BİLİŞİM HUKUKU DERGİSİ

DIGITAL LAW REVIEW

Cilt: 3 Sayı: 1 | Vol. : 3 No: 1 | 2021

BİLİŞİM HUKUKU DERGİSİ

DIGITAL LAW REVIEW

Cilt: 3	**Sayı**: 1	**Haziran 2021**
Vol.: 3	Issue: 1	**June 2021**

ASBÜ Yayınevi

Ankara 2021

BİLİŞİM HUKUKU DERGİSİ

DIGITAL LAW REVIEW

e-ISSN: 2667-6109

Cilt: 3 **Sayı**: 1 **Vol**.: 3 **Issue**:1

Haziran 2021 **June 2021**

Dergi İletişim Bilgileri/Review Contact Information:
ASBÜ Hukuk Fakültesi Dekanlığı
Hükümet Meydanı No: 2, 06030 Ulus, Altındağ, ANKARA
Tel: +90 312 596 44 44–45 **Fax**: +90 312 311 86 00

E-mail: bilisimhukukudergisi@asbu.edu.tr
https://dergipark.org.tr/bilisimhukukudergisi

Bilişim Hukuku Dergisi Asos İndeks kapsamında taranmaktadır. 06.05.2021 tarihi itibarıyla iki yıllık TR Dizin izleme sürecine alınmıştır.
Digital Law Review is listed in Asos Index. As of 06.05.2021, the journal has been admitted into a two-year monitoring phase by TR Dizin.

Yayına Hazırlayan
Mizanpaj: ASBÜ Yayınevi
Kapak Tasarımı: Basın Yayın Daire Başkanlığı
Hükümet Meydanı No: 2, 06030 Ulus, Altındağ, ANKARA
Tel: +90 312 596 44 46 Fax: +90 312 311 86 00
E-mail: asbu.library@asbu.edu.tr

Baskı: Dijital Yayın

Sertifika No: 33365

Tel: 596 46 12

Doç. Dr. Barış ERMAN	Yeditepe Üniversitesi Hukuk Fakültesi
Doç. Dr. Erdal YERDELEN	Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi
Doç. Dr. Gülsün Ayhan AYGÖRMEZ UĞURLUBAY	İstanbul Gedik Üniversitesi Hukuk Fakültesi
Doç. Dr. Armağan Ebru BOZKURT YÜKSEL	Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi
Doç. Dr. Hasan SINAR	Altınbaş Üniversitesi Hukuk Fakültesi
Dr. Öğr. Üyesi Erman BENLİ	Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi
Dr. Öğr. Üyesi Fatih KAPLANHAN	İstanbul Sabahattin Zaim Üniversitesi İşletme ve Yönetim Bilimleri Fakültesi
Dr. Öğr. Üyesi Mehmet Bedii KAYA	İstanbul Bilgi Üniversitesi Hukuk Fakültesi
Dr. Ahmet KILIÇ	Bilgi Teknolojileri ve İletişim Kurumu
Dr. Mustafa KÜÇÜKALİ	Bilgi Teknolojileri ve İletişim Kurum

YAZIM KURALLARI

Başlangıç

1. Makale başlığı: Amerigo Md BT, 15 pt., Tüm harfler büyük, Kalın, Ortalanmış.
2. Yazar adı: Amerigo Md BT, 13 pt., Kalın, Sağa yaslı, İlk harfler büyük, yıldız ile dipnotta yazarın mesleği.
3. Öz, Abstract ve Anahtar Kelimeler: Kalın, İlk harfler büyük.

Metin

1. Metin içi başlıklar: Amerigo Md BT, 12 pt.
2. Başlık başındaki işaretler için yeni liste stili tanımlanması (Word'de Giriş sekmesinde paragraf kutucuğunun içinde üst sıradaki liste işareti/numaralandırma işaretlerinden çok düzeyli liste başlığı altında yeni liste stili tanımla daha sonra sol alttan biçimden numaralandırma seçeneği seçilecek) sıralaması:
    1. **Seviye:** Numaralandırma stili: I, II, III... Kalın, Tümü büyük harfler
    2. **Seviye:** Numaralandırma stili: A, B, C... Kalın, İlk harfler büyük
    3. **Seviye:** Numaralandırma stili: 1, 2, 3... Kalın, İlk harfler büyük
    4. **Seviye:** Numaralandırma stili: a, b, c... Kalın, İlk harfler büyük
    5. **Seviye:** Numaralandırma stili: i, ii, iii... Normal, İlk harfler büyük, İtalik.
3. Ana metin: Palatino Linotype, 11 pt.
4. Metin paragrafları: İlk satır 0,75 cm içeride, her iki tarafa yaslanmış, sağ ve sol girinti 0, paragraf öncesi 5nk paragraf sonrası 0 nk aralık, satır aralığı 1.

