapılması hususlarını içermektedir (mad. 16-17).

Model Kanun'da, bu Kanun'a ilişkin hükümlerin ticari faaliyetler sahasında kullanılan veri mesajı şeklindeki her türlü bilgiye uygulanacağı belirtilmektedir (mad. 1). Veri mesajının tanımı ise, Kanun'un 2'inci maddesinin 1'inci fıkrasında verilmiştir. Buna göre, "*veri mesajı, elektronik, optik veya benzeri araçlarla yaratılan, gönderilen, alınan ya da kaydedilen bilgidir; veri mesajı, elektronik veri değişimi (EDI), e-posta, telgraf, telex ya da telefaxla sınırlı değildir*". Kanun'un 11'inci maddesine göre, taraflar aksini kararlaştırmadığı sürece, veri mesajı yoluyla, sözleşmenin kurulmasına ilişkin icap ve kabul beyanında bulunabilir; bu yolla kurulan bir sözleşme, sırf veri mesajı yoluyla kuruldu diye geçersiz sayılamaz ve yerine getirilmesinden kaçınılamaz. Yine Kanun'un 5'inci maddesine göre, elektronik beyanların, sadece elektronik yolla ifade edilmeleri sebebiyle, hukukî etki ve geçerliliği ve icra edilebilirliği engellenemez.

Model Kanun'un 6 ve 7'inci maddeleri yazılı şekil ve imza hususlarını ele almaktadır. 6'ncı maddeye göre, ulusal hukukun bir beyan için yazılı şekli şart koştuğu durumlarda, bu şekil şartı bu beyan daha sonra referans amacıyla erişilebilir olduğu sürece, veri mesajı yoluyla da yerine getirilebilir. Buradaki "erişilebilirlik" sözcüğü, bilgisayar verisi şeklindeki bilginin, okunabilir ve yorumlanabilir olması, bu bilginin okunabilmesi için gerekli olan yazılımın (software) muhafaza edilmesi anlamında kullanılmıştır<sup>22</sup>. Madde 7 ise, elektronik imzanın, güvenilir bir şifreleme yöntemi kullanılması şartıyla el yazısıyla imzaya eşdeğer olduğunu ifade etmektedir. Bu maddeye göre, (ulusal) hukukun kişinin imzasını şart koştuğu durumlarda, göndericinin kimliğini tespit eden ve bu kişinin veri mesajının muhtevasını kabul ettiğini gösteren bir yöntemin kullanılması halinde imza şartı yerine getirilmiş sayılacaktır [mad. 7 (1) (a)]. Özel bir yöntem Kanun'da belirlenmemiştir. Bununla beraber, bu yöntemin, tüm hal ve şartlar dikkate alındığında (sözleşme şartları da dahil), veri mesajının hazırlanma ve gönderiliş amacını gerçekleştirecek ölçüde güvenilirlik taşıması gerekir.

Kanun'un 13'üncü maddesi veri mesajının göndericiye izafesini, 14'üncü maddesi göndericinin alıcıdan teyit talep ettiği ya da tarafların veri

<sup>22</sup> Guide, Nr.50.

mesajının teyit edilmesini kararlaştırdıkları durumları, 15'inci madde ise veri mesajlarının gönderme ve varma anını düzenlemektedir.

### B. UNCITRAL Elektronik İmza Model Kanun Tasarısı<sup>23</sup>

Milletlerarası Ticaret Komisyonu'nun Elektronik Ticaret Çalışma Grubu tarafından, Elektronik Ticaret Model Kanunu'nda benimsenen yaklaşımlar esas alınarak, grubun 31-37'inci oturumlarında, bir Elektronik İmza Model Kanun Tasarısı hazırlanmıştır. Bu Tasarı'nın, Tasarı'ya eşlik eden (Grubun 38'inci oturumunda çalışmalarını tamamlamış olduğu) Rehber Tasarısı'yla birlikte Viyana'da 25 Haziran – 13 Temmuz 2001 tarihleri arasında yapılacak olan oturumda (gözden geçirilmesi ve kabulü amacıyla), Milletlerarası Ticaret Komisyonu'na sunulması gerekmektedir<sup>24</sup>.

Tasarı'da (mad. 1), Elektronik Ticaret Model Kanunu'nda olduğu gibi, bu Kanun'un, elektronik imzanın ticari faaliyetlerde kullanılması durumunda uygulanacağı belirtilmiş ve Kanun hükümlerinin tüketicinin korunmasıyla ilgili kuralları yürürlükten kaldırmadığı hususu ifade edilmiştir. Tasarı'da elektronik imza teknolojileri açısından tarafsızlık ilkesi (ortamın tarafsızlığı ilkesi) benimsenmiştir (mad. 3). Tasarı'ya göre, elektronik imza "*bir veri mesajına eklenen veya bununla mantıksal bir bağlantı içerisinde olan; veri mesajıyla bağlantılı olarak imza sahibinin kimliğinin tespitini mümkün kılan ve imza sahibinin veri mesajının muhtevasını kabul ettiğini gösteren elektronik verilerdir*" [mad. 2 (a)]. Elektronik Ticaret Model Kanunu'nun "elektronik imzada kullanılan yöntemin güvenilirliğine dair" hükmü<sup>25</sup>, Tasarı'nın 6'ncı maddesinin (1)'inci paragrafına aynen alınarak, söz konusu maddenin (3)'üncü paragrafında, bu güvenilirliğin kabul edilme şartları sayılmıştır. Bu şartlar arasında, elektronik imzayı yaratan verinin (signature creation data), imzanın atılması anında, sadece imza sahibinin kontrolü altında bulunması, imzalamadan sonra da elektronik imzadaki herhangi bir değişikliğin tespit edilebilirliği ve bilginin muhtevasının bütünlüğünün, imzadan sonra bu muhtevada yapılacak değişikliğin tespitini mümkün kılacak derecede sağlanması olarak sayabiliriz [mad. 6 (3) (a) (b) (c) (d)]. Bu şartların, aşağıda ele alınacak olan Avrupa Birliği'nin Elektronik İmza Yönergesi'nde yer alan "gelişmiş elektronik imzanın (fortgeschrittene elektronische Signatur)" tanımı ile paralellik arz ettiği görülmektedir<sup>26</sup>. Tasarı'da, sözü edilen şartların, kişilerin [(1) 'inci paragraftaki çerçevede], elektronik imzanın güvenilirliğini başka bir şekilde gerçekleştirme veya elektronik imzanın güvenilir olmadığını ispat etme imkanını ortadan kaldırmadığı belirtilmektedir [mad. 6 (4)].

<sup>23</sup> UNCITRAL Draft Model Law on Electronic Signatures with Draft Guide to Enactment 2001, ([http://www.uncitral.org/english/workinggroups/wg\\_ec/wp-88e.pdf](http://www.uncitral.org/english/workinggroups/wg_ec/wp-88e.pdf))

<sup>24</sup> Model Kanun Tasarısı, s.1, Nr.1-2.

<sup>25</sup> Model Kanun Tasarısı, mad. 7 (1) (b).

<sup>26</sup> Gelişmiş elektronik imza kavramı için bkz. aşağıda II 2 B.

Tasarı'nın 8'inci maddesinde imza sahibinin, 9'uncu maddesinde sertifika hizmet sağlayıcılarının, 11'inci maddesinde ise üçüncü kişinin (güvenen taraf-relying party) yükümlülükleri sayılmıştır. Söz konusu yükümlülükler, elektronik imza sahibinin bu imzayı kullanırken ve şayet sertifikaya dayalı olarak bir imza kullanıyorsa sertifika alırken<sup>27</sup>; sertifika hizmet sağlayıcısının hizmetlerini yerine getirirken<sup>28</sup>; sertifikaya güvenen üçüncü kişilerin elektronik imzayı ve sertifikayı kontrol ederken göstermek zorunda oldukları özen yükümlülükleridir<sup>29</sup>. Elektronik imza sahibi, sertifika hizmet sağlayıcıları ve üçüncü kişiler, bu yükümlülüklerin yerine getirilmesindeki ihmallerinden sorumlu tutulmuşlardır [mad. 7 (2) ; mad. 9 (2); mad. 11].

Tasarı'nın 12'nci maddesinde ise yabancı menşeli sertifika ve elektronik imzaların tanınmasına ilişkin şartlar belirlenmiştir.

## 2. Avrupa Birliği Yönergeleri

### A. 2000/31 sayılı ve 8 Haziran 2000 tarihli Elektronik Ticaret Hakkındaki Avrupa Birliği Yönergesi<sup>30</sup>

Avrupa Birliği üyesi ülkelerin 16. 1.2002 tarihine kadar iç hukuka uyarlamak zorunda olduğu Elektronik Ticaret Yönergesi'yle, Avrupa iç

<sup>27</sup> Elektronik imza sahibinin yükümlülükleri, özetle, elektronik imza yaratma verisinin (signature creation data) yetkisiz kullanımını engelleme konusunda makul bir özen gösterme; imza yaratma verisinin tehlikede olması halinde üçüncü kişiyi (güvenen taraf-relying party) ya da sertifika hizmet sağlayıcısı gibi kişileri gecikmeksizin durumdan haberdar etme; bir sertifikanın kullanılması durumunda, sertifikanın ihtiva ettiği ya da sertifikanın geçerliliği süresince bildirdiği hususların doğruluğunu ve eksiksiz olmasını sağlama konusunda makul bir özen gösterme olarak sayılmıştır [mad.8 (a) (b) (c)].

<sup>28</sup> Sertifika hizmet sağlayıcıları için, hizmetlerini gerçekleştirmede güvenilir sistem, usul ve insan kaynakları kullanma gibi [mad.9 (a) (f)] genel davranış yükümleri yanında, üçüncü kişilere ve imza sahibine karşı, sertifika hizmetleri ile ilgili olarak bir dizi yükümlülük öngörülmüştür. Üçüncü kişilere karşı yerine getirmesi gereken yükümlülükler arasında, *sertifika hizmet sağlayıcısının kimliğini, imza yaratma verisinin sertifikaya verildiğinde sertifikaya adına düzenlenen kişinin kontrolünde olduğunu, imza yaratma verisinin, sertifika düzenlendiğinde geçerli olduğunu* üçüncü kişinin sertifikadan tespit edebileceği makul vasıtaları sağlama yükümlülüğü olarak sayabiliriz [mad.9 (1) (c)]. Öte yandan Tasarı'ya göre, sertifika hizmet sağlayıcıları, -bu türden bir hizmet sundukları takdirde- elektronik imza sahiplerine, örneğin elektronik imza yaratma verisinin kaybı halinde gerekli ihbarda bulunabilmeleri için imkan sağlamalı, 24 saat hizmet veren bir iptal servisinin bunların emrine amade olmasını temin etmelidir [mad.9 (e)].

<sup>29</sup> Tasarı'da üçüncü kişilerin yükümlülükleri, elektronik imzanın güvenilirliğini kontrol etme hususunda makul tedbirler alma; elektronik imzanın sertifikaya dayalı olarak kullanılması halinde sertifikanın geçerliliğini, askıya alınma veya iptal edilme durumlarını kontrol etme ve sertifikadaki herhangi bir sınırlamayı dikkate alma olarak sayılmıştır [ mad. 11 (a) (b)].

<sup>30</sup> Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8 Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehrs"), Amtsblatt Nr.L 178, 17/07/2000 ( <http://www.dud.de/dud/documents/ecomrleu.pdf>).

pazarında elektronik ticaret için önem arz eden iktisadi ve özel hukuka ilişkin çerçeve şartlar belirlenmiştir. Yönerge'nin 9'uncu maddesi, üye ülkeleri, sözleşmelerin elektronik yolla kurulmasına ilişkin hukuki engelleri ortadan kaldırma yükümlülüğü altına sokmaktadır. Söz konusu hükme göre, üye ülkelerin sözleşmelerin kurulmasına ilişkin hukuki düzenlemelerinin, sözleşmelerin elektronik yolla kurulmasına ve bu sözleşmelerin elektronik yolla kurulmuş olmaları nedeniyle hukuki geçerlilik ve etki kazanmasına engel teşkil etmemesi gerekir<sup>31</sup>. Bununla beraber, ulusal hukuk düzenlerinin elektronik ticaretin ihtiyaçlarına uygun hale getirilmesi talebi, bazı istisnalarla yumuşatılmıştır. Taşınmazlar üzerinde hak tesis eden ya da devreden sözleşmeler (kira hariç olmak üzere); mahkemelerin, resmi makamların ya da kamu yetkisi icra eden meslek sahiplerinin iştiraki gereken sözleşmeler; kefalet ve kişilerin sımai, ticari ya da mesleki faaliyeti dışında akdettiği teminat sözleşmeleri ile aile hukuku ve miras hukuku alanlarına ilişkin sözleşmeler söz konusu hükmün dışında kalmaktadır.

#### **B. 1999/93 sayılı ve 13 Aralık 1999 tarihli, Elektronik İmzanın Müşterek Çerçeve Şartlarının Belirlenmesi Hakkındaki Avrupa Birliği Yönergesi<sup>32</sup>**

Elektronik İmza Yönergesi'nin amacı, Topluluk içinde elektronik imzanın kullanımı ve hukuken tanınmasını sağlamaktır<sup>33</sup>. Söz konusu Yönerge'de, elektronik imzaların hukuken tanınmasına ve sertifika hizmet sağlayıcılarının akreditasyonuna ilişkin farklı kuralların elektronik ticaret ve iletişim için ciddi bir engel teşkil edebileceği, üye devletlerin hukuki düzenlemelerinin, mal ve hizmetlerin iç pazarda serbest dolaşımını engellememesi gerektiği tespiti yapılmaktadır. Yönerge'deki açıklamalara göre, elektronik imzaya ilişkin sarih ve müşterek çerçeve şartlar, yeni teknolojilere güven duyulmasını ve bunların genel kabul görmesini sağlayacaktır<sup>34</sup>.

Söz konusu Yönerge'nin 19 Temmuz 2001 tarihine kadar üye ülkelerin iç hukuklarına uyarlanması gerekmektedir (mad. 13/fk.1).

Yönerge, elektronik imza olarak, "gelişmiş elektronik imzayı (fortgeschrittene elektronische Signatur)" esas almaktadır. Gelişmiş elektronik imzanın; 1) Sadece imza sahibine izafe edilebilmesi, 2) İmza

<sup>31</sup> Benzer hüküm, Elektronik Ticaret Model Kanunu'nun 5'inci maddesinde yer almaktadır.

