Son Gelişmeler Işığında Elektronik İmza Tanımı ve Türleri

Definition and Types of Electronic Signatures in the Light of Latest Developments

Dr. Öğr. Üyesi **M. Ertan YARDIM**(*)

Öz:

Elektronik imza en basitinden en karmaşığa çok farklı teknik ve teknolojileri kapsayan bir üst kavramdır. Elektronik imza teknik ve teknolojileri gün geçtikçe değişmekte ve gelişmektedir. Avrupa Birliği nezdinde de son yıllarda arka arkaya yeni düzenlemeler ve standartlar kabul edilmektedir. Elektronik İmza Kanunu'nda (EİK) da elektronik imza oldukça geniş ve kapsayıcı şekilde tanımlanmıştır. Buna karşılık, EİK'da sadece tanım verilmiş ve güvenli elektronik imza dışında hiçbir elektronik imza teknik veya teknolojisine hukuki sonuç bağlanmamıştır. Güvenli elektronik imza hem altyapısı hem de hukuki etkisi itibariyle özel düzenlemiştir ve halihazırda hukuki etkisi düzenlenmiş tek elektronik imza türüdür. Bu sebeple, biyometrik imza gibi gelişmekte olan farklı elektronik imza türlerinin ancak ve sadece genel hükümler çerçevesinde değerlendirilmesi mümkün olmaktadır. Belirtilen hususlar çerçevesinde, teknoloji yönüyle genel olarak elektronik imza kavramını; uluslararası düzenlemelerde ve EİK'da elektronik imza tanımını ve türlerini; son olarak elektronik imza bakımından oldukça önemli olan teknoloji tarafsızlığı prensibini ele alacağız.

Anahtar Kelimeler:

Elektronik İmza, Güvenli Elektronik İmza, Biyometrik İmza, eIDAS, Teknoloji Tarafsızlığı Prensibi.

Abstract:

The electronic signature is an upper concept that covers many different techniques and technologies, from the simplest to the most complex. Electronic signature techniques and technologies are changing and developing day by day. New regulations and standards have been adopted one after another in the European Union in recent years. The Turkish Electronic Signature Act (TESA) defines electronic signature comprehensively and inclusively. On the other hand, only a definition is given in the TESA, but no legal consequences are attached to any electronic signature technique or technology other than a secure electronic signature. The secure electronic signature is specially regulated in terms of both its infrastructure and legal effect, and it is the only electronic signature type whose legal effect is currently regulated. For this reason, it is possible to evaluate different types of electronic signatures, such as biometric signatures, only within the framework of general provisions. Within the framework of the specified issues, the concept of electronic signature in general in terms of technology; definition and types of electronic signature in international regulations and TESA; Finally, we will discuss the principle of technology neutrality, which is very important in terms of electronic signature.

Keywords:

Electronic Signature, Secure Electronic Signature, Biometric Signature, eIDAS, Technology Neutrality Principle.

(*) Kadir Has Üniversitesi, Medeni Usul ve İcra İflas Hukuku Anabilim Dalı,
E-posta: ertan.yardim@khas.edu.tr; Orcid Id: https://orcid.org/0000-0001-5483-6995.

Bu makale, Yazarın "*Elektronik İmza ve Medeni Usul Hukukumuza Etkileri*" başlıklı, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Anabilim Dalı bünyesinde hazırlanan 2006 tarihli yüksek lisans tezinden türetilmiştir.

Yayın Kuruluna Ulaştığı Tarih: 30.04.2022 / **Kabul Tarihi:** 06.07.2022.

Giriş

Ülkemizde elektronik imzaya ilişkin temel düzenleme olan 5070 sayılı Elektronik İmza Kanunu (EİK) 13/01/2004 tarihinde kabul edilmiş ve 23/01/2004 tarihinde Resmi Gazete'de yayınlanmıştır. 5070 sayılı EİK'nın amacı, kanunun genel gerekçesinde belirtildiği üzere, elektronik imzanın hukuki ve teknik yapısını, elektronik imzayla ilgili işlemler ile elektronik sertifika hizmet sağlayıcılarının faaliyetlerini düzenlemektir. Oldukça teknik düzenlemeler içeren EİK bakımından ilk ele alınması gereken hususlardan biri elektronik imza tanımı ve türleri olabilir. Nitekim EİK'da sadece, belirli bir teknoloji ile sağlanması mümkün bulunan belirli kriterleri sağlayan güvenli elektronik imzanın hukuki etkisi düzenlenmiş; güvenli elektronik imza olmayan herhangi bir elektronik imza türü veya teknolojisi için hiçbir hukuki etki öngörülmemiştir.

EİK'da elektronik imza tanımını ve türlerini değerlendirmek için öncelikle elektronik imza kavramı üzerinde durulması gerekir. Elektronik imza kökeni oldukça eskiye dayanan, sıkça kullanılan ve oldukça geniş bir alanda çok farklı teknik ve teknolojileri ifade etmek için kullanılan bir kavramdır. Elektronik imzada geçen "elektronik" kelimesi teknik anlamda "elektron temeline dayanan, elektronla ilgili" anlamında değil; fiziki olmayan her ortamı ve iletimi kapsar şekilde kullanılmaktadır. Esasen sayısal veya dijital kelimeleri yerine elektronik kelimesi kullanılması dahi başlı başına kavramın genişliğine delalet etmektedir. İmza terimi bakımından ise yine "imza" kelimesi teknik anlamda imzadan çok daha geniş şekilde herhangi bir teknik veya teknolojinin kimlik doğrulama veya onaylama amacıyla kullanılmasını ifade etmektedir. Elektronik imza kavramında geçen "imza" kelimesinin genel olarak (elektronik imzanın belirli türleri dışında) elle atılan imzanın fonksiyonlarını karşılamadığı gibi bu yönde de bir iddia da bulunmamaktadır. Elektronik imza kavramının bu şekilde geniş anlaşılması sebeplerinden biri teknolojinin hızlı gelişimi karşısında zamansal olarak eskimeyen bir kavram ortaya konulma amacıdır. Çalışmamızın ilk bölümünde, elektronik imza kavramını ve çeşitli elektronik imza türlerini teknik olarak ele alacağız.

Çalışmamızın ikinci bölümünde, çeşitli ulusal ve uluslararası düzenlemelerde ve EİK'da elektronik imza tanımını ve türlerini karşılaştırmalı olarak inceleyeceğiz. 2000 yılların başında hem Birleşmiş Milletler hem de Avrupa Birliği nezdinde düzenlemelerle elektronik imza tanınmış ve bir hukuki altyapı içine alınmış ise de ticarette elektronik imza kullanımı beklendiği şekilde hızlı artmamıştır.[1] Elektronik imzanın ve neticede uluslararası elektronik ticaretin yaygınlaştırılması için önce Avrupa Birliği nezdinde, 1999/93/EC sayılı Elektronik İmza Direktifi 2014 yılında kaldırılarak yerine Elektronik İşlemler İçin Elektronik Kimlik ve Güven (Onay) Hizmetleri Tüzüğü - Elektronik İşlemler Tüzüğü (Regulation on electronic identification and trust services for electronic transactions in the internal market eIDAS) düzenlemesi kabul edilmiş ve hızlıca birçok alanda standartlar belirlenmiştir. Hemen arkasında, 2017 yılında, (2001 tarihli Elektronik İmza Hakkında Model Kanun kaldırılmadan) Birleşmiş Milletler nezdinde İletilebilen Elektronik Kayıtlar Hakkında Model Kanun (UNCITRAL Model Law on Electronic Transferable Records) kabul edilmiştir. Çalışmamızda, uluslararası düzenlemeleri değindikten sonra özellikle EİK bakımından mevcut durumu ortaya koyarak görüşlerimizi aktarmaya çalışacağız.

Çalışmamızın son bölümde, elektronik imza tanımında ve türlerinde oldukça önemli rol oynayan teknoloji tarafsızlığı prensibi üzerinde duracağız. Görebildiğimiz tüm ulusal ve uluslararası düzenlemeleri etkileyen bu temel prensibin ayrı bir başlık altında ele alınmasının yararlı olacağı kanaatindeyiz. Teknoloji tarafsızlığı prensibi, temel olarak elektronik imzanın yasal etkisinin belirli bir elektronik imza teknolojisinden arındırılmasını ve geniş bir çerçevede, bazı temel kriterleri sağlayan farklı elektronik imza teknolojilere hukuki etki tanınmasını amaçlamaktadır. Prensibin öngörülen amaca ne kadar hizmet ettiği ve başarılı olduğu ayrıca tartışmaya açıktır. Konuyu farklı yönleriyle ele almaya çalışarak sonuç bölümü ile çalışmamızı sonlandıracağız.

[1] H. BOSS, Amelia, "The Evolution of Commercial Law Norms: Lessons to be Learned From Electronic Commerce" Drexel University Thomas r. Kline School of Law, 2009, pp. 673-708; s. 699-701.

I. Elektronik İmza Kavramı

A. Elektronik İmza Kavramının Kapsamı ve İçeriği

Elektronik imza kavramı uluslararası kuruluşların düzenlemelerinde, pek çok ülke kanununda ve konu ile ilgili çalışmalarda farklı şekilde tanımlanmıştır. Kavramın nispeten yeni ve gelişen bir kavram olması sebebiyle içeriğinin ve kapsamının net olarak belirlenmesinde zorluk çekilmektedir. Aşağıda uluslararası düzenlemelerde yer verilen tanımlara ayrıca yer vereceğiz; bu aşamada, özellikle mevcut teknik ve teknolojilere istinaden elektronik imza ile kastedildiğini açıklamaya çalışacağız. Öncelikle belirtmek gerekirse, elektronik imza, bir elektronik dokümana veya maile adın yazılmasından, açık anahtar altyapısına; bir ekrana kalemle veya fare ile imza çizilmesinden retina, parmak izi kullanılması gibi biyometrik imzalara kadar çok geniş teknik ve teknolojileri kapsamaktadır.[2] İçerdiği teknik ve teknolojilerden yola çıkan bir tanıma göre ise, "kişilerin biyometrik özelliklerine dayalı (ses, göz retinası taraması, parmak izi taraması gibi) biyometrik yöntemler, kredi kartlarında kullanılan PIN kodları, elle atılmış imzanın tarayıcıdan geçirilerek elektronik ortama aktarılmış hali, bilgisayar ekranında bu amaçla yapılmış bir kalemle atılan imza tekniği veya çift anahtarlı kriptografiyle oluşturulan dijital (sayısal) imzayı da içeren bir üst kavram"[3] şeklinde tarif edilebilir. Elektronik imza günümüzde, kişinin elektronik ortamda tanınmasına olanak veren en basitten en karmaşığa kadar her türlü teknik çözüm için kullanılan[4] bir üst kavramdır. Bir elektronik imza birçok biçimde görünebilir; mesela, dijital imza, dijitalize edilmiş parmak izi, retina taraması, pin kodu, bir elektronik veriye eklenmiş -sıklıkla bir elektronik postanın sonuna eklenmiş- bir isim,[5] elle atılan imzanın dijital görünümü birer elektronik imzadır. Elektronik ortamda ıslak imzanın yerini almaya yönelik tüm teknoloji ve teknikler elektronik imza kavramı kapsamındadır.[6] Her vesileyle elektronik imza, kullanıcının beyanının doğrulanmasına ve mesaj ile kullanıcı arasında ilişki kurmaya yöneliktir. Genel maksat, kısmen veya tamamen, sahteciliğin önlenmesi ve fiziksel olarak imzalanmış dokümanın yerine geçerli bir örneğinin sunulabilmesidir.[7]

Görüldüğü üzere, elektronik imzanın kavramsal olarak net bir tanımını ortaya koymak oldukça zordur; bu aşamada, kapsamın genişliğine dikkat çekmek yerinde olabilir. Belirtilen hususlar çerçevesinde, elektronik imzanın elektronik ortamda elle atılan imzanın doğrulama, tanımlama, onaylama gibi fonksiyonlarını kısmen veya tamamen karşılamayı amaçlayan her türlü teknik ve teknolojiyi içeren bir üst kavram olduğunu söyleyebiliriz.

Bu aşamada, belirtmek gerekirse, elektronik imza ile dijital imza kavramları bazen birbiri-

[2] WANG, Minyan, "Do the regulations on electronic signatures facilitate international electronic commerce? A critical review" Computer Law & Security Review: The International Journal of Technology Law and Practice Year: 2007, N: 23, ss. 32-41, s. 33.

[3] ERTURGUT, Mine, Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Ankara, Yetkin Yayınları, 2004, s. 54.

[4] KESER BERBER, Leyla, "Elektronik İmzanın Düzenlenmesi Hakkında Tasarı Hükümlerinin Değerlendirilmesi" (çevrimiçi), https://turk-internet.com/elektronik-imza-kanun-tasarisi-hukumleri-degerlendirilmesi/, 10/06/2022; SARISÖZEN, Serhat, "Elektronik İmza Kanunu'nun Değerlendirilmesi, Elektronik Ticaret ve İnternette Yapılan Sözleşmeler", Kazancı Hakemli Hukuk Dergisi, S. 15-16, Yıl: 2005, s. 133.

[5] E. BLYTHE, Stephen, "Dijital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enchanced Security", Richmond Journal of Law & Technology, Volume IX, Issue 2, 2005, (çevrimiçi) http://law.richmond.edu/jolt/v11i2/article6.pdf, 21/10/2005, s. 3.

[6] FREEMAN J.D., Edward, "Dijital Signatures and Electronic Contracts", (çevrimiçi) https://www.proquest.com/openview/ea208345000de3f800ad504b0bd21e76/1?pq-origsite=gscholar&cbl=52433, 01/04/2022; Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, http://2002.bilisimsurasi.org.tr/, s. 83; GEZDER, Ümit, Mukayeseli Hukuk Açısından İnternet'te Akdedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, Beta Yayınları, 2004, s. 147; ALTINIŞIK, Ulvi Elektronik Sözleşmeler, Ankara, Seçkin Yayıncılık, 2003, s. 79; ERGÜN, Ömer, "5070 Sayılı Elektronik İmza Kanunu ve Dijital İmza", Türkiye Noterler Birliği Hukuk Dergisi, Sayı: 122, Tarih: 15 Mayıs 2004, s. 63-74, (çevrimiçi), https://turk-internet.com/5070-sayili-elektronik-imza-kanunu-ve-dijital-imza-1/, 10/04/2022, s. 65.

[7] FREEMAN, (web).

nin yerine kullanılsa da, aynı kavramlar değildir.[8] Belirttiğimiz üzere elektronik imza ıslak imzanın yerine veya herhangi bir kaydı doğrulamak amacıyla kullanılan tüm teknoloji ve teknikleri kapsar. Buna karşılık, dijital imza, açık anahtar altyapısına dayalı elektronik iletişimi şifreleyen ve mesajın bütünlüğü ve gerçekliğini doğrulayan belli bir teknolojiyi ifade eder.[9] Bu bağlamda, dijital imza elektronik imzanın bir türüdür.[10]

Aşağıda teknolojik bakımdan çeşitli elektronik imza türlerini ele alacağız. Güvenlik seviyeleri, kullanıcının katılımı,[11] şifreleme metotları gibi farklı kriterlere göre farklı sınıflandırmalar yapılabilir. Biz EİK ile benzerlik kurmak adına dijital imza dışında kalan elektronik imzalar ve dijital imza ayrımı çerçevesinde elektronik imza türlerini ele alacağız.

B. Elektronik İmza Teknik ve Teknolojileri

1. Dijital İmza Yöntemi ile Oluşturulmayan Elektronik İmzalar

a. Elektronik İmza Teknikleri

Duyarlı bir bilgisayar ekranına özel kalemi vasıtasıyla elle imza atılması veya kağıt bazlı ıslak imzalı bir metnin tarayıcı vasıtasıyla bilgisayara aktarılması başlıca elektronik imza teknikleri olarak sayılabilir. Bu yöntemler, bir elektronik imza teknolojisi olmaktan ziyade münferit teknolojilerin elektronik imza uğruna kullanılmasıyla meydana gelirler, bu yüzdendir ki, bu yöntemleri elektronik imza teknikleri başlığı altında incelemeyi tercih ettik.

