TBB Dergisi 2024 (174) s. 83-125

# ELEKTRONİK İMZA KANUNU'NDA DÜZENLENEN SUÇLAR

## CRIMES IN THE ELECTRONIC SIGNATURE LAW

Mehmet Onursal CİN*

**Özet:** Gelişen teknoloji, hukuk düzenine de etki etmekte ve hukuki yöntemler farklılaşmaktadır. Elektronik verilerin sık kullanımı dünya çapında yaygınlaşmaktadır. Elektronik verilerin kullanımındaki artış, bu verileri düzenleyenlerin kimliklerinin doğrulanması zorunluluğu da getirmektedir. Elektronik ortamda oluşturulan verilerin doğruluğunun ve güvenirliğinin sağlanması için yine elektronik verilere ihtiyaç duyulmaktadır. Bu nedenle ıslak imza ve mühür, yerini elektronik imza ve elektronik mühre bırakmaktadır. Sıklıkla başvurulan bu yöntemler için gerekli olan yasal düzenleme 5070 sayılı Elektronik İmza Kanunu aracılığıyla yapılmıştır.

5070 sayılı Elektronik İmza Kanunu'nda söz konusu elektronik verilerin izinsiz kullanımı ve bu verileri sağlayan elektronik sertifikalarda sahtekarlıkla alakalı suç tipleri düzenlenmiştir. Elektronik imzanın ve elektronik mührün kamu kurumlarından özel sektöre birçok farklı alanda kullanılması 5070 sayılı Kanun'da yer alan suç tiplerinin ortaya çıkma ihtimalini artırmaktadır. Çalışmamızda elektronik imza kavramı incelenerek söz konusu suç tipleri hakkında değerlendirmede bulunulacaktır.

**Anahtar Kelimeler:** Elektronik İmza, Güvenli Elektronik İmza, İmza Oluşturma Verisi, İmza Oluşturma Aracı, Elektronik Sertifika, Elektronik Mühür

**Abstract:** Developing technology also affects the legal order and legal methods are changing. Frequent use of electronic data is spreading worldwide. The increase in the use of electronic data also brings the obligation to verify the identities of those who make these data. Electronic data is also needed in order to ensure the accuracy and reliability of electronic data. Therefore, wet signature and seal are replaced by electronic signature and electronic seal. The legal regulation required for these frequently used methods has

* Dr. Öğr. Üyesi, Selçuk Üniversitesi Hukuk Fakültesi, onursalcin1@gmail.com, ORCID: 0000-0003-2451-7779, Makalenin Gönderim Tarihi: 11.08.2024, Kabul Tarihi: 02.09.2024

been made through the Electronic Signature Law No. 5070.

The Electronic Signature Law No. 5070 regulates the types of crimes related to unauthorized use of electronic data and fraud in electronic certificates that provide this data. The use of qualified advanced digital signature and electronic seal in many different areas from public institutions to the private sector increases the possibility of occurrence of the types of crimes included in Law No. 5070. In our study, the concept of electronic signature will be examined and an evaluation will be made about the types of crimes in question.

**Keywords:** Digital Signature, Qualified Advanced Digital Signature, Signature Generation Data, Signature Generation Tool, Electronic Certificate, Electronic Seal

## GİRİŞ

Yaşanan teknolojik gelişmeler sonucu hukuk aleminde de pek çok değişiklik görülmekte, evraka dayalı sistemden elektronik sisteme geçiş zaman ve kaynağın verimli kullanılması açısından önemli ve hatta zorunlu hale gelmektedir. Elektronik verilerin kullanımının yaygınlaşması bu verilerin güvenirliğinin en üst derecede korunması için hukuki düzenlemelerin yapılması gerekliliğini de beraberinde getirmektedir. Zira elektronik verilerin kolaylıkla değiştirilmesi, veriler üzerinde oynama yapılması ve hatta verilerin ortadan kaldırılması mümkündür. Elektronik verilerin güvenirliği, veriyi düzenleyen kişinin kimlik doğrulaması[1] ve belgenin bütünlüğünün garanti altına alınması ile sağlanabilir. Elektronik imza ve mühürler tam da bu amaca hizmet eden elektronik veriler olarak karşımıza çıkmaktadır.

Elektronik imza genellikle, elektronik araçlar ile sayılar, harfler, karakterler veya simgeler aracılığıyla sözleşme yapmak ve imzalamak veya yazışma yapmak amacıyla kullanılmaktadır.[2] Güvenli elektro-

---

1 Güvenli elektronik imza, imzalayanın kimlik doğrulamasını yapmayı sağlamaktadır. Gülfer Akın, "Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/Dijital Belge", *Bilişim Hukuku Dergisi*, 2021, C. 3, S. 1, s. 93; Emine Öz, "Elektronik İmza-Hukuki Boyutuyla" Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006, s. 21.

2 Stephen E. Blythe, "Digital Signature Law of The United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security", *Richmond Journal of Law and Technology*, 2005, C. 11, S. 2, s. 3; Elektronik imzanın amacı kimlik doğrulaması yapmaktır. Sözer, Bülent, "Elektronik İmza Kanunu'na Göre Dijital İmza", Prof. Dr. Ergon A. Çetingil ve Prof. Dr. Rayegan Kender'e 50. Birlikte Çalışma Yılı Armağanı, Çizgi Basım Yayın, Ankara, 2007, s. 1002.

nik imzanın[3] kullanımı için güvenli elektronik imza aracını taktıktan sonra bir yazılım ile şifre girişi yapıp yazılımda belirtilen talimatları takip ederek kısa süre içerisinde imzalama işlemi tamamlanabilmektedir. Özellikle güvenlik anlamında sağladığı kolaylık, reddedilemezlik özelliği, kimlik ve veri doğrulama sistemleri nedeniyle elektronik imza kamusal ve özel sektörde sıklıkla tercih edilmektedir.[4] Kalem yerine bilgisayarla oluşturulan bu imza verileri güvenli elektronik imza vasfına sahip olduklarında ıslak imza ile eşdeğer kabul edilmektedir.[5] Kanunda tanımlanan ve ıslak imza ile eşdeğer kabul edilen imza türü güvenli elektronik imzadır. Güvenli elektronik imzada biri açık biri

---

3 Özellikle AB direktif ve tüzüklerinde güvenli elektronik imza kavramından ziyade nitelikli elektronik imza kavramının kullanıldığı görülmektedir. Ancak çalışmamızda karışıklık yaratmamak adına nitelikli elektronik imza kavramı yerine aynı anlamda olan ve Elektronik İmza Kanunu'nda tercih edilen "güvenli" elektronik imza kavramı tercih edilmiştir. Türk doktrininde elektronik imza, "dijital imza" veya "sayısal imza" olarak da isimlendirilebilmektedir. İnci Biçkin, "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler", *TBB Dergisi*, 2006, S. 63, s. 110; Ahmet Sevimli, "Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası", Prof. Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı Cilt II, Beta Yayınevi, İstanbul, 2001, s. 1029. Ancak doktrinde bazı yazarlar "elektronik imza" kavramını üst kavram, "dijital imza" ve "sayısal imza" gibi kavramları ise bunun alt tipleri olarak kabul etmektedir. B. P. Aalberts/S. Van Der Hof, "Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication", *EDI Law Review*, 2000, C. 7, S. 1, s. 2; Öz, s. 25; Sinem Camcı, "İnternet Üzerinden Kurulan Sözleşmelerde Elektronik İmzanın Hukuki Niteliği", *Terazi Hukuk Dergisi*, 2020, C. 15, S. 165, s. 1022; İpek Sağlam, "Elektronik Sözleşmeler", Legal Yayıncılık, İstanbul, 2007, s. 155. Bunun yanı sıra "dijital imza" kavramının "güvenli elektronik imza" kavramı yerine kullanıldığı da görülmektedir. Zarife Şenocak, "Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2001, C. 50, S. 2, s. 98. Her ne kadar dijital imza ve elektronik imza kavramları birbirinin yerine kullanılsa da aynı anlamı ifade etmemektedir. Dijital imza elektronik imzanın bir türüdür. Mehmet Ertan Yardım, "Elektronik İmza ve Elektronik İmzanın Medeni Usul Hukukumuza Etkileri", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 5.

4 Kalama M. Lui-Kwan, "Recent Developments in Digital Signature Legislation and Electronic Commerce", *Berkeley Technology Law Journal*, 1999, C. 14, S. 1, s. 466; Thomas J. Smedinghoff, "Electronic Contracts and Digital Signatures: An Overview of Law and Legislation", *Journal of Equipment Lease Financing*, 1998, C. 16, S. 2, s. 7.

5 Smedinghoff, s. 7. Dolayısıyla güvenli elektronik imzayla imzalanmış bir belge klasik anlamda hazırlanan bir belgenin tüm unsurlarını taşımaktadır. Kalemle atılan ıslak imza yerine güvenli elektronik imza kullanılabilmektedir. Akın, s. 94.

gizli olmak üzere ikili anahtar sistemi kullanılmaktadır.[6] Her imzalanan belgede benzeri olmayan bir güvenli elektronik imza bulunmaktadır. Bu özellik sayesinde ıslak imzadan farklı olarak imzanın taklit edilebilirliği mümkün olmamaktadır.[7] İlgili belge yalnızca gizli anahtara sahip imza yetkilisi tarafından oluşturulabilir ve bu belgeye yalnızca açık anahtara sahip kullanıcı tarafından erişilebilir.[8] Aynı güvenilirlik sebebiyle 2021 yılından itibaren resmi mühür dahil her türlü fiziki mührün yerini elektronik mühür almaya başlamıştır. Gün geçtikçe uygulaması yaygınlaşan elektronik imza son olarak kimlik kartlarına tanımlanabilir hale gelmiştir.[9] Elektronik Devlet (E-devlet) uygulamasıyla birlikte çoğu devlet hizmeti vatandaşa elektronik ortamda sunulmaktadır. Devlet tarafından bu hizmetin hızlı ve güvenli sürdürülebilmesi adına doğrulamaların sağlanabilmesi için elektronik imza kullanımı önemli hale gelmiştir.[10]

Elektronik imza ve elektronik mühür ile alakalı Türk hukukundaki temel mevzuat, 23.01.2004 tarihinde yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu'dur. İlgili Kanun'un 20. maddesi doğrultusunda, bu Kanun'un uygulanmasına yönelik usul ve esaslar Telekomünikasyon Kurumu tarafından ilgili kurum ve kuruluşların görüşü alınmak suretiyle hazırlanacak yönetmelikler ile belirlenmektedir. Kanunlarda elektronik imza ile alakalı yer alan hükümler kıyasen elektronik mühür hakkında da uygulanmaktadır.

Çalışmamızda elektronik imzanın yöntemi ele alınarak 5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suç tipleri ele alınacak olup bu suç tipleri temelde elektronik imza üzerinden incelenecektir. Zira elektronik imza ve elektronik mühür temelde aynı amaca hizmet eden elektronik verilerdir ve bunlar arasındaki ayrım elektronik imza ve

---

6 Aalberts/Van Der Hof, s. 6; Rolf Rissnaes, "Digital Certificates and Certification Services", Scandinavian Studies in Law, 2004, S. 47, s. 134.

7 Smedinghoff, s. 7.

8 Luı-Kwan, s. 467; Rissnaes, s. 134.

9 15.10.2021 tarihinden itibaren "kimlik kartına uzaktan nitelikli elektronik sertifika ve benzer altyapıyı kullanan farklı elektronik sertifikalar" yüklenebilir hale gelmiştir. Bu hususta detaylı düzenleme Elektronik İmza Kanunu'nun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik'te yer almaktadır. RG., 15.10.2021, S. 31629.

10 Gabriel Lentner/Peter Parycek, "Electronic Identity (eID) and Electronic Signature (eSig) for eGoverment Services – A Comparative Legal Study", Transforming Goverment: People, Process and Policy, 2010, C. 10, S. 1, s. 11.

elektronik mühür sahipleri arasındaki farklılıktan kaynaklanmaktadır. Dolayısıyla elektronik imza ile alakalı yapılacak açıklamalar elektronik mühür için de değerlendirmeye alınabilir. Ayrıca elektronik mühür oluşturma verilerinin izinsiz kullanımına yönelik 5070 sayılı Elektronik İmza Kanunu Ek Madde 1 hükmünde yer alan suç tipi, aşağıda detaylı yer verilen elektronik imza oluşturma verilerinin izinsiz kullanımı suçunu düzenleyen 5070 sayılı Kanun m. 16 ile neredeyse aynı olduğundan ilgili kısımlarda yalnızca iki hüküm arasındaki benzerliklere ve farklara değinilmekle yetinilecektir.

## I. ELEKTRONİK İMZA

İmza, "*Bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işaret*" olarak tanımlanmaktadır.[11] Genellikle onaylama ve kabul anlamına gelen imza, aynı zamanda imzalanan belgenin görüldüğü, okunduğu ve anlaşıldığı şeklinde yorumlanmaktadır.[12] İmza, kişinin kural olarak eliyle oluşturması şeklinde günlük yaşantımızda karşımıza çıkmaktadır. Hukuki olarak bakıldığında, 2525 sayılı Soyadı Kanunu m. 2'de yer verilen düzenlemeye göre, kişinin adının önde soyadının arkada olacak şekilde imza atması esastır. Ancak bir imzaya hukukilik kazandıran kişinin eliyle ve belirtilen şekilde imzalanmış olması değildir.[13] Hukuk Muhakemeleri Kanunu (HMK) m. 206'ya göre, okuma yazma bilmediği için imza atılamaması halinde hukuki işlemlerin geçerliliği için noter tarafından düzenleme biçiminde parmak basmak, mühür vurmak gibi haller de imzaya eş değer kabul edilmektedir. Dolayısıyla okuma yazma bilmeyenlerin yapacağı hukuki işlemlerde belgelerin senet niteliğinin kabulü için mühür veya parmak izinin atıldığı belgenin noter tarafından onaylanması veya düzenlenmesi gerekmektedir. Mühür, alet veya parmak izi kullanımının kabulü kanun lafzından da anlaşılacak şekilde ancak kişinin okuma yazma bilmemesine bağlanmıştır.[14]

---

11 TDK., Güncel Türkçe Sözlük, https://sozluk.gov.tr/, E.T. 30.12.2020,

12 Gökhan Ahi, "Hukuki Bakımdan Dijital (Sayısal) İmza", *Bilişim ve Hukuk Dergisi*, 2008, S.8, s. 28.

13 Legal Dictionary, https://legal-dictionary.thefreedictionary.com/signature, E.T. 30.12.2020,

14 "Şu hâlde, mühür veya el işareti (mesela parmak izi) kullanmak, yalnız yazı bilmeyenler veya imza atamayanlar içindir." YHGK., E. 2002/16-763, K. 2002/799, K.T. 09.10.2002, https://www.kararara.com/.