<sup>32</sup> Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13 Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt Nr. L 013, 19/01/2000, s. 0012-0020 ([http:// www.dud.de/dud/documents/eur/1299.zip](http://www.dud.de/dud/documents/eur/1299.zip)).

<sup>33</sup> Richtlinie, Nr. 16 .

<sup>34</sup> Richtlinie, Nr. 4.

sahibinin kimliğinin tespitini mümkün kılması, 3) İmza sahibinin sadece kendi kontrolü altında tutabileceği vasıtalarla yaratılması 4) İlişkin olduğu verilerle, sonraki bir değişikliğin tespitini mümkün kılacak derecede bağlantı içerisinde olması gerekir (mad.2/fk.2). Yönerge'nin 5'inci maddesine göre, üye ülkelerin, nitelikli bir sertifikaya (qualifiziertes Zertifikat)<sup>35</sup> dayanan ve güvenli bir imza aracı (sichere Signaturerstellungseinheit)<sup>36</sup> ile yaratılmış gelişmiş elektronik imzaların, el yazısı ile imza ile eşdeğer tutulmasını sağlaması gerekir. Böylece, nitelikli bir sertifikaya dayanan gelişmiş elektronik imzayla donatılmış bir belge, yazılı şeklin şartlarını yerine getirmiş sayılacaktır. Yönerge'nin 5'inci maddesinde, bundan başka, üye ülkelere, elektronik imzanın davada ispat aracı olarak tanınmasını sağlama yükümlülüğü getirilmiştir.

Nitelikli sertifikaların sahip olması gereken unsurlar Yönerge'nin I no'lu ekinde, nitelikli sertifika düzenleyen sertifika hizmet sağlayıcılarının yerine getirmesi gereken şartlar II no'lu ekte, güvenli imza araçlarının taşıyacağı özellikler ise III no'lu ekte sayılmıştır. Ek IV'de ise, güvenli bir imza doğrulama işlemi için dikkat edilmesi gereken hususlar belirtilmiştir. Söz konusu ekler, nitelikli bir sertifikaya dayanan gelişmiş elektronik imzanın, tekniğe, organizasyona ve alt yapıya ilişkin –ayrıntılı olmamakla beraber- esaslı şartlarını içermektedir. Yönerge'yle, üye devletlerin, kamusal sahada elektronik imzanın kullanımını ek şartlara tâbi tutabileceği belirtilmiştir ( mad. 3 /fk.7 ).

Yönerge'nin 3'üncü maddesinin ilk fıkrasında, üye ülkelerin, sertifika hizmetlerinin sunumunu önceden verilecek bir izne tâbi tutamayacağı belirtilmiştir. Bununla birlikte, üye ülkelerin, sertifika hizmetlerinin standartını yükseltmek amacıyla isteğe bağlı bir akreditasyon sistemi getirilebilecekleri ifade edilmiştir ( mad. 3 /fk.2 ). Bunun yanında, madde 3, fıkra (3)'de, nitelikli sertifika hizmet sağlayıcılarının denetimine ilişkin hukuki düzenlemelere temel teşkil edebilecek bir hüküm öngörülmüş; madde 6'da da, nitelikli sertifika hizmet sağlayıcılarının sertifika hizmetlerinden dolayı sertifikaya güvenen kişilere karşı verdikleri

<sup>35</sup> Mad. 2 Nr. 9'a göre, sertifika, "imza doğrulama verisiyle bir kişiye izafe edilen ve bu kişinin kimliğini teyid eden bir elektronik belgedir". Nitelikli sertifika ise, mad. 2 Nr. 10'a göre, "Yönerge'nin II no'lu ekinde yer alan şartları yerine getiren bir sertifika hizmet sağlayıcısı tarafından düzenlenmiş olan ve I no'lu ekte yer alan şartlara uygun olan bir sertifikadır".

<sup>36</sup> İmza yaratma verisi, mad. 2 Nr. 4'e göre "imza sahibi tarafından elektronik imzanın yaratılması için kullanılan kod ya da gizli anahtar gibi eşi olmayan verilerdir". İmza aracı, mad. 2 Nr. 5'e göre, "imza yaratma verisinin kullanımı amacıyla hizmet eden yazılım (software) veya donanımdır (hardware)". Güvenli imza aracı ise mad. 2 Nr. 6'ya göre "ek III'ün şartlarını taşıyan bir imza aracıdır".

İmza doğrulama verisi ise mad. 2 Nr. 7'ye göre, "elektronik bir imzanın tetkiki için kullanılan, açık anahtar veya kod gibi verilerdir". İmza doğrulama aracı ise aynı şekilde, mad. 2 Nr. 8'e göre, "imza doğrulama verisinin kullanımı amacıyla hizmet eden yazılım (software) veya donanımdır (hardware)".

zararlardan dolayı sorumlulukları kapsamlı şekilde düzenlenmiştir<sup>37</sup>. Yönerge'nin 7'inci maddesi ise, Avrupa Birliği üyesi olmayan bir ülkede yerleşik olan sertifika hizmet sağlayıcılarının düzenlemiş olduğu nitelikli sertifikaların tanınmasına ilişkin hususları ele almaktadır. Yönerge'de, elektronik imza ürünlerine ilişkin teknik norm ve kriterlerin, bir "elektronik imza alt komisyonu" tarafından somutlaştırılacağı ifade edilmektedir (mad. 9-10).

### **3. 16 Mayıs 2001 tarihli Alman Elektronik İmza Kanunu ve 13 Temmuz 2001 tarihli, Özel Hukukun Şekle İlişkin Hükümlerinin Modern Hukuki İlişkilere Uyarlanması Hakkındaki Alman Kanunu**

#### **A. 16 Mayıs 2001 tarihli Alman Elektronik İmza Kanunu<sup>38</sup>**

Almanya'da, Avrupa Birliği'nin yukarıda ele alınan Elektronik İmza Yönergesi'ni iç hukuka uyarlamak amacıyla, yeni bir Elektronik İmza Kanunu hazırlanmıştır. Yeni Elektronik İmza Kanunu, 22 Mayıs 2001 tarihinde yürürlüğe giren "Elektronik İmzanın Çerçeve Şartları ve Diğer Hükümlerin Değiştirilmesi Hakkındaki Kanun'un" 1'inci maddesinde yer almaktadır. Bu yeni Kanun'la, 28 Temmuz 1997 tarihli "Dijital İmza Kanunu"<sup>39</sup> yürürlükten kalkmaktadır (mad.5) .

Elektronik İmza Kanunu'nda, Avrupa Birliği Elektronik İmza Yönergesi'nde (mad.5) el yazısı ile imzayla eşdeğer tutulması ve ispat vasıtası olarak tanınması gerektiği belirtilen, "nitelikli bir sertifikaya dayanan ve güvenli bir imza aracı tarafından yaratılan gelişmiş elektronik imzanın" benimsenmiş olduğu görülmektedir. Söz konusu gelişmiş elektronik imza, Alman Elektronik İmza Kanunu'nda nitelikli elektronik

<sup>37</sup> Söz konusu hükme göre , sertifika hizmetleri sağlayıcısı, nitelikli sertifikanın düzenlenmesi anında sertifikadaki bilgilerin doğru olmaması veya sertifikanın, nitelikli sertifikalar için öngörülen tüm hususları ihtiva etmemesi; sertifikada bildirilen imza doğrulama verisine (açık anahtar) uygun imza yaratma verisinin (gizli anahtar), sertifikanın düzenlenmesi anında, nitelikli sertifikada ismi yazılı imza sahibinin zilyetliğinde olmaması; sertifika hizmet sağlayıcısının hem imza yaratma verisini hem de imza doğrulama verisini ürettiği durumlarda, her ikisinin birbirini tamamlar şekilde kullanılmaması; sertifikanın iptal edilmesi durumunda bunun kayda geçmiş olmaması nedeniyle doğan zararlardan sorumludur. Son iki durumda, sertifika hizmet sağlayıcısına kusurlu olmadığını ispat ederek sorumluluktan kurtulma imkanı tanınmıştır. Bundan başka, söz konusu hükümde nitelikli sertifikada, sertifika kullanım sınırlandırmasına ilişkin kayıtların yer alabileceği, bu takdirde sertifika hizmet sağlayıcısının bu sınırın aşılmasından doğan zararlardan sorumlu olmayacağı belirtilmiştir (mad. 6 /fk. 3-4).

<sup>38</sup> Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16.05 2001, BGBI. 2001, Teil I, Nr.22, s.876 vd. (<http://www.parlamentsspiegel.de> web sayfasındaki "Bundesgesetzblatt" tarama motoru vasıtasıyla temin edilebilir).

<sup>39</sup> Eski Alman Elektronik İmza Kanunu hakkında bilgi için bkz. Keser-Berber, s. 510 vd.

imza (qualifizierte elektronische Signatur) olarak adlandırılmıştır (§ 2 /Nr. 3).

1997 tarihli eski Elektronik İmza Kanunu'nun 4'üncü paragrafının 2'inci fıkrasına göre, özel anahtarın gizliliğinin sağlanması ve bunların kopyalanmaması zorunluydu; Kanun, chip karta, dolayısıyla donanıma (hardware) dayalı bir dijital imza sistemini benimsemişti. Buna karşılık, 2001 tarihli Elektronik İmza Kanunu'nda, Elektronik İmza Yönergesi'ne (mad. 2 /Nr. 5) paralel olarak, kart okuyucusuna gerek olmayan, bu nedenle de ucuz mal olan, yazılıma (software) dayalı imza sistemini de caiz kılan bir düzenleme getirilmiş gibi gözükmemektedir.<sup>40</sup> Zira Kanun'a göre, güvenilir imza araçları (sichere Signaturerstellungseinheiten), "en azından ..... hükümlerinde öngörülen şartlara uygun olan ve nitelikli elektronik imza için gerekli anahtarın kaydedilmesi ve kullanımı için zorunlu olan yazılım (software) ya da donanım (hardware) araçlarıdır (§ 2/ Nr.10).

Yeni Elektronik İmza Kanunu, Elektronik İmza Yönergesi'nin 3'üncü maddesinin 1'inci fıkrasını göz önünde tutarak, eski Elektronik İmza Kanunu'nun aksine, sertifika hizmetleri işletmeciliğini izne tâbi tutmamıştır<sup>41</sup>. Bununla birlikte Kanun, sertifika hizmet sağlayıcılarına, en geç faaliyete başladıkları anda, yetkili makamlara bu hususu bildirme yükümlülüğü getirmiştir (§ 4/fk. 3). Kanun hükümlerine göz atıldığında, bunların nitelikli sertifika düzenleyen sertifika hizmet sağlayıcılarını esas aldığı görülmektedir. Nitekim Kanun'da sertifika hizmet sağlayıcıları, "nitelikli sertifika ya da nitelikli zaman kaşesi düzenleyen gerçek ya da tüzel kişilerdir" şeklinde tarif edilmiştir (§ 2/Nr. 8).

Diğer taraftan Kanun'da, sertifika hizmetlerindeki güvenlik standartının artırılması açısından, isteğe bağlı 'Akreditasyon' sistemi (freiwillige Akreditierung) getirilmiştir (§ 15 ve § 16)<sup>42</sup>. Bu sistemde, yüksek seviyede

<sup>40</sup> Sieber, S/Nöding, T.: Die Reform der Elektronischen Unterschrift, ZUM 2001, s.202.

<sup>41</sup> Eski Elektronik İmza Kanunu'na göre (SigG § 4 Nr. 1), sertifika hizmetleri işletmeciliği lisansa tabi tutulmuştur.

<sup>42</sup> Türkiye'de de, dijital imzaya ilişkin alt yapı çalışmaları tamamlanıp sertifika hizmetleri işletmeciliği için bir akreditasyon sistemi kabul edildiği takdirde, bu sisteme temel teşkil edecek bir kanun ve bu Kanun'a dayalı olarak kurulmuş Türk Akreditasyon Kurumu mevcuttur. Bkz. 27.10.1999 tarih ve 4457 sayılı Türk Akreditasyon Kurumu Kuruluş ve Görevleri Hakkında Kanun, RG. 4 Kasım 1999, S. 23866, s.1 vd. Söz konusu Kanun'un 1'inci maddesine göre " Bu Kanun ile, laboratuvar, belgelendirme ve muayene hizmetlerini yürütecek yurt içi ve yurt dışındaki kuruluşları akredite etmek, bu kuruluşların belirlenen ulusal ve uluslararası standartlara göre faaliyetlerde bulunmalarını ve bu suretle ürün/hizmet, sistem, personel ve laboratuvar belgelerinin ulusal ve uluslararası alanda kabulünü temin etmek amacıyla, merkezi Ankara'da olmak üzere Başbakanlıkta ilgili, özel hukuk hükümlerine tabi, tüzel kişiliği haiz, idari ve mâli özerkliğe sahip, Türk Akreditasyon Kurumu, kısa adı TÜRKAK kurulmuştur".

güvenlik standartlarına sahip “sertifika hizmeti sunanlar”, yetkili makam tarafından düzenlenen bir akreditasyon sertifikası almaktadır.

Sertifika hizmet sağlayıcıları bir ayırım gözetilmeksizin, § 19’a göre, faaliyetlerine başladıkları andan itibaren yetkili makamın denetimine tâbidirler. Bu paragrafta belirtilen hal ve şartlar altında, bu makamlar sertifika hizmeti sunanların faaliyetlerinin devamını geçici olarak ya da kısmen veya tamamen yasaklayabilmektedir<sup>43</sup>.

Ayrıca Kanun’da, sertifika hizmet sağlayıcılarının, örneğin; sertifikanın verilmesi (§ 5) ve blokajına ilişkin yükümlülükleri (§ 8), imza anahtarı sahibini bilgilendirme yükümlülüğü (§ 6), Kanun ve Tüzüğe (Verordnung) göre gerçekleştirmek zorunda olduğu güvenlik standartlarına ilişkin belgeleme yükümlülüğü (§ 10) ve kişisel verileri koruma yükümlülüğü (§14) ayrıntılı olarak düzenlenmiştir.