Tarayıcı ile bilgisayara aktarılmış imza ise elektronik bir dokümana resim yapıştırır gibi, ıslak imzanın taranıp resim haline getirilerek dokümana eklenmesidir. Bu yöntem bazı kuruluşlar tarafından seri hazırlanan pazarlama tekliflerini göndermek için kullanılmaktadır.[12] Maddi ortamda hazırlanan ve imzalanan verinin bir bütün olarak da taranması ve bilgisayara aktarılması mümkündür. Bu uygulamanın da yaygın bir elektronik imza uygulaması olduğu belirtilmiştir.[13] Bu noktada ikili bir ayrıma gidilebilir. Tarayıcı vasıtasıyla yalnız imzanın bilgisayara aktarılması halinde, elektronik imzanın ayrı bir veri olarak, başka bir veriye eklenmesi veya mantıksal olarak bağlanması hususu gerçekleşebilir (Bkz. EİK m. 3/I-b). Çünkü bu halde, birbirinden farklı iki veri söz konusudur. Buna karşılık, ıslak imzalı belgenin tamamının bilgisayara aktarılması halinde ayrı bir elektronik veri söz konusu olmayacaktır. Her iki hal bakımından da kimlik doğrulama amacı kabul edilebilir ve somut olarak da kısmen dahi olsa imza sahibinin teşhisi mümkün olabilecektir.

Elle atılan imzanın veya elle atılan imzalı metnin taranması bir elektronik imza tekniği olarak değerlendirilmektedir. Bu imzalara dijitalize imza da denir. Böylece, bu verilerin internet vasıtasıyla veya veri depolayıcı belleklerle iletilmeleri mümkündür ancak bu tekniğin önemli yüksek seviye güvenlik sağlamadığı açıktır. Bu imza tekniğinin güvenlik seviyesi oldukça düşük ise de nitelikli elektronik imzanın yaygınlaşmaması karşısında günümüzde ciddi bir kullanım

---

[8] RAYSMAN, Richard / BROWN, Peter, "Legislation on Digital Signatures" http://www.brownraysman.com/pubs/articles/techlaw/nylj0499.html, (çevrimiçi), 15/04/2005.

[9] RAYSMAN / BROWN, (web).

[10] ŞENOCAK, Zarife, "Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması", AÜHFD, C. 50, S. 2, 2001, s. 98; ORTA, Mesut, Elektronik İmza ve Uygulaması, Ankara, Seçkin Yayınları, 2005, s. 37.

[11] Bu ayrıma göre elektronik imzalara dörde ayrılabilir; kullanıcı veya alıcının bilgisine dayalı (şifre veya pin numarası ile kullanılan) elektronik imzalar; kişinin fiziksel özelliklerine dayalı (biyometrik) elektronik imzalar; kişinin taşıdığı nesneye dayalı (manyetik kartlar, usb bellekler) elektronik imzalar ve bunların dışında kalan çeşitli elektronik imza teknikleri (Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, United Nations Commission on International Trade Law, Vienna, 2009, s. 13 parag. 16.

[12] "Electronic Authentication", http://www.e-ra.org.uk/electronic_authentication.htm, (çevrimiçi), 22/10/2005.

[13] AHİ, Gökhan, "Türk Hukukunda Yeni Bir Boyut Elektronik İmza Kanunu", http://dergi.tbd.org.tr/ yazarlar/10052004/m.gokhan_ahi.htm, (çevrimiçi), 04/05/2005.

alanına sahiptir.[14] Dijitalize imzanın biodinamik versiyonu da bilgisayar ekranına elle atılan imzadır. Bilgisayar ekranına elle imza atılması, uygun donanım ve yazılım vasıtasıyla özel kalemlerle touchpad'e veya dizüstü bilgisayar ekranına el yazısı ile imza atılmasıdır.[15] Aşağıda biyotmetri imzalar bölümünde, bu imzalar üzerinde ayrıca duracağız.

Anılan teknikler dışında, bilgisayar ekranındaki "Ok" yazısının tıklanması[16] veya onay olarak duyulan sesler, alıcıya göndericiyi tanıtmaya yönelik her türlü şifre, ATM kartlarında kullanılan kart ve kredi kartları[17] da elektronik imza örneği teşkil etmektedir. Anılan teknikler dışında, ABD hukukunda elektronik postanın altına eklenen isim de elektronik imza sayılmış ve bağlayıcı olduğu kabul edilmektedir.[18] Aynı yönde, İngiltere Ticaret Mahkemesi'nin 1997 yılında Hall ve Cognos şirketleri arasındaki davada elektronik postanın altına yazılmış gönderici isminin elektronik imza sayılması gerektiğine karar verdiği belirtilmiştir.[19]

b. Biyometrik Yöntemlere Dayalı Elektronik İmzalar

Biyometrik imzalar, bir kişinin kimliğinin doğrulanması için kullanılan ölçülebilir fizyolojik ve/veya davranışsal özellikler olarak tanımlanabilir.[20] Biyometrik imzalara örnek olarak çok yaygın olarak kullanılan parmak izi, avuç içi izi, ses, retina ve DNA kopyalama sistemleri sayılabilir. Biyometrik imzalar, internette yapılacak işlemlerin güvenliği bakımından değil, daha çok bilgisayar sistemine girişte güvenliği sağlamak veya dijital imzalara ek olarak,[21] dijital imzaları aktive eden parolalar yaratmak[22] veyahut e devlet uygulamalarına güvenli giriş sağlanması[23] gibi amaçlarla kullanılmaktadır. Ayrıca günümüzde, ekrana yansıyacak şekilde uygun bir kalemle elle imza atılması belirli standartlara tabi bir biyometrik imza teknolojisi haline gelmiştir.

2006 tarihli yüksek lisans tezimizde, dijital imza kullanımı ile biyometrik yöntemler arasında, bilgisayar tekniği ve hazırlanış ve kullanılış (işleyiş) şekilleri bakımından oldukça büyük farklar olduğunu; biyometrik teknolojinin, tek başına, iletilen verinin bütünlüğünü sağlamadığını (hash fonksiyonu bulunmadığını);[24] kişilerin biyometrik özelliklerinin dijital imzadaki gibi bir sertifika kurumu tarafından kopyalanması ve sistemin bu tür kurum veya kurumlar aracılığı ile işletilmesi, dijital imzadakinden daha farklı bir alt yapıyı ve güvenliği gerektirdiğini[25] belirtmiş bu sebeplerle, en azından o dönemde biyometrik imzaların dijital imzaların alternatifi olarak kullanılmadığını belirmiştik. Diğer yandan, ilerleyen yıllarda yeni teknolojik gelişmeler olasılığında, biyometrik yöntemlerin elektronik ortamda kullanımının artabileceğini de belirtmiştik. Nitekim aradan geçen uzun yıllarda özellikle Avrupa Birliği'nin 910/2014 sayılı "Elektronik İşlemler İçin Elektronik Kimlik ve Güven (Onay) Hizmetleri

[14] Promoting confidence in electronic commerce UN, s. 30 parag. 66.

[15] "Electronic Authentication", http://www.e-ra.org.uk/electronic_authentication.htm, (çevrimiçi), 22/10/2005.

[16] Promoting confidence in electronic commerce UN, s. 16, parag. 23.

[17] J. SMENDINGHOFF, Thomas / BRO, Ruth Hil, "Electronic Signature Legislation", http://profs.lp.findlaw.com/signatures/, (çevrimiçi), 18/20/2005.

[18] "Does typing your name count as a signature?" https://www.pandadoc.com/ask/typing-name-as-signature/ (çevrimiçi) 10.03.2022.

[19] SMENDINGHOFF / BRO, (web); "Electronic Authentication", http://www.e-ra.org.uk/electronic_authentication.htm, (çevrimiçi), 22/10/2005.

[20] EROL, H. Tarık, Electronic Signatures, İstanbul, Beta Yayınları, 2003, s. 42.

[21] Bu konuda bir çalışma için bkz. "Integrating Biometric Technics with an Electronic Signature for Remote Authenticaton", http://www.ercim.org/publication/Ercim_News/enw49/bechelli.html, (çevrimiçi), 29/10/2005.

[22] EROL, s. 47.

[23] Promoting confidence in electronic commerce UN, s. 28, parag. 59.

[24] SCHELLKENS, M.H.M., Electronic Signatures Authentication Technology from a Legal Perspective, Netherlands, T.M.C. Asser Press, 2004, s. 76.

[25] KESER BERBER, (Tasarı Hükümlerinin Değerlendirilmesi); biyometrik imzalar hakkında bkz. KESER BERBER, Leyla / LOSTAR, Murat Bilişimde Biyometrik Yöntemler, Ankara, Yetkin Yayınları, 2006; ER, Cüneyd, Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, Yetkin Yayınları, 2007.

Tüzüğü (Regulation on electronic identification and trust services for electronic transactions in the internal market eIDAS)[26] düzenlemesi ve ayrıca biyometrik imza hakkında "ISO/IEC 19794-7:2021 Bilgi Teknolojileri - Biyometrik veri değişim biçimleri, 7. Bölüm, İmza/İşaret Hakkında Zaman Damgası Verisi" (ISO/IEC 19794-7:2021 Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data) ve 19794-11:2013 11. Bölüm, İmza/İşaret Hakkında İşlenmiş Dinamik Veri" (Part 11: Signature/sign processed dynamic data) ve yayımlanan teknik standartlar biyometrik imzaların kullanımını arttırma potansiyeline sahiptir. 7. Bölüm, biyometrik imzaya dair oluşan verinin korunması ve zaman damgası ile güvenliğinin arttırılması prosedürü açıklanmıştır. 11. Bölümde ise ekran üzerine uygun kalemle atılan biyometrik imzanın, imza sahibi tarafından inkar edilmesi halinde (ilgili adli birimler tarafından) incelemenin nasıl yapılacağı konusunda yeknesak prosedürler öngörmektedir. Grafoloji çalışmalarına benzer şekilde, imza sahibini ayırt etmeye yarayacak eğim, basınç, ivme ve hız gibi özellikler esas alınır. Biyometrik imza çözümlerinin uygulanması için imza sahibinin biyometrik verilerini yakalayabilecek kabiliyete sahip özel bir cihaza bağlantı olması gereklidir. Bu cihazlar hem statik verileri (imzanın resmi gibi) hem de dinamik verileri (hızlanma, hız, eğim açısı, basınç vb.) yakalayabilir ve kaydedebilir. Sonuç olarak, hem statik hem de dinamik veriler elektronik belgede saklanır.[27] Zaman damgası ise bir nevi mürekkep yaşı gibi belgenin ne zaman imzalandığını ortaya koyar.[28] Böylece elle atılan imzaya çok benzer bir güvenlik seviyesine ulaşılmış olur.[29]

Doktrinde, Keser Berber, ekran üzerine uygun kalemle atılan biyometrik imzanın belirli standartlara kavuştuğunu; imza bakımından tek kriterin elle atılma olduğunu; kullanılan güvenlik özellikleri sebebiyle ıslak imzadan daha güçlü bir delil değerine sahip olduğunu ve daha güçlü bir hukuki delil vasfını kazandığını; biyometrik imza ile adi senet düzenlenebileceğini belirtmiştir.[30] Öncelikle belirtmek gerekirse, "delil değeri" ve "daha güçlü hukuki delil vasfı" hakkındaki açıklamalara katılmamaktayız. Nitekim medeni usul hukukumuzda, deliller takdiri deliller ve kesin deliller olarak ikiye ayrılmaktadır ve delillerin kendi içlerinde delil değeri farkı veya daha güçlü daha güçsüz delil ayrımı bulunmamaktadır. Örneğin bir resmi senet ile adi senedin delil değeri arasında fark bulunmamaktadır. Burada muhtemelen biyometrik imzanın kimlik doğrulama işlevinin daha güçlü olduğu belirtilmek istenmiş olabilir. Kendi araştırmamız çerçevesinde, biyotmetrik imza ve elle atılan imzanın imza sahibine aidiyetinin tespitinde, bu yöntemlerin başarı oranlarını objektif olarak karşılaştıran ve birinin diğerine göre daha üstün olduğunu ortaya koyan bilimsel bir çalışmaya rastlamış değiliz. Kaldı ki, yöntemlerin kimlik doğrulama konusundaki başarıları belirleyici olmamalıdır; nitekim kurşun kalemle imzalanmış bir sözleşme dahi senet niteliğinde kabul edilmektedir.[31] İmza bakımından

[26] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[27] ISO/IEC 19794-11:2013, Information technology - Biometric data interchange formats Part 11: Signature/sign processed dynamic data, "Normative references" https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-11:ed-1:v1:en (çevrimiçi), 20/03/2022; ŞİMŞEK, Merve Melis / ÖZCAN, Tuğba / ERGUN, Tamer / ÇELİK, Vural, Elektronik İmza Seviyeleri, Bilgi Yönetimi Dergisi Cilt: 2 Sayı: 2 Yıl: 2019 (çevrimiçi) https://dergipark.org.tr/tr/pub/by, ss. 136-144, s. 141; KESER BERBER, Leyla, Biyometrik İmza ve Türk Borçlar Kanunu'ndaki Yazılı Şekil Şartı ile Hukuk Muhakemeleri Kanunundaki İmza Açısından Yeri, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, https://itlaw.bilgi.edu.tr/media/document/2019/08/biyometrik-imza.pdf (çevrimiçi), 20/03/2022.

[28] KESER BERBER, (Biyometrik İmza), s. 8.

[29] Vurgulamak gerekirse, güvenli elektronik imzanın veri bütünlüğünü sağlama (verinin aktarım sırasında değişip değişmediğini tespit) işlevi, elle atılan imzanın veya biyotmerik imzanın işlevlerinin ötesinde üstün bir güvenlik işlevidir.

[30] KESER BERBER, (Biyometrik İmza), s. 7-10.

[31] KURU, Baki, Hukuk Muhakemeleri Usulü, C.II, 6. Baskı, 2001, s. 2075; TUĞSAVUL, Muhsin, "İspat Külfeti Kanuni Deliller ve İkamesi", AD, S. 7, Yıl: 42, Temmuz 1951, ss. 1060-1095, s. 1080.

elle atılmanın tek kriter olduğu dair görüşe de katılamamaktayız. Elle fiziki ortamda atılan imzanın en önemli özelliklerinden biri teklik yani orijinalliktir. Elle atılan imzanın bulunduğu belge tektir ve orijinaldir; bu belgenin kopyaları (mesela fotokopisi, fotoğrafı çıktısı) aynı nitelikte değildir. Mesela, bir senedin fotokopisi senet sayılmaz. Ekran üzerine atılan imzada ise orijinallik (teklik) yoktur; elektronik veri önce geçici belleğe, sonra kalıcı belleğe, belki buluta (aynı zaman damgasıyla) kopyalanabilir. Bu veriler arasında bir fark yoktur.[32] Veri karşı tarafa da aynı şekilde kopyalanır; teorik olarak zaman damgası ile bazı kopyalama anları tespit edilebilir ancak bunun için zaman damgasının ilgili kişilerce uygun şekilde kullanılması gerektiği gibi zaman damgası tek başına iletimin veri onayını, bütünlüğünü, gizliliğini sağlamadığını belirtmeliyiz. Zaman damgası, elle atılan imzaya benzer bir orijinallik sağlama işlevine sahip değildir. Nitekim, 7. Bölüm, İmza/İşaret Hakkında Zaman Damgası Verisi Standartlarında, saklanan veya iletilen biyometrik imza verisi bakımından onay, veri bütünlüğü, gizlilik sağlanması için ayrıca şifreleme yöntemlerinin kullanılması tavsiye edilmiştir.[33] Belirtilen hususlar çerçevesinde, biyometrik imzanın elle atılan imza ile aynı özelliklere sahip olmadığı düşüncesindeyiz.

Biyometrik imza ve elle atılan imzanın işlevsel farklarından belki daha önemlisi, biyometrik imzanın (konumuz bakımından ekran üzerinde elle atılan imzanın), görünürde bir imza olmakla beraber esasında bir dijital veri olmasıdır. Ekrana yansıyan her nokta görüntü gibi imzanın ekrandaki görüntüsü de 0 ve 1'lerden oluşan bir digital veridir. Bağlanan elektronik verinin ne zaman bir güvenli elektronik imza sayılacağı EİK'da net şekilde düzenlenmiştir. Yine EİK sadece güvenli elektronik imzanın elle atılan imza ile aynı hukuki sonuçları doğuracağını ve HMK m. 203'de sadece güvenli elektronik imzalı belgelerin senet sayılabileceği açıkça düzenlenmiştir. Düşüncemize göre, konumuz biyometrik imzanın tek başına (dijital imza teknolojisi ile birleşmeden) güvenli elektronik imzanın unsurlarını (EİK m. 4) sağlamadığı açık olduğundan biyometrik imzalı belgenin de senet sayılması (günümüzde) mümkün değildir.