Teknolojik gelişmeler, ticaretin uluslararası boyuta ulaşması, idari teşkilatlanmasının hızlanmasının gerekliliği, yazışma ve sistemlerin güvenlik gerekçeleri ile ıslak imza yerine elektronik imza kullanımı hayatımıza dahil olmuştur. Günümüzde elektronik imzalar sıklıkla kullanıldığından elektronik belge yönetim sistemleri ve elektronik arşivler de fiziki arşivlemenin yerine geçmeye başlamıştır.[15] Elektronik imzanın ıslak imzanın yerine kullanılmaya başladığı bu süreçte hukuki düzenlemeye duyulan ihtiyaç neticesinde 5070 sayılı Elektronik İmza Kanunu yürürlüğe girmiştir.[16] Yabancı hukuk sistemlerindeki uygulamalar da Elektronik İmza Kanunu ile benzer düzenlemelerin yer aldığı mevzuatlar bulunmaktadır. Teknolojinin yaygınlaştığı 1990'ların sonları itibariyle demokratik hukuk devletlerinde elektronik imzanın kullanımı yasal zemine oturtulmaya çalışılmıştır.[17] Özellikle 1999 yılından itibaren Elektronik İmza Kanunun benzeri kanuni düzenlemeler pek çok ülkede yapılmıştır. Öncelikle 1997 tarihinde Almanya mevzuatında düzenlenen[18] elektronik imzaya ilişkin hükümlere daha sonra 1998 yılında Malezya ve Singapur;[19] 1999'da ise İtalya,[20] Avusturalya[21] ve Kore[22] mevzuatlarında yer verilmiştir.[23] 2000 yılında Amerika Birleşik Devletleri'nde elektronik imzanın ıslak imza ile eşdeğer tutulduğu E-SIGN Act (Electronic Signatures In Global And National Commerce Act) yürürlüğe girmiştir.[24] Ayrıca örneğin, 2002'de

---

15 Mesut Ertanhan, Kamu Görevlilerinin İmza, Paraf ve Elektronik İmzalarından Doğan Sorumlulukları, Seçkin Yayıncılık, Ankara, 2018, s. 25.

16 RG., 25355, 23.01.2004.

17 Sezen Yeşil/Mustafa Alkan/Tayfun Acarer, "E-İmza Uygulamalarında AB ve Türkiye'de Mevcut Durum ve Öneriler", Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, ed. Mustafa, Alkan/Şeref, Sağıroğlu, 2006, s. 1.

18 Mesut Orta, Elektronik İmza ve Uygulaması, Seçkin Yayıncılık, Ankara, 2005, s. 144.

19 Aalberts/Van Der Hof, s. 22.

20 Aalberts/Van Der Hof, s. 18.

21 George B Delta/Jeffrey H. Matsuura, Law of The Internet-I, Wolters Kluwer Law & Business, New York, 2021, s. 90.

22 Jaeso Ahn, "Analyzing and Evaluating the 2020 General Amendments to the Koran Digital Signature Act", *Journal of Korean Law*, 2021, C. 20, S. 2, s. 579.

23 Şeref Sağıroğlu/Mustafa Alkan, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara, 2005, s. 54.

24 Electronic Signatures In Global and National Commerce Act, Public Law 106–229—June 30, (2000), 19.04.2021, https://www.govinfo.gov/content/pkg/

İngiltere'de[25] ve Yeni Zelanda'da,[26] 2004'te Çin'de,[27] 2011'de Rusya Federasyonu'nda[28] elektronik imza mevzuatı düzenlenmiştir. Avrupa Birliği[29] kapsamındaki ülkelerde de elektronik imza ile alakalı kanuni düzenlemelere yer verilmiştir.[30] Elektronik imza için topluluk çerçevesini çizen 13 Aralık 1999 tarih ve 1999/93/EC sayılı Avrupa Parlamentosu ve Konsey Direktifi model alınarak Elektronik İmza Kanunu oluşturulmuştur. 1999 tarihli direktif sonrasında, teknolojik yenilikler doğrultusunda 2016'da yeni tüzük olan eIDAS (910/2014/EC)[31] hazırlanmış ve elektronik imza ve güven hizmetleriyle alakalı çeşitlendirmeler yapılmıştır.

2016 tarihli eIDAS'da basit, gelişmiş ve güvenli olmak üzere üç tip elektronik imza tanımlaması yapılmaktadır.[32] Basit elektronik imza,

---

PLAW-106publ229/pdf/PLAW-106publ229.pdf,. Amerika Birleşik Devletleri mevzuat ve doktrininde ıslak imza ile eş tutulan güvenli elektronik imza kavramı "digital signature" olarak ifade edilmektedir. Aalberts/ Van Der Hof, s. 17.

25 Electronic Signatures Regulation Act 2002, 19.04.2021, https://www.legislation.gov.uk/uksi/2002/318/contents/made.

26 Delta/Matsuura, s. 93.

27 Law of the People's Republic of China on Electronic Signatures, 19.04.2021, http://www.china.org.cn/business/2010-01/21/content_19281152.htm.

28 Russian Federation The Federal Law On Electronic Signature, 19.04.2021, https://afyonluoglu.org/PublicWebFiles/e-imza/int-legislation/Russia-Federal%20Law%20on%20e-Signatures.pdf.

29 Daha önce örneğin, 2000 yılında İsveç, 2009 yılında Finlandiya gibi bazı ülkeler bireysel olarak elektronik imzayı kabul etmiştir. Countries That Have Made Electronic Signatures Legal, 19.04.2021, https://pdf.co/articles/countries-where-electronic-signature-legal. 2016 yılında eIDAS ile topluluk açısından yeknesaklık sağlanmıştır.

30 Farklı ülkelerdeki elektronik imza mevzuatları hakkında detaylı bilgi için bkz. Keser Berber, Leyla, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Yetkin Yayınları, Ankara, 2002, s. 128-134; Yeşil/Alkan/Acarer, s. 2-4.

31 İngilizce açılımı "Electronic Identification and Trust Services For Electronic Transactions In The Internal Market" olan eIDAS elektronik işlemler için kimlik tanımlama ve güven hizmetleri için getirilen Avrupa Birliği düzenlemesi standartıdır. eIDAS ile güvenilir ve kolay kullanımlı sektörler arası elektronik işlemlerin çerçevesi çizilmek istenmiştir. Bu düzenleme ile 1999/93/EC Direktifinin müktesebatı genişletilmiştir. Regulation (EU) No. 910/2014 Of The European Parliament and Of The Council, Official Journal of the European Union, 1, 31.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

32 Doktrinde bu ayrım elektronik imza, ileri elektronik imza ve güvenli elektronik imza olarak da isimlendirilebilmektedir. Baki Yiğit Çakmakkaya, Türk Vergi

imzalayanın belgeyi kabul ettiği veya onayladığını ortaya koyan elektronik imza tipidir.[33] Basit elektronik imza bir butona basılması gibi nispeten kolay bir şekilde gerçekleşmektedir. Bunun yanı sıra çok sayıda ilgiliye gönderilmesi gereken bir belgeyi imzalamak gerektiğinde yetkili kişinin el yazısıyla imza atması mümkün olmayacağından basit elektronik imza olarak değerlendirilen bilgisayar ortamından tarama yoluyla imzalama söz konusu olabilmektedir. Basit elektronik imzaların güvenilirliği tam manasıyla sağlanamamaktadır.[34] Zira basit elektronik imza ile imzalanmış bir veride değişiklik yapılabileceği gibi kimlik tespiti de mümkün değildir.[35] Basit elektronik imzanın güvenlik konusundaki yetersizliği daha güvenilir elektronik imzalar oluşturulmasını zorunlu kılmıştır. Gelişmiş elektronik imza, basit elektronik imzaya güvenlik için eklenen birtakım özellikler doğrultusunda ortaya çıkmış imza tipidir.[36] Gelişmiş elektronik imza, imza sahibiyle bağlantılı olduğundan imza sahibinin belirlenebildiği, imza sahibinin kontrolünde verilerin düzenlendiği ve verilerde yapılan değişikliğin tespit edilebildiği bir imza tipidir.[37] Ancak gelişmiş elektronik imza da hukuki güvenlik açısından tam manasıyla yeterli kabul edilememiştir.[38] Güvenli elektronik imza, ıslak imza ile eşdeğer kabul edilen gü-

---

Hukukunda Elektronik İmza Uygulamaları ve Adaptasyonu, Legal Yayıncılık, İstanbul, 2013, s. 5.

33 Islak imza veya ıslak imzalı metin tarandığı durumda basit elektronik imza ile imzalanmış veri ortaya çıkmış olur. Yardım, s. 7; Kamu Sertifikasyon Merkezi, Biyometrik İmza ve Nitelikli Elektronik İmza Karşılaştırması, 30.12.2020, http://kamusm.gov.tr/dosyalar/beyazbulten/Biyometrik_Imza_ve_Nitelikli_Elektronik_Imza_Karsilastirmasi_Whitepaper.pdf. Basit elektronik imzada sadece veri bütünlüğünün koruma altında olduğu gösterilir. Orta, s. 106.

34 Yardım, s. 7.

35 Nadim Farah, "What's the Difference between Advanced and Qualified Signatures in eIDAS?", 2020, https://www.globalsign.com/en-in/blog/difference-between-eidas-advanced-and-qualified-electronic-signatures.

36 Orta, s. 106; Öz, s. 69.

37 eIDAS, 28, 31.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

38 Gelişmiş elektronik imzanın mevzuatımızda bir yeri bulunmamaktadır. Emine Halman Çetin, "Elektronik Belgelerin Hâkim Tarafından Delil Olarak Değerlendirilmesi", *Terazi Hukuk Dergisi*, 2011, C. 6, S. 54, s. 62; Mine Erturgut, "Elektronik İmza Kanunu Bakımından E-belge ve E-imza", *Bankacılar Dergisi*, 2003, S. 48, s. 70; Mustafa Yılmaz, "Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta ve İdarî Yargılama Hukukunda Delil Niteliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Özel Sayısı Cevdet Yavuz'a Armağan*, 2016, C. 22, S. 3, s. 3442.

nümüzde güvenlik açısından en çok tercih edilen nitelikli imza tipidir. Güvenli elektronik imzanın basit ve gelişmiş elektronik imzadan farkı, sertifikaya dayanması[39] ve yalnızca imza oluşturma aracı ile kullanılabilmesidir.[40] Güvenli elektronik imzanın üç özelliği vardır: Bilgi bütünlüğü, kimlik doğrulama ve inkar edilemezlik.[41] Güvenli elektronik imzalar elektronik bir sertifikaya dayanmaktadır ve bu sertifikalar da ancak ilgili ülkenin belirlediği kurumlar tarafından akredite edilmiş bir Elektronik Hizmet Sertifika Sağlayıcı tarafından verilmesi halinde geçerli olur.

Türk hukukunda elektronik imzanın yasal çerçevesi 5070 sayılı Elektronik İmza Kanunu ile çizilmiştir. Elektronik İmza Kanunu düzenlemesi, elektronik imzanın teknik ve hukuki yönlerinin anlaşılması ve kullanımına ilişkin esasların belirtilmesi amaçlamıştır.[42] 5070 sayılı Kanun ile düzenlenen elektronik imza, "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*" olarak tanımlanmıştır. Tanımda yer alan elektronik veri ise, "*Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar*" olarak ifade edilmektedir. Elektronik imzayla ilgili bir başka tanım Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik'te bulunmaktadır. İlgili Yönetmeliğin amacı, elektronik imza ile ıslak imzalı yazışmalara ilişkin kuralları

---

39 Burcu Erbayraktar, Güvenli Elektronik İmza, On İki Levha Yayıncılık, İstanbul, 2016, s. 6.

40 "Güvenli elektronik imza; münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imzadır." Öz, s. 65; eIDAS, s.12,31.12.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN.

41 Michael Bromby, "Identification, Trust and Privacy: How Biometrics Can Ais Certification of Digital Signatures", Interntional Review of Law, Computers & Technology, 2010, C. 24, S. 1, s. 135; Thomas J. Smedinghoff/Bro Ruth Hill, "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce", John Marshall Journal of Information Technology & Privacy Law, 1999, C. 17, S. 3, s. 745-748; Ferda Topcan, "E-İmza Teknolojisi", TODAİE e-Devlet Merkezi Uygulamalı E-İmza Semineri (2011), s. 13, https://cdn2.beun.edu.tr/bidb/119ce0b4466f34d9159e2fe63b78bfd5/1eimzateknolojisi.pdf, E.T. 31.12.2020; Öz, s. 29-32.

42 Kanunun amaç ve kapsamı yönünden eleştirel yaklaşım için bkz. Sözer, s. 1003.

belirleyerek hızlı ve güvenli bilgi veya belge alışverişinde uygulama birliği sağlamaktadır. Yönetmelik m. 3/j'de güvenli elektronik imza, *"Münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan elektronik imza"* olarak tanımlanmıştır. Yönetmelikte verilen bu detaylı tanım elektronik imza türlerinden biri ve en çok tercih edileni olan güvenli elektronik imzaya ilişkindir. Doktrinde de elektronik imza, veri mesajını gönderen kişinin kimliğini belirlemeye yarayan ve harf karakter ve sembollerden oluşan elektronik veri bütünü olarak tanımlanmaktadır.[43]

Güvenli elektronik imzanın geçerliliği için nitelikli elektronik sertifikaya sahip olması gerekmektedir. Nitelikli elektronik sertifikanın taşıması gereken özellikler 5070 sayılı Kanun m. 9'da yer almaktadır. Elektronik sertifika Elektronik Sertifika Hizmet Sağlayıcı tarafından verilir. Dolayısıyla kişi, ıslak imza yerine elektronik imza kullanmak amacında ise usulüne uygun akredite edilmiş bir hizmet sağlayıcıya başvurması ve elektronik sertifika ile güvenli hale gelmiş bir elektronik imza alması gerekmektedir.[44] Elektronik sertifika, 5070 sayılı Kanun'a göre, *"İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı"* ifade etmekte ve ehliyet veya pasaport gibi kimlik doğrulama kartlarının elektronik karşılığı olarak kabul edilmektedir.[45] Elektronik sertifikayı vermeye yetkili Elektronik Sertifika Hizmet Sağlayıcıları Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu tarafından akredite edilmektedir. Elektronik Sertifika Hizmet Sağlayıcı, 5070 sayılı Kanun m. 8'e göre, *"Elektronik sertifika hizmet sağlayıcısı, elektronik sertifika, zaman damgası ve elektronik imzalarla ilgili hizmetleri sağlayan kamu kurum ve kuruluşları ile gerçek veya özel hukuk tüzel kişilerdir."*

---

43 Sağlam, s. 154.

44 Mustafa Fadıl Yıldırım, "Nitelikli Elektronik Sertifika Hizmet Sağlayıcısının Hukukî Sorumluluğu", *AÜEHFD*, 2004, C. 8, S. 3-4, s. 266.

45 Orta, s. 45; Sevim, Tuğrul, "Elektronik İmza Uygulamasında Kullanılan Zorunlu ve İhtiyari Dokümanlar", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 8.