Dipnotlar

1. Dipnot: Palatino Linotype, 9 pt.
2. Dipnot paragrafları: Asılı 0,5 cm içeride, her iki tarafa yaslanmış, sağ ve sol girinti 0, paragraf öncesi 2 nk paragraf sonrası 0 nk aralık, Aynı stildeki paragraflar arasına boşluk ekleme seçeneği seçilmemiş, satır aralığı 1. Ancak aynı dipnotta birden çok paragraf verilecekse bu durumda söz konusu iki paragraf arasında aralık 0 olmalıdır (üstteki paragrafın paragraf ayarlarından "sonra" kısmı 0 nk, alttaki paragrafın ise "önce" kısmı 0 nk yapılmalıdır).
3. Dipnottaki cümle ile dipnotta sol baştaki numara arasında 1 boşluk bırakılmalıdır.
4. Dipnotta sonu nokta ile biten bir ifade varsa tekrar nokta konulmasına gerek yoktur, bunun haricinde herhangi bir işaretten sonra mutlaka nokta konulmalıdır.
5. Metin içerisinde gösterilen dipnot numaraları şayet bir noktalama işareti varsa onun hemen ardından boşluk bırakılmaksızın belirtilecektir.

Yanlış: verilecektir[1]. **Doğru:** verilecektir.[1]

Kaynakça

1. Kaynakça ayrı sayfada başlayacaktır.
2. Alfabetik sıralı, Palatino Linotype, 11 pt.
3. Kaynakça paragrafları: 0,75 cm asılı (ilk satırdan sonraki satırlar 0,75 cm içeride), her iki tarafa yaslanmış, sağ ve sol girinti 0, paragraf öncesi aralık 3 nk paragraf sonrası aralık 0 nk, Aynı stildeki paragraflar arasına boşluk ekleme seçeneği seçilmemiş, satır aralığı 1.
   Yazım şekline ilişkin kurallara uygun olarak hazırlanmış örnek word formu için bkz. http://dergipark.org.tr/download/journal-file/14917

Yazım-İmla Kuralları ve Atıf Usulü

1. Derginin yazım ve imla kurallarında Türk Dil Kurumunun yayınları ve kararları esas alınmaktadır.
2. Dipnot ve kaynakçalarda "The Chicago Manual of Style" atıf sistemi benimsenmiştir. Atıf sistemine ilişkin detaylı bilgi için bkz.
   https://librarybestbets.fairfield.edu/citationguides/chicagonotes-bibliography#BookwithTwoorThreeAuthors
   https://www.chicagomanualofstyle.org/book/ed17/frontmatter/toc.html

3. Eserin yayın dilinin Türkçe olması halinde atıf yapılırken;

   ◊ "and" yerine "ve"
   ◊ "unpublished" yerine "yayımlanmamış" veya "yayınlanmamış"
   ◊ "Anonymous" yerine "Anonim"
   ◊ birden fazla ciltten oluşan eserlerde "volume/vol." yerine "Cilt."
   ◊ "see" yerine "bkz."
   ◊ "in" yerine "iç."
   ◊ "accessed" yerine "erişim tarihi"
   ◊ "trans." yerine "çev."
   ◊ "edited by" yerine "editör"
   ◊ "translated by" yerine "çeviren"
   ◊ "interview by" ifadesi yerine "röportajı yapan"
   ◊ "PhD diss." yerine "doktora tezi"
   ◊ "thesis" yerine "tez"
   ◊ "last modified" yerine "son değiştirilme"
   ◊ "filmed" yerine "çekim" ifadeleri kullanılmalıdır.
   ◊ Tarih belirtirken kullanılan ay isimleri Türkçeleştirilmiştir ancak yazım formatı korunmuştur. Örneğin; Mayıs 8, 2019 şeklinde yazılmalıdır.
   ◊ Dergi sayısını ifade eden "no." ifadesi korunmuştur. Keza "ed." ifadesi aynen korunmuştur.
   ◊ Sayfa numarasında "vd." kullanılmamalıdır. Bunun yerine ilgili numara ile arasına boşluk konulmaksızın "ff." İfadesi konulmalıdır. Eğer "ff."dan sonra "." gelecekse kullanılmaz ancak ";", "?" vb. gelecekse onlar "ff."deki noktaya bitişik yazılır.

◊ Metin içerisinde dipnotta gösterilen mevzuat veya mahkeme kararı kaynakçada gösterilmeyecektir. Yargı kararlarına yapılan atıflarda aşağıdaki kural ve kısaltmalar dikkate alınmalıdır:
◊ Mahkemenin/kurumun adı varsa dairesi, E. esas numarası K. karar numarası tarih [gün.ay.yıl formatında], (kararın ulaşıldığı kaynak, varsa ulaşıldığı kaynaktaki sayfa numarası veya URL veya DOI numarası).
◊ Yabancı kararlarda ilgili mahkemenin veya kurumun kendisinin benimsemiş olduğu karar atıf usulü kullanılabilir. Tercih edilirse Türk kararları için kullanılan sistem de uygun düştüğü ölçüde uygulanabilir. Ancak, bir eserde aynı mahkemenin veya kurumun bir kararı için hangi sistematik kullanılmışsa diğer kararlarında aynı sistematiğin kullanılması gerekir.