Avrupa Birliği'nin 910/2014 sayılı "Elektronik İşlemler İçin Elektronik Kimlik ve Güven Hizmetleri Tüzüğü, önemli yenilikler (aşağıda inceleyeceğimiz) içermektedir. Tüzük, özellikle sertifika hizmet sağlayıcılarının yerel ülkelerde kurulması ve karşılıklı tanınması zorlukları karşısında, merkezi bir çatı geliştirilmesine; ayrıca, farklı üye ülkelerde kullanılan farklı dijital imza servis sağlayıcılarının ve teknolojilerinin karşılıklı tanınmasına odaklanmış ve böylece elektronik imzanın uluslararası alanda kullanımının kolaylaştırılması hedeflenmiştir.[34]

AB Elektronik İşlemler Tüzüğü birçok yenilik getirmiş ve akabinde standartları belirleyen birçok ikincil düzenleme kabul edilmiştir. Bunlardan biri, sunucu imzası (server signing) uygulamasıdır. Bu uygulama önce, 2014'de (CEN/TS 419241:2014 - Security Requirements for Trustworthy Systems Supporting Server Signing) düzenlenmiş; bu protokol, akabinde çok daha gelişmiş şekilde ve nitelikli elektronik imza unsurlarını karşılar şekilde 2018 tarihinde yeniden düzenlenmiştir.[35] Sunucu imzası (servis signing) sisteminde, uygun protokol ve güvenlik yazılımları çerçevesinde, bir uygulama yazılımı ile sunucu tarafından muhafaza edilen ve uzaktan kumanda edilen imza oluşturma aracı cihazı bulunur. İmza sahibi ilgili yazılım ve uzaktan kumanda edilen bu cihaz sayesinde kapalı anahtarını uzaktan kontrol edebilir ve oluşturabilir. Belirtmek gerekirse, kapalı anahtar sertifika hizmet sağlayıcısında değildir ve ondan aktarılmaktadır;

[32] GÖKSU, Mustafa, Hukuk Yargılamasında Elektronik Delil, İstanbul, Adalet Yayınevi, 2011, s. 50-51.

[33] Önsöz, https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-7:ed-3:v1:en, çevrimiçi), 20/03/2022.

[34] JA, Ashiq, "The eIDAS Agenda: Innovation, Interoperability and Transparency". https://www.cryptomathic.com/news-events/blog/the-eidas-agenda-innovation-interoperability-and-transparency (çevrimiçi), 20/03/2022.

[35] (SIST EN 419241-1:2018 Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements ve EN 419241-2:2019 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing).

sunucu ayrı bir sistemdir. İmza sahibi gerekli yazılım ve cihazla, kapalı anahtarını uzaktan kullanabilmektedir;[36] böylece kapalı anahtarını bir akıllı kart ve usb vasıtasıyla yanında taşımak zorunda kalmamaktadır. Sistemin önemli avantajlarından biri, imza sahibinin (ayrıca yanında bulundurduğu bir kapalı anahtarı olmaksızın) sadece kimliğini doğrulamak (şifre, biyometrik imza gibi) suretiyle dijital imza altyapısını (nitelikli elektronik imzasını) kullanmasına imkan tanımasıdır.[37] Biyometrik imzanın sunucu imzası yöntemi ile beraber kullanılması bir nitelikli elektronik imza niteliğindedir. Bu yöntemin yaygınlaşması ile biyometrik imzanın kullanımı oldukça artabilir. Vurgulamak gerekirse, iletim sırasında veri bütünlüğünü sağlayan biyometrik imza değildir; biyometrik imza kimlik doğrulama aşamasında oldukça etkin kullanılabilmektedir. Biyometrik imzanın bu özelliği yeni kurulan dijital imza altyapısı (sunucu üzerinden imzalama yöntemi) ile birleşince hızlı, basit ve bir nitelikli elektronik imza (EİK bakımından bir güvenli elektronik imza) teknolojisi elde edilebilmektedir. Bu bağlamda, her iki teknolojinin beraber kullanılması önemli avantajlar sağlayabilir.

Vurgulamak gerekirse, biyometrik imzaların ileride de nitelikli/güvenli elektronik imza yerine geçmesi ve tek başına kullanılması önünde zorluklar vardır. Biyometrik imzanın aktarım sırasında veri bütünlüğünü nitelikli/güvenli elektronik imza seviyesinde sağlaması niteliği gereği mümkün görünmemektedir. Ayrıca biyotmetrik imzanın kişiye özgü olması, teorik olarak taklit edilemez olması gibi çok önemli avantajları olduğu gibi bazıları güvenlik açıklarına sebep olan önemli dezavantajları da vardır. Öncelikle biyometrik veriler bir pin kodu veya usb bellekte taşınan kapalı anahtar gibi değiştirilemezler ve yerine yenileri konulamaz. Bu sebepler, biyometrik verilerin çok iyi saklanması gerekir;[38] bir kez kopyalandıklarında geri dönüşü bulunmamaktadır. Bunun yanında, bazı biyometrik veriler doğası gereği değişken olabilir ve ölçümle sapma gösterebilir. Bu bağlamda, bazı biyometrik veriler tamamen benzersiz değil yarı benzersiz kabul edilirler. Mesela kullanıcın ses komutu ile kullanıcının kayıtlı ses verisi karşılaştırıldığında çok katı bir benzerlik/eşleşme aranırsa, gerçek sesin dahi reddedilmesi mümkündür; nispeten katı olmayan bir benzerlik/eşleşme aranırsa bu kez sistemin aldatılması mümkün olacaktır.[39] Ayrıca biyometrik verilerin saklanması, kişisel verilerin korunması mevzuatı açısından farklı sorunlara yol açabilir veya ayrıca tedbirler alınmasını gerektirebilir.[40]

Yukarıda belirtilen hususlar çerçevesinde, biyometrik imzaların kullanım kolaylığı gibi önemli avantajları olması yanında önemli güvenlik sorunlarında da vardır ayrıca biyometrik imza niteliği gereği veri bütünlüğü koruması bakımından nitelikli elektronik sertifika ve imza doğrulama araçlarının işlevlerini yerine getiremez. Önümüzdeki dönemde, biyometrik imzaların, dijital imza ile kombine edilen uygulamalarda[41] veya nispeten daha az güvenlik seviyesi gerektiren işlemlerde veyahut elektronik mühürleme gibi farklı güvenlik uygulamalarında kullanılması ve yaygınlaşması beklenebilir.

c. Kapalı Anahtar Şifrelemesine (Single Key Encryption) Dayalı Elektronik İmzalar

Kapalı anahtar teknolojisi, elektronik imza meydana getirmek için kullanılan teknolojilerden biridir ve simetrik şifreleme yöntemine dayanır. Bu bağlamda, şifrelemenin ve şifrelemenin bir türü olarak simetrik şifrelemenin incelenmesi gerekecektir.

(1). Şifreleme (Encryption)

Şifrelemenin değişik türlerinin, bilgi güvenliğinin temin edilmesi amacıyla, kullanılma-

[36] General Information, https://standards.iteh.ai/catalog/standards/cen/0a3d58ed-04b4-4d14-a69e-2647c47e-26ba/en-419241-1-2018, (çevrimiçi), 20/03/2022.

[37] KESER BERBER, (Biyometrik İmza), s. 3.

[38] Promoting confidence in electronic commerce UN, s. 27, parag. 55.

[39] Bkz. Promoting confidence in electronic commerce UN, s. 27, parag. 56.

[40] Promoting confidence in electronic commerce UN, s. 28, parag. 57; ayrıca bkz. ŞİMŞEK / ÖZCAN / ERGUN / ÇELİK, s. 142-143.

[41] Bkz. ERBAYRAKTAR, Burcu, Güvenli Elektronik İmza, İstanbul, Oniki XII Levha Yayınları, 2016, s. 31.

sı dört bin yıldan önceye dayanır.[42] Şifreleme (Kriptoloji), haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür.[43] Şifreleme işlemi, şifreleme anahtarı ile özgün bilginin, içerik açısından anlamsız bir sayısal veriye dönüştürülmesi olarak düşünülebilir. Şifrelemede mesajı şifreleyen taraf (gönderici) korunmasız bir bilgiyi kodlanmış ve korunmalı bir metin haline getirir. Karşı taraf (alıcı) ise kodlanmış metni çözerek orijinal haline geri döndürür.

Şifreleme, matematiksel fonksiyonları (şifreleme algoritması) kullanarak düz dokümandan, dokümanı ifade eden bir seri sayı ve yine bir sayı serisi olan anahtar çıkartır. Sonuç şifrelenmiş dokümandır.[44] Orijinal metin "sade metin", dönüştürülmüş metin ise "şifreli metin" olarak adlandırılır.[45] Şifreleme teknolojisi güvenliğinin kalitesi, şifreli bir mesajın gizli şifreye sahip olmayan kimse tarafından çözülme girişimine karşı ne kadar dayanıklı olduğu ile ölçülür. Şifreleme anahtarı ne kadar uzun olursa, şifreli metne erişim de o kadar zor olacaktır. Bir anahtarın uzunluğu bitlerle ifade edilir. Her bir bit 0 veya 1 den oluşur. Mesela, 56 bit şifrelemede 2 üzeri 56 farklı ve muhtemel anahtar kullanılmaktadır.[46] Belirtmek gerekir ki, teknoloji ile birlikte anahtarlarda uzamakta ise de, teknoloji ile birlikte anahtarları çözebilecek teknolojide gelişmektedir. Örnek vermek gerekirse 1945'de bir milyar dolara kırılabilen şifreleme sistemleri günümüzde 10.000 dolara kırılabilmektedir.[47] Buna karşılık, anahtar uzunluğu, kural olarak bu anahtarları fiziksel saldırı ile çözebilecek teknolojinin ilerisinde seyreder. Bu bağlamda, son teknoloji ile korunmuş ve gerekli tedbirlerin alınmış olduğu bir şifrenin çözülmesi, çok düşük bir olasılıktır.

Şifrelemeyi açıklamak için en eski ve basit şifreleme yöntemlerinden birisi olan Sezar yöntemi örnek gösterilebilir. Sezar döneminde kullanılan bu yöntemde harflerin yeri değiştirilir. Şifrelenecek metindeki harfler alfabede 3 harf kaydırılarak değiştirilir.[48] Mesela,

Sezar Şifresi: ci= E(pi) = pi+3 mod 29

Açık Mesaj (Sade Metin): Gizli Bilgi

Şifreli Mesaj (Şifreli Metin): Ilcol Dloıl

(2). Simetrik Şifreleme (Symetric Encryption)

Simetrik şifreleme yöntemi, şifreleme ve çözmek için aynı anahtarı kullanan şifreleme yöntemidir.[49] Bu yöntemde şifrelemek ve çözmek için tek anahtar kullanıldığından alıcı ve göndericinin aynı şifreye sahip olması gerekir.

Simetrik şifrelemede kural olarak üçüncü şahıs yoktur. Gönderici anahtar vasıtasıyla veriyi şifreler, oluşan anlamsız veri, alıcı tarafından aynı anahtarla eski haline getirilir. Şifrelemede temel güvenlik problemi şifrelenmiş verinin üçüncü şahıslar tarafından elde edilmesi değil, şifreyi çözecek anahtarın yetkisiz kişilerce elde edilmesidir. Yoksa güçlü bir anahtar ile şifreli bir verinin bu anahtara sahip olmadan çözülmesi imkansıza yakın düşük bir olasılıktır. Onun içindir ki güvenilir bir şekilde anahtarın dolaşımını sağlayacak (göndericiden alıcıya ulaştıracak) anahtar dağıtım yapısına[50] ihtiyaç duyulur. Bu altyapı da aşağıda inceleyeceğimiz açık anahtar altyapısıdır.

[42] Kriptolojinin tarihçesi için bkz. TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr.

[43] TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr; karş. İNALÖZ, Ayşe, Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Uzmanlık Tezi, Telekomünikasyın Kurumu, Ankara, 2003 s. 28.

[44] REED, Chris, "What is a Signature?", Journal of Information, Law and Technology 2000(3), https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/, 10/03/2022.

[45] K. WINN, Jane, "Bagajsız Kuryeler: Kıymetli Evrak ve Dijital İmzalar", Çev. Hayri Bozgeyik, Hüseyin Altay, http://www.e-akademi.org/makaleler/bozgeyik-altay-1.htm, (çevrimiçi), 05/03/2022 parag. 43.

[46] WINN, parag. 46.

[47] WINN, parag. 45.

[48] TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr.

[49] ALTINIŞIK, s. 81.

[50] WINN, parag. 55.

Günümüzde farklı matematiksel metotlardan hareket eden şifreleme yöntemleri mevcuttur. Bu simetrik şifreleme yöntemlerinden en çok kullanılanlardan biri (DES) Veri Şifreleme Standart'tıdır (Data Encryption Standard - DES). Bu standartta 56 bit anahtar kullanılır; bazı Şirketler daha güvenli şifreler kurmak için üçlü DES kullanmaktadır.[51] Üçlü DES (3DES), üç adet DES anahtarının artçı şekilde kombine edilmesidir. Temel mantık, verinin anahtar olmadan çözülemeyecek kadar fazla karıştırılmasıdır.[52] AES, NIST (National Institute of Standards and Technology) tarafından 2001 yılında yeni Amerikan standardı olarak belirlenmiştir. 2003 yılından itibaren yaygın olarak kullanılmaya başlanmıştır.[53]

2. Dijital İmzalar (Sayısal İmzalar)[54]

Elektronik imza çeşitleri içinde, en çok üzerinde durulan ve kullanımı en kolay, verimli, etkin ve düşük maliyetli olabileceği belirtilen tür ise açık anahtar şifrelemesine (public key criptography) dayanan dijital imzalardır.[55] Dijital imza, el yazısı ile atılan imzanın sahip olduğu özelikleri, elektronik belgeler bakımından sağlamaya çalışan bir yöntemdir.[56] Bu konuda en gelişmiş, en güvenilir ve en yaygın çözüm dijital imzadır.[57] Dijital imzanın kör imza, tuzak imza, vekalet imza, inkar edilemez imza gibi kendi içinde bazı çeşitleri vardır.[58]

Elektronik imzalar güvenlik seviyelerine göre dört gruba ayrılabilir. Birinci seviye, sıklıkla "tamam", "onaylıyorum" ikonlarının tıklanması ile meydana gelen elektronik imzadır. İkinci seviye için genellikle şifre (password) uygulamaları ve kredi kartları örnek gösterilmektedir. Üçüncü seviyede biyometrik imzalar sayılır. Dördüncü ve en güvenli seviyede ise, açık anahtar altyapısına dayalı dijital imzalar sayılmaktadır.[59]

Dijital imzalar asimetrik şifrelemeye dayalı oluşturulan imzalardır. Belirttiğimiz üzere simetrik şifrelemede tek ve gizli bir anahtar kullanılmaktır. Asimetrik şifrelemede tek anahtar yerine iki anahtar kullanılmaktadır. Bu anahtarlardan biri açık, diğeri gizli anahtardır. Bu anahtarlar birbirini tamamlar şekilde kullanılmaktadır.[60] Bu teknolojinin ayırt edici unsuru açık anahtar olduğundan, asimetrik şifrelemenin karşılığı

---

[51] "Data Encryption Standart", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html, (çevrimiçi), 23/10/2021.

[52] REED, (web); WINN, parag. 43.

[53] TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr.