Güvenli elektronik imza ikili anahtar yöntemi ile oluşturulmaktadır.[46] Anahtar, şifrelemenin temel unsuru olan bir algoritmadır.[47] İkili anahtar yönteminde biri açık biri gizli olmak üzere iki anahtar bulunmaktadır. Gizli anahtar göndericide açık anahtar ise alıcıdadır.[48] Açık anahtar sayesinde alıcı gönderilen belgenin gönderici tarafından gönderildiğini doğrulamaktadır.[49] Alıcının bilgisayarı gönderici ile aynı algoritmayı kullanan bir program sayesinde veriyi aldığında açık anahtarı kullanır ve otomatik olarak elektronik imza şifresini çözer.[50] Bunun nedeni, göndericinin gizli anahtarı ile şifrelenmiş bir belgenin yalnızca alıcının açık anahtarı ile çözülebilecek olmasıdır.[51]

Göndericinin kimliğinin doğrulanmasının yanında belgede değişiklik yapılıp yapılmadığı da anahtarlar sayesinde anlaşılabilmektedir.[52] Alıcının bilgisayarı, göndericiyle aynı algoritmayı kullanan bir programda iletilen veriyi aldığında iki mesajın şifreleri otomatik olarak eşleşmelidir. Eşleşme olduğunda göndericinin iletisinin değişmeden alıcıya iletildiği doğrulanacaktır.[53] Elektronik imza, belgenin değiştirilemez biçimde düzenlenmesini sağlamakta ve bu şekilde güvenilirliğini artırmaktadır.[54]

Açık ve gizli anahtar kavramları 5070 sayılı Elektronik İmza Kanunu'nda farklı şekilde ifade edilmiş olup; gizli anahtar yerine "*imza*

---

46 Yee Fen Lim, "Digital Signatures, Certification Authorities: Certainty in The Allocation of Liability", *Singapore Journal of International & Comparative Law*, 2003, C. 7, S. 1, s. 185; Smedinghoff, s. 7; Topcan, s. 4. Elektronik imzanın asıl unsurunu oluşturan "hash değeri" hakkında detaylı bilgi için bkz. Sözer, s. 1012-1014.

47 Sözer, s. 1009.

48 Sevim, s. 9; Yardım, s. 14.

49 Brian W. Smith/Paul S. Tufaro, "To Certify or Not To Certify The 0CC Opens the Door To Digital Signature Certification", *Ohio Northern University Law Review*, 1998, C. 24, S. 4, s. 815. Açık anahtar altyapısının temel görevi, elektronik ortamda güvenilir ortamın oluşturulmasının sağlanmasıdır. Sağıroğlu/Alkan, s. 75.

50 Smedinghoff, s. 8-9; Topcan, s. 5.

51 Rissnaes, s. 134; Smedinghoff, s. 9; Topcan, s. 5. Bu özellik "erişim kontrolü" olarak isimlendirilmektedir. Biçkin, s. 114.

52 Smedinghoff, s. 8.

53 Farah, https://www.globalsign.com/en-in/blog/difference-between-eidas-advanced-and-qualified-electronic-signatures, 30.12.2020; Smedinghoff, s. 9.

54 ENISA EUROPA, "Security Guidelines on The Appropriate Use of Qualified Electronic Signatures", 2016, s. 13, https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures, E.T. 30.12.2020.

*oluşturma verisi"* [55]; açık anahtar yerine ise *"imza doğrulama verisi"*[56] kavramının kullanıldığı görülmektedir. İki anahtardan (veriden) biri olmadıkça diğeri kullanılamaz.[57] Güvenli elektronik imzanın oluşturulması amacıyla kullanılan imza oluşturma verisini kullanan yazılım veya donanım aracı (imza oluşturma aracı) ile veri oluşturulduktan sonra alıcı tarafından kullanılacak araç ile (imza doğrulama aracı) doğrulanmaktadır. İmza oluşturma ve doğrulama aracı da elektronik imza gibi Elektronik Sertifika Hizmet Sağlayıcı tarafından sağlanmakta ve korunmaktadır.[58] İmza oluşturma araçları, imza oluşturma verilerinin (gizli anahtarlar) gizliliğini sağlayan, başkalarınca kullanılmasını ve sahteciliği önleyen ve imza sahibi dışında değiştirilememesini sağlayan araçlardır. İmza sahibine ait olan bu araç imza sahibinin tasarrufundadır.[59] İmza oluşturma araçları sayesinde imza oluşturma verilerinin (gizli anahtar) bir eşi daha oluşturulamamaktadır. Güvenli elektronik imza gönderici tarafından oluşturulduktan sonra alıcının bunu doğrulaması için imza doğrulama verisini ve aracını kullanması gerekmektedir. Dolayısıyla imza oluşturma verisi gönderiyi şifrelerken; imza doğrulama verisi deşifre etmektedir.[60]

Elektronik imza ile veri hazırlanıp gönderilmesi sürecinde üçüncü kişi ile güvenli elektronik imza sahibi arasında nitelikli sertifikaya dayalı bir güven ilişkisi söz konusu olmaktadır.[61] Bu güven ilişkisi elektronik imzaya atfedilen hukuki değerden kaynaklanmaktadır. Zira elektronik imzaların hukuki etkisi ve delil değeri reddedilemez.[62] Islak

---

55 "İmza oluşturma verisi, imza sahibine ait olup kişinin imzasıyla kişi arasında bağlantı kurar." Gürseln Orer, Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu, Adalet Yayınevi, Ankara, 2011, s. 57.

56 Elektronik İmza Kanunu m. 3'te imza doğrulama verisi, "Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler" olarak tanımlanmıştır.

57 Sözer, s. 1020.

58 Farah, https://www.globalsign.com/en-in/blog/difference-between-eidas-advanced-and-qualified-electronic-signatures, E.T. 30.12.2020.

59 Sözer, s. 1020.

60 Orta, s. 43.

61 Erbayraktar, s. 250.

62 ENISA EUROPA, s. 13. Güvenli elektronik imza, imza sahibine ve üçüncü kişiye bazı yükümlülükler yükler. Buna göre imza sahibi, nitelikli elektronik sertifikaya dayandırılarak oluşturulan güvenli elektronik imzanın gerçeğe uygunluğunu sağlamaya yönelik özen yükümlülüğü yüklenirken; üçüncü kişi de görünüşün

imza ile aynı sonuçları doğuran güvenli elektronik imza, kural olarak hukuki işlemlerin tümünde geçerlidir. Bu hususa hem 5070 sayılı Kanun m. 5/1 ve Borçlar Kanunu m. 15'te yer verilmiştir. 5070 sayılı Kanun m. 5'e göre, özellikle tamamlanması için tarafların imzasının yeterli olduğu yazılı işlemlerin güvenli elektronik imza ile yapılması mümkündür.[63] Kuralın istisnası ise, 5070 sayılı Kanun m. 5/2'de düzenlenmektedir. Kanunlarda resmi şekle veya özel bir merasime bağlanmış hukuki işlemler ile banka teminat mektupları dışındaki teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez. 5070 sayılı Kanun m. 22, 23, 24 farklı kanunlarda yapılan değişiklikler ile ilgilidir. Hukuk Muhakemeleri Kanunu m. 205'e göre, "*Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir.*" Buna göre, güvenli bir elektronik imza usulüne uygun şekilde oluşturulmuş ve bu imza ile imzalanmış bir veri adi senet hükmündedir. Güvenli elektronik imzanın usulüne uygun düzenlenmediği iddia edilebilir. Bu hususu ispat yükümlülüğü ise, nitelikli imzanın geçerliliğinden şüphe duyan tarafa aittir.[64] Ancak güvenli elektronik imzanın doğruluğu hâkim tarafından resen incelenir. Hukuk Muhakemeleri Kanunu m. 205/3'te de bu husus açıkça düzenlenmiştir: "*Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler.*" Hukuk Muhakemeleri Kanunu m. 210'a göre, güvenli elektronik imza ile oluşturulmuş bir veri inkâr ediliyorsa hâkim öncelikle veriyi inkâr eden tarafı dinler. Hâkim yaptığı dinlemeden kanaate ulaşamamışsa bilirkişi incelemesine başvurulabilecektir. Kanuna göre yazılı şekil şartı olan sözleşmeler için de bir güvenli elektronik imza düzenlemesine yer verilmiştir. Borçlar Kanunu m. 14'te göre, güvenli elektronik imza ile gönderilip saklanabilen metinler de yazılı şekil olarak kabul edilir.

Bu noktada Elektronik İmza Kanunu'nda yer alan elektronik imzanın benzeri bir elektronik veri tipi olarak elektronik mühür düzenlemesine de değinmek gerekmektedir. 7263 sayılı Teknoloji Geliştirme Bölgeleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına

---

gerçekliğini kendisinden beklenebilecek dikkat ve özen yükümlülüğü kapsamında kontrol etmek yükümlülüğü altındadır. Erbayraktar, s. 253-254.

63 Sözer, s. 1022.

64 FARAH, https://www.globalsign.com/en-in/blog/difference-between-eidas-advanced-and-qualified-electronic-signatures, E.T. 30.12.2020,

Dair Kanun m. 14 yoluyla 28.01.2021 tarihinde 5070 sayılı Elektronik İmza Kanunu'nda yapılan değişiklikle elektronik mühür ile ilgili bir düzenlemeye yer verilmiştir.[65] 5070 sayılı Kanun Ek Madde 1'e göre, "*Elektronik mühür, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve mühür sahibinin bilgilerini doğrulama amacıyla kullanılan elektronik veridir.*" Görüldüğü üzere esasen elektronik imza ve elektronik mührün tanımı ve kullanım amacı aynı olup sahipleri yönünden bir ayrıma gidilmektedir. Bu açıdan elektronik imza ve elektronik mühür arasındaki ayrım fiziki imza ve fiziki mühür arasındaki ayrımla eş değerdir. Elektronik imza gibi elektronik mühür de "*resmî mühür dâhil her türlü fiziki mühür ile aynı hukuki niteliği haizdir.*"

Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlara eklenen veya bunlarla mantıksal bir bağlantısı bulunan bir elektronik veri olarak elektronik mühür kullanılabilir. Burada amaç elektronik mühür sahibinin bilgilerini doğrulamaktır. Elektronik mühür kullanıldığında, mührün kullanıldığı elektronik verinin mühür sahibi tarafından oluşturulduğu anlaşılmakta ve bu sayede verinin güvenliği sağlanmaktadır. Kanun koyucu bu hususu 5070 sayılı Kanun Ek Madde 1/3'te "*Elektronik mühür, elektronik belgenin*[66] *veya verinin mühür sahibi tarafından oluşturulduğunu, belgenin veya verinin kaynağını ve bütünlüğünü garanti eden delil kaydıdır*" düzenlemesiyle vurgulamaktadır. Bu açıdan elektronik mühür ile resmi mühürler dahil fiziki mühür arasında bir fark bulunmamaktadır. Elektronik imza sahibinin yalnızca gerçek kişiler olabileceğini belirten Kanun, elektronik mühür sahiplerini ise "*elektronik mührü oluşturan kamu kurum ve kuruluşları, kamu idareleri, kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları, kamu ve özel hukuk tüzel kişileri ile yargı mercileri ve noterlikler*" olarak göstermiştir.

---

65 RG., 03.02.2021, 31384. Elektronik imza gibi sahibinin kimliğini doğrulamaya yarayan bir veri olarak kullanılan elektronik mühür için elektronik imza gibi detaylı bir düzenlemeye gidilmemiş olup Ek Madde 1'de yapılan düzenlemeler haricinde, Kanunlarda yer alan elektronik imzaya ilişkin hükümlerin kıyasen elektronik mühür hakkında da uygulanacağı belirtilmiştir.

66 Elektronik belge, "elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler" olarak tanımlanmaktadır. Erturgut, s. 66.

## II. ELEKTRONİK İMZA KANUNU'NDA DÜZENLENEN SUÇLAR

### A. Genel Olarak

5070 sayılı Elektronik İmza Kanunu İkinci Bölüm Üçüncü Kısmında cezai hükümler düzenlenmiştir. 5070 sayılı Kanun m. 16 ve m. 17'de hapis ve adli para cezası gerektirir iki adet suç tipi düzenlenmiş iken m. 18'de Kanun'da belirtilen maddelerde yer alan yükümlülüklere aykırılık halinde ortaya çıkacak idari para cezası ile ilgili düzenlemeler yapılmıştır. Aynı Kanun Ek Madde 1'in 5. fıkrası kapsamında ise elektronik mühür oluşturma verilerinin izinsiz kullanımı suçu yer almaktadır. Çalışmamızda söz konusu tipleri unsurları itibariyle benzerlikler taşıdıklarından suçların incelemesi "fiil" unsuru haricinde aynı başlık altında yapılmaktadır.

5070 sayılı Elektronik İmza Kanunu m. 16 ve m. 17'de yer alan suç tipleri, 23.01.2008 tarihinde kabul edilen 5728 No'lu Temel Ceza Kanunlarına Uyum Amacıyla Çeşitli Kanunlarda ve Diğer Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile yapılan değişiklik ile mevcut halini almıştır.[67] 5070 sayılı Kanun'un Ek Madde 1/5'te hüküm altına aldığı elektronik mühür oluşturma verilerinin izinsiz kullanımı suçu ise 7263 sayılı Teknoloji Geliştirme Bölgeleri Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun m. 14 ile eklenmiştir.

İmza oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekârlık 5070 sayılı Elektronik İmza Kanunu'nda suç olarak

---

67 5728 sayılı Kanun değişikliğinden önce 16. ve 17. madde düzenlemelerinde "Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir." şeklinde bir fıkra yer almaktaydı. Kanun koyucu 2008 yılında yaptığı değişiklik ile bu hükmü kaldırmıştır. Ayrıca 17. maddede yer alan "yetkisi olmadan elektronik sertifika oluşturanlar" ifadesi ile "fiilleri başka bir suç oluştursa bile ayrıca…" ifadeleri de 2008 yılında yapılan değişiklik ile kanun metninden çıkarılmıştır. Bununla beraber ilgili hükümlerin 2008'den önceki halleri adli para cezası yaptırımları bakımından farklılık göstermektedir. 5070 sayılı Kanun m. 16 için öngörülen yaptırım önceki düzenlemede "bir yıldan üç yıla kadar hapis ve beş yüz milyon liradan aşağı olmamak üzere ağır para cezası" olarak düzenlenmiştir. Aynı şekilde 5070 sayılı Kanun m. 17'de de yaptırım "iki yıldan beş yıla kadar hapis ve bir milyar liradan aşağı olmamak üzere ağır para cezası" olarak öngörülmüştü. Türk ceza adaleti sisteminde 2005 sonrası yapılan kanun değişiklikleri ile ağır-hafif para cezası ayrımı ortadan kalktığından 5070 sayılı Kanun'da da bu cezalar adli para cezası olarak yeniden düzenlenmiştir.

düzenlenmiştir. 5070 sayılı Kanun m. 16'ya göre, elektronik imza oluşturma amacı ile ilgili kişinin yani elektronik imza yetkilisinin rızası dışında; elektronik imza oluşturma verisinin yani göndericide bulunan gizli anahtarın ya da elektronik imza oluşturma aracının yani gizli anahtarın kullanıldığı yazılım veya donanımın elde edilmesi, bir başka kişiye verilmesi, kopyalanması, yeniden oluşturulması ve izinsiz elde edilmiş imza oluşturma aracının kullanılması ile izinsiz elektronik imza oluşturulması suç sayılmıştır. Ayrıca 5070 sayılı Kanun m. 17'ye göre, elektronik sertifikanın tamamen veya kısmen sahtesinin oluşturulması ile geçerli bir elektronik sertifikanın taklit ya da tahrif edilmesi ve ayrıca sahte, taklit veya tahrif edilmiş sertifikanın bilerek kullanılması suç kabul edilmiştir. Aynı Kanun'un Ek Madde 1/5 hükmünde ise, elektronik mühür sahibinin rızası veya talebi dışında, elektronik mühür oluşturma aracının elde edilmesi, verilmesi, kopyalanması ve bu araçların yeniden oluşturulması ile izinsiz elde edilen mühür oluşturma araçlarının kullanılması suretiyle izinsiz elektronik mühür oluşturulması suç olarak düzenlenmiştir. İlgili hükümlerin elektronik sertifika hizmet sağlayıcısı çalışanları tarafından ihlal edilmesi hali ise üç suç tipi açısından da nitelikli hal olarak yer almaktadır.