Kanun’un 11’inci paragrafında sertifika hizmet sağlayıcılarının nitelikli bir sertifikaya, nitelikli bir zaman kaşesine ya da sertifika listesi hizmetleriyle vermiş olduğu bilgilere güvenen üçüncü kişilere karşı sorumluluğu düzenlenmiştir. Sertifika hizmet sağlayıcıları söz konusu sorumluluktan kusursuzluklarını ispat ederek kurtulabilirler (§ 11/fk.2)<sup>44</sup>. Elektronik İmza Yönergesi, bu konuda bir uyarılma zorunluluğu öngörmediği halde, sertifika hizmet sağlayıcılarının, bu Kanun ve Tüzük’e (Verordnung) göre yükümlü oldukları ödevlerin yerine getirilmesinde kullandıkları yardımcı kişilerin davranışlarından dolayı sorumluluktan kurtuluş kanıtı getirme imkanı tanınmamıştır. Ancak bu düzenleme, sadece belirli yardımcı şahıslara münhasırdır (§ 11/fk. 4). Bu kişiler, sertifika hizmet sağlayıcılarının, § 4 fk. 5’ e göre ödevlerini devrettiği kişiler ile § 23 fk. 1 Nr. 2’ye göre kefil olduğu sertifikaları düzenleyen -Avrupa Birliği’ne üye olmayan üçüncü bir ülkede yerleşik- sertifika hizmet sağlayıcılarıdır. Diğer yardımcı kişiler için ise, sertifika hizmet sağlayıcıları, BGB § 831 çerçevesinde, “yardımcı kişilerin seçiminde, denetlenmesinde ve gerekli araçları temin etmede gerekli özeni gösterdiğini veya böyle bir özeni

<sup>43</sup> Bunun yanında, söz konusu makamlar, sertifikanın ya da elektronik imzanın güvenilirliğini ortadan kaldıran hal ve şartların varlığı halinde, sertifikaları bloke edebilmektedirler (§ 19/fk.4).

<sup>44</sup> Kanun’un 11’inci paragrafının 2’nci fıkrasında, *Federal Konsey’in* (Bundesrat) görüşüne uygun olarak, haksız fiil sorumluluğundaki kusur (Verschulden) kavramı kullanılarak sorumluluğun haksız fiil mahiyeti vurgulanmak istenmiştir. Bu suretle, üçüncü kişiyi koruma etkili sözleşme konstrüksiyonu vasıtasıyla, sertifika hizmet sağlayıcısının üçüncü kişilere karşı sözleşmeden doğan sorumluluk kurallarına göre sorumlu tutulması ihtimali bertaraf edilmiştir. Bkz. *Beschlussempfehlung und Bericht des Ausschusses für Wirtschaft und Technologie*, BT, Drs. 14/5324, § 11 Abs. 2, (s. 25) (“[http:// www.bundesrat. de](http://www.bundesrat.de)” web sayfasındaki DIP arama motoru vasıtası ile temin edilebilir).

*göstermiş olsaydı bile zararın ortaya çıkacağını” ispatla sorumluluktan kurtulabilmektedir<sup>45</sup>.*

Elektronik İmza Kanunu’nda, sertifika hizmet sağlayıcısının, imza anahtarı sahibine karşı aralarındaki sözleşmeden doğan sorumluluğu bilinçli olarak düzenlenmemiştir. Bunların, bizzat ya da yardımcı kişilerin davranışları dolayısıyla Kanun ve Tüzük’ten (Verordnung) doğan yükümlülüklerini ihlal etmesi halinde doğabilecek akdî sorumluluğuna, Alman Medeni Kanunu’nun genel hükümleri (BGB §§ 276, 278) uygulanacaktır<sup>46</sup>.

### **B. 13 Temmuz 2001 tarihli, Özel Hukukun Şekle İlişkin Hükümlerinin Modern Hukuki İlişkilere Uyarlanması Hakkındaki Alman Kanunu<sup>47</sup>**

Özel Hukukun Şekle İlişkin Hükümlerinin Uyarlanması Hakkındaki Kanun, Avrupa Birliği’nin Elektronik İmza ve Elektronik Ticaret Yönergeleri de dikkate alınarak, Alman Özel Hukukunun, modern bilgi ve iletişim teknolojilerinde meydana gelen gelişimlere uyarlanmasını amaçlamaktadır.

Söz konusu Kanun’la, özel olarak elektronik iletişime yönelik bir şekil türünü düzenleyen § 126a hükmü BGB’ye eklenmiştir. Elektronik şekil (elektronische Form) olarak adlandırılan bu şekil türü, kanuni yazılı şekle (BGB §126) alternatif olarak getirilmiştir. Bu Kanun’la BGB’nin 126’ncı paragrafına eklenen 3’üncü fıkraya göre, Kanun’da aksi öngörülmediği sürece, yazılı şekil, elektronik şekle ikame edilebilir. Kanun’da elektronik şeklin caiz olmadığı istisnalar, kefalet (§ 766 BGB), borç vaadi (§ 780 BGB), borç ikrarı (§ 781 BGB) tüketici kredisi sözleşmesi (§ 4 VerbrKrG) ve kaydı hayat ile irat sözleşmesi (§761 BGB) gibi yazılı şeklin uyarı işlevinin ağır bastığı hukuki işlemlere ilişkin olarak getirilmiştir.

BGB’ye eklenen §126 a hükmüne göre, bir hukuki işlem, kanunen öngörülen yazılı şekil yerine elektronik şekle uyularak yapılmak isteniyorsa, beyan sahibi, beyanına ismini eklemeli ve bu elektronik belge, Elektronik İmza Kanunu’nda öngörülen nitelikli elektronik imza ile donatılmalıdır.

<sup>45</sup> Bu hükmün eleştirisi için bkz. **Stellungnahme des Bundesrates vom 29.09.00**, § 11, s. 4. BR Drs. 496/000 ([http:// www.bundesrat.de](http://www.bundesrat.de)” web sayfasındaki DIP arama motorundan temin edilebilir).

<sup>46</sup> Karş. **Stellungnahme des Bundesrates vom 29.09.00**, § 11, s. 4.

<sup>47</sup> **Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr**, BGBI. 2001, Teil I, Nr. 35, s. 1542 vd. (<http://www.parlamentsspiegel.de> web sayfasındaki “Bundesgesetzblatt” tarama motoru vasıtasıyla temin edilebilir).

Eğer bir sözleşme söz konusu ise, her iki tarafın da, aynı ifadeleri taşıyan bir belgeyi elektronik olarak imzalaması gerekir. Bu hükme göre, taraflardan herbirinin sadece kendi icap ya da kabul beyanını elektronik olarak imzalaması yetmemektedir. Tasarı'nın gerekçesine göre, varması gerekli irade beyanlarında, beyanın elektronik şekle uygun olarak hazırlanması yeterli değildir, beyanın aynı zamanda elektronik şekle bürünmüş olarak karşı tarafa varması gerekir. Bu nedenle, sözleşmenin diğer tarafına, elektronik şekilde imzalı olarak bütün sözleşme dökümanlarının gönderilmesi zorunludur<sup>48</sup>.

Bunun yanında, söz konusu Kanun'la BGB'ye eklenen § 126 b hükmü, bir başka şekil türü olarak, "metin şeklini (Textform)" düzenlemektedir. Bu şekil türü, imzanın aranmadığı yazılı şekli düzenleyen değişik kanun hükümlerindeki kavram kargaşası ve hukuki güvensizliği ortadan kaldırmak amacıyla getirilmiştir<sup>49</sup>. Bu hükme göre, Kanun'un metin şeklini (Textform) öngördüğü durumlarda, beyanın okunabilir yazı harfleri ile tespit edilmesi ve beyan sahibinin isminin bildirilmesi yeterlidir; imza şartı aranmaz. Bundan başka metnin tamamlandığının da anlaşılabilir olması gerekir (örneğin; metnin sonuna eklenen isim ya da scanner'le kopya edilip metnin altına yerleştirilen bir imza ile)<sup>50</sup>. Metin şekli, şeklin ispat ve uyarı fonksiyonunun söz konusu olmadığı, dökümantasyon ve karşı tarafı bilgilendirme amacının ön planda olduğu durumlar için öngörülmüştür. Bu şekil türü, el yazısı ile imza aranmadığı için, -sözlü iletişim hariç- mektup, fax, e-posta gibi her türlü iletişim yolu ile gerçekleştirilebilir.

Yazılı şekle ilişkin kanun hükümlerinde öngörülen bu değişiklikler nedeniyle, iradi şekil alanında da bir uyarılama ihtiyacı doğmuş ve Alman Medeni Kanunu'nun iradi şekli düzenleyen 127'inci paragrafı da değiştirilmiştir. Yeni düzenlemeye göre, hukuki bir işlemle *yazılı şekil* kararlaştırıldığı takdirde, aksi öngörülmediği sürece, e-posta, telefax, telex, gibi telekomünikasyon vasıtalarıyla beyanın iletilmesi yeterlidir (§127/Abs.2); imza şart değildir. Buna karşılık, beyanın sözlü şekilde iletilmesi hiçbir şekilde yeterli değildir. Böyle bir şekil türü kararlaştırıldığı takdirde, sonradan BGB § 126'ya uygun bir senedin düzenlenmesi talep edilebilir (§127/Abs.2).

Taraflar hukuki işlemin geçerliliğini *elektronik şekle* tabi tuttukları takdirde, aksi kararlaştırılmadığı sürece, Elektronik İmza Kanunu'nda öngörülmüş nitelikli elektronik imzadan başka bir elektronik imza (basit

<sup>48</sup> Kabinettsbeschluss zum Gesetz zur Anpassung der Formvorschriften des Privatrechts.... und Begründung vom 6 September 2000, zu § 126a Abs.2, s.33 (<http://www.dud.de>).

<sup>49</sup> Sieber/Nöding, s. 206.

<sup>50</sup> Begründung, zu 126b, s. 39 (bkz.dpn.48).

elektronik imza ya da Avrupa Birliği Elektronik İmza Yönergesi anlamında gelişmiş elektronik imza) kullanılabilir. Sözleşmelerde, elektronik imzalı icap ve kabul beyanlarının değişimi, iradi elektronik şekil için yeterlidir. Bu tür bir şekil kararlaştırıldığı takdirde, daha güvenilir bir ispat aracı elde etme amacıyla, hukuki işlemi tespit eden belgenin, bilahere § 126a'ya uygun bir imza (yani nitelikli elektronik imza) veya taraflardan biri için bu mümkün değilse, § 126'ya göre el yazısı ile imzalanması talep edilebilir (§127/Abs.3).

Özel Hukukun Şekle İlişkin Hükümlerinin Modern Hukuki İlişkilere Uyarlanması Hakkındaki Kanun'la yapılan değişiklikler ve getirilen yeni düzenlemeler sonucu, bundan böyle, BGB'de geleneksel yazılı şekil yanında, elektronik şekil ve metin şekli de yer almaktadır.

Bunun yanında, söz konusu Kanun'la Alman Usul Kanunu'na eklenen § 292a hükmü, elektronik imzanın muhatabı lehine, ilk görünüş ispatı prensiplerine göre bir ispat kolaylığı öngörmektedir.<sup>51</sup> Bu hükme göre, BGB §126a'da düzenlenen elektronik şekle uygun bir irade beyanının gerçekliğine dair görünüş, sadece, imza anahtarı sahibinin iradesiyle beyanda bulunduğu konusunda ciddi şüpheler uyandıran vakialarla sarsılabilir. Elektronik imzanın muhatabının, kendisine gönderilen irade beyanının gerçekliği konusundaki ilk görünüş ispatından yararlanabilmesi için, madde hükmünden anlaşıldığı üzere, elektronik imzanın, nitelikli bir elektronik imza olması gerekir; bu konudaki ispat yükü ise muhataba aittir.<sup>52</sup>

#### 4. Elektronik İmza Sahasında Sertifika Hizmetleri Hakkındaki İsviçre Federal Kanun Tasarısı<sup>53</sup>

İsviçre'de 12 Nisan 2000 tarihinde, Elektronik Sertifika Hizmetleri Hakkında Tüzük (Verordnung)<sup>54</sup> çıkarılmış, bu Tüzük 1 Mayıs 2000 tarihinde yürürlüğe girmiştir. Söz konusu Tüzük çıkarılırken Federal Konsey (Bundesrat), özellikle özel hukuk ilişkilerinde dijital imzanın tanınması (Anerkennung) ile ilgili bir tasarının kısa zamanda hazırlanacağı vaadinde bulunmuştur<sup>55</sup>. Nitekim, zaten 1'inci maddesinin ilk fıkrasında tecrübe amacıyla çıkarıldığı ifade edilen bu Tüzüğün yerine, Elektronik İmza

<sup>51</sup> İlk görünüş ispatı kavramı hakkında bilgi için bkz. Taşpınar, S.:Fiili Karinelerin İspat Yükünün Dağıtılmasındaki Rolü, AÜHFD 1996, s. 541 vd.

<sup>52</sup> Aynı zamanda bu düzenlemenin eleştirisi için bkz. Stellungnahme zum Gesetzentwurf "Formvorschriften des Privatrechts" von Gesellschaft für Informatik, DuD 2001, s.38 vd.

<sup>53</sup> Der Entwurf des Bundesgesetzes über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES), (<http://www.admin.ch>).

<sup>54</sup> Verordnung über Dienste der elektronischen Zertifizierung (<http://www.admin.ch>)

<sup>55</sup> Elektronische Signatur-elektronischer Geschäftsverkehr (Bericht des Bundesrates vom 31. Mai 2000) (<http://www.ofj.admin.ch/themen/e-commerce/vn-com-d.htm>).

Kanunu Ön Tasarısı hazırlanmıştır<sup>56</sup>. Bu Ön Tasarı, daha sonra kantonların, değişik kurum ve kuruluşların görüşleri doğrultusunda yeniden ele alınarak, “Elektronik İmza Sahasında Sertifika Hizmetleri Hakkındaki Tasarı” adı altında Parlamento’da yetkili komisyonların tetkikine sunulmuştur. Tasarı’nın kanunlaşıp yürürlüğe girmesiyle Sertifika Hizmetleri Tüzüğü yürürlükten kalkacaktır (Sertifika Hizmetleri Tüzüğü mad. 21/ fk. 2).