[54] Türk Dil Kurumu Türkçe Sözlüğüne göre "dijital" ve "sayısal" terimleri aynı anlama gelmektedir. Konu hakkındaki yazılarda da dijital imza ve sayısal imzanın aynı anlamda kullanıldığını sıkça rastlanmaktadır. Örnek olarak bkz. İNALÖZ, s. 15; H. KÜÇÜKÖZYİĞİT, Galip, "Elektronik Ticaret, Elektronik İmza ve Hukuk", http://www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc, (çevrimiçi), 04/05/2005; Elektronik Ticaret Hukuk Çalışma Raporu 03/05/1998, http://www.e-ticaret.gov.tr/raporlar/hukuk.htm, 04/10/2005; "Elektronik İmza Faydalı Bilgiler", http://www.tk.gov.tr/eimza/E-Imza_Faydali_bilgiler.htm, (çevrimiçi), 22/10/2005; AHİ, Gökhan, "Hukuki Bakımdan Dijital (Sayısal İmza)", http://www.hukukcu.com/bilimsel/ kitaplar/sayisalimza.htm, (çevrimiçi), 23/10/2005; ÖZYILMAZ, Ayşe / EVSENAL, Saliha, "Elektronik İmzalar", Aktive E-Ticaret, 2000, (çevrimiçi) , 25/10/2005.

[55] SMENDIGHOF / HILL, (web).; BİRSEN, Acır, Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, SPK Yeterlilik Etüdü, Ankara, 2000, s. 30.

[56] KESER BERBER, Leyla, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Ankara, Yetkin Yayınları, 2002 s. 127.

[57] SPYRELLI, Christina, "Electronic Signatures: A Transatlantic Bridge? An EU und US Legal Approach Towards Electronic Authentication", Journal of Information, Law and Technology, 2002(2), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/, (çevrimiçi), 22/10/2005; MURRAY, Jamie, "Public Key Infastructure Dijital Signatures and Systematic Risks", Journal of Information, Law and Technology, 2003(1), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/murray/, (çevrimiçi), 23/10/2004; EKŞİ, Nuray, "Elektronik İmzalara İlişkin UNCITRAL Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme", Yasa Hukuk Dergisi, İstanbul, 2001/03, s. 336-337; ORTA, s. 41.

[58] Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, http://2002.bilisimsurasi.org.tr/, s. 83; ACIR, s. 30.

[59] Bkz. STERN, Jonathan, "The Electronic Signatures in Global and National Commerce Act", www.law.berkeley.edu/institutes/bclt/pubs/annrev/exmplrs/csum/jscs.doc, (çevrimiçi), 20/10/2005; BLYTHE, s. 3-4.

[60] R. MERRILL, Charles, "Proof, What and When in Electronic Commerce", http://abanet.org/scitech/ammerr.html, (çevrimiçi), 10/04/2005; RAYSMAN / BROWN, (web).

olarak açık anahtar şifrelemesi terimi kullanılmaktadır. Dijital imza teknolojisini, açık anahtar şifrelemesine dayalı açık anahtar altyapısına dayanmaktadır.

Açık anahtar şifrelemesinde, anahtar çifti genellikle şu şekilde kullanılmaktadır. Kapalı anahtar gönderici tarafından taşınır bir hafıza kartında[61] taşınır. Gönderici, ne zaman şifreli bir veri iletmek isterse, bilgisayar veya bilgisayar fonksiyonu gören bir cihaza kartını okutur, veriyi şifreler, cihaz vasıtasıyla internet üzerinden şifreli veriyi alıcıya gönderir artık göndericinin işi bitmiştir. Gönderici kartını cebine koyar ve saklamaya devam eder. Alıcı internet bağlantılı cihazına şifreli veri geldiğini gördüğü zaman göndericinin açık anahtarına ulaşarak verinin şifresini çözer.[62]

a. Açık Anahtar Şifrelemesi (Public Key Encryption)

Günümüzde internet üzerinden yapılan işlemlerde güvenliği sağlamak için üzerinde en çok durulan şifreleme sistemi açık anahtar şifrelemesidir.[63] Bu yapıda birbirini tamamlayıcı açık ve kapalı anahtarlar kullanıldığını belirtmiştik. Kapalı anahtar, sadece imza sahibi tarafından dijital imza oluşturmak amacıyla kullanılan anahtardır. Açık anahtar, imzaya güvenen tarafça dijital imzanın doğrulunu denetlemek için kullanılan anahtardır.[64] Gönderici elinde bulunan metni gizli anahtarını kullanarak şifreler ve alıcıya gönderir. Alıcı şifrelenmiş mesajı ancak açık anahtarı[65] kullanarak çözebilecektir.

Kullanıcısının, kapalı anahtarı gizli tutması beklenir, imzanın alıcısının kapalı anahtarı bilmesine gerek yoktur.[66] Bu yönde dijital imzalar akıllı kartlar içinde,[67] kişisel bir tanımlama kodunun arkasında veya biyometrik yöntemlerle tutulurlar.[68] Kapalı anahtarın bir akıllı kart veya usb yerine doğrudan kullanıcının bilgisayarında tutulması da mümkündür. Ancak bu halde imzanın taşınması mümkün olmayacağı gibi kopyalanamaya daha açık olacağından güvenlik zafiyeti de ortaya çıkabilir.[69]

Açık anahtar ise herkesin ulaşabileceği şekilde tutuluyor olmalıdır (mesela elektronik ortamdaki bir sicilde veya dizinde) ki, alıcı bu anahtara ulaşarak şifreli metni çözsün. Bu yöntemde gizli şifre hiçbir zaman alıcının veya üçüncü şah-

[61] Bu kart genellikle "akıllı kart (smart card)" olarak adlandırılır. Güvenlik sebepleriyle tercih edilmemekle beraber kapalı anahtarın sabit diske (bilgisayara) yüklenmesi de mümkündür (ALTINIŞIK, s. 81). Günümüzde buluta (server signing) yüklenmesi de mümkün hale gelmiştir.

[62] REED, (web); SPYRELLI, (web); MENAIS, (web).

[63] ERSOY, Zeynep, Elektronik Ticaret ve Ticaret Noktaları, T.C. Başbakanlık Dış Ticaret Müsteşarlığı İhracatı Geliştirme Etüd Merkezi, 1999, s. 50; Bu şifreleme metodunun üçüncü kişiler tarafından çözülmesinin (deşifre edilmesinin) hemen hemen imkansız olduğu ifade edilmiştir (Savaş Bozbel, "İnternet Üzerinden Yapılan Hukuki İşlemler ve Bu Konudaki 97/7 sayılı AB Yönergesi ile Almanya ve İsviçre'deki Düzenlemeler", (çevrimiçi), http://www.hukukcu.com/bilimsel/kitaplar/ internet_uzerinden_hukuki_islem.htm, 16/05/2005); aynı doğrultuda günümüzde kullanılan en güvenli elektronik imzanın dijital imza olduğu belirtilmiştir. (EKŞİ, s. 338; KUBİLAY / AKINTÜRK, s. 339).

[64] "UNCITRAL model Law on Electronic Signatures with Guide to Enactment 2001", http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf, (çevrimiçi), 20/10/2005. parag. 38.

[65] Açık anahtar, kural olarak daha önce kanunen tespit edilmiş bir sicile kaydedilmiş, ancak her halükarda alıcı tarafından ulaşılabilecek bir şifredir (BOZBEL, (web).; aynı yönde, COX, Buket Öztuna, Avrupa Birliği Hukukunda Elektronik Ticaret ve Türkiye'deki Gelişmeler, İstanbul, Pusula Yayıncılık, 2002, s. 34).

[66] MERRILL, (web).

[67] Bu noktada kapalı anahtar şifresinin kullanıcının bilgisayarına yüklenerek bilgisayar içinde tutulması sağlanabilir. Böylece kullanıcının kapalı anahtar şifresini yanında taşımak yerine bilgisayarında tutması sağlanabilir. Ancak bu yöntemin kullanılması, kullanıcının bilgisayarına yetkisiz bir kişinin fiziksel olarak veya internet üzerinden erişmesi halinde büyük sakıncalar doğurabilecektir. Öte yandan, kapalı anahtar şifresinin (akıllı kart vasıtasıyla) adeta bir kredi kartı gibi kullanıcı tarafından taşınması ise kartın kaybolması veya çalınması tehlikesi doğuracaktır. Bu tehlikelere karşı akıllı kartlar PIN kodu veya biyometrik yöntemlerle korunur.

[68] UNCITRAL Electronic Signatures Guide, parag. 38.

[69] Bkz. ÖCAL, Ayşe, "Elektronik Ticaret Hakkında UNCITRAL Model Kanunu ve Elektronik İmzalar Hakkında UNCITRAL Model Kanunu Üzerine Değerlendirme" Terazi Hukuk Dergisi, 2017, Cilt 12, Sayı 129, ss. 96-114, s. 109-110.

sın eline geçmez. Gönderici ile alıcı farklı şifreler kullandığından gizli şifrenin alıcıya transferine gerek olmamaktadır. Bu şekilde gizli şifrenin çözülmesi de teorik olarak mümkün olmayacaktır.

Her ne kadar açık ve kapalı anahtarlar matematiksel olarak ilişkili de olsalar, güvenli bir şekilde tasarlanmış ve geliştirilmiş bir kapalı anahtar şifreleme sisteminde kapalı anahtarı açık anahtar olmadan kullanmak mümkün değildir.[70] Başlıca açık anahtar şifreleme yöntemleri (algoritmaları) RSA, Eliptik Eğri Sistemleri, El Gamal ve Diffie-Hellman olarak sayılabilir.[71] Açık ve kapalı anahtarlar üzerinden en sık kullanılan algoritmalar, çok geniş sayıların önemli şekilde belirleyiciliğine dayanmaktadır. Bunlar bir kere birbiri ile çarpıldı mı oluşan yeni ve daha geniş sayının hangi sayılardan meydana geldiğini belirlemek çok zor ve zaman alıcıdır. Bu sayede birçok kişi imza sahibinin açık anahtarını bilse de ve imzanın doğrulanmasında kullansa da imza sahibinin kapalı anahtarını keşfedemez veya dijital imzayı taklit edemez.[72]

b. Hash Fonksiyonu - Öz Değeri (Hash Value)

Dijital imza sahibi, öncelikle gizli anahtarıyla, hazırladığı metni şifreleyecektir. Gizli anahtar ile verilerin tamamının şifrelenmesi halinde gönderilecek mesajın boyutu iki katına kadar artabilmektedir. Bunun yanında, algoritma yapısından dolayı böyle bir şifreleme uzun sürede gerçekleşecektir. Aynı şekilde şifrelenmiş mesajın çözülmesi de zaman alacaktır. İşte hiçte pratik olmayan bu işlemi kolaylaştıracak bir yöntem geliştirilmiştir.[73] Mesajın, kullanılan algoritmaya göre 124 bitlik, 196 bitlik veya 256 bitlik (boyut daha fazla da artabilir), özetleri çıkartılır (verilerin hash değeri alınır) ve bu özet gizli anahtar ile şifrelenir. Bu hash değeri tamamen bilgisayarda seçilen ve işaretlenen metne özgü olup, bu metinde yapılacak bir değişiklik, elde edilen hash değerini değiştirecektir.[74] Hash değerinin bu özelliği sayesinde, dijital imzalı belgenin alıcısı kendisine gelen metnin hash değerini alarak, bu değeri gönderilen mesajın hash değeri ile karşılaştırır. Sonuç aynı değil ise mesaj değiştirilmiştir. Hash fonksiyonu sayesinde, zamandan ve bilgiden tasarruf edildiği gibi, daha önemlisi, dijital imzalı belgenin doğruluğu, bütünlüğü kontrol edilebilmektedir. Başka bir deyişle, metnin şifrelenmeden önceki hali ile deşifre edilmiş halinin aynı olup olmadığının tespiti sağlanır. Dijital imza bu fonksiyonunu, hash (öz) değerler sayesinde yerine getirir.

Hash fonksiyonu, genellikle mesajın özeti olarak adlandırılan mesajın dijital bir sunumu, mesajın sıkıştırılmış halini yaratan algoritma temelli matematiksel bir işlemdir. Hash fonksiyonu mesajdan genellikle daha kısa standart bir uzunluğa sahip ve temel olarak mesaj ile aynı olmayan "hash değeri" veya "hash sonucu" biçiminde görülür.[75] Teknik açıdan dijital imza, imzalanmış belgenin özünü (Hash) içerir. Şifrelenen metnin içeriğinde yapılacak herhangi bir değişiklik dijital hash'ı geçersiz kılacaktır. Hazırladığı mesajı imza etmek isteyen kimse, mesajının hash değerini hesaplamak için, bir hash fonksiyonu kullanacaktır. Bu şekilde elde edilen hash değeri, gizli şifre ile şifrelenir. Alıcı kendisine gelen belgenin hash değerini, öncelikle gönderenin açık şifresi yardımıyla tespit eder. Bunun dışında, alıcı bir kez de, kendisine gelen metnin hash değerini saptar, son olarak elde edilen her iki hash değeri karşılaştırır. Her iki hash değeri tutuyorsa (aynı ise), alıcı, bu belgenin göndericinin orijinal belgesi olduğunu ve mesajın sonradan değiştirilmediğini anlayacaktır. Şifreli mesajın değiştirilmiş olması halinde ise, hash değerleri farklı olacaktır.[76] Bu yöntemle taraflar şifreli mesaj gönderildiği sıra-

[70] FREEMAN, (web).

[71] TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr.

[72] UNCITRAL Electronic Signatures Guide, parag. 38.

[73] ÖZGÜL, Mehmet Emin, "İnternette Hukuki Güvenlik Dijital İmza", inet-tr.org.tr/inetconf8/bildiri/ 141. doc., (çevrimiçi), 09/11/2005.

[74] ŞENOCAK, s. 100; EROL, 57; SÖZER, Bülent, Elektronik Sözleşmeler, İstanbul, Beta Yayınları, Mart 2002, s. 127 vd..

[75] UNCITRAL Electronic Signatures Guide, s. 22-23; parag. 40.

[76] LUPTON, W. Everett; "The Digital Signature: Your Identiy by the Numbers", http://law.richmond. edu/jolt/v6i2/note2.html, (çevrimiçi), 03/11/2005; KESER BERBER, [Dijital İmza], s. 150; ACIR, s. 32.

da ve yer değiştirme sırasında[77] mesajın içerdiği metnin orijinalliğinin bozulup bozulmadığı, mesaja müdahale edilip edilmediği konusunda yüksek derecede güvenliğe sahip olurlar.

Hash fonksiyonunun çalışma prensibinden anlaşılacağı üzere, hash değerlerinin birbirini tutmadığı anda mesajın değiştiği anlaşılmaktadır. Bir harfin değişmesi dahi hash değerlerinin farklı çıkmasına yol açar.[78] Buna karşılık, bu fonksiyon ile, iletilen verindeki değişikliğin verinin hangi kısmında olduğu anlaşılamamaktadır. Kısaca dijital imzalar, imzalanmış belgenin değiştirilip değiştirilmediğini kullanıcısına gösterse de değişikliğin ne yönde olduğunu göstermemektedir.

c. Açık Anahtar Altyapısı - AAA (Public Key Infrastructure - PKI)

Bir dijital imzanın doğrulanabilmesi, için doğrulayıcının (alıcının) imza sahibinin açık anahtarına ulaşabilmesi ve ulaştığı açık anahtarın, imza sahibinin açık anahtarını karşıladığına güvenmesi gerekir.[79] Açık anahtar şifrelemesi, açık anahtarı sağlayacak ve yönetecek güvenilir üçüncü kişilerin yani dijital imza sisteminde onay kurumunun (elektronik sertifika hizmet sağlayıcılarının) varlığını gerektirir. Dijital imza kullanılabilmesi, açık anahtar şifrelemesi doğrultusunda açık anahtar altyapısı geliştirilmesi sayesinde mümkün olabilecektir. Açık anahtar altyapısı sistemi, temel olarak dijital imzalarının kullanımını sağlayan şifreleme anahtarlarının ve dijital sertifikaların oluşturulması, kullanılması ve yönetimi kurumunu şart koşar[80] ve bu altyapı sayesinde açık anahtar şifrelemesinin, onay kurumunun (elektronik sertifika hizmet sağlayıcısının) ve sayısal sertifikaların (nitelikli elektronik sertifikaların) bütünleşmesi sağlanır.[81]

Bir açık anahtar altyapısının temeli, genellikle çeşitli hiyerarşi içindeki otoritelerden meydana gelir. Örnek olarak, bazı ülkelerde açık anahtar altyapısı kurmak üzere meydana getirilmiş modeller şu seviyede referanslar içerir, a) kullanılan teknolojiyi onaylayacak ve tüm kuruluşların yetkili şifreli anahtar çiftlerini kullanmasını sağlayacak veya şifreli anahtar çiftlerinin kullanımını ve bunların alt kök sertifika otoritesine kaydını sertifikalandıracak temel bir "kök otorite" b) bir kullanıcının açık anahtarının, o kullanıcının kapalı anahtarını karşıladığını onaylayacak kök otoritenin altında çeşitli sertifika otoriteleri c) şifreli anahtar çiftleri kullanıcılarının isteklerine bakacak veya ilişkili sertifikaların şifreli anahtar çiftlerinin kullanımı ile, kimliğin kanıtlanmasını sağlayacak ve potansiyel kullanıcıların kimliklerini denetleyecek sertifika otoritelerinin altında çeşitli yerel kayıt otoriteleri.[82]

d. Onay Kurumu (Sertifika Hizmet Sağlayıcıları)

Onay kurumu, farklı hukuk mevzuatlarında ve açık anahtar altyapısı kapsamındaki farklı sistemlerde farklı adlarla adlandırılmaktadır. Onay Makamı, Sertifikasyon Otoritesi, Bağımsız Sertifika Otoritesi, Güvenli (Güvenilir) Üçüncü Taraf, Sertifikalandırma Kurumu, Belgelendirme Mercii ve benzeri ifadelerle[83] kastedilen temelde onay kurumu olarak adlandırabileceğimiz kurumdur.[84]

Onay Kurumu, internet servis sağlayıcılarının veya bilgi teknolojisi donanımı ve yazılımını sağlayıcılarının tipik bir örneğidir. Bu kurum, açık anahtar altyapısının etkili bir biçimde çalışmasını sağlayacak çok çeşitli servisler içerir. Hizmet sağlayıcısının temel servisi kayıt kurumudur, bunun yanında sertifika sağlanması amacıyla anahtar üretme servisi (sertifika makamı), anahtar yönetim servisi, açık anahtar iptal servisleri, anahtarın

77 WINN, parag. 59.

78 RAYSMAN / BROWN, (web).

79 UNCITRAL Electronic Signatures Guide, s. 25; parag. 45.

80 FREEMAN, (web).

81 İNALÖZ, s. 34.