**B. Korunan Hukuki Değer**

Kişinin suç oluşturan bir fiil işlemesi ile sosyal değerler ve hukuk düzeni bozulmuş olur. Kanun koyucu suç tipi düzenlemesi yaparak bir veya birden çok hukuki değeri korumak ve bu hukuki değerler ihlal edilirse sorumluları cezalandırmak amacı güder. 5070 sayılı Kanun m. 16 ve m. 17 açısından bakıldığında, her iki suç için de korunan hukuki değer elektronik imza sürecinin hukuki çerçevede ilerlemesini sağlamak adına elektronik imzanın, elektronik imza oluşturma araçlarının ve nitelikli elektronik sertifikaların doğruluğu ve bu sisteme olan güvenin korunmasıdır.[68] 5070 sayılı Kanun Ek Madde 1 hükmü ile ise elektronik mührün güvenilirliğini korumak amaçlanmaktadır.[69] Henüz son 20 yıldır ciddi biçimde hayatımıza dahil olan bu elektronik imza ve elektronik mühür alt yapısı ve sistemi üzerinden yürüyen

---

68 Ali Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayıncılık, Ankara, 2005, s. 189.

69 Zira 5070 sayılı Kanun Ek Madde 1/4 hükmü uyarınca, "Elektronik mühür, resmi mühür dahil her türlü fiziki mühür ile aynı hukuki niteliği haizdir."

kamusal ve özel her türlü iş ve işlem bir güven ilişkisi çerçevesinde yürütülmeye çalışılmaktadır. Bu nedenle getirilen cezai hükümler ile elektronik imza ile elektronik mührün doğruluğu ve bu yolla oluşturulan verilerin güvenilirliği korunmaya çalışılmaktadır.[70] Bunun yanı sıra, elektronik imzayı kullanma hakkına sahip olan kişinin kişisel verileri ile elektronik mühür sahibinin bilgileri de korunmaktadır.

### C. Suçların Maddi Unsurları

#### 1. Fiil

##### a. İmza Oluşturma Verilerinin İzinsiz Kullanılması[71]

5070 sayılı Kanun m. 16'da düzenlenen imza oluşturma verilerinin izinsiz kullanılması suçunda tipik fiil kanunda yer alan hareketlerden birinin gerçekleşmesi ile oluşmaktadır. Buna göre, imza oluşturma verisi olan gizli anahtarın yani gizli şifrenin veya bu imza oluşturma verisini kullanmaya yarayan imza oluşturma aracının fail tarafından elde edilmesi, elde ettikten sonra başkasına verilmesi, kopyalanması; imza oluşturma aracının yeniden oluşturulması ve izinsiz elde edilen imza oluşturma aracı ile izinsiz elektronik imza oluşturması fiillerinden birinin yapılması 5070 sayılı suçun fiil unsurunu oluşturmaktadır.

İmza oluşturma verilerinin izinsiz kullanımı suçunun seçimlik hareketli bir suç tipi olduğu ifade edilmektedir.[72] Seçimlik hareketli suçlar, icrasının gerçekleşmesi için kanunda seçenek birden fazla hareketin gösterildiği ve bu hareketlerden birinin gerçekleşmesi halinde

---

70 Aynı yönde bkz. Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara, 2020, s. 563.

71 İmza Oluşturma Verilerinin İzinsiz Kullanılması başlığında incelenen suçun fiil unsuruna ilişkin özellikler, 5070 sayılı Kanun Ek Madde 1/5'te yer alan suç tipi için de geçerli olup ilgili hüküm için çalışmamızda ayrıca inceleme yapılmamaktadır. Bu başlık altında "imza oluşturma verileri" ifadeleri 5070 sayılı Kanun Ek Madde 1/5 için "mühür oluşturma verileri" olarak anlaşılmalıdır.

72 Yusuf Başlar, "Elektronik İmza Kanunu'nda Düzenlenen Bilişim Suçları", *Uluslararası Antalya Üniversitesi Hukuk Fakültesi Dergisi*, C. 4, S. 7, 2016, s. 51; Orer, s. 161; Alper Özboyacı, "5070 sayılı Elektronik İmza Kanunu'nda Yer Alan Cezai Hükümler", *Terazi Hukuk Dergisi*, 2009, C. 4, S. 39, s. 129.

suçun tamamlandığı suç tipleridir.[73] Seçimlik hareketli suçlar söz konusu olduğunda her zaman tek bir hareket gerçekleşmeyebilir; birden fazla hareketin gerçekleşmiş olması da mümkündür. Örneğin, bir kişi yetkilisinin rızası hilafına hem imza oluşturma aracını elde edip hem de bu aracı kopyalayabilir. Bu halde birden fazla suç işlenmesi söz konusu olmayacak ve bu suç bir defa işlenmiş kabul edilecektir. Ancak bu durum, 5237 sayılı Kanun m. 61 kapsamında temel cezanın belirlenmesi açısından değerlendirilebilecektir.[74]

Seçimlik hareketli suçlar bakımından temel olan bir hususun bu madde nezdinde de değerlendirilmesi gerekmektedir. Şöyle ki, seçimlik hareketli suçlarda suçun konusunun değişmesi halinde iki ayrı suç işlenmiş olmaktadır. Bir başka deyişle seçimlik hareketli suç dolayısıyla tek suç oluşabilmesi için hareketlerin nesnel olarak aynı konu üzerinde işlenmiş olması zorunludur.[75] İmza oluşturma verilerinin izinsiz kullanımı suçu açısından bakıldığında ise, seçimlik suç olup olmadığı ile alakalı bir değerlendirme yapmak gerekir. İmza oluşturma verisi ve imza oluşturma aracı konu bakımından ayniyeti sağlamakta mıdır?

İmza oluşturma verilerinin izinsiz kullanımı suçu açısından bakıldığında, tek elektronik sertifikaya tabi yani bir kişiye ait olan bir imza oluşturma verisi ve imza oluşturma aracı birbiri olmadan kullanılamayan ve ikisinden biri olmadan bir anlam ifade etmeyen elektronik imza ögeleridir. Örneğin, imza oluşturma verisinin ve imza oluşturma aracının elde edilmesi halinde kişi madde metninde de açıkça belirtildiği üzere elektronik imza oluşturmak amacındadır. Elektronik imza oluşturulabilmesi amacıyla zaten kişinin her ikisine de sahip olması gerekmektedir. İmza oluşturma verisini elde edemeyen ancak elektronik imza oluşturma aracı ilgilinin rızası olmaksızın elinde bulunduran fail elektronik imza oluşturmak amacında ise bu suçu işlemiş olur. Aynı şekilde hem imza oluşturma verisini hem de imza oluşturma elinde bulunduran ve imza oluşturma aracını aynı zamanda kopyalayan faile de ayrıca ceza vermemek gerekir. Zira amaç elektronik imza oluştur-

---

73 İzzet Özgenç, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara, 2020, s. 185-186.

74 Mahmut Koca/İlhan Üzülmez, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara, 2020, s. 122.

75 Özgenç, s. 186.

maktır ve tek bir sertifikaya dayalı tek kişiye ait bir imza oluşturma verisi ve imza oluşturma aracı söz konusudur. Her ikisi de tek nitelikli elektronik sertifikadan kaynaklı bu elektronik imza ögeleri konu bakımından ayniyeti sağlamaktadır. Dolayısıyla madde seçimlik hareketli suç düzenlemesi içermektedir. Ayrıca imza oluşturma verilerinin izinsiz kullanımı ancak icrai hareketler ile işlenebilen bir suç tipidir.[76] Bu suçun ihmal suretiyle işlenmesi söz konusu değildir.

Elektronik imza oluşturmak amacıyla kullanılan imza oluşturma verisi,[77] bir eşi daha tanımlanmamış şifrelerden oluşan verilerdir. İmza oluşturma aracı[78] ise imza oluşturma verisini kullanan yazılım veya donanım aracıdır. Bu araçlar mevzuatın getirdiği standartlara[79] sahip akıllı kartlar veya akıllı çubuklar olabileceği gibi yazılımlar da olabilmektedir. İlgilinin rızası dışında elektronik imza oluşturma amacı ile imza oluşturma verisi veya imza oluşturma aracı üzerinde gerçekleştirilen fiiller suç oluşturmaktadır.

**i. İmza Oluşturma Verisinin veya Aracının Elde Edilmesi**

Kanunda belirtilen ilk seçimlik hareket imza oluşturma verisinin veya aracının elde edilmesidir. İmza oluşturma verisinin elde edilmesi, veriyi oluşturan şifrelerin ve algoritmanın ele geçirilmesidir. Bu şifre ve algoritmanın ele geçirilmesi bir başkasının bilişim sistemine girilerek olabileceği gibi fiziki alınması şeklinde de olabilir.[80] Bunun yanı sıra imza oluşturma aracı olan akıllı kart veya akıllı çubukların ya da yazılımların elde edilmesi yoluyla da bu suç işlenebilmektedir. Akıllı kart veya akıllı çubukların fiziken ele geçirilmesi ya da veri tabanına erişilerek yazılımsal olarak imza oluşturma aracının ele geçirilmesi mümkündür. Bu suçların oluşumu bilişim sistemleri üzerinden olabileceği gibi fiziki elde etme şeklinde de olabilir. Ancak bunun

---

76 Dülger, s. 567.

77 5070 sayılı Elektronik İmza Kanunu m. 3'e göre: "İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler" imza oluşturma verisidir.

78 5070 sayılı Elektronik İmza Kanunu m. 3'e göre: "Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracı" imza oluşturma aracıdır.

79 Elektronik İmza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ, RG., 06.01.2005, 25692.

80 Orer, s. 161.

için bilişim sistemine girişin ya da fiziksel elde etme imkânı sağlayan durumun hukuka aykırı olması gerekmez.[81] Örneğin, bir fakültenin dekanı fakülte sekreterinden kullandığı bilgisayardan kendisine bir belge göndermesini istiyor. Bu talep üzerine bilgisayarı açmaya giden fakülte sekreteri elektronik imza oluşturma aracını masanın üzerinde görüyor ve bu aracı gerekli belgileri imzalamak düşüncesi ile odasına götürüyor. Bu olayda fakülte dekanının gerekli olan belgeleri imzalaması için sekretere verdiği bir rıza bulunmamaktadır. İmza oluşturma aracı olan akıllı çubuğun ilgilinin rızası hilafına sekreter tarafından elde edilmesi halinde bu suç oluşmuş olur.

**ii. İmza Oluşturma Verisinin veya Aracının Verilmesi**

İmza oluşturma verisi olan şifre ve algoritmaların veya imza oluşturma aracının ilgilinin rızası dışında bunları elde eden kişilerce bir başka kişiye verilmesi suç olarak düzenlenmiştir. Esasen zaten verinin veya aracın elde edilmesi suç olarak düzenlenmiştir. İlgilinin rızası dışında bir elde etme varsa veriler ve araçlar başka kişiye verilmese de suç oluşmaktadır. Zira bir veri veya araç elde edilmeden başka bir kişiye de verilemez.[82] Ancak burada önemli olan nokta, elde etme hukuka uygun iken verme fiili hukuka aykırı olabilir.[83] Yani ilgili, gerçekten de imza oluşturması amacı ile imza oluşturma verisini ve/veya aracını vermiş olabilir. Ancak imza oluşturma verisini ve/veya aracını alan kişi, ilgili kişinin rızası doğrultusunda ancak belirtilen işlemleri yapabilir. Dolayısıyla bunu aşar biçimde ilgilinin rızası olmaksızın hukuka uygun veya hukuka aykırı elde edilen imza oluşturma veri ve/veya aracını bir başka kişiye veren kişi "verme" fiili ile suçu gerçekleştirmektedir. Kişi, ilgilinin rızası dışında ilgilinin imza oluşturma verisini veya aracını herhangi bir şekilde üçüncü kişiye iletebilir. Bilişim sistemi kullanılarak bu iletim yapılabileceği gibi aracın fiziki olarak iletimi de bu anlamda "verme" fiili kapsamında değerlendirilir.

**iii. İmza Oluşturma Verisinin veya Aracının Kopyalanması**

İmza oluşturma veri veya aracına hukuka uygun veya aykırı olarak erişen kişi, bu veri veya aracı kopyalamaktadır. Kopyalama ge-

81 Dülger, s. 567.
82 Dülger, s. 567; Özboyacı, s. 130.
83 Dülger, s. 567.

nellikle bilişim sistemi üzerinden gerçekleştirilmektedir.[84] Kopyalama, imza oluşturma verisi veya aracını tedarik eden elektronik sertifika hizmet sağlayıcı tarafından da yapılabilir. Elektronik imza oluşturma verisi veya aracı tek olarak üretilmektedir. 5070 sayılı Elektronik İmza Kanunu m. 10 elektronik sertifika hizmet sağlayıcının yükümlülüklerini düzenlemektedir. Buna göre, elektronik sertifika hizmet sağlayıcı üretilen imza oluşturma verisinin bir kopyasını alamayacaktır. İmza oluşturma verisinin kopyalanması halinde imza oluşturma verisini kopyalama ile suç oluşur ve elektronik sertifika hizmet çalışanları tarafından bu suç işlendiğinden nitelikli hal uygulanması gerekir.

**iv. İmza Oluşturma Aracının Yeniden Oluşturulması**

Elektronik imza oluşturmak amacıyla imza oluşturma verisinin kullanılmasını sağlayan yazılımsal ve donanımsal araçların yeniden oluşturulması fiili de imza oluşturma verilerinin izinsiz kullanımı suçunu oluşturmaktadır. Mevcut bulunan imza oluşturma aracının ortadan kaybolması ile tipiklik oluşabileceği gibi ilk imza oluşturma aracı kaybolmadan birbiri ile aynı işlevde ikinci bir imza oluşturma aracının üretilmesi ile de fiil gerçekleşebilecektir. Dolayısıyla imza oluşturma aracı yazılımının silinmesi veya donanımın fiziki olarak yok edilmesi ve yerine geçecek yeni bir imza oluşturma aracı oluşturulması ya da aynı işlevdeki ikinci elektronik imza oluşturma aracının oluşturulması suç kapsamında değerlendirilmektedir. Esasen imza oluşturma aracı, imza oluşturma verisi gibi elektronik sertifika hizmet sağlayıcı tarafından üretilir/ürettirilir ve temin edilir. Hukuka uygun olarak elektronik sertifika hizmet sağlayıcı tarafından oluşturularak verilen imza oluşturma aracının hukuka aykırı olarak yeniden oluşturulması ile suç gerçekleşmiş olmaktadır.