Tasarı, esas itibariyle Sertifika Hizmetleri Tüzüğü ile aynı muhtevaya sahiptir. Tasarı’da Tüzük’ten farklı olarak, imza anahtarı sahibinin ve sertifika hizmet sağlayıcılarının sorumluluğuna ilişkin hükümler yer almaktadır. Bundan başka Tasarı’nın sonunda, elektronik imza ve elektronik şekilde bağlantılı olarak bazı federal kanunların değiştirilmesine ilişkin bir ek yer almaktadır.

Tasarı’nın 1’inci maddesine göre, bu Kanun, sertifika hizmet sağlayıcılarının tanınma şartlarını ve bunların hak ve yükümlülüklerini düzenlemektedir. Tasarı, sertifika hizmetleri işletmeciliği için, isteğe bağlı bir tanınma sistemi (freiwillige Anerkennung) getirmiştir<sup>57</sup>. Tasarı’ya göre, ticaret siciline kayıtlı gerçek ya da tüzel kişiler sertifika hizmet sağlayıcısı olarak tanınabilirler (mad. 3/ fk. 1)<sup>58</sup>.

Sertifika hizmet sağlayıcılarının tanınabilmesi için, bunların, bu Kanun’un şartlarına göre nitelikli sertifika düzenleyebilecek ve sertifika hizmetlerini yürütebilecek durumda olması; gerekli uzmanlık bilgisi, tecrübe ve niteliğe sahip personel çalıştırması; güvenilir informatik sistemi ve ürünleri (özellikle güvenli imza aracı) kullanması; yeterli finans araçlarına ve garantilere sahip olması; tazminat taleplerini ve bu Kanun’a göre alınması gerekli tedbirlerden doğan masrafları (mad.13 / fk.2 ve 3) karşılamak amacıyla sigorta yaptırması; uygulama alanı bulabilecek hukuki düzenlemelere (özellikle bu Kanun’a ve bu Kanun’un uygulanmasını gösteren hükümlere) uyulmasını sağlaması gerekmektedir (mad. 3/fk.1).

Tanınma işleminin tanıma makamları (Anerkennungsstellen) tarafından yapılması gerekmektedir. Tanınma makamlarının da Federal Konsey (Bundesrat) tarafından yetkili kılınan Akreditasyon makamı

<sup>56</sup> Bundesgesetz über die elektronische Signatur (BGES), Vernehmlassungsvorlage, Entwurf, Januar 2001 (<http://www.admin.ch/themen/e-commerce/vn-ve-a>).

<sup>57</sup> Begleitbericht zum Entwurf (Bundesgesetz über die elektronische Signatur (BGES) (Vernehmlassungsvorlage), mad.1, Nr. 210.011 (<http://www.admin.ch/themen/e-commerce/vn/ber-a>).

<sup>58</sup> Özel hukuk tüzel kişilerinin ve gerçek kişilerin ticaret siciline kaydolunması, bunlar hakkında iftasa ve ticari defter kullanmaya ilişkin hükümlerin uygulama alanı bulması sonucunu doğurmaktadır. Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur, Art.3, Nr.2.1.2.1 (<http://www.admin.ch>).

(Akreditierungsstelle) tarafından akredite edilmesi zorunludur (mad. 2 h ve mad. 4). Gereğe'ye göre, tanıma, özel hukuka ilişkin bir hukukî işlem olup, idari bir tasarruf değildir<sup>59</sup>. Tanınmış sertifika hizmet sağlayıcıları, tanıma makamlarının denetimine tâbidirler (mad. 15).

Tasarı, sertifika hizmet sağlayıcısının yükümlülüklerini, ana hatlarıyla, Alman Elektronik İmza Kanunu'na benzer bir şekilde düzenlemektedir (mad.8-14).

Tasarı'da, Avrupa Birliği Elektronik İmza Yönergesi, mad.5 anlamında gelişmiş elektronik imzanın, yani güvenli bir imza aracına ve nitelikli sertifikaya dayanan gelişmiş elektronik imzanın benimsendiği görülmektedir (mad. 2 c). Bu imza, Tasarı'da, Alman Elektronik İmza Kanunu'nda olduğu gibi nitelikli elektronik imza (qualifizierte elektronische Signatur) olarak adlandırılmıştır.

Elektronik imzanın yetkisiz kullanımından doğan risklerin imza anahtarı sahibi ve sertifikaya güvenen üçüncü kişiler arasında dağılımı hususu, Borçlar Kanunu'na eklenmesi teklif edilen 59a maddesinde düzenlenmektedir. Tasarı'ya göre, imza aracının yetkisiz kullanımından doğan riski, esas itibarıyla nitelikli sertifikaya güvenen kişi (muhatap) taşımaktadır<sup>60</sup>. Bununla beraber, teklif edilen 59a maddesine göre, kusuru bulunduğu takdirde imza anahtarı sahibi, üçüncü kişilerin, Sertifika Hizmetleri Hakkındaki Kanun anlamında "tanınmış bir sertifika hizmet sağlayıcısının" geçerli bir nitelikli sertifikasına güvenmeleri dolayısıyla uğramış olduğu zararları tazminle yükümlüdür<sup>61</sup>. Söz konusu maddenin 2'nci fıkrasına göre, imza anahtarı sahibi, imza anahtarının gizli tutulması

<sup>59</sup> Bu nedenle sertifika hizmet sağlayıcıları ile tanıma makamları arasında çıkması muhtemel uyuşmazlıklar için adli mahkemeler görevlidir (**Botschaft**, Art.4. , Nr. 2.1.2.2).

<sup>60</sup> Ön Tasarı'nın 17'nci maddesinin 2'nci fıkrasına göre , özel anahtarın rızası dışında kullanıldığını iddia eden kişi, bunu ispatla yükümlüdür. Burada ispat yükü ters çevrilmiş olup, sertifikaya güvenerek hukukî işlem yapan üçüncü kişi, imza aracının bizzat imza anahtarı sahibi tarafından kullanıldığını değil; aksine imza sahibi imza aracının rızası dışında bir başkası tarafından kullanıldığını ispat etmek zorundaydı. İmza sahibi bu hususu ispat edemediği takdirde, yetkisiz üçüncü kişinin sertifikaya güvenen kişi ile kendi adına yapmış olduğu hukukî işlemin sonuçlarına katlanmak zorundaydı; yani, bu durumda hukukî işlemi kendisi yapmış ya da bu konuda bir temsilci atamış gibi hüküm ve sonuç doğacaktı (**Begleitbericht**, Art. 17, Nr. 210.072). Sertifika Hizmetleri Hakkındaki Kanun Tasarısı'nda ise, elektronik olarak imzalanan beyanın imza anahtarı sahibinden neşet ettiğini kabul sonucu doğuracak böyle bir düzenlemeden, bu düzenlemenin imza anahtarı sahibini çok büyük bir risk altına soktuğu düşüncesiyle kaçınılmıştır (**Botschaft**, Art. 59a, Nr. 2.2.2.3).

<sup>61</sup> **Botschaft**, Art. 59a, Nr. 2.2.2.3. Ön Tasarı'ya göre, imza anahtarı sahibi, imza aracının üçüncü kişiler tarafından rızası dışında kullanıldığını ispatlaması durumunda yapılan hukukî işlemle bağlı tutulmamakla beraber, Sertifika Hizmetleri Hakkındaki Kanun Tasarısı'yla teklif edilen OR 59a maddesindeki düzenlemede olduğu gibi, sertifikaya güvenen üçüncü kişinin, tanınmış bir sertifika hizmet sağlayıcısının geçerli bir sertifikasına güvenmekten dolayı uğradığı zararı tazminle yükümlüdür (mad. 17/fk. 2). Söz konusu sorumluluk da, bir kusur sorumluluğu şeklinde düzenlenmiştir.

için hal ve şartların gerektirdiği tedbirleri almış olduğunu ya da temyiz kudretinin eksikliği nedeniyle sorumlu tutulamayacağını ispatlayarak sorumluluktan kurtulabilir. Tasarı'nın gerekçesinde, elektronik imza kullanımında olumsuz bir etki yaratacağı düşüncesiyle imza anahtarı sahibinin sorumluluğunun bir sebep sorumluluğu şeklinde düzenlenmediği ifade edilmektedir<sup>62</sup>.

Tasarı'nın 59a maddesinin 3'üncü fıkrası, imza anahtarı sahibinin, imza anahtarını teslim ettiği kişilerin davranışlarından da sorumlu olduğunu öngörmektedir. Bu nedenle imza anahtarı sahibi, kendisinin değil üçüncü bir kişinin imza anahtarının gizli tutulmasında dikkatsiz davrandığını ileri sürerek sorumluluktan kurtulamaz<sup>63</sup>. Son fıkraya göre, imza anahtarının gizli tutulması için alınması gerekli tedbirleri, çıkaracağı bir tüzükle Federal Konsey belirler.

Tasarı'ya göre sertifika hizmet sağlayıcıları da, bu Kanun ya da (bu Kanun'a dayanılarak çıkarılacak) tüzüğün öngördüğü yükümlülüklerin yerine getirilmemesi dolayısıyla, sertifikaya güvenen üçüncü kişilerin ya da imza anahtarı sahibinin uğramış olduğu zararları tazminle yükümlüdür (mad.16). Söz konusu hüküm, tanınmak için tanıma makamına (Anerkennungsstelle) başvurmaksızın nitelikli sertifika sunan sertifika hizmet sağlayıcıları için de geçerlidir<sup>64</sup>. Burada tazmin edilmesi gereken zararların kapsamına, salt malvarlığı zararları da (reine Vermögensschäden) dahildir<sup>65</sup>.

Tasarı'nın 16'ncı maddesinin 2'nci fıkrasına göre, sertifika hizmet sağlayıcıları, bu Kanun ve Tüzük'den doğan yükümlülüklerin yerine getirildiğini ispat ederek sorumluluktan kurtulabilirler. Tasarı'nın gerekçesinde, bu hükmün bir sebep sorumluluğunu düzenlediği, sertifika hizmet sağlayıcısının ya da onun ifa yardımcılarının kusuru olmasa dahi (örneğin, hasta olma durumu) meydana gelen zarardan sorumlu oldukları; ancak bu sorumluluğun bir tehlike sorumluluğuna yol açar şekilde, sebebini etki sahası (Einflussbereich) dışında bulan (örneğin, bir virüsten korunma amacıyla sertifika listesinin kısa süreli olarak on line bağlantıya kapalı tutulması) bir zarardan dolayı sorumluluğu içermediği belirtilmektedir<sup>66</sup>. Öte yandan sertifika hizmet sağlayıcıları, kendilerinin ya da yardımcı kişilerin davranışlarından dolayı bu Kanun'dan doğan sorumluluklarını ortadan

<sup>62</sup> **Botschaft**, Art. 59a, Nr. 2.2.2.3. Söz konusu hükmün, sadece, "tanınmış bir sertifika hizmet sağlayıcısının", "nitelikli sertifikasına" güvenen üçüncü kişilerin zararından dolayı sorumluluğu düzenlediğine dikkat çekmek gerekir.

<sup>63</sup> **Botschaft**, Art. 59a, Nr. 2.2.2.3.

<sup>64</sup> **Botschaft**, Art. 16, Nr.2.1.7.1.

<sup>65</sup> **Botschaft**, Art. 16, Nr.2.1.7.1.

<sup>66</sup> **Botschaft**, Art. 16, Nr.2.1.7.1.

kaldıran anlaşmalar yapamazlar (mad. 16 /fk. 3). Dolayısıyla, bu türden kayıtlar batıldır (BK. mad. 20/fk. 1). Ancak, sertifikada bir kullanım sınırlaması (örneğin bedel üzerinden bir limit) öngörülmüşse, bu sınırlamadan sertifika hizmet sağlayıcısı da yararlanmaktadır. Dolayısıyla sertifika hizmet sağlayıcısı, bu sınırı aşan zararlardan sorumlu değildir (mad.16/fk.3).

18'inci maddeye göre, bu Kanun'dan doğan talepler, hak sahibinin zararı ve zararı tazminle yükümlü kişiyi öğrendiği andan itibaren bir yıl içerisinde, en geç zarar doğuran fiilin vukuundan itibaren 10 sene içerisinde zamanaşımına uğrar. Gerekçede, burada haksız fiillere ilişkin zamanaşımının (BK. mad. 60) iktibas edildiği, sertifika hizmet sağlayıcılarının, bu Kanun'dan bağımsız olarak sözleşmeyle üstlenmiş oldukları edimlerden (örneğin, özel anahtar için gerekli yazılımın – software- devrine ilişkin) doğan talepler hakkında BK'nun 125'inci (OR mad. 127) maddesinin uygulama alanı bulacağı belirtilmektedir<sup>67</sup>.

Sertifika Hizmetleri Hakkındaki Kanun Tasarısı, bundan başka, İsviçre Borçlar Kanunu'na eklenmesi teklif edilen mad.14 / fk. 2bis hükmüyle, elektronik imzanın el yazısı ile imza ile eşdeğer tutulmasını sağlayan bir değişiklik öngörmektedir. Bu hükme göre, *Elektronik İmza Sahasında Sertifika Hizmetleri Hakkındaki Federal Kanun* anlamında tanınmış bir sertifika hizmet sağlayıcısının nitelikli sertifikasına dayanan ve bir gerçek kişi adına düzenlenmiş olan nitelikli elektronik imza, el yazısı ile imzayla aynı hüküm ve sonuçları doğurur. Tasarı, Borçlar Kanunu'nun imzalı mektup ve telgrafın da yazılı şeklin yerini tutacağını öngören 13'üncü maddesinin 2'nci fıkrasının, gereksiz olduğu düşüncesiyle yürürlükten kaldırılmasını teklif etmektedir<sup>68</sup>. Resmî şekil ve bazı hal ve şartlar altında faximile imzayı caiz kılan hüküm (OR. Art.14/Abs.2 - BK. mad. 14/fk.2) olduğu gibi muhafaza edilmiştir.

Tasarı, elektronik imzanın caiz olmadığına ilişkin herhangi bir istisna öngörmemektedir; bu durumda alacağın temliki bile elektronik şekilde yapılabilecektir<sup>69</sup>. Tasarı, elektronik ticarete irade beyanlarının ne zaman gönderilmiş, ne zaman muhataba varmış sayılacağı hususlarını bilinçli olarak düzenlememiş; bu soruların, elektronik ticaretin gelişim ve ihtiyaçları doğrultusunda cevaplanmasını uygulamaya bırakmıştır<sup>70</sup>.

<sup>67</sup> Botschaft, Art.18, Nr. 2.1.7.3.