82 UNCITRAL Electronic Signatures Guide, parag. 51.

83 Elektronik İmzalar Hakkında UNCITRAL Model Kanunu'nda, Avrupa Birliği Direktifi'nde ve Türk Elektronik İmza Kanunu'nda Onay Kurumu, "Sertifika Hizmet Sağlayıcısı" olarak anılmaktadır.

84 İlkesel olarak güvenilir ve tarafsız üçüncü kişiler olmaları itibariyle noterlere de benzetilmektedirler (ÖCAL, s. 108) ancak bu ancak şekli bir benzerlik olabilir zira onay makamının statüsü ve onay prosedürü oldukça farklıdır.

son kullanıcılara sağlanması servisi (Sertifika Deposu)[85] ve benzeri servisler de hizmet sağlayıcının bünyesinde çalışır.[86] Açık anahtar altyapısı elektronik imza üretmek için kullanılan uzak ara en karmaşık yapı olması yanında, tam olarak internetin açık ortamında nelere ihtiyaç duyulduğuna yönelik tasarlanmış bir yapıdır.[87] Bu servislerin güvenilir bir biçimde sağlanması "onay kurumunun" sorumluluğundadır.[88] Onay kurumu olmadan dijital imzanın kullanılması da mümkün değildir.[89]

Onay Kurumu'nun temel işlevi, sertifika hizmeti sağlamak olarak özetlenebilir. Sertifika ise en basit anlamıyla onay belgesi olarak adlandırılabilir. Bu belge, göndericinin kimlik bilgilerini ve açık anahtarını içeren ve açık anahtarın göndericiye (kullanıcıya, imza sahibine) ait olduğunu gösteren, başka bir deyişle, açık anahtar ile kullanıcı kimliğini birbirine bağlayan elektronik veridir. Onay kurumu, dijital imza sahibi olmak isteyen kimsenin başvurusu üzerine bu kimse adına sertifika çıkartarak, bu sertifikayı yayımlar. Onay kurumuna veya onun temsilcisi belirli kimlik tanımlama prosedürleri doğrultusunda, imza sahibi olmak için sertifika başvurusu yapan kimsenin, gerçekten o kimse olduğunu onaylar, yani kimliğini tespit eder. Onay kurumu, sertifikasyon prosedürü çerçevesinde, başvuru, onaylama, (sertifika) ihraç ve kabul prosedürlerini yürütür.[90]

Temelde, uluslararası bir AAA sistemi yoktur. Bu nedenle açık anahtar altyapıları ülkesel bazda kurulur. Ülkesel bazda kurulan bir onay kurumunun zamanla diğer ülke vatandaşlarına da sertifika sağlaması mümkündür. Lakin ülkesel olarak faaliyette bulunan bir onay kurumunda verilen bir sertifikanın başka ülkelerde geçerliliğinin sağlanması gerekir. Onay kurumları arasında dijital imzaların geçerliliklerinin sağlanması çapraz sertifikalama yöntemi ile mümkün olabilmektedir.[91] Bu yöntem ayrı ülke onay kurumlarınca düzenlenen sertifikaların geçerliliğini sağlamak yanında aynı ülke içindeki farklı onay kurumlarınca düzenlenen elektronik sertifikaların geçerliliğinin sağlanması için de kullanılmaktadır. Ancak onay kurumunu yerel bazda kurulmasının zorlukları uzun yıllar aşılmamış; tam da bu zorluklar karşısında AB Elektronik Kimlik ve Güven Hizmetleri Tüzüğü kabul edilerek, onay kurumlarının uluslararası işlemlerde etkin, basit ve hızlı bir şekilde çalışmasının yolu açılmıştır.

e. Zaman Damgası (Zaman Kaşesi)

Elektronik verilerin gönderilmesinde, saklanmasında ve kontrol edilmesinde elektronik imzanın oluşturulma zamanı önem kazanabilir.[92] Mesela, hisse senedi alım-satımı ve döviz işlemleri gibi işlemlerde tam zamanın tespit edilmesi gerekecektir.[93] Bu gibi günlük işlemlerin yanında, elektronik imzanın yürürlüğü bakımından da dijital imzanın oluşturulma zamanı belirleyici olabilecektir. Mesela, bir sertifika (çalınması veya kaybolması akabinde) bloke edilmişse, mesajın veya metnin, bloke zamanından önce mi, yoksa sonra mı imzalandığı durumu, zaman damgası sayesinde tespit edilebilir. Bundan başka, elektronik imzanın sertifika geçerlilik süresi içinde kullanıp kullanılmadığı dolayısıyla bağlayıcı olup olmadığı da zaman damgasıyla belirlenebilir.[94]

Zaman damgası, kişinin kendisinin kullandığı bilgisayar sistemi içinde oluşturulduğu takdirde, bunun değiştirilmesi de kolay olacaktır.[95] Buna karşılık, zaman damgası hizmeti onay kurumu tarafından verildiğine, hem zaman damgasının gösterdiği zaman hem de dijital imzanın fonksiyonları daha güvenilir olur.[96] Bu sebeple zaman damgası görevi güvenilir üçüncü kişilere,

[85] UNCITRAL Electronic Signatures Guide, parag. 50.

[86] Onay kurumunun servisleri için hakkında bkz. TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr; İNALÖZ, s. 26-38.

[87] MURRAY, (web).

[88] MURRAY, (web); KÜÇÜKÖZYİĞİT, (web).

[89] AKİPEK, Şebnem, "Özel Hukuk ve İnternet", http://inettr.org.tr/inetconf5/tammetin/hukuk.html, (çevrimiçi), 26/05/2005.

[90] ACIR, s. 32-33.

[91] ERSOY, s. 52.

[92] ERTURGUT, [Delil], s. 125.

[93] KESER BERBER, [Dijital İmza], s. 152; ORTA, s. 56.

[94] ERTURGUT, [Delil], s. 125.

[95] ORTA, s. 56.

[96] MERRILL, (web).

yani sertifika hizmet sağlayıcılarına yüklenmiştir. Zaman damgasının sonradan değiştirilmesini engellemek için, zaman damgasına ilişkin veri de, imzalı veriye eklenir ve sertifika hizmet sağlayıcısı tarafından imzalanır. Bu yöntem sayesinde imza verisiyle zaman damgası birbirine bağlanır ve sonradan zaman damgasında yapılacak değişikliklerin tespit edilmesini mümkün kılar.[97]

II. Bazı Uluslararası Düzlenmelerde ve EİK'da Elektronik İmza Tanımı ve Türleri

A. UNCITRAL Elektronik İmza Hakkında Kanun'dan Elektronik İmza Tanımı ve Türleri

UNCITRAL Elektronik İmza Hakkında Kanun[98] halen yürürlükte bulunan ve birçok devletin mevzuatını büyük ölçüde etkileyen temel uluslararası düzenlemelerden biridir. Model Kanunun 2/a bendinde; elektronik imza, veri mesajıyla ilişkili olarak, imzalayanın kimliğini tespit etmekte ve imzalayanın veri mesajının içeriğinde yer alan bilgiyi onayladığını göstermekte kullanılabilen, bir veri mesajına eklenmiş veya bununla mantıksal olarak bağlanmış elektronik biçimindeki veri şeklinde tanımlanmıştır. Tanım, elle atılan imzaya denk sayılan elektronik imza yanında genel olarak elektronik imza olarak adlandırılan diğer teknolojiler de kapsamaktadır. Tanımda -bilen eki kullanılarak esnek bir içeriğe sahip olması amaçlanmıştır.[99] Tanımın bir diğer özelliği ise elle atılan imzaya denk elektronik imza tanımının meydana getirilmesinin ilk koşulunu oluşturuyor olmasıdır.[100] Başka bir deyişle, elle atılan imzaya denk elektronik imzanın öncelikle genel olarak elektronik imza tanımındaki unsurları taşıyor olması gerekir. Bu aşamada vurgulamak gerekirse, genel tanıma tabi elektronik imza (basit elektronik imza) için özel ve ayrıca düzenlemiş bir hukuki etki öngörülmemiştir. Bu durum pek tabii ki tanımın önemini azaltmaktadır.

Tanımda geçen "veri mesajı" terimi Model Kanun'un 2. maddesinin c bendinde açıklanmıştır. Bu bende göre veri mesajı, elektronik bilginin karşılıklı değişimi (EDI), elektronik posta, telgraf, teleks ve telekopyalama ile sınırlı olmamak üzere, elektronik, optik veya benzer araçlarla yaratılan, gönderilen, alınan ve saklanan bilgi anlamına gelir. Tanım UNCITRAL Ticaret Model Kanunu'ndan aktarılmıştır. Tanımın neredeyse hiçbir sınırı yoktur verilen terimlerin benzerlerinin de veri mesajı oluşturması mümkündür. Bu şekilde ilerisi için öngörülemeyen teknolojik gelişmelerin de kapsam içine alınması amaçlanmıştır.[101]

Model Kanun m. 6'da, elektronik imzanın hangi şartlarda elle atılan imzayla fonksiyonel eşitliğe sahip olacağı düzenlemiştir. Buna göre, bir kanunun bir kişinin imzasını gerektirdiği hallerde, ilgili herhangi bir anlaşma da dahil olmak üzere, tüm koşullar ışığında, veri mesajının oluşturulması veya iletilmesi amacı için uygun olduğu kadar güvenilir de olan bir elektronik imza kullanıldığı takdirde, bu gereklilik (şart) yerine gelmiş sayılır. Bir elektronik imza şu şartlarda güvenilir sayılmıştır;

a) imza oluşturma verileri, kullanıldıkları koşullar içinde, sadece imza sahibi ile irtibatlı ise ve imza sahibinden bir başkası ile irtibatlı değil ise,

b) imza oluşturma verileri, imza esnasında sadece imza sahibinin kontrolünde ise herhangi başka bir kişinin kontrolünde değilse,

c) elektronik imzada, imza anından sonra yapılmış her türlü değişiklik, fark edilebilir nitelikte ise, ve,

d) bir imza için yasal şart öngörülmesinin amacı, ilgili olduğu bilginin bütünlüğü (doğruluğu) konusunda teminat sağlamakta ise, bu bilgiye ait, imza anından sonra yapılan her türlü değişikliğin fark edilebilir olması gereklidir.

[97] ERTURGUT, [Delil], s. 125-126; ERBAYRAKTAR, s. 101.

[98] UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001; halihazırda Model Kanunu'nun temel alınmak veya etkilenmek suretiyle 38 devlet tarafından kabul edildiği belirtilmiştir. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures/status, (çevrimiçi) 10.04.2022.

[99] UNCITRAL Electronic Signatures Guide, parag. 93.

[100] UNCITRAL Electronic Signatures Guide, parag. 93.

[101] UNCITRAL Electronic Signatures Guide, parag. 99.

Bu şartları sağlayan elektronik imza güvenilir elektronik imza sayılacak ve el ile atılan imza ile aynı hukuki sonucu doğuracaktır. Belirtmek gerekir ki, şartlar sınırlayıcı sayılmamıştır. Model Kanunu m. 6/IV uyarınca bir imzanın güvenilir olduğu herhangi başka bir biçimde de ortaya konulabilir veya bu şartları sağlayan bir elektronik imzanın güvenilmezliği ortaya konabilir. Model Kanun m. 7 uyarınca, yukarıda sayılan şartların yerine getirilip getirilmediği uluslararası standartlara uygun şekilde devlet tarafından yetkili kılınan kamu ve özel nitelikteki her türlü kişi ile tespit edilebilir.

B. AB Elektronik İşlemler Hakkında Tüzüğü'nde Elektronik İmza Tanımı ve Türleri

Elektronik imzanın ve neticede uluslararası elektronik ticaretin yaygınlaştırılması için önce Avrupa Birliği nezdinde, 1999/93/EC sayılı Elektronik İmza Direktifi kaldırılarak kabul edilen eIDAS Elektronik Kimlik ve Güven Hizmetleri Tüzüğü ile birçok yönden köklü değişiklikler getirdiği görülmektedir. En başta Direktif yerine bir Tüzük olması; elektronik ticaret ve elektronik imza için çok önemli standartlar getirmesi ve çok sayıda ikincil düzenlemeye yol açması; elektronik imza dışında güvenilir üçüncü kişi/kurumlarca sağlanan elektronik mühür, elektronik zaman damgası, elektronik kayıtlı iletim servisi, internet siteleri için onaylama sertifikaları farklı güvenlik servisleri konusunda kapsamlı düzenlemeler getirmesi;[102] hizmet sağlayıcıların uluslararası alanda tanınmasını sağlaması; server signing gibi yeni teknolojilere imkan tanıması; tüm AB üye devletleri vatandaşları için ortak standartlara tabi bir elektronik kimlik sağlanması gibi değişiklikler oldukça önemlidir ve bu konuların farklı bilimsel çalışmalarda ayrı ayrı ele alınması yararlı olabilir. Konumuz olan elektronik imza tanımı ve türleri bakımından ise Tüzük'ün köklü değişiklikler içerdiğini söylemek güçtür. Mülga Direktift'de kabul edilen basit, gelişmiş ve nitelikli elektronik imza tanımları ve ayrımı Tüzük'te de takip edilmiştir.

Mülga AB Direktifi m. 2/1'de, elektronik imza, diğer bir elektronik veriye eklenen ya da elektronik veriyle mantıksal bağı olan ve onaylama yöntemi olarak kullanılan elektronik formdaki veri olarak tarif edilmiştir. Tüzük'da ise, elektronik imza, diğer bir elektronik veriye eklenen ya da elektronik veriyle mantıksal bağı olan ve imza sahibi tarafından imzalamak için kullanılan elektronik formdaki verileri ifade edeceği düzenlemiştir. Görüldüğü üzere, onaylama yöntemi olarak kullanılması yerine amaçtan hareket eden bir kriterle imza sahibinin elektronik imzayı imzalamak amacıyla kullanılmasını yeterli görülmüştür. Nihayetinde, elektronik imza kullanımında amacın imzalamak olduğu açıktır. Burada imzanın temel işlevlerinden onaylama işlevi de (diğer işlevler mülga Direktif'de de atlanmıştı) atlanarak sadece amaç itibariyle bir tanım yapılmıştır. Pek tabii bu unsuru basit ve genel bir sübjektif unsur olarak kabul etmek ve elektronik imzanın elle atılan imzanın tüm işlevlerini eksiksiz yerine getirme amacıyla kullanılmasını aramamak gerekir.[103] Sonuç olarak verilen elektronik imza tanımı uyarınca, gelişmiş ve nitelikli elektronik imza dışında kalan ancak gayet kapsayıcı nitelikteki elektronik imza tanımı içerisine giren tüm elektronik imza teknik ve teknolojileri basit elektronik imza olarak adlandırılabilir.[104]

Basit elektronik imza bakımından en dikkat çekici durum, elektronik imzanın hukuki etkisi ve delil olarak kabul edilebilirliğinin elektronik imzanın elektronik formda olması veya nitelikli elektronik sertifika şartlarını sağlamaması sebebiyle reddedilememesidir (Elektronik Kimlik ve Güven Hizmetleri Tüzüğü m. 25/I; aynı yönde, mülga AB Direktifi m. 5/II). Böylece elektronik imzanın hukuki etkisi dolaylı olarak kabul edilmiş ve delil olarak dikkate alınması zorunlu kılınmıştır.