**v. İzinsiz Elektronik İmza Oluşturulması**

Kanunun ilgili hükmüne göre: *"izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluştur"*mak suç olarak kabul edilmektedir. Elektronik imza oluşturmak amacıyla ilgilinin rızası dışında elde edilen imza oluşturma aracı kullanılarak izinsiz elektronik imza oluşturulması suçu oluşturan hareketlerin sonuncusu olarak dü-

84 Kopyalama imza oluşturma aracının bilgisayar üzerinde unutulması suretiyle yapılabileceği gibi, açık ağ sistemi üzerinden de yapılabilmektedir. Orer, s. 161.

zenlenmiştir. Burada failin ilgilinin izni dışında iki farklı hareket yapması beklenmektedir. İlk olarak imza oluşturma aracının izinsiz olarak ele geçirilmesi gerekir ki zaten bu halde suç oluşmuş olmaktadır. Daha sonra da bu ele geçirilen araç kullanılarak yine izinsiz olarak elektronik imza oluşturulması söz konusudur. Dolayısıyla elektronik imza oluşturmak amacıyla izinsiz şekilde imza oluşturma aracını elde eden ancak izinsiz elektronik imza oluşturamadan hareketin yarım kaldığı durumda da teşebbüsten değil imza oluşturma verilerinin izinsiz kullanımından cezalandırmak gerekecektir.

Kanun hükmü değerlendirildiğinde izinsiz elde edilen imza oluşturma araçlarının kullanılmasından bahsedildiğinden izin kapsamında kullanılan imza oluşturma araçları ile izinsiz elektronik imza oluşturulmasının suç olarak kabul edilmediği sonucu çıkarılmaktadır.[85] Bu da demektir ki, kanun koyucu imza oluşturma aracının izin dahilinde elde edilmesini imza oluşturulmasına da verilen zımni bir izin olarak nitelendirmektedir.[86] Araç izin dahilinde verildikten sonra ayrıca imza oluşturmak için de izin verilmesi harekete verilen izinlerin değerlendirilmesi noktasında kopuk ve incelenmesi zor bir durumun yaratacağı ifade edilmektedir.[87] Kanun koyucunun ifadesi incelendiğinde bu görüşe katılmaktayız. Ancak önemle vurgulamak gerekir ki, özel olarak imza oluşturma aracının imza oluşturmaktan başka bir amaç ile verildiği kişiye belirtilmiş ise bu amacı aşarak imza oluşturma aracının kullanılması ve imza oluşturulması suç kabul edilmelidir.[88] Bir başka deyişle, kişi açıkça farklı bir amaçla imza oluşturma aracını verdiğini belirtmiyor ise imza oluşturma aracının izin dahilinde verilmesi ile imza oluşturulması amacı ile bu amacın verildiği şeklinde bir yorum yapılabilecektir. Zira kanun koyucunun bu hükmü ele alış biçiminden, imza oluşturma aracının imza oluşturma amacı dışında bir amaçla verilmeyeceği yönünde bir mantık yürüttüğü anlaşılmaktadır. Ancak imza oluşturma aracının farklı bir amaç ile verilmiş ve bunun açıkça kişiye bildirilmiş olması durumunda failin hareketinin suç oluşturduğu ifade edilebilecektir. Aksi halde, failin hukuka uygun başlayan elde etmesinin hukuka aykırı hale dönüşmesinin kanun koyucu tarafından cezalandırılmadığı bir durum ortaya çıkacaktır.

---

85 Özboyacı, s. 131.
86 Dülger, s. 569.
87 Dülger, s. 569.
88 Aynı yönde bkz. Başlar, s. 55.

**b. Elektronik Sertifikalarda Sahtekârlık**

Elektronik sertifika, 5070 sayılı Elektronik İmza Kanunu'nda "*İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı*" olarak tanımlanmıştır. Elektronik sertifika ile elektronik imza kullanıcısının kimlik tespiti mümkün olmaktadır. Bu nedenle elektronik sertifikalar genellikle imza doğrulama verisi yani açık anahtar ile ilişkilendirilmektedir.[89] Güvenli elektronik imza nitelikli elektronik sertifikaya bağlı olarak oluşturulmaktadır. Dolayısıyla esasen nitelikli elektronik sertifika güvenli elektronik imzayı oluşturan yapı olduğundan sahtelikten, taklit veya tahriften korunması gerekmektedir. Aksi halde elektronik sertifikanın güvenliliğinden de bahsedilemez.

Elektronik İmza Kanunu m. 17'de elektronik sertifikalarda sahtekârlık suçunun hareketlerine yer verilmektedir. Buna göre, geçerli bir elektronik bir sertifika olmamasına rağmen sahte bir elektronik sertifika oluşturmak veya geçerli bir elektronik sertifikayı taklit veya tahrif etmek suç olarak düzenlenmiştir. Ancak kanun koyucu aynı zamanda sahte, taklit veya tahrif edilen elektronik sertifikayı bilerek kullanmayı da bu madde kapsamında cezalandırılacak bir hareket olarak değerlendirmiştir. Dolayısıyla kişi elektronik sertifika oluşturmak veya üzerinde oynama yapmak fiillerini gerçekleştirmese de hukuka aykırılığı bilerek sertifikayı kullanırsa suç oluşturan hareketi gerçekleştirmiş kabul edilmektedir.

Elektronik sertifikalarda sahtekârlık suçunun düzenlenme şeklinden hareketle seçimlik hareketli bir suç tipi olduğu ifade edilmektedir.[90] Örneğin, fail, bir elektronik imza için ister sahte ister taklit elektronik sertifika oluştursun tek suçtan cezalandırılacaktır. 5070 sayılı Kanun m. 16'da olduğu gibi bu suç tipi de ancak icrai hareketlerle işlenebilir; ihmal suretiyle işlenmesi mümkün değildir.

Elektronik İmza Kanunu'nda düzenlenmiş olan bu suç tipi esasen özel bir belgede sahtecilik suçu düzenlemesidir. Elektronik sertifikalar da hukuksal açıdan önem taşıyan, yazılı, düzenleyeni belli ve belirli bir içeriğe sahip yazı olduklarından belge niteliğinde değerlendirile-

89 Rissnaes, s. 134.
90 Başlar, s. 55; Dülger, s. 569.

bilirler.[91] Sertifikalar üzerinde yapılan oynama ve olmayan bir sertifikanın oluşturulması 5070 sayılı Kanun m. 17 başlığında genel manada "sahtekârlık" olarak ifade edilmiştir. Bu nedenle 5070 sayılı Kanun m. 17'de düzenlenen suçu yorumlamak bakımından 5237 sayılı Kanunda yer alan belgede sahtecilik suçlarından yardım alınabilmektedir.

**i. Sahte Elektronik Sertifika Oluşturulması**

Sahte elektronik sertifika oluşturulması 5070 sayılı Elektronik İmza Kanunu'nda suç kabul edilmektedir. Sahte, *"bir şeyin aslına benzetilerek yapılan, düzme, düzmece; uydurma, gerçek olmayan"* olarak tanımlanmaktadır.[92] Oluşturmak ise olmayan bir şeyin meydana getirilmesi olarak ifade edilebilir. Yapılan bu tanımlamalardan yola çıkılacak olursa, sahte elektronik sertifikanın oluşturulması, gerçek olmayan bir elektronik sertifika meydana getirilmesidir. Sahte elektronik sertifika oluşturulmasında olmayan bir şeyi oldurmak söz konusudur. Sahte bir elektronik sertifikanın oluşturulması suçun oluşumu yeterlidir; failin sahte olarak düzenlediği elektronik sertifikayı kullanması gerekmez.

Madde metninde sahteciliğin kısmen veya tamamen yapılabileceğinden bahsedilmiştir. Tamamen sahte elektronik sertifika düzenlemek, aslında mevcut olmayan elektronik sertifikanın mevcutmuş gibi oluşturulmasıdır. Kısmen sahtecilik, bir elektronik sertifikanın bir kısmında yapılacak sahteciliktir. Kanun koyucunun kısmen sahte elektronik sertifika düzenlemek ile neyi kastetmek istediği tam manasıyla anlaşılamamaktadır.[93] Geçerli olmayan bir elektronik sertifika üzerinde kısmi sahtecilik yapılması zaten tamamen sahte bir elektronik sertifikanın varlığı söz konusu olduğundan bir anlam ifade etmeyecektir. Ancak geçerli bir elektronik sertifika üzerinde kısmi sahtecilik yapılmasını da gerçek bir elektronik sertifikayı tahrif etmek hareketinden ayırmak zordur. Kaldı ki, kanun koyucu "geçerli bir elektronik sertifika" ifadesini taklit ve tahrif fiilleri için kullanmaktadır. Kanaatimizce,

---

91 Durmuş Tezcan/Mustafa Ruhan Erdem/R. Murat Önok, Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara, 2020, s. 1037.

92 TDK., https://sozluk.gov.tr/, E.T. 03.01.2021.

93 Doktrinde, kısmen sahteciliğini sahte olmayan bir elektronik sertifikaya bir şeyler eklemeyi veya bundan bir şeyler çıkarmayı ifade ettiği belirtilmektedir. Ancak bu durumda taklit veya tahrif ile kısmen sahteciliğin ayrımının yapılamadığı da kabul edilmektedir. Karagülmez, s. 193.

elektronik veriyi çözmeye yarayan şifreler yani imza doğrulama verisi ve kimlik bilgilerini bağlayan kaydın içeriğinin gerçeği yansıtmayacak şekilde oluşturulması ve bunun elektronik sertifikanın bir kısmında yapılması halinde kısmen sahte elektronik sertifika oluşturulması; geçerli oluşturulan elektronik bir sertifikadaki elektronik veriyi çözmeye yarayan şifreler ve kimlik bilgilerini bağlayan kaydın içeriğinin değiştirilmesi, içerikte yer alan hususların yerlerinin değiştirilmesi, sertifikaya ekleme çıkarma yapılması halinde de geçerli elektronik sertifikanın tahrif edilmesi hareketi oluşacaktır. Örneğin, elektronik imza almak için başvurulan nitelikli elektronik sertifikada kimlik bilgileri girilmesi gereken kısma gerçek olmayan isim soy isim eklenmesi ile oluşturulması sertifikanın diğer tüm kısımları doğru olsa bile kısmen sahte elektronik sertifika olduğu ifade edilebilir. Zira burada daha önceden gelen geçerli bir elektronik sertifika yoktur yeni bir sertifika oluşturulmaktadır. Bunun yanı sıra geçerli elektronik sertifikada yer alan kimlik belgelerinin değiştirilmesi halinde geçerli elektronik sertifikanın tahrif edilmesinden bahsedilebilecektir.

**ii. Geçerli Elektronik Sertifikanın Taklit veya Tahrif Edilmesi**

Taklit etmek, "*bir kimseye ya da bir şeye benzemeye çalışmak; bir şeyin sahtesini yapmak, benzetmek*"; tahrif etmek, "*bozmak, değiştirmek*" şeklinde tanımlanmaktadır.[94] Öncelikle ifade edilmelidir ki geçerli elektronik sertifikanın taklit veya tahrif edilmesi hareketi de elektronik sertifikalarda sahtekarlık madde başlığı altında düzenlenmiştir. Yani bu hareketler bünyesinde sahtecilik barındırmaktadır. Taklit etmenin sözcük anlamı bir şeyin sahtesini yapmak olarak ifade edilmektedir. Bu durumda sahte elektronik sertifika oluşturmak ile geçerli elektronik sertifikanın taklidi arasındaki farkın ortaya koyulması gerekmektedir. Buradaki tek fark kanaatimizce, taklitten önce gerçekten geçerli bir belgenin bulunmasının şart olmasına rağmen sahtecilik için bu şekilde bir şart aranmıyor olmasıdır. Dolayısıyla sahteciliğin konusu öncesinde gerçekten var olan bir elektronik sertifika olabileceği gibi gerçekte var olmayan bir elektronik sertifika olabilmekte iken taklitte öncesinde gerçekten var olan bir elektronik sertifika olması gerekmektedir.[95]

---

94 TDK., https://sozluk.gov.tr/, E.T. 03.01.2021.

95 Veli Özer Özbek/Koray Doğan/Pınar Bacaksız, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara, 2020, s. 843.

Esasen her taklit içinde sahteciliği de barındırmaktadır. Bir elektronik sertifikanın tahrif edilmiş sayılması için gerçekte ifade edilen hususlar ile sertifikada görülen hususların farklı olması gerektiğinden bu da bir sahteciliktir.

Geçerli bir elektronik sertifikanın taklidi genellikle kopyalama biçimde olmaktadır.[96] Kopyalama sonucunda geçerli olan sertifikanın aynı oluşturulmaktadır. Oluşturulan bu taklit sertifikanın ise kullanılması suçun oluşması açısından şart değildir. Geçerli bir elektronik sertifikanın tahrif edilmesi ise, geçerli var olan elektronik sertifika verilerine ekleme çıkarma yapılması, verilerin yerlerinin değiştirilmesi şeklinde olabilecektir.[97] Doktrinde yapılan ekleme çıkarmanın kısmen veya tamamen sahte elektronik sertifika oluşturması halinde artık tahrif hareketinden değil sahte elektronik sertifika oluşturulmasından bahsedileceği ifade edilmektedir.[98]

Daha önce de belirttiğimiz gibi, sahte elektronik sertifika oluşturma, geçerli elektronik sertifikayı taklit veya tahrif etme fiilleri birbirinden ayrımı teorik olarak da kolay değildir. Bununla beraber bu fiillerin hepsi sahtekarlık içerisinde değerlendirilmektedir. Dolayısıyla kanaatimizce yapılması gereken temel ayrım öncelikle ortada geçerli bir elektronik sertifikanın bulunup bulunmadığıdır. Geçerli bir elektronik sertifika yok ise, taklit veya tahriften bahsedilemez. Zira bu fiiller tanımları gereği öncesinde geçerli bir elektronik sertifikanın varlığının aranmasını gerektirmektedirler. Geçerli bir elektronik sertifika bulunması halinde ise, elektronik sertifika her özelliği ile bire bir kopyalanıyorsa taklit edilmesinden; sertifikada yer alan içerikte ekleme çıkarma söz konusuysa veya içerikte yer alan bilgilerin yerlerinde bir değişiklik yapılıyorsa tahriften bahsedilecektir. Ancak sıkıntı yaratan durum şudur ki; geçerli bir elektronik sertifikanın varlığı durumda aslında yapılan tahrifler ile kısmen sahte belge oluşturmak arasındaki ayrım anlaşılamaz hale gelmektedir. Bu nedenle illa bu şekilde bir ayrıma gidilecekse kanun koyucunun *"geçerli olarak oluşturulan elektronik sertifika"* ifadesini yalnızca taklit veya tahrif fiilleri için kullanmasının gereği olarak geçerli bir elektronik sertifika üzerinde yapılan her türlü sah-

96 Dülger, s. 570.
97 Dülger, s. 571.
98 Dülger, s. 571.

tekarlık fiili taklit veya tahrif olarak değerlendirilmelidir. Dolayısıyla geçerli elektronik sertifika bulunmaması halinde de yapılan her türlü sahtekarlık sahte elektronik sertifika oluşturmak olarak değerlendirilecek böylece aradaki ayrım da buna göre belirlenebilecektir.