<sup>68</sup> Gerekçede, telgrafın artık kullanılmadığı, imzalı mektubun ise zaten OR Art. 13/1 (BK.mad. 13/1) gereği yazılı şekli yerini tutacağı, tarafların fiziki olarak aynı senedi imzalamalarının gerekmediği ifade edilmektedir. Botschaft, Art. 13 Abs.2 OR, Nr.2.2.2.1.

<sup>69</sup> Botschaft, Art.14 Abs. 2bis OR, Nr. 2.2.2.2.

<sup>70</sup> Botschaft, Nr.1.4.2.3.

Tasarı'da bundan başka, Medeni Kanun ve Borçlar Kanunu'nda, tapu sicilinin ve ticaret sicilinin elektronik olarak tutulmasına ve bunlarla elektronik iletişime hukuki temel oluşturan değişiklikler öngören hükümler yer almaktadır. Bunun yanında, Markaların Korunması Hakkındaki Tüzük'te ve Patent Tüzüğü'nde kurumlar arası elektronik iletişimi mümkün kılan mevcut hükümlerin az yada çok değiştirilerek Markaların Korunması Hakkındaki Kanun'a ve Patent Kanunu'na alınması önerilmektedir.

### 5. Türkiye'deki Çalışmalar

Türkiye'de elektronik ticaret ve dolayısıyla elektronik imza ile ilgili çalışmalar, Bilim ve Teknoloji Yüksek Kurulu ve bu Kurul'un aldığı karar neticesinde oluşturulan Elektronik Ticaret Koordinasyon Kurulu tarafından yürütülmektedir. Elektronik Ticaret Koordinasyon Kurulu, çalışmalarını, Dış Ticaret Müsteşarlığı'nın koordinasyonunda ve kamu özel sektörü ile üniversitelerin katılımıyla yürütmektedir. Çalışmalar halen devam etmektedir<sup>71</sup>.

## III. DİJİTAL İMZANIN BORÇLAR KANUNU HÜKÜMLERİ AÇISINDAN DOĞURDUĞU BAZI SORUNLAR

### 1. Dijital İmzalı Elektronik Belgelerde Şekil Sorunu

#### A. Borçlar Kanunu Hükümleri Açısından Şekil

BK. mad. 11/fk. 1'de, bütün modern hukuk sistemlerinde geçerli olan ve hukuki ilişkilerde kolaylık sağlayan "şekil özgürlüğü" prensibi hükme bağlanmıştır. Bununla beraber, bu fıkrada yer alan, "kanunda sarahat olmadıkça" çekincesinden de anlaşılacağı üzere, kanun koyucu, hukuk politikasına ilişkin bazı sebeplerden dolayı, bazı hukuki işlemleri özel bir şekle tabi tutmuştur. Aynı maddenin 2'nci fıkrasına göre, hakkında başka hüküm olmadığı sürece, kanunun belirlediği bu şekil, ispat şartı değil, geçerlilik şartıdır<sup>72</sup>. Borçlar Kanunu'nun 11'inci maddesinde "sözleşme"

<sup>71</sup> Bilgi için bkz. <http://www.e-ticaret.gov.tr/KAMU.htm>

Sermaye Piyasası Kanunu'nun, Sermaye Piyasası Kurulu'nun görev ve yetkilerini düzenleyen 22'nci maddesinin (u) bendinde, Sermaye Piyasası Kanunu'nun uygulama alanına giren işlemlerde elektronik imzanın kullanım esaslarını düzenlemek ve denetlemek, Sermaye Piyasası Kurulu'nun görev ve yetkileri arasında sayılmıştır. Söz konusu kurum nezdinde elektronik imza uygulaması henüz başlatılmamıştır.

<sup>72</sup> Bunun yanında, yazılı şeklin, belirli bir hukuki görünüşün temelini oluşturması dolayısıyla, bu hukuki görünüşe dayanarak bir hakkın kazanılmasının şartı olarak öngörüldüğü durumlar da vardır (örneğin, BK. mad. 18/fk. 2'ye göre, yazılı bir borç ikrarına dayanarak iyiniyetle alacağı devralan üçüncü kişiye karşı muvazaa iddiası ileri sürülemez). Diğer örnekler için bkz. *Digitale Signatur und Privatrecht, Gutachten des Bundesamtes für Justiz vom 24 November 1998*, <http://www.admin.ch>

kavramı kullanılmakla beraber, bu madde, kanunun geçerlilik için şekil şartı öngördüğü bütün tek taraflı (özellikle yenilik doğuran haklar) veya çok taraflı hukuki işlemlere uygulanır<sup>73</sup>. Şekle ilişkin hükümler, özellikle bu hükümlerin hukuki işlemin yazıyla tespit edilmesini şart koştuğu durumlarda, irade beyanlarında açıklık ve kesinlik sağlar ve ispatı kolaylaştırır; dolayısıyla, hukuk düzeninin hukuki güvenliği sağlama amacına hizmet eder<sup>74</sup>. Diğer taraftan, şekle ilişkin hükümler, kişileri düşüncesizce ve acelece hareket etme tehlikesine karşı koruma amacı da güderler.<sup>75</sup>

Yapılış tarzına göre, kanuni şekil esas itibarıyla üçe ayrılır: *Adi yazılı şekil* (örneğin alacağın temliki, BK. mad. 163/fk. 1; bağışlama vaadi, BK. mad. 238/fk. 1), *nitelikli yazılı şekil* (örneğin el yazısı ile vasiyetname, MK. mad. 485; kefalet sözleşmesi, BK. mad. 484) ve *resmi şekil* (örneğin taşınmaz satım sözleşmesi, BK. mad. 213/fk. 1; resmi vasiyetname, MK. mad. 479 vd.; miras sözleşmesi, MK. mad. 492).

Bunun yanında Medeni Kanun, sadece evlenme (MK. mad. 108-109) ve sözlü vasiyete (MK. mad. 486)<sup>76</sup> ilişkin olarak sözlü şekil türünü öngörmüştür.

Adi yazılı şekil için, borç altına girenlerin el yazısı ile imzası şarttır (BK. mad. 13/fk. 1; BK. mad. 14/fk. 1). Borçlar Kanunu, imzalı bir mektubun veya borçlu tarafından imzalanmış aslının PTT'ye tevdi şartıyla,

<sup>73</sup> **Kramer, Ernst. A./Schmidlin, B.:** Berner Kommentar, Das Obligationenrecht, B. VI, 1.Abt. (Allgemeine Bestimmungen), 1. Teilbd., Art. 1-18, Bern 1986, Art. 11, Nr. 175; **Merz, H.:** Vertrag und Vertragsschluss, 2. Aufl., Freiburg 1992, Nr. 348. Şekle tabi yenilik doğuran haklara, tacirler arasında, diğer tarafı temerrüde düşürme veya mukaveleyi fesih yahut ondan rücu maksadıyla yapılacak ihbar veya ihtarları (TTK mad. 20/fk. 3); şekle tabi çok taraflı hukuki işlemlere ise, kolektif şirket mukavelesini (TTK mad. 154) örnek olarak gösterebiliriz. Bunun yanında, bazen hukuki işlem mahiyetini taşımayan fiillerin de kanun tarafından şekle tabi tutulduğu görülmektedir (**Schmidlin**, Art. 11, Nr. 177-178). Örneğin, TTK. mad. 368'e göre, anonim şirketlerde, hisse senetleri nama yazılı pay sahipleri ile önceden şirkete hisse senedi tevdi ederek ikametgahını bildiren pay sahiplerine, genel kurul toplantısına çağrı taahhütlü mektupla yapılır. Bu hükme aykırılık, BK. mad. 11/fk. 2'ye göre bu toplantıda alınan genel kurul kararının butlanını değil, olsa olsa TTK. mad. 381 çerçevesinde bu kararın iptal edilebilirliği sonucunu doğurur. Bkz. **Poroy, R./Tekinalp, U./Çamoglu, E.:** Ortaklıklar ve Kooperatif Hukuku, B. 7, İstanbul 1997, s. 385'de anılan kararlar.

<sup>74</sup> **Forstmoser, P./Schluep, W. R.:** Einführung in das Recht, 2. Aufl., Bern 1998, Nr. 256 vd.

<sup>75</sup> Şeklin amaçlarına ilişkin olarak bkz. **Gauch, P./Schluep, W. R.:** Schweizerisches Obligationenrecht, Allgemeiner Teil, B. I, 5. Aufl., Zürich 1991, Nr. 497 vd.; **Schmidlin**, Art. 11, Nr. 13 vd.; **Kocayusufpaşaoğlu, N.:** Borçlar Hukuku, Genel Hükümler, s. 220; **Tekinay, S.S./Akman, S./Burcuoğlu, H./Altıp, A.:** Tekinay Borçlar Hukuku, B.7, İstanbul 1993, s.99-100; **Eren, F.:** Borçlar Hukuku, C. I, B. 6, İstanbul 1998, s.244 vd.; **Altaş, H.:** Şekle Aykırılığın Olumsuz Sonuçlarının Düzeltilmesi, Ankara 1998, s. 6 vd.

<sup>76</sup> Sözlü vasiyet, sadece başlangıç aşamasında sözlü olup, bu vasiyetin daha sonra yazıya bağlanması zorunludur (MK. mad. 487).

telgrafnamenin de yazılı şekil şartını yerine getireceğini kabul etmektedir (BK. mad. 13/ fk. 2).

İmzanın el yazısı ile atılması şartına, BK. mad. 14/fk. 2 bir istisna getirmektedir. Söz konusu hüküm, iş hayatında yerleşmiş adetlere uygun düştüğü hallerde ve özellikle çok sayıda tedavüle çıkarılan kıymetli evrakta, faximile imza kullanılmasına izin vermektedir. Bunun dışında Borçlar Kanunu, amaların imzalarının geçerli olmasını, bu imzaların usulen tasdik olunması ya da imza ettikleri zaman, belgenin muhtevasını bildiklerinin sabit olması şartına bağlamıştır (BK. mad. 14/fk. 3). Okuma yazma bilmeyenlere ise, usulüne uygun olarak tasdik edilmiş bir el işareti ya da resmi belge düzenlettirme imkanı tanınmıştır (Bk. mad. 15)<sup>77</sup>.

Bunun yanında, Borçlar Kanunu (mad. 16), tarafların anlaşarak, kanunen şekle bağlı olmayan bir hukuki işlemi belirli bir şekle tâbi tutmaları hususunu da düzenlemiştir. Borçlar Kanunu'nun 16'ncı maddesi, iradi şekil konusunda iki karine öngörmektedir. Bu maddeye göre taraflar, kanunen şekle bağlı olmayan bir hukuki işlemi şekle tâbi tutmuşlarsa, aksi anlaşılmadıkça, taraflarca kararlaştırılan şekil bir ispat şekli değil, geçerlilik şekli sayılır (BK. mad. 16/fk. 1). Yine aynı maddeye göre, iki taraf, sözleşmenin yazılı şekilde yapılmasını kararlaştırmakla beraber, yazılı şeklin nasıl bir şekil olacağını belirlemediyse, bunun yerine getirilmesine ilişkin olarak Borçlar Kanunu'nun âdi yazılı şekle ilişkin hükümleri uygulanır.

### B. Dijital İmzalı Elektronik Belgelerde Yazılı Şekil

Elektronik yolla iletilen beyanların da, beyan sahibi fiil, işlem ve beyan iradesine<sup>78</sup> sahip olduğu sürece hukuken bir irade beyanı olduğu konusunda herhangi bir şüphe yoktur<sup>79</sup>. Bu konuda elektronik yolla iletilen irade beyanının, sonradan beyan sahibi tarafından yazılı şekilde teyid edilmesinin ya da bu beyanın muhatap tarafından bilgisayarın ana belleğine ya da diskete süreklilik taşıyacak şekilde kaydedilip kaydedilmemesinin bir önemi yoktur;

<sup>77</sup> Ayrıntılı bilgi için bkz. Kocayusufpaşaoğlu, s. 230 vd.; Eren, C.1, s. 257 vd.; Oğuzman, K/Öz, T.: Borçlar Hukuku, Genel Hükümler, B.2, İstanbul 1998, s.118; Schmidlin, Art. 13 Nr. 1 vd.; Art. 15, Nr. 1 vd.; Art. 16, Nr. 1 vd.

<sup>78</sup> İrade beyanının unsurları konusunda ayrıntılı bilgi için bkz. Eren, C. I, s. 123 vd.; Kocayusufpaşaoğlu, s. 121; Tekinay/Akman/Burcuoğlu/Altop, s. 62 vd.

<sup>79</sup> Fritzsche, J. / Malzer, Hans M.: Ausgewählte zivilrechtliche Probleme elektronisch signierter Willenserklärungen, DNotZ 1995, s.17; Hohenegg, Ch./Tauschek, S.: Rechtliche Problematik digitaler Signaturverfahren, BB 1997, s. 1542; Fringuelli, P.G./Wallhäuser, M.: Formerfordernisse beim Vertragsschluss im Internet, CR 1999, s. 93; Ultsch, M.L.: Zivilrechtliche Probleme elektronischer Erklärungen, DZWIR 1997, s. 467 vd.; Mehrings, J.: Vertragsabschluss im Internet, MMR 1998, s. 31; otomotikleşmiş irade beyanlarına ilişkin tartışma için bkz. Kocayusufpaşaoğlu, s.122-123; Fringuelli/Wallhäuser, s.93; Fritzsche/Malzer, s. 7 vd.

bu hususlar sadece, bir irade beyanında bulunmuş olup olmadığının ve bunun muhtevasının ispatı ile ilgili hususlardır. Dolayısıyla, kişilerin şekil özgürlüğü prensibi çerçevesinde, kanunun geçerliliği için herhangi bir şekil öngörmediği hukuki işlemleri internet üzerinden veya diğer bir elektronik yolla yapmalarına herhangi bir engel yoktur. Sorun, kanunen yazılı şekle tâbi tutulmuş bir hukuki işlemin (özellikle sözleşmenin) internet üzerinden yapılması halinde, bu suretle yazılı şeklin şartlarının yerine getirilmiş olup olmayacağı noktasında doğmaktadır.