[102] Elektronik İmza Kanunu'nda da 28.01.2021 tarihli ve 7263 sayılı Kanun ile yapılan değişiklikler çerçevesinde, elektronik mühür, internet sitesi için kimlik doğrulama servisleri ayrıca düzenlenmiştir.

[103] DOMINGO, Ignacio Alamillo, SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market, https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf çevrimiçi) 10.03.2022, s. 60-61.

[104] DOMINGO, s. 71; ŞİMŞEK / ÖZCAN / ERGUN / ÇELİK, s. 138.

AB Elektronik Kimlik ve Güven Hizmetleri Tüzüğü, yine mülga AB Direktif'inde olduğu gibi, gelişmiş elektronik imza tanımıyla ayrı bir elektronik imza türüne yer vermiştir. Bir elektronik imza şu şartları taşıyorsa, bir gelişmiş elektronik imzadır: (a) imza sahibine özgün (benzersiz) şekilde bağlı olmalı, (b) imza sahibini teşhis etme kapasitesi bulunmalı, (c) imza sahibinin kendi kontrolünde bulunan ve güvenliği konusunda yüksek güven duyduğu elektronik imza yaratma verisi ile oluşturulmalı ve (d) bağlandığı veride sonradan yapılan değişiklik fark edilebilir olmalıdır. Anlaşıldığı üzere, gelişmiş elektronik imza (nitelikli elektronik imza gibi) sertifika tabanlı bulunan ve genel elektronik imza yöntemlerine göre daha yüksek güvenlik seviyesi taşıyan[105] bir imza türüdür. Her ne kadar, tanımda yine teknoloji tarafsızlığı amaçlanmış ise de düzenleme yapılırken Avrupa kanun koyucunun aklından açık anahtar altyapısının geçtiği rahatlıkla söylenebilir.[106] Gelişmiş elektronik imzanın nitelikli elektronik imzadan en önemli farkı, sertifika tabanlı olmakla birlikte sertifikanın ve sertifika sağlayıcının öngörülen kapsamlı şartları sağlamasının (nitelikli olmasının) beklenmemesidir. Gelişmiş elektronik imza için ayrıca bir hukuki etki de öngörülmüş değildir. Bu yönüyle üçlü ayrımda, gelişmiş elektronik imzanın işlevini ortaya koymak zordur. Özellikle nitelikli elektronik imza gibi açık anahtar altyapısına atıf yapılması ancak herhangi bir hukuki etki düzenlenmemiş olması eleştiriye açıktır.

AB Elektronik Kimlik ve Güven Hizmetleri Tüzüğü uyarınca, elle atılan imzanın hukuki etkilerini doğuran tek imza türü nitelikli elektronik imzadır. Gelişmiş elektronik imzanın sağlaması gereken tüm koşullara ek olarak imza sahibine dair (nitelikli) elektronik sertifikanın akredite bir ESHS tarafından verilmesini ve nitelikli elektronik imza oluşturma aracı içerisinde tutulmasını zorunlu kılar. Nitelikli elektronik imzanın oluşturulması için kullanılan nitelikli elektronik sertifikanın sağlaması gereken koşullar Tüzük Ek 1'de ayrıntılı olarak açıklanmıştır. Nitelikli elektronik imza oluşturma aracına dair aranan koşullar ise EK 2'de ayrıntılı şekilde düzenlenmiştir.

C. Elektronik İmza Kanunu'nda Elektronik İmza Tanımı ve Türleri

Tüzük'te yer alan nitelikli elektronik imza, EİK'da düzenlenen güvenli elektronik imza ile denktir. EİK'da "nitelikli" yerine neden "güvenli" kelimesinin seçildiği açık değildir. UNCITRAL Model Kanun'dan etkilenilmiş olabilir ancak bu düzenlemede "güvenilir olarak değerlendirilen" "güvenilir olarak kullanılan" gibi ibarelere yer verilmiş olmakla beraber doğrudan "güvenli elektronik imza" terimi kullanmış değildir. Belki mülga Fransız Elektronik İmza Kanunu'ndan etkilenilmiştir; zira bu Kanun'da "güvenli elektronik imza" terimi kullanılmış idi.[107]

EİK'da sadece iki elektronik imza tanımına yer verilmiştir. Biri üst kavram niteliğinde bulunan elektronik imza[108] tanımı; diğeri ise nitelikli elektronik imzanın dengi olan güvenli elektronik imza tanımıdır. Bu çerçevede, elektronik imza tanımı kapsamında bulunan ancak güvenli elektronik imza olmayan tüm elektronik imza teknik ve teknolojileri basit elektronik imza olarak adlandırılabilir. Görüldüğü üzere, basit ve güvenli elektronik imza hukuki bir ayrımdır; güvenli elektronik imza özelliklerini taşımayan (mesela nitelikli elektronik sertifikaya dayanmayan) bir dijital imza teknolojisi de basit elektronik imza tanımı içine girecektir.[109] EİK'da gelişmiş elektronik imza tanımına ise yer verilmemiştir. Sonuç olarak, EİK çerçevesinde, elektronik imza, basit

[105] ŞİMŞEK / ÖZCAN / ERGUN / ÇELİK, s. 138.

[106] DOMINGO, s. 65; sonradan yayımlanan teknik standartların da açık anahtar altyapısına işaret ettiği yönünde bkz. ŞİMŞEK / ÖZCAN / ERGUN / ÇELİK, s. 139.

[107] MENAIS, Alexandre, "Electronic Signatures in France", (çevrimiçi), http://www.juriscom.net/en/ pro/1/ ec20020730.htm, 10/02/2006.

[108] EİK Genel Gerekçesinde, öncelikle elektronik imzanın üst bir kavram olarak tanımlandığı; yapılan tanım ile sayısal imza ve biyometrik tanımlama yöntemlerinin kullanımına olanak sağlandığı belirtilmiştir. EİK'da yapılan elektronik imza tanımı ile sayısal imza ve biyometrik imzaların da kullanımına olanak sağladığının belirtilmesi yerinde olmamıştır düşüncesindeyiz. Çünkü, sayısal imza ile dijital imza aynı anlamdadır.

[109] Karş. ACAR, s. 77 dp. 36.

elektronik imza ve güvenli elektronik imza olmak üzere ikiye ayrılabilir.

EİK m. 3/b bendinde, elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri olarak ifade edilmiştir. Tanım, mülga AB Direktifi'nden de AB Elektronik İşlemler Tüzüğü'nden de küçük farklılıklar içermektedir. Aktarılan tanım çerçevesinde, elektronik imzanın, biri maddi diğeri manevi iki unsuru olduğu söylenebilir. Maddi unsur, elektronik imzanın, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan elektronik veri olmasıdır. Bu yönüyle düzenlemeler arasında ciddi bir fark yoktur. Tanımın ikinci unsuru ise elektronik imza verisinin kimlik doğrulama amacı ile kullanılmasıdır.[110] Tanımın amaç dikkate alınarak manevi unsur içermesi, yukarıda açıkladığımız üzere, mülga AB Elektronik İmza Direktif'inden farklı ancak AB Elektronik Kimlik ve Güven Hizmetleri Tüzüğü ile uyumludur.

Mülga AB Direktifi'nden ayrılan başka bir husus, Direktifi'te yer alan "onaylama-authentication" teriminin, hukukumuza "kimlik doğrulama" şeklinde aktarılmasıdır. Aradaki fark nedeniyle, EİK'ya göre, elektronik imzanın imza sahibinin bilgilerini (kimliğini) göstermesi (veya göstermeyi amaçlaması) gerekir.[111] Bu bağlamda, hukukumuzda, "OK" veya "Tamam" ikonunun tıklanması elektronik imza kabul edilemeyecektir. EİK'da yer alan tanımın AB Direktifi'nin çevirisi niteliğinde olduğu, EİK'da yer alan "kimlik doğrulama" teriminin onaylama şeklinde anlaşılması gerektiği belirtilmiştir.[112] Düşüncemize göre, kanun koyucunun tercihi bilinçli bir tercihidir ve dikkate alınması gerekir. Nitekim, AB Elektronik İmza Direktifi'ni mevzuatlarına aktaran bazı ülkeler de tanımda küçük değişikliklere gitmişti.[113] Ülkemizde de kısmen tanımı daraltmak için "kimlik doğrulama" ibaresinin bilinçli olarak seçildiğini düşünüyoruz. Buna karşılık, elektronik imza tanımının kapsamının pek de önemi yoktur. Zira elektronik imza için AB düzenlemelerinin aksine genel bir hukuki etki tanınmış değildir. Bu sebeple, tanımın pratik bir önemi görülmemektedir.

Güvenli elektronik imza EİK m. 4'te şu şekilde tarif edilmiştir: güvenli elektronik imza; a) Münhasıran imza sahibine bağlı olan, b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır. Tanımdan anlaşılacağı üzere, kanun koyucu, AB düzenlemelerinde yer alan gelişmiş elektronik imza ve nitelikli elektronik imza ayrımı yer vermemiş ve bu imza tanımlarını birleştirerek güvenli elektronik imzayı şartlarını belirlemiştir.[114]

III. Teknoloji Tarafsızlığı Prensibi Bakımından Değerlendirme

Teknoloji tarafsızlığı prensibi görebildiğimiz kadarıyla EİK dahil tüm ulusal ve uluslararası elektronik imza düzenlemelerin nispeten biraz daha katı veya yumuşak kabul edilmiş temel bir prensiptir. Teknoloji tarafsızlığı prensibi, elektronik ortamda iletişim veya bilginin depolanması için kullanılan çeşitli teknolojiler arasında ayrım yapılmaması şeklinde tarif edilebilir.[115] Bir başka tarife göre, teknoloji tarafsızlığı prensibi, hukuki düzenlemenin sonuçları itibariyle teknolojiden bağımsız olmasını ifade eder.[116] Belki ilk düzen-

[110] Elektronik imzanın üç unsuru olduğu yönünde bkz. ORTA, s. 39.

[111] Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, s. 23.

[112] Elektronik İmza Ulusal Koordinasyon Kurulu Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu, s. 23.

[113] YILDIRIM, Mehmet Kamil / PÜRSELİM, Hatice Selin, "Elektronik İmza Kanunu ve Türk İspat Hukukundaki Etkileri", İstanbul Barosu Dergisi, C. 79, S. 2005/4, s. 1105-1106 dp. 52.

[114] EİK m. 4 gerekçesi; II. Türkiye Bilişim Şurası Hukuk Çalışma Raporu, s. 8; İNAL, Emrehan, E-Ticaret Hukukundaki Gelişmeler ve İnternette Sözleşmelerin Kurulması, İstanbul, Vedat Kitapçılık, 2005, s. 143.

[115] UNCITRAL Electronic Signatures Guide, parag. 5.

[116] ERBAYRAKTAR, s. 45.

lemelerden biri olan ve halihazırda mülga bulunan Alman Dijital İmza Kanunu[117] bu prensipten istisna tutulabilir. Zira 13.7.1997 tarihinde kabul edilen 01.08.1997'de yürürlüğe giren Kanunda, adından da anlaşılacağı üzere doğrudan dijital imza teknolojisine atıf yapıldığı gibi, "onay makamı" (Kanun m. 2/II) gibi doğrudan dijital imza teknolojisi terimlerine yer verilmiştir. AB Elektronik İmza Direktifi kabul edilmesi ile Kanun yürürlükten kaldırılmış ve 22/07/2001 Elektronik İmza Kanunu[118] adı altında yürürlüğe girmiştir.[119] Temel uluslararası düzenlemelerden önce kabul edilmiş ve ardından yürürlükten kaldırılmış olması itibariyle mülga Alman Dijital İmza Kanunu gerçek bir istisna kabul edilmeyebilir.

Teknoloji tarafsızlığı prensibi, elektronik imzanın işlevi bakımından belirli kriterler öngörülerek bu kriterleri karşılayan tüm elektronik imza teknik ve teknolojilerine aynı hukuki etkinin tanınmasını gerektirir. Tabii ki amaç, teknolojinin devamlı gelişen ve değiştiği gerçeği karşısında farklı teknolojilerden yararlanma imkanı tanınması ve sıklıkla yeni düzenlemeler yapılmadan hukuk kurallarını teknolojiye ayak uydurabilmesini sağlamaktır.[120] Buna karşılık, prensibin pratikte ne kadar etkili ve yararlı olduğu değerlendirmeye açıktır. Uzun yıllar içerisinde, dijital imza teknolojisi ile sağlanan özellikle veri bütünlüğü işlevi karşısında çok temel değişiklikle olduğunu ileri sürmek güçtür. Bazı temel düzenlemeleri değerlendirdikten sonra EİK hükümlerini dikkate alarak görüşümüzü açıklamaya çalışacağız.

Yukarıda açıkladığımız üzere, UNCITRAL Elektronik İmza Model Kanunu'nun elektronik imza tanımının farklı elektronik imza teknolojilerini kapsadığı belirtilmiştir. Model Kanun m. 6'da, elektronik imzanın elle atılan imzaya denkliği dört objektif şarta bağlanmıştır. Bu şartlar hangi teknoloji ile yerine getirilirse getirilsin, bu şartları haiz bir elektronik imza elle atılan imzaya denk sayılacaktır. Model Kanunu'nun "İmza Teknolojilerine Eşit Davranılması" başlıklı 3. maddesi, aynı kanunun 6. maddesinde sayılan bir imzanın güvenilir addedilmesi şartlarını (göndereni teşhis, gönderinin sadece gönderici kontrolünde olması, her türlü değişikliğin fark edilebilir olması ve mesaj bütünlüğü) ve uygulanacak hukukun şartlarını herhangi bir şekilde yerine getiren tüm teknolojilerin hukuki etki doğuracağını ve bu hukuku etkinin sınırlanamayacağını ve ortadan kaldırılamayacağını belirtilmiştir. Aynı doğrultuda Elektronik İmza Model Kanunu Yasalaştırma Rehberi'nin 82. paragrafında, teknoloji tarafsızlığı çerçevesi başlığı altında, Model Kanun'un kullanılan teknolojiden bağımsız olarak elektronik imzaların tanınmasına ilişkin hukuki kriterler koyduğunun altı çizilmiştir.

Model Kanun'da yer alan tüm bu düzenlemelere rağmen, Model Kanun Rehberinde, belirli bir teknolojinin -dijital imza teknolojisininyürürlüğe konulduğu ve bunun uygulanması için altyapı oluşturulduğu belirtilmektedir.[121] Model Kanun ne kadar minimal düzenlemelere yer vermek istemişse de (ister istemez) kapalı anahtar, açık anahtar ve onay makamına karşılık gelen terimlere yer verilmiş; dolaylı olarak dijital imza teknolojisi konu alınmıştır.

Elektronik İmza Hakkında Model Kanun'dan önce kabul edilen UNCITRAL Elektronik Ticaret Hakkında Model Kanun madde 7'de, bir elektronik imzanın elle atılan imza ile eşit sayılabilmesi için (dört değil) sadece basit iki şart öngörülmüştü. Buna göre, bir elektronik imza metodu, kişinin kimliğini teşhis için kullanılıyor ve metne kişinin onayı olduğuna işaret ediyorsa ayrıca bu metot üretilen veya iletilen veri mesajına ilişkin amaç için uygun derecede güvenli ise elle atılan imzanın hukuki sonucunu doğurabileceği düzenlenmişti. Bu geniş

[117] Bundesgesetzblatt 1997 I s. 1872.