**iii. Sahte Sertifika Kullanılması**

Kullanma, elektronik sertifika sahte olmasaydı hangi amaç için kullanılacaksa sahte elektronik sertifikanın o amacı gerçekleştirmek için değerlendirilmesidir.[99] Hangi amaç doğrultusunda kullanılırsa kullanılsın kanun koyucu "bilerek" kullanılmasını özel olarak belirtmiştir. Bu husus manevi unsurda ele alınması gereken bir konudur. Kullanılan sahte elektronik sertifikanın kim tarafından ne şekilde sahte hale getirildiğinin bir önemi bulunmamaktadır. Dolayısıyla sahte oluşturulmuş, taklit veya tahrif edilmiş bir elektronik sertifikanın bilerek kullanılması suçun bu fiil ile oluşumu için yeterlidir.

Kullanma hareketi elektronik sertifikalarda sahtekarlık suçunun seçimlik hareketlerinden biri olarak düzenlenmiştir. Bu durumda sahte elektronik belge oluşturan veya geçerli elektronik belgeyi taklit veya tahrif eden failin aynı zamanda bu belgeyi kullanması halinde de tek suçtan cezalandırılması söz konusu olacaktır.

5070 sayılı Elektronik İmza Kanunda yer alan her üç suç tipi de fiilin gerçekleşmesi ile tamamlandığından sırf hareket suçlarının birer örneğini oluşturmaktadırlar. Bu suçlarda herhangi bir neticenin gelmesi aranmaz.[100]

Kanuni tanımda fiilin icrası suçun tamamlanması için yeterli görülüp netice aranmadığından netice ile fiil arasında bulunması gereken nedensellik bağı incelemesi de bu suçlar açısından yapılmayacaktır. Zira nedensellik bağı kanuni tanımda bir neticenin gerçekleşmesi gerekliliğinin belirtildiği neticeli suçlar açısından incelenmesi gereken bir suç unsurudur.

**2. Fail**

Suçlar kural olarak herkes tarafından işlenmekte ancak bazı suçlar için yalnızca belli bir faillik vasfı bulunan kişiler suçu işleyebilmekte-

99 Özbek/Doğan/Bacaksız, s. 846.
100 Karagülmez, s. 190.

dir. Bu hususun kanuni tanımda belirtilmesi gerekmektedir. 5070 sayılı Elektronik İmza Kanunu m. 16 ve m. 17 ve Ek Madde 1'de yer alan suçlar için fail açısından bir özellik bulunmamaktadır. Bu nedenle, bu suçların faili herkes olabilir. Ancak söz konusu suçlar açısından kanun koyucu failin elektronik sertifika hizmet sağlayıcısı çalışanı olması durumunda cezanın yarısına kadar artırılacağı ifade edilmektedir. Elektronik sertifika hizmet sağlayıcının sorumluluğu nitelikli elektronik sertifika düzenlenmesi için gerekli bilgilerin tümüne haiz olmasından kaynaklanmaktadır.[101] Dolayısıyla failin çalıştığı iş bu suçlar açısından cezayı artırıcı bir nitelikli hal olarak öngörülmektedir.

Bir suçun faili ancak gerçek kişi olabilir; tüzel kişiler suçun faili olamaz.[102] Tüzel kişiler hakkında 5070 sayılı Kanun kapsamında yer alan suçlardan bahisle 5237 sayılı Türk Ceza Kanunu m. 60 uyarınca, güvenlik tedbirlerine hükmedilebilecektir. Nitekim 5070 sayılı Elektronik İmza Kanunu m. 19/1'de de 5070 sayılı Kanundan doğan suçlar ile ilgili tüzel kişiler hakkında 5237 sayılı Kanun m. 60'a göre güvenlik tedbirlerine hükmolunacağı ifade edilmiştir. 5070 sayılı Kanun m. 21'de, elektronik sertifika hizmet sağlama faaliyeti yerine getiren kamu kurum ve kuruluşları hakkında aynı Kanun m. 19'un uygulanamayacağı hükmüne yer verilmiştir. Dolayısıyla ilgili kamu kurum ve kuruluşları ile alakalı Elektronik İmza Kanunu'ndan doğan suçlardan dolayı güvenlik tedbirine hükmedilmesi mümkün değildir.

### 3. Suçun Konusu

5070 sayılı Elektronik İmza Kanunu m. 16 ve m. 17 açısından suçun konusu temelde elektronik sayısal verilerdir. Elektronik imza da elektronik sertifika da sayısal veriler ve algoritmalardan oluşmaktadır. 5070 sayılı Kanun m. 16 ve m. 17'de imza oluşturma verileri veya elektronik sertifika verilerinin üzerinde suç işlenmektedir. 5070 sayılı Kanun Ek Madde 1/5 açısından ise suç, elektronik mühür verileri veya araçları üzerinde gerçekleşmektedir.

5070 sayılı Kanun m. 16'da "İmza Oluşturma Verilerinin İzinsiz Kullanımı" başlığında düzenlenen suç tipinin konusu imza oluştur-

101 Yıldırım, s. 263.
102 Özgenç, s. 213.

ma verisi veya imza oluşturma aracıdır. Aynı Kanunun Ek Madde 1/5 hükmünde yer alan paralel düzenlemeye göre suçun konusu, elektronik mühür oluşturma verisi veya mühür oluşturma aracıdır. Her ne kadar bu suç tiplerinde iki farklı maddi konu varmış gibi görünse de esasen imza/mühür oluşturma verisi ve aracı birbirini tamamlayan ve ikisi birlikte kullanıldığında bir anlam ifade eden genel olarak elektronik imza/mühür oluşturmaya yardımcı ögelerdir. 5070 sayılı Kanun'un 17. maddesinde düzenlenen "Elektronik Sertifikalarda Sahtekarlık" suçunun konusu ise nitelikli elektronik sertifikalardır.

5070 sayılı Elektronik İmza Kanunu'na göre güvenli elektronik imza, imza sahibine özel olarak bağlanan ve sadece onun tasarrufundaki imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliği ile imzalanmış elektronik veride değişiklik yapılıp yapılmadığının tespitini sağlayan ıslak imza yerine kullanılabilen elektronik veridir. Dolayısıyla güvenli elektronik imzayı oluşturan unsurlar imza oluşturma verisi, imza oluşturma aracı, nitelikli elektronik sertifika olarak belirlenebilir. Bu unsurlar birbirlerine bağlı olduğundan 5070 sayılı Kanun m. 16'da tanımlanan suç için imza oluşturma verisi veya aracı olarak münhasıran tek bir elektronik imzaya tanımlanmış ögelerin suçun konusu olduğu kabul edilmelidir. Aynı husus 5070 sayılı Elektronik İmza Kanun Ek Madde 1 hükmüne göre elektronik mühür açısından da geçerlidir. Elbette ki A kişisi adına tanımlanmış elektronik imza oluşturma verisi ile B kişisi adına tanımlanmış imza oluşturma aracının ele geçirilmesi halinde farklı konular üzerinde suç işlenmektedir. Ancak A kişisine ait imza oluşturma verisi ve imza oluşturma aracının ele geçirilmesi halinde hukuki konunun tek olduğu kabul edilmelidir.

Suçun konusu kapsamında değerlendirilen bir husus da zarar veya tehlike suçu ayrımıdır. Suçun işlenmesiyle suçun konusuna zarar verilebilir ya da suçun konusu tehlikeye atılabilir. Zarar suçu ancak neticeli suçlar açısından söz konusu olabilmektedir. Fiilin işlenmesi ile tamamlanan suçlarda zarar meydana gelmesi söz konusu olamaz ancak zarar meydana gelme tehlikesi bulunabilir. 5070 sayılı Elektronik İmza Kanunu m. 16 ve m. 17 ve Ek Madde 1/5 kapsamında düzenlenen suç tipleri herhangi bir netice öngörmediğinden zarar suçu değil tehlike suçu olarak nitelendirilebilirler.

**4. Mağdur**

Suçun mağduru suç konusunun ait olduğu kişidir.[103] Suçun konusuna yönelik tipik hukuka aykırı fiil ile korunan hukuki değer ihlal edilmektedir.[104] 5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suçlarla korunan hukuki değer elektronik imzanın doğruluğu ve elektronik imza ile oluşturulan verilerin güvenilirliğidir.

5070 sayılı Elektronik İmza Kanunu m. 16'da suçun konusu imza oluşturma verisi veya aracı; Ek Madde 1/5'te elektronik mühür oluşturma verisi veya aracı iken; aynı Kanun'un 17. maddesinde suçun konusu nitelikli elektronik sertifikadır. Dolayısıyla imza ve mühür oluşturma verisi veya aracı ile nitelikli elektronik imzaya veya elektronik mühre sahip olan ilgili kişi[105] suçun mağdurudur. Doktrinde bir görüşe göre suçun mağduru Devlettir.[106] Bir başka görüş ise, suçla korunan hukuki değerin elektronik imzanın ve verilerin güvenilirliği olması gerekçesiyle mağdurun kamu olduğu ifade edilmektedir. Bu görüşe katılmadığımızı ifade etmek isteriz. Kanun koyucu 5070 sayılı Kanun m. 16'da *"ilgili kişinin rızası dışında"* ve Ek Madde 1/5'te *"mühür sahibinin rızası veya talebi dışında"* ifadelerini kullanarak elektronik imza ve elektronik mühür oluşturma verisi veya aracının ilgili kişinin veya kurumun hakimiyetinde olduğunu ve bunlara yönelik yapılan hukuka aykırı hareketin suç oluşturacağını kabul etmiştir. Dolayısıyla burada rızayı vermeye yetkili elektronik imza veya mühür sahibi ilgilinin kişinin mağdur olduğunda tereddüt bulunmamaktadır. 5070 sayılı Kanun m. 17 açısından ise doğrudan böyle bir cevap vermek doğru değildir. Zira 5070 sayılı Kanun m. 16'da var olan imza oluşturma verisi veya

---

103 Özgenç, s. 223. Doktrinde mağdur, suç teşkil eden fiil ile ihlal edilen ve cezai korumanın konusunu oluşturan varlık ya da menfaatin sahibi olarak da tanımlanmaktadır. Katoğlu, Tuğrul, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2012, C. 61, S. 2, s. 662; Bahri Öztürk/Mustafa Ruhan Erdem, Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, Seçkin Yayıncılık, Ankara, 2020, s. 201.

104 Özgenç, s. 223.

105 Elektronik imza sahibi, 5070 sayılı Kanun m.3'e göre yalnızca gerçek kişiler olabilirken; Aynı Kanun Ek Madde ¼ kapsamında "elektronik mührü oluşturan kamu kurum ve kuruluşları, kamu idareleri, kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları, kamu ve özel hukuk tüzel kişileri ile yargı mercileri ve noterlikler" elektronik mühür sahibi olabilmektedir.

106 Orer, s. 162.

aracına yönelik bir suç işlenmekte iken; m. 17'de daha önce var olmayan bir sertifikanın oluşturulması da söz konusu olabildiğinden ikili bir ayrım yapılması daha doğrudur. Nitelikli elektronik sertifika güvenli bir elektronik imzanın unsurudur ve elektronik sertifika hizmet sağlayıcı tarafından elektronik imza talep edenin başvurusu üzerine münhasıran başvuranın kullanımına özgü oluşturulmaktadır. Dolayısıyla 5070 sayılı Kanun m. 17'de yer alan suçlar açısından bakıldığında, daha önce var olmayan bir elektronik sertifikanın oluşturulması halinde mağdurun kamu olduğundan bahsedilebilecekse de geçerli elektronik sertifikanın taklit veya tahrif edilmesi fiili halinde adına düzenlenmiş geçerli elektronik sertifikanın ilgilisi suçun mağduru olacaktır.[107] Aksi yönde yapılan yorum suç teorisi kapsamında yapılmış olan mağdur tanımı ile bağdaşmaz. Mağdurun, suç konusunun ait olduğu kişi olduğu ve 5070 sayılı Kanunda düzenlenen suçlarda da temelde suç konusunun ait olduğu bir elektronik imza veya elektronik mühür sahibinin bulunduğu kabul edilmelidir.

**5. Nitelikli Haller**

Elektronik İmza Kanunu m. 16, m. 17 ve Ek Madde 1/5 açısından failin vasfı gereği bir nitelikli hal söz konusudur. Zira ilgili suçların temel şekli herkes tarafından işlenebilirken nitelikli şekli ancak kanunda belirlenmiş özel faillik vasfını taşıyan kişilerce işlenebilmektedir.[108] İmza veya oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekarlık suçları da herkes tarafından işlenebilmekle beraber failin elektronik sertifika hizmet sağlayıcısı çalışanı olması halinde fail daha ağır bir ceza ile cezalandırılmaktadır.

**D. Suçların Manevi Unsuru**

5070 sayılı Elektronik İmza Kanunu kapsamında düzenlenen suç tipleri taksirli halleri düzenlenmediğinden ancak kast ile işlenebilmektedir. Bununla birlikte 5070 sayılı Kanun m. 16'da düzenlenen suç tipinin *"elektronik imza oluşturma amacıyla"* işlenmesi gerektiği ifade

---

107 Aynı yönde bkz. Başlar, s. 50. Elektronik İmza Kanunu m. 17'de düzenlenen suçun her zaman mağdurunun olmayacağı ifade edilmektedir. Karagülmez, s. 194. Mağduru olmayan bir suç olamayacağından bu görüşe iştirak etmiyoruz.

108 Özgenç, s. 228.

edilmektedir. Aynı şekilde Ek Madde 1/5'te yer alan suç tipinde de failin *"elektronik mühür oluşturma amacı"* ile hareket edilmesi beklenmektedir. Suçun kanuni tanımında yer alan ve failin taşıması gerektiği ifade edilen amaç suçun manevi unsuru açısından önem taşımaktadır. Zira failin kastının bu amaca yönelik olması yani failin özel bir kasta sahip olması gerekmektedir.[109] Doktrinde özel kast kavramı altında incelenen bu husus,[110] 5070 sayılı Kanun m. 16 ve Ek Madde 1'de yer alan suçların basit şekline ilişkindir. 5070 sayılı Kanun m. 17'de düzenlenmiş suç açısından tartışma yaratan hususlardan biri, "*elektronik sertifikaları bilerek kullanmak*" fiili için de özel kast aranıp aranmayacağıdır.[111] Kanun koyucu ilgili maddede elektronik sertifikanın sahte olduğunun bilinmesine rağmen kullanılmasını suç olarak düzenlemiştir. 5237 sayılı Türk Ceza Kanunu m. 21'de kastın unsurları "bilmek" ve "istemek" olarak belirtilmiştir. Dolayısıyla elektronik sertifikanın bilerek kullanılması açısından "bilmek" zaten kastın varlığı için şart olarak aranmaktadır. Failde suçun konusuna yönelik gerçekleştirilen fiilde bilme unsuru olmaksızın kasttan söz edilemeyecektir. Elektronik sertifikanın sahteliği bilinerek kullanılması halinde failin olası kastla hareket etmesinin mümkün olmadığı ifade edilmelidir.