Elektronik şekilde imzalanmamış irade beyanları, zaten beyan sahibinin kimliğini güvenli şekilde tespiti imkan veren herhangi bir imza mevcut olmadığı için, yazılı şeklin şartlarını yerine getirmiş sayılmaz. Diğer taraftan, doktrinde, yazılı şeklin fonksiyonlarından hareketle, bir "scanner" aracılığıyla grafik şeklinde elektronik bir belgenin üzerine kopya edilen imzanın da el yazısı ile imzaya eşdeğer tutulması gerektiği yönünde bir görüş ileri sürülmekte ise de<sup>80</sup>, bu görüş haklı olarak, metinle imza arasında sıkı bir cismani bağın eksikliği sebebiyle reddedilmektedir<sup>81</sup>. Bu tür belgeler, istenilen kişinin imzasının istenilen metnin altına kopya edilmesini mümkün kılması dolayısıyla, arkada bir iz bırakmaksızın istenildiği şekilde manipülasyon yapılması imkanına açıktırlar; Bu nedenle söz konusu belgede ifade edilen irade beyanının, imzada ismi gözükken kişiye ait olduğu konusunda güvenilir bir ispat sağlamazlar. Gerçi el yazısı ile imzalı bir belgede de sahte imza atmak veya belge metnini tahrif etmek mümkündür; fakat el yazısı ile imza ve metnin, üzerinde yazıldığı şeyle olan cismani bağıllığı, genellikle bu tip manipülasyonların tespitine imkan verir. İşte klasik anlamda yazılı irade beyanları ve elektronik yolla iletilen irade beyanları bu noktada birbirinden ayrılır<sup>82</sup>.

Diğer taraftan elektronik bir belgenin, el yazısı ile imzalanması da mümkün değildir. Gerçi bir irade beyanını elektronik yolla ilettikten sonra, belgenin el yazısı ile imzalı bir örneğini posta ile göndermek imkanı mevcuttur; fakat bu imkan, elektronik ticaretin zaman, kağıt ve yerden tasarruf sağlaması, elektronik belgelerin muhafazasının daha kolay olması gibi yararları ile bağdaşmamaktadır<sup>83</sup>.

İşte elektronik belgelerdeki bu tür manipülasyonlar, elektronik ticaretin kaçınılmaz gelişimi karşısında, dijital imza tekniğiyle engellenmeye

<sup>80</sup> Ebbing, F.: Schriftform und E-mail. CR 1996, s. 275-276.

<sup>81</sup> Schippel, H.: Die elektronische Form, Festschrift für Walter Odersky, Berlin-New York 1996, s. 659; Reh binder, M./Schmaus, St.: Rechtsprobleme bei Vertragsschluss im Internet, Ufita 2000, s. 331; Koch, Fr. A.: Internet-Recht, München: Oldenburg 1998, s. 148 vd.

<sup>82</sup> Schippel, s. 659.

<sup>83</sup> Karş. Vehslage, Th.: Das geplante Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr, DB 2000, s. 1801.

çalışılmaktadır. Dijital imza teknolojisinin bugün büyük ölçüde, el yazısı ile imzanın işlevlerini yerine getirdiği ifade edilmektedir.

El yazısı ile imzanın işlevleri altı grup altında toplanmaktadır: Sonuçlandırma işlevi (Abschlussfunktion), kimliği tespit işlevi (Identitätsfunktion), gerçeklik işlevi (Echtheitsfunktion), uyarı işlevi (Warnfunktion), devamlılık işlevi (Perpetuierungsfunktion) ve ispat işlevi (Beweisfunktion). İlk dört işlev el yazısı ile imzaya özgü işlevlerdir<sup>84</sup>.

El yazısı ile imza metni örter ve imzanın üstündeki metnin imza sahibinin iradesiyle ve eksiksiz kaleme alındığını, bunun bir tasarı olmadığını gösterir. Dolayısıyla imza, üstünde yazılı beyanın hukuken bağlayıcı olduğunu, metinde sonradan yapılan değişiklik ve eklemelerin ise imza sahibi için bağlayıcı olmadığını ifade eder (Sonuçlandırma işlevi – Abschlussfunktion). Diğer taraftan imza, senedi düzenleyen kimliğini tespiti yarar (Kimliği tespit etme işlevi – Identitätsfunktion). İmza, beyanın gerçekten imza sahibinden neşet ettiğini, dolayısıyla ona ait olduğunu da temin eder (Gerçeklik işlevi – Echtheitfunktion). Bunun yanında imza, sahibini acele ve düşüncesizce hareket etmekten korur (Uyarı fonksiyonu – Warnfunktion). Öte yandan esas itibarıyla kağıda dayalı olan yazılı şekil, şekle bürünmüş hukuki işlemin her zaman okunabilirliğini ve imzanın tetkik edilebilirliğini sağlar (Devamlılık işlevi – Perpetuierungsfunktion). Bu açıdan yazılı şekil (dolayısıyla el yazısı ile imza), ispatı kolaylaştırır (İspat fonksiyonu-Beweisfunktion)<sup>85</sup>.

Dijital imza, el yazısı ile imza gibi, “sonuçlandırma” işlevini yerine getirmektedir. Dijital imza işleminde, ilk önce imzalanacak metnin tamamından, bu metnin hash değeri (mesaj özeti) elde edilmekte, daha sonra bu değer gizli anahtarla şifrelenerek imzalama prosedürü tamamlanmaktadır. Dijital imza için ilk önce metnin hazırlanması gerektiğinden ve imza prosedürü tamamen bu metin üzerinde gerçekleştiğinden, imzalanan metin ve dijital imza arasındaki bu mantıki bağ dolayısıyla, dijital imzanın “sonuçlandırma” işlevi, el yazısı ile imzadan daha kesin şekilde gerçekleşmektedir.<sup>86</sup>

<sup>84</sup> Devamlılık işlevi (Perpetuierungsfunktion) ve ispat işlevi (Beweisfunktion), aynı zamanda, yazılı şeklin senet (Urkunde) unsuruna bağlı işlevlerdir. Bkz. **Hohenegg/Tauschek**, s. 1547.

<sup>85</sup> Yazılı şeklin ve el yazısı ile imzanın işlevleri konusunda açıklamalar için bkz. **Bizer, J.:** Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 1997, s. 171; **Runge**, s. 17 vd.; **Köhler, H.:** Problematik automatisierter Rechtsvorgänge, AcP 182 (1982), s. 148 vd.; **Fritzsche/Malzer**, s. 18.

<sup>86</sup> **Runge**, s. 17-18; **Bizer**, s. 170; **Vehslage**, s. 1802; **Sieber / Nöding**, s. 204; **Begründung zu § 126 a Abs. 1**, s. 31 (bkz. yukarıda dpn. 48); **Cordes, A.:** Form und Zugang von Willenserklärungen im Internet, Münster 2001, s.133.

Dijital imza, el yazısı ile imzada olduğu gibi imza sahibinin isim ve soyadından değil, gönderilen metnin şifrelenmiş bir özetinden ibaret olduğundan, imza sahibinin kimliğinin doğrudan doğruya bu imza vasıtasıyla tespiti mümkün değildir. Bununla beraber, dijital imzada kimlik tespit etme işlevi, bir defaya mahsus alınan anahtar çiftinin, sertifika hizmet sağlayıcıları tarafından belirli bir kişiye izafesi ile sağlanmaktadır. Bu izafe, bir imza anahtarı sertifikası ile belgelenmektedir. Böylece, imza sahibinin açık anahtarını bilen muhatap, kamuya açık sertifikalar vasıtasıyla bu kişinin kimliği ve diğer hususlar hakkında (örneğin, imzanın kullanım sınırları) kesin bilgi sahibi olabilmektedir<sup>87</sup>. Almanya'da, Şekil Hükümlerinin Uyarlanması İlişkin Kanun'la getirilen hükümde, elektronik şeklin gerçekleştirilmesi için, Elektronik İmza Kanunu'na uygun bir imza şartına ek olarak, elektronik olarak iletilen beyanın sahibinin isminin de imzalanacak metne eklenmesi şart koşulmaktadır (§ 126 a BGB).

Dijital imzanın atılmasında kullanılan imza aracının (örneğin, chip kartı), yeterli güvenlik tedbirleri alınmaması durumunda üçüncü kişilerin eline geçmesi ihtimal dahilindedir. Bu kişiler PIN'i tanıdıkları veya deşifre ettikleri takdirde, anahtar sahibi adına hukuki işlem yapabileceklerdir. Bu durumda dijital imzayı fiili olarak atan kişi ile imza anahtarının sahibi olan kişi aynı değildir. Bu nedenle, Elektronik İmza Kanunlarında, yeni teknolojiyi kullanma yönünde karar alan imza anahtarı sahiplerine, bunların muhafazasına ilişkin ağırlaştırılmış özen yükümlükleri getirilmektedir<sup>88</sup>. Diğer taraftan, beyan sahibinin kimliğinin daha güvenilir şekilde tespiti için, (imza aracının kullanımında kimlik denetleyen) biometrik özellikli yöntemlere başvurulması tavsiye edilmektedir<sup>89</sup>.

Öte yandan, sahte bir kimlik belgesine dayanılarak, sertifika hizmet sağlayıcısından bir imza anahtarı sertifikası alınması ve başka bir isim altında hukuki ilişkilere iştirak edilmesi de mümkündür. Bu ihtimal, sertifika hizmet sağlayıcılarının, sertifika için başvuran kişilerin kimliğini güvenilir şekilde tespit etme yükümlülükleriyle aza indirgenmeye çalışılmaktadır. Bu tür hizmet veren işletmelerin, güvenilirlik hususunda gerçekleştirmek zorunda oldukları sıkı şartlar ve bunların hizmetlerinin denetimi de aynı amacın gerçekleştirilmesine yardımcı olacaktır<sup>90</sup>.

<sup>87</sup> Herkes bir program aracılığıyla dijital imza için gerekli anahtar çiftini üretme ve bir başka isim altında bu anahtar çiftini kullanarak internet üzerinden hukuki işlem kurma imkanına sahip olduğundan, muhatabın ya da bir makamın (örneğin mahkemelerin), imza sahibinin gerçek kimliğini tespit etmesi, sertifika hizmet sunucularının sertifika hizmetleri olmaksızın mümkün değildir.

<sup>88</sup> Örneğin, Sertifika Hizmetleri Hakkındaki İsviçre Kanun Tasarısı'na ilişkin olarak bkz. II 4

<sup>89</sup> *Begründung* zu § 126 a Abs. 1, s. 31 (bkz. yukarıda dpn.48); *Vehslage*, s. 1801.

<sup>90</sup> *Vehslage*, s. 1802; *Begründung* zu § 126 a Abs. 1, s. 31 (bkz. yukarıda dpn.48).

Diğer taraftan, bir manipulasyon durumu ortaya çıkmadığı takdirde, dijital imza, imzanın gerçekliğini, yani beyanın gerçekten imza sahibinden neşet ettiğini ve bu beyanın sonradan değiştirilmediğini göstermektedir (Echtheitfunktion). Bu işlem, dijital imza teknolojisindeki metin ve imza arasındaki sıkı mantıki bağ sayesinde temin edilmektedir. İmza sahibinin, bilgisayar ekranında görmediği bir metni imzalaması tehlikesine karşı, onun dijital imzayı güvenli bir ortamda atması gereğine işaret edilmekte ve sertifika hizmet sağlayıcıları imza anahtarları sahiplerini, alması gereken tedbirler hakkında açıkça bilgilendirme yükümü altına sokulmaktadır<sup>91</sup>. Diğer taraftan, dijital imzalı belgelerin hazırlanmasından yıllar sonra da, gerçekliğini muhafaza etmesinin gerektiği durumlar (örneğin, ticaret sicilinde) söz konusu olabilir; buna karşılık birkaç yıl sonra, daha hızlı işlemciler (Prozessor) ve gelişmiş şifre çözme teknikleriyle, daha önce usulüne uygun olarak imzalanmış bir belgenin, arkasında iz bırakmaksızın değiştirilmesi daha kolay olabilir. Bu ihtimal, uzun süre muhafazası gereken belgelerde dijital imzanın gerçeklik işlevini zayıflatmaktadır<sup>92</sup>.

Dijital imza, el yazısı ile imzanın uyarı işlevini (Warnfunktion) tam olarak yerine getirememektedir<sup>93</sup>. El yazısı ile imza, uzun bir geçmişe dayalı geleneği sayesinde, insanlarda imzalanan şeyin hukuken bağlayıcı olduğuna dair bir bilinç geliştirmiştir. Chip kartın kart okuyucusuna yerleştirilmesi - tabii imza aracı olarak chip kartının kullanımı zorunlu olduğu sürece- ve PIN girişinin yapılmasının, bilahare dijital imza prosedürünü başlatmak ve imzalı metni göndermek için birden fazla tuşa basılmasının, dijital imzada uyarı işlevi gördüğü ileri sürülmekteyse de<sup>94</sup>, bu görüş haklı olarak reddedilmektedir<sup>95</sup>. Zira, irade beyanlarını online olarak ileten kişilerin büyük çoğunluğu, bu beyanlara klasik anlamda yazılı irade beyanlarına verdikleri önemi göstermemektedirler. Dijital imzanın bağlayıcılığı hususunda kişilerin bilinç kazanması zaman alacaktır. Bu bilinç ise, dijital imza teknoloji konusunda alışkanlık ve tecrübe edinilmesiyle mümkündür.<sup>96</sup>Dijital imza ile ilgili hukuki düzenlemelerde, sertifika hizmet sağlayıcısı, sertifika düzenlenmesi için başvuran imza anahtarları sahiplerini, dijital imzanın, hukuki ilişkilerde el yazısı ile imza ile aynı etkiye sahip olduğu hususunda bilgilendirme yükümlülüğü altına sokulmaktadır.<sup>97</sup>.

<sup>91</sup> Begründung zu § 126 a Abs. 1, s. 32 (bkz. yukarıda dpn.48)..

<sup>92</sup> Sieber/Nöding, s. 204.

<sup>93</sup> Sieber/Nöding, s. 205; Kindl, s. 37; Malzer, s. 107-108; Melullis, K-J.: Zum Regelungsbedarf bei der elektronischen Willenserklärung, MDR 1994, s. 112; Cordes, s.133.

<sup>94</sup> Vehslage, s. 1802; Deville /Kalthegener, s. 172.

<sup>95</sup> Bkz. dpn. 93'de yapılan atıflar.

<sup>96</sup> Sieber/Nöding, s. 205; Müglic, A. : Neue Formvorschriften für den E-Commerce, MMR 2000, s. 11.