[118] Bundesgesetzblatt 2001 I s. 876.

[119] Bu Kanun da yürürlükten kaldırılmış ve yerine eIDAS'ın Uygulanması Hakkında Kanun kabul edilerek yürürlüğe girmiştir (Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, Bundesgesetzblatt 2017 I Nr. 52 s. 2745).

[120] Bkz. ERBAYRAKTAR, s. 53.

[121] UNCITRAL Electronic Signatures Guide, s. 19, parag. 28; BOSS, s. 693, dp. 82.

çerçevede, bir elektronik imzanın güvenilir olduğu ancak somut şartlar çerçevesinde mahkemece belirlenebilirdi. Buna karşılık, (Elektronik İmza Hakkında) Model Kanun, güvenilir olarak tanınan belirli teknolojiler bakımından ayrım yapmıştır ve sadece madde 6'da öngörülen şartlara haiz elektronik imza için elle atılan imzanın sonuçlarını tanımıştır.[122] Görüldüğü üzere, teknoloji tarafsızlığı prensibi oldukça yumuşatılmıştır; UN Elektronik İmza Hakkında Model Kanunu'nda dijital imza teknolojisinin esas alındığı söylenebilir.

Mülga Elektronik İmza Hakkında AB Direktifi'nde teknoloji tarafsızlığı prensibi açıkça kabul edilmiş ve ayrıca düzenlenmiş değildi. Buna karşılık, Direktif'de dijital imzaya dair terimler kullanılmamış; belirli kriterlere sahip her türlü elektronik imza için elle atıla imza ile eşdeğerlik öngörülmüştü. Direktif'in açıklamalar kısmında ise, hızlı teknolojik gelişmelerin ve internetin küresel niteliğinin, verileri elektronik olarak doğrulayabilen çeşitli teknolojilere ve hizmetlere açık bir yaklaşımı zorunlu kıldığını belirtilmişti (no. 8). Buna karşılık, bir kısım yazarlar bu durumun görünürde olduğunu Direktif eklerinde belirtilen şartlarla isim verilmeden açık anahtar altyapısına dayalı dijital imza teknolojisinin benimsendiğini savunmuştu.[123] Direktif'de düzenlenen basit elektronik imza ve gelişmiş elektronik imza bakımından teknoloji tarafsızlığı prensibinin benimsendiği rahatlıkla ileri sürülse dahi nitelikli elektronik imza bakımından bu görüşe katılmamak zordu.

Elektronik imzaya dair hükümler içeren yeni AB Tüzüğü teknoloji tarafsızlığı prensibi bakımından daha iddialı görünmektedir. Nitelikli elektronik imzanın unsurlarından, "yalnızca imza sahibine ait olan" (münhasıran imza sahibine bağlı olan) unsuru "yüksek bir güvenilirlik seviyesine sahip olan" şeklinde yeniden düzenlenmiştir. Yeni düzenleme, daha geniş ve nispeten sübjektif bir ifade ile unsurun gerçekleşme ihtimalini kolaylaştırmıştır. Nitekim, eski düzenlemenin nesnel bir öğeyi çağrıştırması karşısında, yeni düzenlemenin sunucu imzası uygulamasına (server signing) dair tereddütte mahal bırakmayacağı söylenebilir.

AB Elektronik Kimlik ve Güven Hizmetleri Tüzük'ünün açıklamalar kısmında, Tüzük'ün teknoloji tarafsız olduğu; elektronik imzanın yasal etkilerinin öngörülen şatları karşılamak koşuluyla her türlü teknik veya teknoloji ile sağlanabilir bulunması gerektiği açıkça belirtilmiştir (No. 27). Yine açıklamalarda, nitelikli elektronik sertifikaların tahsisinde yüksek güvenlikli kimlik kanıtlama prosedürlerine dair ikinci düzenlemelerin teknoloji tarafsız olması gereği vurgulanmıştır (No. 16). Buna karşılık, elektronik imzaya dair somut hukuki etkiler mülga Kanundan çok farklı düzenlemiş değildir. Elektronik Kimlik ve Güven Hizmetleri Tüzüğü birçok bakımından çok önemli yenilikler getirmiş olmakla beraber elektronik imza tanımı ve türleri ve ayrıca açık anahtar altyapısına dair temel hususların esaslı şekilde değiştiğini söylemek güçtür. Nitekim elle atılan imza bakımından nitelikli elektronik sertifika, nitelikli elektronik imza oluşturma aracı kullanılması şartlarının teknoloji tarafsızlığı prensibine aykırı olduğu ileri sürülmüştür.[124] Belirtilen hususlar çerçevesinde, mülga Elektronik İmza Direktifi için ileri sürülen eleştiriler burada geçerlidir kanaatindeyiz.

Teknoloji tarafsızlığı prensibi, sadece elektronik imza bakımından değil, AB Elektronik Kimlik ve Güven Hizmetleri Tüzüğü ile kabul edilen tüm elektronik uygulamalar ve hizmetler için genel bir ilke niteliğindedir. Bu Prensibin yararlı etkileri olduğu gibi çok sıkı takip edilmesi halinde istenmeyen etkileri de olabilir. Bir örnek olarak, elektronik kimlik uygulamalarında, belirli ve güvenli teknolojilerin seçilmemesinin, kişinin hükümetten veya halktan gelebilecek tepkiler sebebiyle medeni haklara dair tartışmalara (eşcinsellik, din, etnik kökenler gibi) girmekten çekinmesine sebep olabileceği belirtilmiş; güvenlik ve mahremiyet sağlanması için sadece tasarım olarak genel kurallar konulması değil, belirli ve açık düzenlemelerle uygulamaya yönelik hukuki metinlere yer verilmesi gerektiği

[122] UNCITRAL Electronic Signatures Guide, s. 53, parag. 118;

[123] BLYTHE, s. 9; FALCIOĞLU, s. 84; ANDERSEN, Mads Byrde, "Özel Hukukta Elektronik Meydan Okuma", AB'ne Üye Bazı Devletlerde ve Türkiye'de Elektronik Ticaretin Hukuksal Sorunları: Elektronik Sözleşmeler Semineri, 12 Mayıs 2000, İTO Yayını, Şubat 2001, s. 84.

[124] DOMINGO, s. 66.

savunulmuştur.[125] Belirtilen hususlar çerçevesinde, teknoloji tarafsızlığının uygulama yöntemleri çerçevesinde adı gibi bir prensip veya ilke seviyesinde değerlendirilmesi; bir amaç olarak görülmemesi ve yine prensip niteliği itibariyle gerekli görülen yerlerde belirli teknolojilere doğrudan atıf yapılmasından kaçınılmaması gerektiği kanaatindeyiz.

Bu aşamada, uluslararası düzenlemeler dışında, farklı ülkelerin elektronik imza düzenlemelerinin de incelenmesi yararlı olabilir. Ancak önemle belirtmek gerekirse, AB nezdinde temel düzenleme artık bir Direktif değil Tüzük'tür. Üye devletler, Direktiflerden farklı olarak düzenlemeyi yorumlayarak kendi özel düzenlemeleri ile yerel mevzuatlarına aktarmazlar; bir uyum süreci yoktur. Tüzükler tüm AB üye devletleri genelinde yeknesak şekilde doğrudan mevzuata dahil edilirler. Bununla beraber, üye devletlerin ek düzenlemelerle, nitelikli elektronik imza dışında bazı basit elektronik imza türleri için daha kuvvetli özel bir hukuki etki öngörmesi ve hatta nitelikli elektronik imza yanında bazı basit elektronik imza türleri için elle atılan imza ile eşdeğerlik tanınması mümkündür.[126]

Teknoloji tarafsızlığı bakımından belki de en ileri seviye Amerika Birleşik Devletleri düzenlemeleridir. Tabii bu sonucun oluşmasından hukuk sistemlerindeki önemli yapısal farklılığın etkili olduğu açıktır. Amerikan Hukukunda federal düzeyde uyulması zorunlu elektronik imzalara ilişkin temel düzenleme Federal Global ve Ulusal Ticarette Elektronik İmza Kanunu (The Electronic Signatures in Global and National Commerce Act)'dur,[127] bunun yanında, yeknesak kanun[128] niteliğindeki 1999 tarihli Yeknesak Elektronik İşlemler Kanunu'nda (Uniform Electronic Transactions Act)[129,130] da elektronik imzaya ilişkin önemli düzenlemeler yer almaktadır. 30/06/2000 tarihli Amerika Elektronik İmza Kanunu, elektronik işlemlere itimadı arttırmak ve devam eden büyümesine ve güvenirliliğine destek olmak amacıyla kabul edilmiştir[131] Amerika Elektronik İmza düzenlemelerinde açık anahtar altyapısına yönelik tanımlara yer verilmediği gibi herhangi bir teknolojiyi çağrıştıran yaklaşımlardan kaçınılmıştır. Amerika Elektronik İmza Kanunu'nun 104(b)(2)(c)(iii) hükmü uyarınca, elektronik imza için seçilen yöntemlerin elektronik kayıtların veya elektronik imzaların düzenlenmesi, saklanması, oluşturulması, alınması, iletilmesi veya onaylanması işlevlerini yerine getirmek için özel bir teknolojinin veya teknik özelliklerin uygulanmasını gerektirmez veya seçilen elektronik imza yöntemi için daha fazla hukuki statü veya etki tanınmaz. Kullanılan teknolojilerin, Kanunun öngördüğü nitelikleri bünyesinde barındırıp, barındırmadığı ve dolayısıyla bu teknolojilerin kullanımıyla oluşturulan ve imzalanan sözleşme ve belgelerin yasaya uygunluğu hakkında bir kanıya varmak, ABD yargı organlarına düşmektedir.[132] Mevcut düzenlemelerin tarafların duruma uygun gördüğü herhangi bir elektronik imza çözümünü seçmesinde çok geniş bir elastikiyet sağladığı, elektronik imzanın geçerli olması önceden tanımlanmış özel bir biçim bulunmadığı; örneğin New York mahkemelerinin Docusign, elle atılan

[125] HÖLBL, Marko, "Position on the Electronic identification and trust services (eIDAS)", CEPIS Statement, http://cepis.org/app/uploads/2020/01/Position-on-the-Electronic-identification-and-trust-services-eIDAS.pdf, (çevrimiçi), 10.03.2022.

[126] bkz. ŞİMŞEK / ÖZCAN / ERGUN / ÇELİK, s. 140.

[127] Kanun metni için bkz. http://uscode.house.gov/lawrevisioncounsel.shtml.

[128] Amerikan hukukunda düzenlemeler, temel olarak federal kanun, yeknesak kanun ve eyalet kanunları şeklinde üç grup altında toplanabilirler. Federal kanunlar, federal devlet tarafından çıkarılan ve her eyalet için uyulması zorunlu kurallar getiren düzenlemelerdir: eyalet kanunları ise her eyaletin kendi iç hukukuna ilişkin olarak çıkardığı ve sadece eyalet sınırları içinde uygulanan kurallardır. Buna karşılık yeknesak kanunlar ise eyalet hukuklarını uyumlaştırmak üzere çeşitli kurumlar tarafından hazırlanan, federal devlet tarafından uyulması zorunlu kurallar olarak belirlenmemekle beraber, kabulleri teşvik edilen düzenlemelerdir. [Uniform Laws, https://www.law.cornell.edu/uniform, (çevrimiçi), 10.04.2022].

[129] Kanun metni için bkz. http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

[130] Bu kanun hemen hemen tüm eyaletlerce kabul edilmiştir. (BLYTHE, s. 6).

[131] FREEMAN, (web).

[132] SEVİMLİ, K. Ahmet, "Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası" Prof. Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı, C. II, İstanbul, Beta Yayınları, 2001, s. 1039.

imzanın pdf taraması, facsimile (mekanik kopya çıkartılan bir imza türü), elektronik postanın geçerli elektronik imzalar olduğuna karar verdiğini; elektronik imza tanımına göre "niyet'in" belirleyici olduğu belirtilmiştir.[133]

Mukayeseli hukuk çalışmasından sonra şimdi EİK'yi değerlendirme çalışacağız. Öncelikle belirtmek gerekirse, Kanun gerekçesinde ve içeriğinde, teknoloji tarafsızlığı prensibinin benimsendiği belirtilmemiş ise de herhangi bir teknolojiye doğrudan atıf yapılmamış ve belirli bir teknolojiye dair terimler kullanılmamıştır. Bu uğurda, "güvenli elektronik imza oluşturma araçları" güvenli elektronik imza doğrulama araçları" "nitelikli elektronik sertifika hizmet sağlayıcısı" gibi yeni terimler üretilmiş ve kullanılmıştır. Belki de en önemlisi, güvenli elektronik imza için dört kriter benimsenmiş (EİK m. 4) bu kriterleri sağlayan her teknolojinin aynı hukuki etkiyi göstereceği kabul edilmiştir. Erturgut, EİK m. 3/b bendinde yapılan elektronik imza tanımının herhangi bir teknolojiye üstünlük tanınmadan, sadece ondan beklenen fonksiyonlar dikkate alınarak tanım yapıldığını; bu hususun "teknolojik tarafsızlık" kavramıyla açıklanabileceğini; bu tanımla beraber elektronik imza alanında gerçekleşen değişikliklerin kanun değişikliğine gerek kalmaksızın uygulanabilmesinin sağlandığını; kanuni düzenlemenin, bu anlamda teknolojinin gerisinde kalmadığını ve her değişikliğe uygulanabilir bir duruma getirildiğini belirtmiştir.[134]

Düşüncemize göre, güvenli elektronik imzanın mevcut tanımı ile elektronik imza alanındaki her değişikliğin kanun değişikliğine gerek kalmadan uygulanabileceğini söylemek oldukça güçtür. Açıkça belirtilmemişse bile "güvenli elektronik imza oluşturma araçları" kapalı anahtara, "güvenli elektronik imza doğrulama araçları" açık anahtara ve "nitelikli elektronik sertifika hizmet sağlayıcısı" ise onay kurumuna karşılık gelmektedir. Ayrıca basit elektronik imza için herhangi bir hukuki etki tanınmadığı gibi gelişmiş elektronik imza gibi basit ve güvenli elektronik imza arasında bir türe de yer verilmiş değildir. Başka bir deyişle, mevzuatımızda basit elektronik imzaların geçerliliği ve ispat gücü konusunda herhangi bir kanun hükmü yoktur; basit elektronik imzalı belgelerin hukuki durumu EİK ile değişmemiştir. EİK'da yer alan elektronik imzanın teknik yönlerini düzenleyen hükümler tamamen dijital imza teknolojisini hedef almaktadır. Bu şartlar altında EİK'da kısmen dahi olsa teknoloji tarafsızlığı prensibini benimseyen bir düzenleme olduğunu belirtmek güçtür. Bu aşamada, EİK'nın özellikle güvenli elektronik imza bakımından (sunucu imzası gibi) yeni teknolojilere imkan tanıması ayrıca güvenli elektronik imza dışında da elektronik imzanın hukuki etkisini öngörmesi ve düzenlenmesini beklemek yersiz olmayacaktır.

Sonuç

Elektronik imza en basitinden en karmaşığına dünya genelinde çok farklı teknik ve teknolojileri kapsayan bir üst kavramdır. Elektronik imza kavramı, kutucuk işaretleme veya metin altına isim yazma gibi çok basit ve özel bir güvenlik sağlamayan teknikler yanında, biyometrik veya dijital imza gibi üst seviyede güvenlik sağlayabilen teknik ve teknolojileri kapsar. Bu sebeple değişken ve teknik bir konudur.

Biyotmetrik imzalar retina, parmak izi, ses gibi biyolojik izlerin kullanılması yoluyla kimlik doğrulama sağlayan; digitalize imza, elle veya kalemle ekran üzerine imza gibi doğruda imza şeklinde kullanılan yöntemleri içeren geniş bir alanı kapsayan bir elektronik imza türüdür. Biyometrik imzaların, kullanım kolaylığı, kimlik doğrulamada ek güvenlik sağlama gibi önemli avantajları olduğu gibi; biyolojik özelliklerin niteliğinden kaynaklanan önemli dezavantajları ve güvenlik sorunları da vardır. Ayrıca, yapıları itibariyle, nitelikli elektronik sertifika ve nitelikli imza doğrulama araçları ile sağlanan veri bütünlüğünü sağlamaları mümkün gözükmemek-

[133] Coronavirus: The U.S. Legal Framework Supporting the Validity of Electronic Signatures, https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/07/Coronavirus-the-US-Legal-Framework-Supporting-the-Validity-of-Electronic-Signatures-2.pdf (çevrimiçi), 10.04.2022.