**E. Suçların Hukuka Aykırılık Unsuru**

5070 sayılı Elektronik İmza Kanunu m. 16'da ifade edilen "ilgili kişinin rızası dışında" ifadesi gereğince, imza oluşturma verisi veya aracının ilgili kişinin rızası ile elde edilmesi, verilmesi, kopyalanması, araçların yeniden oluşturulması ve elektronik imza oluşturulması suç sayılmamaktadır. Aynı şekilde 5070 sayılı Kanun Ek Madde 1/5 kapsamında "ilgili mühür sahibinin rızası veya talebi dışında" yapılan tipik hareketlerle suç oluşacağından mühür sahibinin rızası veya talebi var ise suç oluşmamaktadır. Hukuka uygunluk nedenlerinden

---

109 Karagülmez, s. 190.

110 Kayıhan İçel, "Ceza Hukukunda Temel Kusurluluk Şekli "Kast"", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 2007, C. 6, S. 12, s. 66-67. 5237 sayılı Kanun sisteminde özel-genel kast ayrımının kaldırıldığı ve amacın kastın bir türü olmadığı ifade edilmektedir. Özgenç, s. 311. Bu amaç doğrultusunda hareket edilmesi yeterlidir; elektronik imzanın oluşturulması gerekmez. Karagülmez, s. 190.

111 Doktrinde "kullanmak" fiili için özel kast bulunması gerektiği görüşü için bkz. Karagülmez, s. 194.

ilgilinin rızası kapsamında değerlendirilen bu husus[112], 5237 sayılı Kanun m. 26/2'ye göre yorumlanmalıdır: *"Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez."* Buna göre, imza veya mühür oluşturma verisi veya aracına sahip ilgili kişinin rızası ile kişinin yaptığı fiiller hukuka uygun kabul edilmektedir. 5070 sayılı Kanun m. 16 kapsamında ilgili kişi, kural olarak aynı Kanun'un 3. maddesinde tanımlanan imza sahibi olarak kabul edilmekte ve *"Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişi"* olarak tanımlanmaktayken; Ek Madde 1 kapsamında elektronik mühür sahibi, *"elektronik mührü oluşturan kamu kurum ve kuruluşları, kamu idareleri, kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları, kamu ve özel hukuk tüzel kişileri ile yargı mercileri ve noterlikler"* olarak tarif edilmektedir.

İmza veya mühür sahibi, kullanım yetkisini bir başka kişiye belirli bir süre için vermiş ise bu durumda bu kişinin rıza vermeye yetkili olup olmadığı sorusu gündeme gelmektedir. Doktrinde bir defaya mahsus olmayacak şekilde kullanım hakkının imza sahibi tarafından başkasına verilmesi halinde kullanım hakkı olan kişinin üçüncü bir kişinin kullanımına rıza göstermesinin mümkün olduğu ifade edilmektedir.[113] Örneğin, A kişisi imza sahibi iken kullanım yetkisini bir defaya mahsus olmayacak şekilde B kişisine vermiş ise, B kişinin rızaen imza oluşturma verisini veya aracını C kişisine vermesinin hukuka uygunluk nedeni oluşturacağı belirtilmektedir. Kanaatimizce, kanun koyucunun 5070 sayılı Kanun m. 16'da "imza sahibi" yerine "ilgili kişi" ifadesini tercih etmesi nedeniyle doktrindeki görüş doğru kabul edilmelidir. Bununla beraber kanun koyucu neredeyse aynı düzenleme olan 16. maddeden ayrılarak 5070 sayılı Kanun Ek madde 1/5'te "ilgili mühür sahibi" şeklinde bir düzenleme yapmıştır. Dolayısıyla bu hüküm için ancak ilgili mühür sahibinin kullanım hakkını vermesi gerekir. Söz konusu hükümde *"ilgili mühür sahibinin … talebi"* özellikle yer aldığından mühür sahibinin rızası veya talebiyle kullanım hakkı

---

112 Rızanın tipikliğe ilişkin bir unsur olduğu ve bu sebeple rızanın tipikliği kaldıracağı hususunda detaylı bilgi için bkz. Muhammet Demirel, "Ceza Hukukunda Rızanın İki Boyutu: Tipikliğe Engel Olan Rıza ve Hukuka Uygunluk Nedeni Olan Rıza", *İstanbul Hukuk Mecmuası*, 2020, C. 78, S. 3, s. 1476.

113 Başlar, s. 59; Dülger, s. 573.

elde eden kişinin üçüncü kişinin kullanımına rıza göstermesi mümkün değildir. Söz konusu rızanın suçun işlenmesinden önce veya en geç suçun işlenmesi anında verilmesi gerekmektedir. Suç işlendikten sonra verilen rıza eylemi hukuka uygun hale getirmez. İlgilinin rızası haricinde 5070 sayılı Kanunda düzenlenen suçlar açısından değerlendirilmesi gereken bir hukuka uygunluk nedeni bulunmamaktadır. Ancak 5237 sayılı Kanun kapsamında yer alan hukuka uygunluk sebepleri olan özellikle hakkın kullanılması ve görevin ifası sebeplerinin somut olayın özelliklerine göre uygulanmasının mümkün olacağı durumlar ortaya çıkabilir. Doktrinde, özellikle 5371 sayılı Ceza Muhakemesi Kanunu kapsamında koruma tedbirleri söz konusu olduğunda kolluk görevlilerinin fiillerinin görevin yerine getirilmesi hukuka uygunluk sebepleri kapsamında mütalaa edilebileceği ifade edilmektedir.[114]

### F. Suçların Özel Görünüş Biçimleri

#### 1. Teşebbüs

5070 sayılı Elektronik İmza Kanunu kapsamında düzenlenen suçlar daha önce ifade edildiği üzere neticenin aranmadığı, fiilin gerçekleşmesi ile suçun tamamlandığı sırf hareket suçlarıdır. 5237 sayılı Türk Ceza Kanunu'na göre, kastedilen suçun icrasına elverişli hareketlerle başlanıp failin elinde olmayan nedenlerle tamamlanamaması halinde teşebbüs söz konusu olmaktadır. Suçun tamamlanamaması iki şekilde olabilir: İcra hareketlerinin tamamlanamaması veya suçun gerçekleşmesi için gerekli görülen neticenin gerçekleşememesi. 5070 sayılı Kanunda yer alan suçlar açısından suçun tamamlanması için neticenin gerçekleşmesi gerekmediğinden bu husus ilgili suçlar açısından tartışılamaz. İcra hareketlerinin tamamlanamaması bakımından ise, suç tipinde icra hareketlerinin bölünmesinin mümkün olduğu durumlarda teşebbüsten söz edilebileceği ifade edilmektedir.[115] Örneğin, bilişim sistemi üzerinden imza verilerinin kopyalanması esnasında bilgisayarın arıza vermesi nedeni ile kapanması veya elektronik sertifika oluşturulduğu sırada elektriklerin kesilmesi[116] nedeni ile icra hareketlerinin

---

114 Başlar, s. 59.

115 Aydın, Devrim, "Suça Teşebbüs", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2006, C. 55, S. 1, 109-110.

116 Özboyacı, s. 135.

tamamlanamaması durumlarında suç teşebbüs aşamasında kalmış sayılacaktır. Ancak bu durumda da failin hazırlık hareketlerini tamamlamış ve icra hareketlerine başlamış olmalıdır. Zira hazırlık hareketleri ilgili suçtan dolayı cezalandırılamaz.[117]

**2. İştirak**

5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suçlar açısından iştirak herhangi bir özellik arz etmemektedir. Dolayısıyla belirtilen suçlar bir kişi tarafından işlenebileceği gibi birden fazla kişinin katılımı ile de işlenebilir. 5237 sayılı Türk Ceza Kanunu m. 37 ve devamı hükümleri 5070 sayılı Kanunda düzenlenen suç tipleri açısından da uygulama alanı bulur.

**3. İçtima**

5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suç tipleri seçimlik hareketli suç tipleridir. Dolayısıyla ilgili suç tiplerinde yer alan fiillerin birinin veya tümünün gerçekleşmesi farklılık yaratmayacak; seçimlik hareketli suçun özellikleri dolayısıyla tek bir suçun varlığından söz edilecektir. Ancak 5070 sayılı Kanun m. 16, m. 17 ve Ek Madde 1'in ayrı suç düzenlemeleri oldukları unutulmamalıdır.

5070 sayılı Kanun m. 16'da düzenlenen imza oluşturma verilerinin izinsiz kullanımı; m. 17'de yer alan elektronik sertifikalarda sahtekarlık ve Ek Madde 1'de hüküm altına alınan elektronik mühür oluşturma verilerinin izinsiz kullanımı suçlarını oluşturan fiiller 5237 sayılı Türk Ceza Kanunu'nda yer alan bazı suç tiplerini de oluşturmaktadır. Örneğin, bilişim sistemi üzerinden imza oluşturma verilerinin elde edilmesi ve kullanılması yoluyla yarar elde edilmesi halinde 5237 sayılı Kanun m. 243'te düzenlenen "Bilişim Sistemine Girme", m. 244'te düzenlenen "Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu" ve m. 135'te düzenlenen "Kişisel Verileri Hukuku Aykırı Olarak Verme veya Ele Geçirme Suçu" da oluşmaktadır. Bunun yanı sıra, 5070 sayılı Kanun m. 16'da imza oluşturma ve Ek Madde 1'de yer alan mühür oluşturma verisinin veya aracının elde edilmesi halinde, 5237 sayılı Kanun m. 141 ve devamı hükümlerinde düzenlenen hırsız-

117 Özgenç, s. 501.

lık suçuna ilişkin tipik hareket de gerçekleşebilmektedir. Fakat burada hırsızlık suçunun yarar sağlama maksadının somut olayda olup olmadığına dikkat edilmesi gerekir. Aynı şekilde 5070 sayılı Kanun m. 17 hükmünde yer alan fiiller ile 5237 sayılı Kanun kapsamında yer alan belgede sahtecilik suçlarının oluştuğundan da bahsedilebilmektedir. Dolayısıyla tek fiil ile birden fazla farklı suç oluşmaktadır. Ancak 5070 sayılı Elektronik İmza Kanunu 5237 sayılı Türk Ceza Kanunu'na göre özel kanun olarak düzenlendiğinden özel kanun-genel kanun değerlendirmesi yapılması ve özel kanun olan 5070 sayılı Kanun hükümlerinin uygulanması gerekmektedir.[118]

### G. Suçlarda Soruşturma ve Kovuşturma ile Yaptırım

5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suçların takibi şikâyete bağlı değildir. Bu suçlar resen soruşturulur ve kovuşturulurlar. Bu nedenle söz konusu suçların işlendiğine yönelik basit şüphenin varlığı halinde, herhangi bir muhakeme koşulu olmaksızın Cumhuriyet savcısı derhal soruşturma başlatmak durumundadır. İlgili suçların ceza miktarları dikkate alındığında ilgili suçlarda davaya bakmakla görevli mahkeme asliye ceza mahkemeleridir.

İmza oluşturma verilerinin izinsiz kullanılması ve elektronik sertifikalarda sahtekarlık suçlarının yaptırımı 5070 sayılı Kanun'da hapis ve adli para cezası olarak öngörülmüştür. 5070 sayılı Kanun m. 16'da yer alan imza ve Ek Madde 1/5'te yer alan mühür oluşturma verilerinin izinsiz kullanılması durumunda fail, *"bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılır."* Elektronik sertifikalarda sahtekarlık suçunun işlenmesi halinde ise fail, *"iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır."* Üç suç tipi açısından da failin elektronik sertifika hizmet sağlayıcısı çalışanı olması halinde verilecek ceza yarısına kadar artırılır.

İmza veya mühür oluşturma verilerinin izinsiz kullanılması suçunun yaptırımı dikkate alındığında, 5271 sayılı Kanun m. 253/1-c hükmünde yer aldığı üzere suça sürüklenen çocuk bakımından uzlaştırmanın uygulanıp uygulanmayacağının tartışılması gerekmektedir.

---

118 Başlar, s. 61; Dülger, s. 574.

5271 sayılı Kanun m. 253/1-c'ye göre, "*Mağdurun veya suçtan zarar görenin gerçek veya özel hukuk tüzel kişisi olması koşuluyla, suça sürüklenen çocuklar bakımından ayrıca, üst sınırı üç yılı geçmeyen hapis veya adli para cezasını gerektiren suçlar*" uzlaştırma kapsamındadır. Bununla beraber aynı maddenin 2. fıkrasında "*Soruşturulması ve kovuşturulması şikâyete bağlı olanlar hariç olmak üzere; diğer kanunlarda yer alan suçlarla ilgili olarak uzlaştırma yoluna gidilebilmesi için, kanunda açık hüküm bulunması gerekir.*" düzenlemesi bulunmaktadır. 5070 sayılı Kanun'da yer alan imza oluşturma verilerinin izinsiz kullanımı suçu şikâyete tabi olmayan bir suç olarak düzenlenmiş; kanunda uzlaştırma ile alakalı bir hükme yer verilmemiştir. Dolayısıyla bu suç için uzlaştırma hükümleri uygulanamayacaktır.

5070 sayılı Kanunun 18. maddesinde ise idari para cezası verilmesi gereken haller düzenlenmiştir. Burada değinilmesi gereken husus, elektronik sertifika hizmet sağlayıcısı çalışanının kurumu adına yürüttüğü faaliyet sırasında hem örneğin, 5070 sayılı Kanun m. 12 kapsamındaki hükümlere aykırı hareket etmesi hem de m. 17 kapsamındaki suçu işlemesi halidir. Bir örnek üzerinden gitmek gerekirse, elektronik sertifika hizmet sağlayıcısı çalışanı olan A, B kişisinin elektronik sertifikada yer alan kişisel bilgilerini m. 12'ye aykırı olan bir suç işleme kararı kapsamında C'ye vermiş ve C de bu bilgileri kullanmak suretiyle elektronik sertifikayı taklit etmiş olsun. Bu durumda A ile C müşterek fail olarak 5070 sayılı Kanun m. 17'den dolayı sorumludur. Bununla birlikte elektronik sertifika hizmet sağlayıcı 5070 sayılı Kanun m. 18 kapsamında idari para cezası ile cezalandırılacaktır.

5070 sayılı Kanun m. 18 düzenlemesi, aynı Kanun m. 12 kapsamındaki hükümler açısından önemlidir. Zira m. 18 kapsamında idari para cezasını gerektirdiği öngörülen tüm haller için "elektronik sertifika hizmet sağlayıcısına" verilecek idari para cezasından bahsedilirken yalnızca m. 18/1-c hükmünde yer alan m. 12 kapsamındaki hükümlere aykırı davrananlara idari para cezası verileceğinden bahsedilmekte bu hükümde "elektronik sertifika hizmet sağlayıcısı" şeklinde bir ibare bulunmamaktadır. Halbuki diğer hükümlerde olduğu gibi 5070 sayılı Kanun m. 12'de de elektronik hizmet sağlayıcısının yükümlülüklerinden bahsedilmektedir. 5070 sayılı Kanun gerekçesinde de m. 18 hükmü için; "*Maddede, elektronik sertifika hizmet sağlayıcılarının Kanunla düzenlenen yükümlülüklerini yerine getirmemesi hâlinde Telekomüni-*

*kasyon Kurulu tarafından verilecek idarî nitelikli para cezalarının miktarı ve şartları tespit edilmiş"* olduğu ifade edilmektedir. Dolayısıyla m. 18/1-c hükmü sonucu verilecek para cezasının da elektronik sertifika hizmet sağlayıcısına verileceği kabul edilmelidir.