<sup>97</sup> Örnek olarak bkz. Alman Elektronik İmza Kanunu, § 6 Abs. 2 ve 3.

Dijital imzalı elektronik bir belge, cismani bir niteliğe sahip olmamasına rağmen, muhafaza edilmesi, yani süreklilik taşıyacak şekilde kaydedilmeleri şartıyla, gerek bilgisayar ekranında, gerekse yazıcı vasıtasıyla basılarak her zaman okunabilir ve tetkik edilebilir. Bu nedenle, dijital imzalı elektronik bir belge, yazılı şeklin devamlılık işlevini yerine getirmektedir<sup>98</sup>. Dijital imzalı belgelerin hazırlanmasında kullanılan programların eskimesi ve kullanımdan kalkması ihtimali ise, bu işlevin temini için, gerekli tedbirlerin alınmasını gerektirmektedir<sup>99</sup>.

El yazısı ile imzanın inkarı halinde imza karşılaştırması yoluna gidilirken; dijital imzalı belgede, bu belgenin, gerçekten beyan sahibinin gizli anahtarı ile imzalanıp imzalanmadığı, bunu için gerekli bir yazılım (Software) vasıtasıyla tespit edilmektedir. Bunun yanında, kanun tasarılarında dijital imzalı belgelerin ispat gücünün yüksek tutulmasıyla, bu belgelerin ispat işlevi güçlendirilmeye çalışılmaktadır<sup>100</sup>.

Dijital imza, alt yapı çalışmaları, organizasyon ve güvenlik standartlarına ilişkin olarak getirilecek hukuki düzenlemelerle, el yazısı ile imzanın işlevlerini yukarıda açıklandığı üzere büyük ölçüde yerine getirse bile, dijital imzalı bir belge, Borçlar Kanunu'nun adi yazılı şekle ilişkin şartlarını taşımamaktadır. Dijital imzalı bir belge, yazılı şeklin, "yazılı olarak tespit edilen düşünce açıklamasının "optik olarak doğrudan doğruya (kendiliğinden) algılanabilir, farkedilebilir olması" niteliğini taşımadığı gibi<sup>101</sup>, el yazısı ile imza şartını da yerine getirmemektedir. Borçlar Kanunu'nun şekil ile ilgili hükümlerine göz atıldığında, telgrafnamenin de yazılı şeklin yerini tutacağına ilişkin düzenlemeden (BK. mad. 13/fk. 2), kanun koyucunun yeni teknolojilere açık olduğu sonucuna varılabilir; fakat telgrafnamenin yazılı şekli yerine getirmesi için, bunun borçlu tarafından imzalı aslının PTT'ye tevdiî gerekmektedir. Diğer taraftan, BK. mad. 15'e göre imza atamayanlar, imza yerine usulen tasdik olunmuş el ile yapılmış bir işareti (parmak izi de olabilir) kullanılabilir. Dijital imzada da, hukuki işlemin online ortamda yapılması dolayısıyla, el ile imza atmayı

<sup>98</sup> Sieber / Nöding, s. 204; Runge, s. 19; Hoheneegg / Tauschek, s. 1543.

<sup>99</sup> Sieber / Nöding, s. 204; Runge, s. 19.

<sup>100</sup> Karş. Vehslage, s. 1802; Begründung zu § 126 a Abs. 1 s. 32 (bkz. yukarıda dpn.48).

<sup>101</sup> Fringuelli / Wallhäuser, s. 94; Hoheneegg / Tauschek, s. 1543; Rehbinder / Schmaus, s. 330. Söz konusu görüş taraftarları, elektronik bir belgede, beyanın, dijital kodlar (veriler) halinde tespit edildiğini, bilgisayar veya yazıcı olmaksızın bunların okunması mümkün olmadığından, bu belgelere senet vasfı verilemeyeceğini savunmaktadır. Aksi görüşte olan Ebbing ise, bugün bilgisayar kullanımının masa lambası ya da gözlük kullanımı kadar tabii olduğunu ifade etmektedir. (Ebbing, s. 274). Kanaatimizce de, yazılı şeklindeki "yazılılık" şartını çağın ihtiyaçlarına cevap verecek şekilde geniş yorumlamak mümkündür. Bugün online iletişim yapan kişinin bilgisayar kullanması, Ebbing'in de belirttiği gibi tabii bir şey olup, bilgisayarlar ve yazılım sayesinde dijital veriler, mutlak şekilde (gerçeğine uygun olarak) yazıya çevirmektedir. Dijital imzalı elektronik bir belgede asıl sorun, yazılı şeklin "el yazısı ile" imzayı şart koşmasından kaynaklanmaktadır.

imkansız kılan paralel bir durum söz konusudur<sup>102</sup>. Fakat, kanun koyucu BK. mad. 15’de el yazısı ile imza yerine, yine onun gibi sahibinin kişisel özelliklerini taşıyan bir el işaretini şart koşturmuştur. Nitekim, Noterlik Kanunu’na göre de (mad. 75/fk. 2, c. 2), “Mühür kullanılması halinde parmağın da bastırılması zorunludur”. Diğer taraftan Borçlar Kanunu (mad.14/fk.2), faksimile imzayı, ancak örf ve adetçe kabul edilen hallerde ve özellikle çok miktarda çıkarılan kıymetli evrakta caiz görmektedir. Bu durumda dijital imzaya, el yazısı ile imzanın hüküm ve sonuçlarını bağlayacak şekilde herhangi bir maddenin kıyas yoluyla uygulanması mümkün görülmemektedir.

Gerçi bugün, sözleşmeler hukukunda dijital imzaya el yazısı ile imzayla eşdeğer hüküm ve sonuç bağlanması ihtiyacı ekonomik açıdan olduğu gibi hukuken de cüz’idir<sup>103</sup>. Günümüzde online olarak yapılan hukuki işlemlerin çoğu zaten, kanunen herhangi bir şekle tâbi değildir. İnternet üzerinden istediği gibi alışveriş yapabilen bir tüketici kendisine sorumluluk riski yükleyen bir dijital imzayı kullanmak istemeyecektir<sup>104</sup>.

Buna karşılık, dijital imza özellikle iradi şekil açısından önem kazanmaktadır. Taraflar isterlerse BK. mad. 16 çerçevesinde, online kurulan bir sözleşmenin geçerliliğini, dijital imzanın kullanılması şartına bağlayabilirler. Bu durum özellikle internet bankacılığında, şirketler arasındaki mal ve para transferlerinde ve mesafeli satışlarda söz konusu olmaktadır. Böylece, geleneksel banka kartları sadece ödeme (ifa) amacıyla kullanıldığı halde, dijital imza bütün borçlandırıcı işlemlerin ve diğer hukuki işlemlerin (örneğin, ödeme talimatı verilmesi) irade özgürlüğü çerçevesinde yapılmasını mümkün kılmaktadır<sup>105</sup>.

Kanunen adi yazılı şekle tabi tutulan sözleşme sayısının az olması ve bu tür sözleşmelerin internet üzerinden nadiren yapılması, kanun koyucunun dijital imzayı hukuken tanıma ve yazılı şekle ilişkin hükümlerde gerekli uyarlamaları yapma konusunda herhangi bir tavır almamasını haklı kılmaz. Öte yandan, ilişkiler çok hızlı geliştiğinden, elektronik ticaretin hangi yönde, nasıl gelişeceğini ve dijital imzanın ve bunun kanuni düzenlemelerle tanınmasının elektronik ticarete katkısının ne olacağını önceden kestirmek güçtür.

---

<sup>102</sup> Malzer, s. 104.

<sup>103</sup> Rosenthal, D.: Digitale Signaturen: von Missverständnissen und gesetzlichen Tücken, Jusletter 29 Januar 2001, s. 4 (<http://www.jusletter.ch>).

<sup>104</sup> Rosenthal, s. 4.

<sup>105</sup> Malzer, s. 99.

Kanun koyucu Borçlar Kanunu'nda ve diğer kanunlarda çağın ihtiyaçlarını gözeterek dijital imza ile ilgili bir düzenleme yapmak istediğinde, önünde üç alternatif belirmektedir: Ya Borçlar Kanunu'nun yazılı şekle ilişkin hükümlerinde bir değişiklik yapmayarak, adi yazılı şeklin arandığı kanun maddelerinin bir kısmında, ihtiyaçları ve bu maddelerde öngörülen şeklin somut olayda ağır basan işlevlerini göz önünde tutarak, el yazısı ile imza yanında dijital imzanın da caiz olduğunu, her bir hüküm içerisinde tek tek belirtir; ya da Almanya'da olduğu gibi, Borçlar Kanunu'nun yazılı şekle ilişkin hükümlerine ek madde getirerek, kanunda aksi öngörülmediği sürece dijital imzanın el yazısı ile imzanın yerini tutacağını hükme bağlar ve uygun bulmadığı hükümlerde dijital imzanın caiz olmadığı hususunu tek tek öngörür. Nihayet, kanun koyucunun dijital imzanın el yazısı ile imzaya eşdeğer olduğunu belirtip, bu kurala herhangi bir istisna getirmemesi de mümkündür<sup>106</sup>.

Şekil Hükümlerinin Uyarlanması Hakkındaki Alman Kanunu'nda, Elektronik İmza Kanunu'na uygun bir dijital imzanın caiz olduğu veya olmadığı hukuki işlemler belirlenirken, bu hukuki işlem için öngörülen şeklin ağır basan işlevinden hareket edilmiştir. Örneğin uyarı işlevi ağır basan kefalet sözleşmesi (§ 766 BGB) ve tüketici kredisi sözleşmesinde (§4VerbrKrG) elektronik şeklin caiz olmadığı hususu hükme bağlanmıştır<sup>107</sup>.

## 2. Dijital İmza Aracının Yetkisiz Kullanımı Sorunu

Dijital imzanın doğurduğu sorunlardan biri de, dijital imza aracının yetkisiz kullanılmasıdır. Biometrik yöntemlerle emniyet altına alınmamış bir imza aracının (örneğin, gizli anahtarın kaydedildiği chip kartın) üçüncü kişilerin eline geçmesi ihtimal dahilindedir. İmzanın, başkasına ait imza aracının kullanılarak atılması durumunda, fiilen imzayı atan ile imza anahtarının sahibi farklı kişilerdir. Şüphesiz imza anahtarının sahibi, böyle bir işleme sonradan icazet verdiği takdirde bu hukuki işlem kendisini bağlar. Buna karşılık, gizli anahtarın sahibi kendisi adına kurulan bu hukuki işleme icazet vermediği takdirde, bir yetkisiz temsil durumu söz konusu olur. Bu

<sup>106</sup> Nitekim *Sertifika Hizmetleri Hakkındaki İsviçre Kanun Tasarısı*'yla birlikte Borçlar Kanunu'na eklenmesi önerilen mad. 14 / fık. 2bis hükmünün düzenlemesi bu şekildedir.

<sup>107</sup> Aynı Kanun'da öngörülen "metin şekline (Textform)" ilişkin bir düzenlemeden kaçınılmalıdır. Böyle bir düzenleme mahkemelerin işini daha da zorlaştıracaktır. Sertifika Hizmetleri Hakkındaki İsviçre Kanun Tasarısı'nun gerekçesinde, Kanun'un el yazısı ile imzayı şart koşmaksızın yazılı şekli öngördüğü durumların tespitini ve bu durumlarda hangi şartlar altında elektronik yolla da söz konusu beyanlarda bulunulabileceğini belirlemeyi, uygulamaya bırakmanın daha doğru olacağı ifade edilmiştir. Bundan başka, teknolojinin gelişimiyle birlikte, gelecekte metin ve sözlü beyan arasındaki ayrımın katılığını yitirebileceğine işaret edilmiş ve bu konuda göndericinin sözlü beyanının muhataba yazılı şekilde varması ya da tam tersine yazılı beyanın sözlü şekilde varması ihtimali örnek olarak gösterilmiştir. Bkz. *Botschaft*, Nr. 1.4.2.3.

noktada, imza aracının üçüncü kişiler tarafından rıza dışı kullanımından doğan risklerin; imza anahtarının sahibi ile hukuki işlem yapan muhatap arasında nasıl paylaşılacağı sorunu ortaya çıkar.

Burada ortaya çıkan risklerden biri, imza aracının rıza dışı kullanıldığıının ispatlanamaması riskidir. Nitekim İsviçre Elektronik İmza Kanunu Ön Tasarısı (mad. 17/fk.1), gizli anahtarının rıza dışında kullanıldığını iddia eden kişinin bu hususu ispatla yükümlü olduğunu hükme bağlamış, daha sonra yeniden ele alınan bu Tasarı'da, imza anahtarı sahibi için ağır sonuçlar doğurması sebebiyle, söz konusu düzenlemeden vazgeçilmiştir<sup>108</sup>. Şekil Hükümlerinin Uyarlanması Hakkındaki Alman Kanunu ile Alman Medeni Usul Kanunu'na eklenen bir hükümle ise (§ 292 a ZPO), bu konuda sertifikaya güvenen muhatap lehine "ilk görünüş ispatı" prensiplerine göre bir ispat kolaylığı getirilmiştir. Bu hükme göre imza anahtarı sahibi, muhataba elektronik yolla gönderilmiş olan (ve BGB § 126 a'daki elektronik şekil şartlarına uygun) irade beyanının gerçekliği konusundaki (Elektronik İmza Kanunu'na uygun bir kimlik doğrulama işleminden doğan) görünüşü, ancak bu görünüş konusunda ciddi şekilde şüphe uyandıracak vakıalar göstermek suretiyle sarsabilir<sup>109</sup>.

Çözüme kavuşturulması gereken diğer sorun ise, imza aracının rıza dışı kullanıldığıının ispatlanması ya da ispatlanmış sayılması halinde, sözleşmenin kurulmamasından doğan zarar riskine kimin katlanacağıdır. Sertifika Hizmetleri Hakkındaki İsviçre Kanun Tasarısı'nda, imza anahtarı sahibi, imza aracının muhafazasında kusuru bulunmadığını ispatlayamadığı takdirde, sertifikaya güvenen muhatabın zararını tazminle yükümlü tutulmuştur.