[134] ERTURGUT, Mine, "Elektronik İmza Kanunu Bakımından E-Belge ve E-İmza", Bankacılar Dergisi, S. 48, Yıl: 2003; (Çevrimiçi), www.tbb.org.tr/ turkce/dergi/dergi48/Mine.doc, 04/05/2005, s. 69.

tedir. Bu bağlamda, biyotmetrik imzaların dijital imzaların yerini alması değil; dijital imzayla birlikte, bir tamamlayıcı teknoloji olarak kullanılması, veri bütünlüğünün nispeten daha az önemli olduğu veya kullanım kolaylığının öne çıktığı işlerde yaygınlaşması beklenebilir. Mevcut koşullar altında, AB düzenlemeleri veya EİK çerçevesinde, biyometrik imzaların, tek başına güvenli/nitelikli elektronik imzanın işlevlerini yerine getiremeyeceği ve dolayısıyla elle atılan imza ile aynı hukuki etkiyi doğurmayacağı kanaatindeyiz.

EİK uyarınca, elektronik imzalar, basit elektronik imzalar ve güvenli elektronik imzalar olarak ikiye ayrılabilir. Ancak EİK'da basit elektronik imzalar için herhangi bir hukuki etki düzenlenmiş değildir. Güvenlik seviyesi ve yaygınlığı ne seviyede olursa olsun her türlü basit elektronik imzanın hukuki etkisi tamamen genel hükümlere tabidir. Bu durumun, elektronik imzanın yaygınlaşması bakımından önemli bir eksilik olduğu rahatlıkla söylenebilir.

Hem uluslararası düzenlemelerde hem de EİK'da teknoloji tarafsızlığı prensibi değişik derecelerde kabul edilmiştir. Teknoloji tarafsızlığı prensibinin benimsenmesi, kapsayıcı ve teknik olmayan düzenlemelerle, kanunların değişen teknolojiye ayak uydurmasına ve elektronik imzanın kullanımını yaygınlaştırmasına ve etkinliğinin arttırılmasına yardımcı olabilir. Diğer yandan, bu prensibin katı uygulanması, uygulama eksikliklerine ve standart sağlamada sorunlara sebep olabilir. Uzun yıllardır, sağlanan veri güvenliği dikkate alınarak AB düzenlemelerinde sadece nitelikli/güvenli elektronik imzaya elle atılan imzanın hukuki sonuçları tanınmıştır. Nitelikli/güvenli elektronik imza ise kolayca görülür şekilde açık anahtar altyapısına dayalıdır. Bu sebeple, nitelikli/güvenli elektronik imzanın açık anahtar altyapısına dayalı bir şifreleme yöntemi olduğunun kabul edilmesinin ve teknoloji tarafsızlığı prensibinin bir istisnası sayılmasının yararlı olacağı kanaatindeyiz. Bununla beraber, nitelikli/güvenli elektronik imza çerçevesinde, açık anahtar altyapısına dayalı farklı şifreleme standartları ve teknikleri itibariyle teknoloji tarafsızlığı prensibinin takip edilmesi yerinde olur.

Kaynakça

ACAR, Ayşe Ece, Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Niteliği, İstanbul, XII Levha Yayınları, 2013.

AHİ, Gökhan, "Türk Hukukunda Yeni Bir Boyut Elektronik İmza Kanunu", http://dergi.tbd.org.tr/ yazarlar/10052004/m.gokhan_ahi.htm, (çevrimiçi), 04/05/2005.

AHİ, Gökhan, "Hukuki Bakımdan Dijital (Sayısal İmza)", http://www.hukukcu.com/bilimsel/ kitaplar/sayisalimza.htm, (çevrimiçi), 23/10/2005.

AKİPEK, Şebnem, "Özel Hukuk ve İnternet", http://inettr.org.tr/inetconf5/tammetin/hukuk.html, (çevrimiçi), 26/05/2005.

ALTINIŞIK, Ulvi, Elektronik Sözleşmeler, Ankara, Seçkin Yayıncılık, 2003, s. 79; ERGÜN, Ömer, "5070 Sayılı Elektronik İmza Kanunu ve Dijital İmza", Türkiye Noterler Birliği Hukuk Dergisi, Sayı: 122, Tarih: 15 Mayıs 2004, s. 63-74, (çevrimiçi), https://turk-internet.com/5070-sayili-elektronik-imza-kanunu-ve-dijital-imza-1/, 10/04/2022.

ANDERSEN, Mads Byrde, "Özel Hukukta Elektronik Meydan Okuma", AB'ne Üye Bazı Devletlerde ve Türkiye'de Elektronik Ticaretin Hukuksal Sorunları: Elektronik Sözleşmeler Semineri, 12 Mayıs 2000, İTO Yayını, Şubat 2001.

BİRSEN, Acır, Elektronik İmza ve Elektronik Kayıtların Medeni Usul Hukukunun İspat Kuralları Yönünden Değerlendirilmesi, SPK Yeterlilik Etüdü, Ankara, 2000.

BOZBEL, Savaş "İnternet Üzerinden Yapılan Hukuki İşlemler ve Bu Konudaki 97/7 sayılı AB Yönergesi ile Almanya ve İsviçre'deki Düzenlemeler", (çevrimiçi), http://www.hukukcu.com/bilimsel/kitaplar/internet_uzerinden_hukuki_islem.htm, 16/05/2005.

COX, Buket Öztuna Avrupa Birliği Hukukunda Elektronik Ticaret ve Türkiye'deki Gelişmeler, İstanbul, Pusula Yayıncılık, 2002, s. 34.

DOMINGO, Ignacio Alamillo, SSI eIDAS Legal Report, How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market, https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf (çevrimiçi) 10.03.2022.

E. BLYTHE, Stephen, "Dijital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce with Enchanced Security", Richmond Journal of Law & Technology, Volume IX, Issue 2, 2005, (çevrimiçi) http://law.richmond.edu/jolt/v11i2/article6.pdf, 21/10/2005.

EKŞİ, Nuray, "Elektronik İmzalara İlişkin UNCITRAL Model Kanun Tasarısı Hakkında Genel Bir Değerlendirme", Yasa Hukuk Dergisi, İstanbul, 2001/03.

ER, Cüneyd, Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, Yetkin Yayınları, 2007.

ERBAYRAKTAR, Burcu, Güvenli Elektronik İmza, İstanbul, Oniki XII Levha Yayınları, 2016.

EROL, H. Tarık, Electronic Signatures, İstanbul, Beta Yayınları, 2003.

ERSOY, Zeynep, Elektronik Ticaret ve Ticaret Noktaları, T.C. Başbakanlık Dış Ticaret Müsteşarlığı İhracatı Geliştirme Etüd Merkezi, 1999.

ERTURGUT, Mine, "Elektronik İmza Kanunu Bakımından E-Belge ve E-İmza", Bankacılar Dergisi, S. 48, Yıl: 2003; (Çevrimiçi), www.tbb.org.tr/turkce/dergi/dergi48/Mine.doc, 04/05/2005 (E-Belge).

ERTURGUT, Mine, Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, Ankara, Yetkin Yayınları, 2004 (Delil).

FREEMAN J.D., Edward, "Dijital Signatures and Electronic Contracts", (çevrimiçi) https://www.proquest.com/openview/ea208345000de3f800ad504b0bd21e76/1?pq-origsite=gscholar&cbl=52433 01/04/2022.

GEZDER, Ümit, Mukayeseli Hukuk Açısından İnternet'te Akdedilen Sözleşmelerde Tüketicinin Korunması, İstanbul, Beta Yayınları, 2004, s. 147.

GÖKSU, Mustafa, Hukuk Yargılamasında Elektronik Delil, İstanbul, Adalet Yayınevi, 2011.

H. BOSS, Amelia, "The Evolution of Commercial Law Norms: Lessons to be Learned From Electronic Commerce" Drexel University Thomas r. Kline School of Law, 2009, pp. 673-708.

H. KÜÇÜKÖZYİĞİT, Galip, "Elektronik Ticaret, Elektronik İmza ve Hukuk", http://www.ceterisparibus.net/arsiv/g_kucukozyigit2.doc, (çevrimiçi), 04/05/2005.

HÖLBL, Marko, "Position on the Electronic identification and trust services (eIDAS)", CEPIS Statement, http://cepis.org/app/uploads/2020/01/Position-on-the-Electronic-identification-and-trust-services-eIDAS.pdf, (çevrimiçi), 10.03.2022.

İNALÖZ, Ayşe, Telekomünikasyon Regülasyonları Çerçevesinde Elektronik Ticaretin İncelenmesi, Uzmanlık Tezi, Telekomünikasyon Kurumu, Ankara, 2003.

J. SMENDINGHOFF, Thomas / BRO, Ruth Hil, "Electronic Signature Legislation", http://profs.lp.findlaw.com/signatures/, (çevrimiçi), 18/20/2005.

JA, Ashiq, "The eIDAS Agenda: Innovation, Interoperability and Transparency". https://www.cryptomathic.com/news-events/blog/the-eidas-agenda-innovation-interoperability-and-transparency (çevrimiçi), 20/03/2022.

KESER BERBER, Leyla, Biyometrik İmza ve Türk Borçlar Kanunu'ndaki Yazılı Şekil Şartı ile Hukuk Muhakemeleri Kanunundaki İmza Açısından Yeri, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, https://itlaw.bilgi.edu.tr/media/document/2019/08/biyometrik-imza.pdf (çevrimiçi), 20/03/2022 (Biyometrik İmza).

KESER BERBER, Leyla, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Ankara, Yetkin Yayınları, 2002 (Dijital İmza).

KESER BERBER, Leyla, "Elektronik İmzanın Düzenlenmesi Hakkında Tasarı Hükümlerinin Değerlendirilmesi" (çevrimiçi), https://turk-internet.com/elektronik-imza-kanun-tasarisi-hukumleri-degerlendirilmesi/, 10/06/2022 (Tasarı Hükümlerinin Değerlendirilmesi).

KESER BERBER, Leyla / LOSTAR, Murat Bilişimde Biyometrik Yöntemler, Ankara, Yetkin Yayınları, 2006 (Biyometrik Yöntemler).

KURU, Baki, Hukuk Muhakemeleri Usulü, C. II, 6. Baskı, 2001.

LUPTON, W. Everett; "The Digital Signature: Your Identiy by the Numbers", http://law.richmond. edu/jolt/v6i2/note2.html, (çevrimiçi), 03/11/2005.

MENAIS, Alexandre, "Electronic Signatures in France", (çevrimiçi), http://www.juriscom.net/en/pro/1/ec20020730.htm, 10/02/2006.

MURRAY, Jamie, "Public Key Infastructure Dijital Signatures and Systematic Risks", Journal of Information, Law and Technology, 2003(1), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/murray/, (çevrimiçi), 23/10/2004.

ORTA, Mesut Elektronik İmza ve Uygulaması, Ankara, Seçkin Yayınları, 2005.

ÖCAL, Ayşe, "Elektronik Ticaret Hakkında UNCITRAL Model Kanunu ve Elektronik İmzalar Hakkında UNCITRAL Model Kanunu Üzerine Değerlendirme" Terazi Hukuk Dergisi, 2017, Cilt 12, Sayı 129, ss. 96-114.

ÖZGÜL, Mehmet Emin, "İnternette Hukuki Güvenlik Dijital İmza", inet-tr.org.tr/inetconf8/bildiri/141.doc., (çevrimiçi), 09/11/2005.

ÖZYILMAZ, Ayşe / EVSENAL, Saliha, "Elektronik İmzalar", Aktive E-Ticaret, 2000, (çevrimiçi) , 25/10/2005.

R. MERRILL, Charles, "Proof, What and When in Electronic Commerce", http://abanet.org/scitech/ammerr.html, (çevrimiçi), 10/04/2005.

RAYSMAN, Richard / BROWN, Peter, "Legislation on Digital Signatures" http://www.brownraysman.com/pubs/articles/techlaw/nylj0499.html, (çevrimiçi), 15/04/2005.

REED, Chris, "What is a Signature?", Journal of Information, Law and Technology 2000(3), https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/, 10/03/2022.

SARISÖZEN, Serhat, "Elektronik İmza Kanunu'nun Değerlendirilmesi, Elektronik Ticaret ve İnternette Yapılan Sözleşmeler", Kazancı Hakemli Hukuk Dergisi, S. 15-16, Yıl: 2005.

SCHELLKENS, M.H.M., Electronic Signatures Authentication Technology from a Legal Perspective, Netherlands, T.M.C. Asser Press, 2004.

ŞENOCAK, Zarife, "Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması", AÜHFD, C. 50, S. 2, 2001.

SEVİMLİ, K. Ahmet, "Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası" Prof. Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı, C. II, İstanbul, Beta Yayınları, 2001.

SPYRELLI, Christina, "Electronic Signatures: A Transatlantic Bridge? An EU und US Legal Approach Towards Electronic Authentication", Journal of Information, Law and Technology, 2002(2), http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_2/spyrelli/, (çevrimiçi), 22/10/2005.

STERN, Jonathan, "The Electronic Signatures in Global and National Commerce Act", www.law.berkeley.edu/institutes/bclt/pubs/annrev/exmplrs/csum/jscs.doc, (çevrimiçi), 20/10/2005.

SÖZER, Bülent, Elektronik Sözleşmeler, İstanbul, Beta Yayınları, Mart 2002.

ŞİMŞEK, Merve Melis / ÖZCAN, Tuğba / ERGUN, Tamer / ÇELİK, Vural, Elektronik İmza Seviyeleri, Bilgi Yönetimi Dergisi Cilt: 2 Sayı: 2 Yıl: 2019 (çevrimiçi) https://dergipark.org.tr/tr/pub/by, ss. 136-144.

TUĞSAVUL, Muhsin, "İspat Külfeti Kanuni Deliller ve İkamesi", AD, S. 7, Yıl: 42, Temmuz 1951, ss. 1060-1095.

YILDIRIM, Mehmet Kamil / PÜRSELİM, Hatice Selin, "Elektronik İmza Kanunu ve Türk İspat Hukukundaki Etkileri", İstanbul Barosu Dergisi, C. 79, S. 2005/4, ss. 1105-1106.

WANG, Minyan, "Do the regulations on electronic signatures facilitate international electronic commerce? A critical review" Computer Law & Security Review: The International Journal of Technology Law and Practice Year: 2007, N: 23, ss. 32-41.

Raporlar ve Internet Siteleri

Coronavirus: The U.S. Legal Framework Supporting the Validity of Electronic Signatures, https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/07/Coronavirus-the-US-Legal-Framework-Supporting-the-Validity-of-Electronic-Signatures-2.pdf (çevrimiçi), 10.04.2022.

"Data Encryption Standart", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213893,00.html, (çevrimiçi), 23/10/2021.

"Does typing your name count as a signature?" https://www.pandadoc.com/ask/typing-name-as-signature/ (çevrimiçi) 10.03.2022.

"Electronic Authentication", http://www.e-ra.org.uk/electronic_authentication.htm, (çevrimiçi), 22/10/2005.

Elektronik Ticaret Hukuk Çalışma Raporu 03/05/1998, http://www.e-ticaret.gov.tr/raporlar/hukuk.htm, 04/10/2005.

"Elektronik İmza Faydalı Bilgiler", http://www.tk.gov.tr/eimza/E-Imza_Faydali_bilgiler.htm, (çevrimiçi), 22/10/2005.

"Integrating Biometric Technics with an Electronic Signature for Remote Authenticaton", http://www.ercim.org/publication/Ercim_News/enw49/bechelli.html, (çevrimiçi), 29/10/2005.

Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods, United Nations Commission on International Trade Law, Vienna, 2009 (Promoting confidence in electronic commerce UN).

"UNCITRAL model Law on Electronic Signatures with Guide to Enactment 2001", http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf, parag. 38, 20/10/2005 (UNCITRAL Electronic Signatures Guide).

TUBİTAK-UEKAE, Açık Anahtar Altyapısı Eğitim Kitabı, www.kamusm.gov.tr.

Türkiye Bilişim Şurası Hukuk Çalışma Grubu Raporu, http://2002.bilisimsurasi.org.tr/.