## III. SONUÇ

Elektronik imza, "*gerçeklik, orijinallik, güvenilirlik ve imza kaynağına itiraz edilemezlik*"[119] özellikleri nedeniyle günümüzde ıslak imzanın yerine kullanılır hale gelmiştir. Zaman ve kaynak kullanımından tasarruf başta olmak üzere güvenilirlik, denetlenebilirlik gibi avantajları nedeniyle tercih edilen elektronik imza ve elektronik mühür kullanımının yaygınlaşması da hukuki temellerinin daha sağlam oturtulması gerekliliğini ortaya çıkarmaktadır. 5070 sayılı Elektronik İmza Kanunu bu anlamda elektronik imza ve mührün çerçevesini çizmiş ve mevzuattaki diğer hükümlerle birlikte söz konusu elektronik veriler günlük hayata dahil edilmiştir.

Özellikle son 20 yılda hem kamu sektöründe hem özel sektörde elektronik imzanın oldukça yaygın kullanılması ile elektronik imzaya bağlı suç tipleri de öngörülmek durumunda kalmış ve özel kanuni düzenlemeler ile hukuka aykırı fiiller suç olarak kabul edilmiştir. 2004 yılında yürürlüğe giren 5070 sayılı Elektronik İmza Kanunu kapsamında düzenlenen suç tipleri ile gerçek kişilerin elektronik imza oluşturmak adına kullandıkları veriler ve elektronik sertifikanın güvenliği ve güvenilirliği koruma altına alınmıştır. Bununla beraber E-Devlet uygulamalarının yaygınlaşması ve elektronik verilerin her alanda sıklıkla kullanılması sonucu, yalnızca gerçek kişilerin kullanabildiği elektronik imzanın yanı sıra elektronik mühür ile alakalı yasal bir düzenlemeye de ihtiyaç duyulmuş ve 2021 tarihinde bu hususta bir hüküm 5070 sayılı Kanun'a dahil edilmiştir. 5070 sayılı Kanun Ek Madde 1'de yapılan düzenlemede elektronik mührün yasal sınırları belirlenmiş ve elektronik mühür oluşturma verisi ve aracının korunması amacıyla cezai hükümlere de yer verilmiştir.

5070 sayılı Elektronik İmza Kanunu İkinci Bölüm Üçüncü Kısmında cezai hükümler düzenlenmiştir. 5070 sayılı Kanun m. 16 ve m. 17'de

119 Keser Berber, s. 127.

hapis ve adli para cezası gerektirir iki adet suç tipi düzenlenmiş iken m. 18'de Kanun'da belirtilen maddelerde yer alan yükümlülüklere aykırılık halinde ortaya çıkacak idari para cezası ile ilgili düzenlemeler yapılmıştır. Aynı Kanun Ek Madde 1'in 5. fıkrası kapsamında ise elektronik mühür oluşturma verilerinin izinsiz kullanımı suçu yer almaktadır. Her iki suç tipinin koruduğu hukuki değer, elektronik imza sürecinin hukuki çerçevede ilerlemesini sağlamak adına elektronik imzanın, elektronik imza oluşturma araçlarının ve nitelikli elektronik sertifikaların doğruluğu ve bu sisteme olan güvenin korunmasıdır. İmza oluşturma verilerinin izinsiz kullanımında fail, elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde etmekte veya kopyalamakta ve bu araçları yeniden oluşturmak ile izinsiz elde edilen imza oluşturma araçlarını kullanmak suretiyle izinsiz elektronik imza oluşturmaktadır. Elektronik sertifikalarda sahtekarlık suçunda fail, tamamen veya kısmen sahte elektronik sertifika oluşturmakta veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etmekte veya bu elektronik sertifikaları bilerek kullanmaktadır. Bu suçlar sırf hareket suçu olarak düzenlenmiştir. 5070 sayılı Elektronik İmza Kanunu m. 16'da suçun konusu imza oluşturma verisi veya aracı; Ek Madde 1/5'te elektronik mühür oluşturma verisi veya aracı iken; aynı Kanun'un 17. maddesinde suçun konusu nitelikli elektronik sertifikadır. Dolayısıyla imza ve mühür oluşturma verisi veya aracı ile nitelikli elektronik imzaya veya elektronik mühre sahip olan ilgili kişi[120] suçun mağdurudur. Doktrinde bir görüşe göre suçun mağduru Devlettir[121]. İmza veya oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekarlık suçları da herkes tarafından işlenebilmekle beraber failin elektronik sertifika hizmet sağlayıcısı çalışanı olması halinde fail daha ağır bir ceza ile cezalandırılmaktadır. Sırf hareket suçu olarak düzenlenen bu suç tiplerinde teşebbüs tartışması yapılmayacak olup iştirak açısından da özel bir durum bulunmamaktadır. İçtima açısından özellikle

120 Elektronik imza sahibi, 5070 sayılı Kanun m.3'e göre yalnızca gerçek kişiler olabilirken; Aynı Kanun Ek Madde ¼ kapsamında "elektronik mührü oluşturan kamu kurum ve kuruluşları, kamu idareleri, kamu kurumu niteliğindeki meslek kuruluşları ve üst kuruluşları, kamu ve özel hukuk tüzel kişileri ile yargı mercileri ve noterlikler" elektronik mühür sahibi olabilmektedir.

121 Orer, s. 162.

TCK'da düzenlenen m. 243, 244 ve m. 135 suçlarının da oluşması ihtimali söz konusu olmaktadır. 5070 sayılı Elektronik İmza Kanunu'nda düzenlenen suçların takibi şikâyete bağlı değildir. Bu suçlar resen soruşturulur ve kovuşturulurlar.

Çalışmamız için taradığımız yargı kararlarında 5070 sayılı Kanun'da düzenlenen suç tipleri ile alakalı bir içtihada ulaşılamamıştır. Kamusal alanda veya özel sektörde güvenliğin ve caydırıcılığın sağlanabilmesi adına düzenlenen bu suç tipleri ile alakalı uygulamacıların teorik bilgisi de sınırlı kalmaktadır. Ancak günümüz toplumunda özellikle devlet işlerinin yürütülmesinde ve ticari alanda elektronik imzanın ve elektronik mührün güvenilirliğinin sağlanması oldukça önemlidir. Bu nedenle uygulamacıların, resen muhakeme edilen bu suç tipleri hakkında da bilgi sahibi olması gerekliliği kaçınılmaz görülmektedir.

## Kaynakça

### Kitaplar

Berber Keser Leyla, İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza, Yetkin Yayınları, Ankara, 2002.

Çakmakkaya Baki Yiğit, Türk Vergi Hukukunda Elektronik İmza Uygulamaları ve Adaptasyonu, Legal Yayıncılık, İstanbul, 2013.

Delta George B./Matsuura Jeffrey H, Law of The Internet- I, New York: Wolters Kluwer Law & Business, 2021.

Dülger Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, Ankara, 2020.

Erbayraktar Burcu, Güvenli Elektronik İmza, On İki Levha Yayıncılık, İstanbul, 2016.

Ertanhan Mesut, Kamu Görevlilerinin İmza, Paraf ve Elektronik İmzalarından Doğan Sorumlulukları, (Ankara: Seçkin Yayıncılık, 2018).

Karagülmez Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayıncılık, Ankara, 2005.

Koca Mahmut/Üzülmez İlhan, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara 2020.

Orer Gürsel, Elektronik İmza ve Elektronik Sertifika Hizmet Sağlayıcısının Hukuki ve Cezai Sorumluluğu, Adalet Yayınevi, Ankara, 2011.

Orta Mesut, Elektronik İmza ve Uygulaması, Seçkin Yayıncılık, Ankara, 2005.

Özbek Veli Özer/Doğan Koray/Bacaksız Pınar, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara, 2020.

Özgenç İzzet, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara, 2020.

Öztürk Bahri/Erdem Mustafa Ruhan, Uygulamalı Ceza Hukuku ve Güvenlik Tedbirleri Hukuku, Seçkin Yayıncılık, Ankara, 2020.

Sağıroğlu Şeref/Alkan Mustafa, Her Yönüyle Elektronik İmza, Grafiker Yayınları, Ankara, 2005.

Sağlam İpek, Elektronik Sözleşmeler, Legal Yayıncılık, İstanbul, 2007.

Sevimli K. Ahmet, "Elektronik Sözleşmeler ve ABD Elektronik İmza Yasası", Prof. Dr. Hayri Domaniç'e 80. Yaş Günü Armağanı Cilt II, Beta Yayınevi, İstanbul, 2001, s. 1023-1041.

Sözer Bülent, "Elektronik İmza Kanunu'na Göre Dijital İmza", Prof. Dr. Ergon A. Çetingil ve Prof. Dr. Rayegan Kender'e 50. Birlikte Çalışma Yılı Armağanı, Çizgi Basım Yayın, Ankara, 2007, s. 994-1030.

Tezcan Durmuş/Erdem Mustafa Ruhan /Önok R.Murat , Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara, 2020.

## Makaleler

Aalberts B. P. /Van Der Hof S "Digital Signature Blindness Analysis of Legislative Approaches to Electronic Authentication", *EDI Law Review*, C. 7, S. 1, 2000, 1-56.

Ahi Gökhan, "Hukuki Bakımdan Dijital (Sayısal) İmza", *Bilişim ve Hukuk Dergisi*, C. 8, 2008, 28-32.

Ahn Jaeso, "Analyzing and Evaluating the 2020 General Amendments to the Koran Digital Signature Act", *Journal of Korean Law*, 2021, C. 20, S. 2, 577-614.

Akın Gülfer, "Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/Dijital Belge", *Bilişim Hukuku Dergisi*, 2021, C. 3, S. 1, 76-138.

Aydın Devrim, "Suça Teşebbüs", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2006, C. 55, S. 1, 85-113.

Başlar Yusuf, "Elektronik İmza Kanunu'nda Düzenlenen Bilişim Suçları", *Uluslararası Antalya Üniversitesi Hukuk Fakültesi Dergisi*, 2016, C. 4, S. 7, 42-64.

Biçkin İnci, "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler", *TBB Dergisi*, 2006, S. 63, 109-126.

Blythe Stephen E, "Digital Signature Law of The United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security", *Richmond Journal of Law and Technology*, 2005, C. 11, S. 2, 1-20.

Bromby Michael, "Identification, Trust and Privacy: How Biometrics Can Ais Certification of Digital Signatures", *Interntional Review of Law, Computers & Technology*, 2010, C. 24, S. 1, 133-142.

Camcı Sinem, "İnternet Üzerinden Kurulan Sözleşmelerde Elektronik İmzanın Hukuki Niteliği", *Terazi Hukuk Dergisi*, 2020, S. 165, 1017-1029.

Çetin Emine Halman, "Elektronik Belgelerin Hâkim Tarafından Delil Olarak Değerlendirilmesi", *Terazi Hukuk Dergisi*, C. 54, 2011, 60-71.

Demirel Muhammet, "Ceza Hukukunda Rızanın İki Boyutu: Tipikliğe Engel Olan Rıza ve Hukuka Uygunluk Nedeni Olan Rıza", *İstanbul Hukuk Mecmuası*, 2020, C. 78, S. 3, s. 1476.

ENISA EUROPA: Security Guidelines on The Appropriate Use of Qualified Electronic Signatures, 2016, https://www.enisa.europa.eu/publications/security-guidelines-on-the-appropriate-use-of-qualified-electronic-signatures, E.T. 30.12.2020.

Erturgut, Mine. "Elektronik İmza Kanunu Bakımından E-belge ve E-imza", *Bankacılar Dergisi*, no. 48, (2003), 66-79.

Farah Nadim, "What's the Difference between Advanced and Qualified Signatures in eIDAS?", 2020, https://www.globalsign.com/en-in/blog/difference-between-eidas-advanced-and-qualified-electronic-signatures. E.T. 30.12.2020.

İçel Kayıhan, "Ceza Hukukunda Temel Kusurluluk Şekli "Kast"", *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 2007, C. 6, S. 12, 61-70.

Kalama M. Lui-Kwan, "Recent Developments in Digital Signature Legislation and Electronic Commerce", *Berkeley Technology Law Journal*, 1999, C. 14, S. 1, 463-482.

Katoğlu Tuğrul, "Ceza Hukukunda Suçun Mağduru Kavramının Sınırları", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 2012, C. 61, S. 2, 657-693.

Lentner Gabriel /Parycek, "Electronic Identity (eID) and Electronic Signature (eSig) for eGoverment Services – A Comparative Legal Study", *Transforming Goverment: People, Process and Policy*, 2010, C. 10, S. 1, 18-25.

Lim Yee Fen, "Digital Signatures, Certification Authorities: Certainty in The Allocation of Liability", *Singapore Journal of International & Comparative Law*, 2003, C. 7, S. 1, 183-200.

Öz Emine, "Elektronik İmza-Hukuki Boyutuyla" Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006.

Özboyacı Alper, "5070 sayılı Elektronik İmza Kanunu'nda Yer Alan Cezai Hükümler", *Terazi Hukuk Dergisi*, 2009, C. 4, S. 39, 127-136.

Rissnaes Rolf , "Digital Certificates and Certification Services", *Scandinavian Studies in Law*, 2004, C. 47, 131-154.

Sevim Tuğrul, Elektronik İmza Uygulamasında Kullanılan Zorunlu ve İhtiyari Dokümanlar", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Smedinghoff Thomas J, "Electronic Contracts and Digital Signatures: An Overview of Law and Legislation", *Journal of Equipment Lease Financing*, 1998, C. 16, S. 2, 2-17.

Smedinghoff Thomas J./Bro Ruth Hill, "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce", *John Marshall Journal of Information Technology & Privacy Law*, 1999, C. 17, S. 3, 724-768.

Smith Brian W. / Tufaro S Paul, "To Certify or Not To Certify The 0CC Opens the Door To Digital Signature Certification", *Ohio Northern University Law Review*, 1998, C. 24, S. 4, 813-830.

Şenocak Zarife, "Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, C. 50, S. 2, 97-135.

Topcan Ferda, "E-İmza Teknolojisi", TODAİE e-Devlet Merkezi Uygulamalı E-İmza Semineri, 2011, https://cdn2.beun.edu.tr/bidb/119ce0b4466f34d9159e2fe63b78bfd5/1eimzateknolojisi.pdf E.T. 31.12.2020.

Yardım Mehmet Ertan, "Elektronik İmza ve Elektronik İmzanın Medeni Usul Hukukumuza Etkileri", Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Yeşil Sezen /Alkan Mustafa/Acarer Tayfun, "E-İmza Uygulamalarında AB ve Türkiye'de Mevcut Durum ve Öneriler", Ulusal Elektronik İmza Sempozyumu Bildiriler Kitabı, ed. Mustafa Alkan/Şeref Sağıroğlu, CMS Yayınları, Ankara, 2006, 1-9.

Yıldırım Mustafa Fadıl, "Nitelikli Elektronik Sertifika Hizmet Sağlayıcısının Hukukî Sorumluluğu", *AÜEHFD*, 2004, C.8, S. 3-4, 257-283.

Yılmaz Mustafa, "Elektronik İmzalı Belgelerin Karşılaştırmalı Hukukta ve İdarî Yargılama Hukukunda Delil Niteliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi Özel Sayısı Cevdet Yavuz'a Armağan*, 2016, C. 22, S. 3, 3435-3486.

## İnternet Kaynakları

www.dergipark.org.tr

www.emarald.com

eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

www.govinfo.gov

www.heinonline.com

www.legislation.gov.uk

http://kamusm.gov.tr

https://sozluk.gov.tr/

www.tandfonline.com

www.turcademy.com