Dijital imzanın hukuken tanınmasına karşın, bu hususta açıkça bir düzenleme olmadığı takdirde, Türk hukukunda da imza aracının yetkisiz (rıza dışı) kullanımı halinde, risklerin paylaşımı hususunda değişik görüşler ortaya çıkabilir. Her şeyden önce, mevcut kanun hükümlerinin herhangi bir zorlama olmaksızın olduğu gibi uygulanması gerektiği, yani, imza aracının yetkisiz kullanılması halinde, sertifikaya güvenen muhatabın, sadece BK. mad.39'a dayanarak yetkisiz temsilciye başvurabileceği görüşü ileri sürülebilir; ne var ki bu sonuç çoğu durumda, özellikle yetkisiz temsilcinin kimliğinin tespit edilememesi durumunda tatmin edici olmaktan uzaktır.

<sup>108</sup> Bu konudaki açıklamalar için bkz. yukarıda dpn. 60'la başlayan metin.

<sup>109</sup> Bu ispatın gerçekleşmesi halinde yetkisiz temsilden doğacak hukuki sorunların çözümü, uygulamanın "görünüşte temsil (zahiri temsil – Anscheinvollmacht) konusunda geliştirdiği prensiplere bırakılmıştır. Bkz. Sieber / Nöding, s. 209.

İkinci olarak, doktrinde bir yazarın ileri sürdüğü gibi, BK. mad. 33/fk. 3'ün kıyasen uygulanarak, imza anahtarı sahibinin yapılan sözleşmeyle bağlı tutulması gerektiği savunulabilir<sup>110</sup>. Söz konusu hüküm, görünüşte (zahiri) temsil durumlarından birini düzenlemekte olup, temsil yetkisinin derecesinin üçüncü kişilere bildirilmesi halinde, bu beyana itibar olunacağını öngörmektedir. Bu hükmün, sadece temsil yetkisinin derecesi hakkında değil, temsil yetkisinin verilmesinde de uygulama alanı bulacağı kabul edilmektedir<sup>111</sup>. Gerçi imza aracının rıza dışı kullanımında (özellikle imza aracının çalınması durumunda), imza anahtarı sahibi, temsil yetkisinin herhangi bir kişiye verildiği hususunda bir bildirimde bulunmamaktadır. Sertifikaya güvenen muhatap, karşısında (internetin öbür ucunda) gerçekten kim olduğunu dahi bilmemektedir; ancak o, gizli anahtar sahibinin almış olduğu sertifikaya güvenerek, sertifikada ismi kayıtlı açık anahtar (dolayısıyla gizli anahtar) sahibi ile işlem yaptığını düşünmektedir. Burada BK. mad. 33 / fk. 3'ün kıyasen uygulanabilirliği için, imza anahtarı sahibinin, kendisi için kanunen tanınmış bir sertifika düzenlettirmekle, hukuki işlemlere katılma ve kendisini bağlayıcı irade beyanlarında bulunma konusunda bir görünüş yarattığı, dolayısıyla bu görünüşe güvenen iyiniyetli üçüncü kişilerin korunması gerektiğinden hareket etmek gerekir ki<sup>112</sup>, bu konuda özel bir düzenleme olmadığı sürece imza anahtarı sertifikalarının böyle bir etki yarattığının kabulünün, kanun hükümlerinin aşırı şekilde zorlanmasından başka bir şey olmadığı kanaatindeyiz.

Nihayet, imza aracının yetkisiz kullanımı hallerine Borçlar Kanunu'nun 36'ncı maddesinin 3'üncü fıkrasının kıyasen uygulanması suretiyle Sertifika Hizmetleri Hakkındaki İsviçre Kanun Tasarısı'nın benimsediği çözüm tarzı, bir görüş olarak ileri sürülebilir. BK. mad. 36/fk. 3, temsil yetkisini içeren belgeyi (yetki belgesini) geri almakta ihmal gösteren temsil olunan ve haleflerinin, iyiniyetli üçüncü kişilerin bundan dolayı uğrayacakları (menfi) zararı tazmin yükümlülüğünü düzenlemektedir. Söz konusu sorumluluk bir kusur sorumluluğudur. Bu hükmün uygulanması, muhafazasındaki kusur nedeniyle üçüncü kişilerin eline geçen imza aracının yetkisiz kullanılması halinde, imza anahtarı sahibinin, sertifikaya güvenen iyiniyetli muhatapın bu suretle uğramış olduğu (menfi) zarardan sorumlu tutulması sonucunu doğuracaktır.

<sup>110</sup> Bu görüşte Rosenthal, s. 3 vd.

<sup>111</sup> Eren, C. I, s. 406.

<sup>112</sup> Rosenthal, s. 3. Buna karşılık, imza anahtarı sahibinin rızasıyla üçüncü kişinin elinde bulunan imza aracının, bu kişi tarafından yetkisi dışında kullanılması durumunda BK. mad. 33/fk.3'ün uygulanabilirliği düşünülebilir.

Ortaya çıkabilecek bütün bu tartışmaları, öngöreceği açık bir düzenleme ile engellemek kanun koyucunun elindedir<sup>113</sup>.

### 3. Sertifika Hizmet Sağlayıcılarının Sorumluluğu

Dijital imza ile ortaya çıkan diğer bir sorun, sertifika hizmet sağlayıcılarının hizmetlerindeki aksaklıkların riskini kimin taşıyacağıdır. Örneğin, sahte bir kimlik belgesine dayanılarak sertifika alınmış olabilir ve üçüncü bir kişi bu sertifikaya güvenerek sözleşme yapmış ve edimini yerine getirmiş olabilir. Sertifikaya güvenen kişinin, adına haberi olmaksızın imza anahtarı hazırlanan ve sertifika düzenlenen kişiye (görünüşte imza sahibine) zararını tazmin ettirmesi mümkün değildir. Bu sahte sertifikayı düzenlettiren kişinin tespit de edilememesi halinde, sertifikaya güvenen üçüncü kişi zarara kendisi mi katlanacaktır? Yine, sertifikanın yanlış yere iptal edilmesinden veya imza anahtarı sahibinin bu husustaki bildirimine rağmen iptal edilmemesinden doğan zararı kim taşıyacaktır?<sup>114</sup>

Bu noktada sertifika hizmetleri sağlayıcısının sorumluluğu önem kazanmaktadır. Gerçi imza anahtarı sahibinin, sertifika hizmet sağlayıcısına karşı, hizmetlerindeki aksaklık nedeniyle uğradığı zararlardan dolayı, aralarındaki sözleşme ilişkisine dayanarak BK. mad. 96 vd.'na (yardımcı kişilerden dolayı BK mad. 100'e) başvurma imkanı vardır; fakat kanun koyucunun, sorumluluğun türü (kusur-olağan sebep-tehlike sorumluluğu), sertifika hizmet sağlayıcısının kendi davranışlarından veya yardımcı kişilerden dolayı sorumluluğunu ortadan kaldırıp kaldırmayacağı (BK. mad. 99 ve mad. 100 /fk. 2 ve 3'de olduğu gibi) ve sorumluluğun kapsamı konusunda getireceği yeni düzenlemelerle farklı bir tercih yapma imkanı vardır.

Diğer taraftan, sertifika makamlarının hangi üçüncü kişilerin zararını tazminle yükümlü olduğu (dijital imzanın, sertifikanın ve sertifika listeleri hizmetinin doğrudan değil, dolaylı muhatabı olan kişiler düşünülecek olursa) ve bunlara karşı olan sorumluluğunun niteliği açık bir düzenleme mevcut olmadığı takdirde tartışma doğurabilir<sup>115</sup>.

<sup>113</sup> Diğer taraftan uygulamada, önceden programlanmış virüsler ya da Hacker programları aracılığıyla, imza anahtarı sahibine, bilgisayar ekranında gördüğü metinden başka bir metin imzalatılmasının mümkün olduğu ya da özellikle tanınmayan bir programda, bilgisayara yanlış komut veya veri girilebileceği (girdi hatası-Inputfehler) ifade edilmektedir. Bkz. Rossmagel, A.: Auf dem Weg zu neuen Signaturregelungen, MMR 2000, s. 459; Rosenthal, s. 3. Bu sorunların duruma göre Borçlar Kanunu'nun beyan hatasına (BK. mad. 24 vd.) ve hileye ilişkin (BK. mad. 28) hükümleriyle çözüme kavuşturulması mümkündür.

<sup>114</sup> Örnekler için bkz. Botschaft, Art. 16, Nr. 2.1.7.1.

<sup>115</sup> Açık bir düzenleme mevcut olmadığı takdirde, sertifika hizmet sağlayıcısının üçüncü kişilerin salt malvarlığı zararlarından dolayı üçüncü kişiyi koruma etkili sözleşmeye dayalı olarak sorumlu olacağı görüşü savunulabilir. Yeni Alman Elektronik İmza Kanunu'ndan önce

Nitekim, Sertifika Hizmetleri Hakkındaki İsviçre Kanun Tasarısı'nda (mad. 16), bu konuda, sertifika hizmet sağlayıcılarının imza anahtarı sahibine ve sertifikaya güvenen üçüncü kişilere karşı sebep sorumluluğuna dayalı özel bir sorumluluk normu öngörülmektedir. Alman Elektronik İmza Kanunu'nda ( § 11) ise, sadece sertifikaya, zaman kaşesine ya da sertifika listeleri aracılığıyla verilen bilgilere güvenen üçüncü kişilere karşı sorumluluk düzenlenmiş olup; anahtar sahibine karşı sözleşmeden doğan sorumluluk BGB'nin genel hükümlerinin ( § § 276, 278 BGB) uygulama alanına bırakılmıştır. Sertifika hizmet sağlayıcılarının üçüncü kişilere karşı sorumluluğu, Alman Kanunu'nda, ispat yükü ters çevrilmiş bir kusur sorumluluğu olarak düzenlemiştir. Yardımcı kişilerden dolayı sorumluluk alanında, sadece belirli yardımcı kişilerin sertifika hizmet sağlayıcılarının kanuni yükümlüklerini ihlal etmesi durumuna münhasır olmak üzere, BGB § 831'e göre sorumluluktan kurtuluş kanıtı getirme imkanı ortadan kaldırılmıştır. (SigG § 11 / fk. 4). Bu hükmün kapsamına girmeyen yardımcı kişilerden dolayı ise, üçüncü kişilere karşı sorumluluğun haksız fiili mahiyeti vurgulandığından, BGB § 831 çerçevesinde kurtuluş kanıtı getirme imkanı mevcuttur<sup>116</sup>.

## SONUÇ

Dijital imza, elektronik yolla iletilen bir belgenin şifrelenmesi esasına dayanmaktadır. Dijital imzalı elektronik bir belge, her şeyden önce el yazısı ile imzada olduğu gibi sahibinin kişisel özelliklerini taşımadığı için, Borçlar Kanunu hükümlerine göre adi yazılı şeklin şartlarını yerine getirmemektedir. Bu açıdan Kanun'da, teknolojik gelişmelerle ortaya çıkan bir boşluk söz konusudur. Dijital imzanın, el yazısı ile imzanın işlevlerini büyük ölçüde yerine getirmesi, hatta bazı işlevlerinin daha güçlü olduğunun ifade edilmesi (örneğin, ispat işlevinin ve sonuçlandırma işlevinin) durumu değiştirmez. Bu boşluğun, kanun koyucu tarafından doldurulması gerekmektedir. Kanun koyucu tarafından dijital imzanın el yazısı ile imzaya eş değer tutulmasının zorunlu şartı, sertifika hizmet sunucularına ilişkin alt yapının kurulmasıdır; zira dijital imza, kimlik tespit etme işlevini, en güvenilir şekilde ancak bu kurumlar aracılığı ile yerine getirebilmektedir.

Dijital imzanın hukuken tanınmasının, elektronik ticaretin gelişiminin ve yaygınlaşmasının belirleyici şartı olduğu ifade edilmektedir. Gerçi, son yıllarda, dijital imzanın kanunen tanınmamasına rağmen, belirli alanlarda (özellikle bankalar ve kredi kartı kurumları tarafından), iradi şekil

---

bu konudaki tartışmalar için bkz. **Büllesbach, A. / Pooth, St. / Stauder J.:** Die Haftung der Zertifizierungsstellen nach dem deutschen Signaturgesetz, Rechtsfragen der digitalen Signatur, Hrsg. Hoeren Th. / Schüngel; M. Berlin 1999, s.205 vd.

<sup>116</sup> Bu konuya ilişkin açıklamalar için bkz. yukarıda dpn. 45'e ilişkin metin.

çerçevesinde dijital imzanın kullanılmasıyla, elektronik ticaretin büyüme oranının arttığı belirtilmektedir. Fakat bu gelişimden, dijital imza ile ilgili kanuni düzenlemelere ihtiyaç olmadığı sonucu çıkartılamaz. Öte yandan, elektronik ticaretin nasıl bir gelişim göstereceği ve dijital imzanın kanuni düzenlemelerle tanınmasının elektronik ticarete katkısının ne olacağını önceden kestirmek de güçtür. Bu açıdan, Borçlar Kanunu ve diğer kanunların, teknolojideki bu gelişime ve ihtiyaçlara uygun şekilde gözden geçirilmesi yerinde olur.

Şekil hükümleri yanında, imza anahtarının kaydedildiği imza aracının, üçüncü kişiler tarafından yetkisiz kullanımı halinde doğacak hukuki problemler ile sertifika makamlarının, imza anahtarı sahibine ve sertifikaya güvenen üçüncü kişilere karşı sorumlulukları da açık bir düzenlemeye kavuşturulmalıdır. Bu düzenlemeler, belirsizlik ve güvensizliklerin ortadan kaldırılması, dolayısıyla, dijital imzalı elektronik belgelerle kurulan hukuki ilişkilerde hukuki güvenliğin sağlanması açısından zorunludur. Şüphesiz, kanun koyucu, uygulamada bir takım kanun boşluklarının ortaya çıkabileceğini hesaba katmalı ve bu boşlukların, mevcut hükümlerin kıyas yoluyla uygulanması suretiyle doldurulmasını sağlayacak şekilde, hukuk sistemimizle bütünleşen düzenlemeler yapmalıdır. Bu arada, bir taraftan internetin ve elektronik ticaretin globaliği, diğer taraftan Türkiye'nin Avrupa Birliği'ne aday bir ülke olması açısından, uluslararası düzenlemelerin, özellikle Avrupa Birliği'nin ilgili yönergelerinde benimsenen esasların dikkate alınması yerinde olur.