Anayasa Mahkemesi	AYM
Bireysel Başvuru	BB
Bölge Adliye Mahkemesi	BAM
Ceza Dairesi	CD
Ceza Genel Kurulu	CGK
Daire	D
Danıştay	Dan.
Esas	E.
Hukuk Bölümü	HukukB
Hukuk Dairesi	HD
Hukuk Genel Kurulu	HGK
İçtihadı Birleştirme Kurulu	İBK
İçtihatları Birleştirme Büyük Genel Kurulu	İBK
İdari Dava Daireleri Kurulu Kararı	İDDK
Karar	K.
Uyuşmazlık Mahkemesi	UM
Vergi Dava Daireleri Kurulu Kararı	VDDK
Yargıtay	Yar.

Örnekler:

AYM, E.2017/172, K.2018/32, 28.03.2018.

Yar. 1. HD, E.2015/1456, K.2017/7086, 05.12.2017, (Kazancı İçtihat ve Bilgi Bankası).

Ankara BAM 2. HD, E.2016/113, K.2017/21, 23.01.2017, (https://legalbank.net/belge/ankara-bolge-adliye-mahkemesi-2-hd-e-2016-113-k-2017-21-t-23-01-2017-bosanmadan-kaynaklanan-tazminat/3040600).

Rekabet Kurulu, K.19-12/136-60, 13.3.2019, (https://www.rekabet.gov.tr/Karar?kararId=c4268558-edce-48b5-996d-152defb6a7e4).

5. Resmi Gazeteye yapılacak atıflar şu şekilde belirtilmelidir: RG. 02.01.2019, S. 30643.

WRITING FORMAT

Beginning

1. Title of the works: Amerigo Md BT, 15 pt., bold and capital letter, centered paragraph style.
2. Names(s) of author(s): Amerigo Md BT, 13 pt., bold, first letter capital, right justified. job of author(s) shall be written with an actinoid footnote.
3. bstract and Keywords: Bold and first letter capital

Text

1. Titles in the text: Amerigo Md BT, 12 pt.
2. Authors should arrange the text utmost with five-degree heading and the number of the titles has a style as follows:
   First level: Numbering style: I, II, III... Title: bold and capital letter.
   Second level: Numbering style: A, B, C... Title: bold and first letter capital.
   Third level: Numbering style: 1, 2, 3... Title: bold and first letter capital.
   Fourth level: Numbering style: a, b, c... Title: bold and first letter capital.
   Fifth level: Numbering style: i, ii, iii... Title: italic and first letter capital.
3. Main text: Palatino Linotype, 11 pt.
4. Paragraphs: 0,75 cm first line indent, justified alignment, left/right indent: 0 cm, pre/post-paragraph spacing: 5/0 nk, 1 line spacing

Footnotes

1. Style: Palatino Linotype, 9 pt.
2. Footnotes paragraphs: 0,5 cm hanging indentation, justified alignment, left/right indent: 0 cm, pre/post-paragraph spacing: 2/0 nk, 1 line spacing. The box for adding space to same styled paragraphs should not be filled. If there are more than one paragraph in a footnote, pre/post-paragraph space should be 0 nk in this footnote.
3. Between the footnote number and footnote text one character space should be left.
4. All footnotes should be completed with a dot.
5. Footnotes numbers should be demonstrated after punctuations.

Wrong: given[1]. **Right:** given.[1]

Bibliography

1. Bibliography should start on a separate page.
2. Style: alphabetically ordered, Palatino Linotype, 11 pt.
3. Bibliography paragraphs: 0,75 cm hanging indentation, justified alignment, left/right indent: 0 cm, pre/post-paragraph spacing: 3/0 nk, 1 line spacing. The box for adding space to same styled paragraphs should not be filled.

For the sample word form edited per the writing form rules of the Journal, please see http://dergipark.org.tr/download/journal-file/14917

Spelling and Footnotes

1. The works should be prepared per official spelling and orthographic rules.
2. "The Chicago Manual of Style" is accepted for footnotes and bibliography. For further information please see
   https://librarybestbets.fairfield.edu/citationguides/chicagonotes-bibliography#BookwithTwoorThreeAuthors
   https://www.chicagomanualofstyle.org/book/ed17/frontmatter/toc.html

İÇİNDEKİLER

CONTENTS

KRİTİK ALTYAPILARA YÖNELİK BİLİŞİM SUÇLARI, TÜRKİYE VE AB UYGULAMALARI

Cyber Crimes Against Critical Infrastructures, Turkey and EU Practices

Muhammet KARACA[*], **Ensar GÜL**[**]

Öz

Kritik altyapılar, işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılardır. Teknolojik gelişmeler birçok bakımdan büyük kolaylıklar sağlasa da çeşitli güvenlik sorunlarını da beraberinde getirmektedir. Siber uzayda işlenen suçların gün geçtikçe artması, devletlerin bu alanda güvenlik önlemlerini artırması gerektiğini ortaya koymaktadır. Türk Ceza Kanunu'nda, Avrupa Siber Suçlar Sözleşmesi'nde bu alanda farklı uygulamalar dikkat çekmektedir. Bu makalede, kritik altyapılara yönelik siber saldırılar incelenmiştir. Bu saldırılara

[*] Savunma İş Geliştirme Sorumlusu, TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, muhammet.karaca@tubitak.gov.tr, ORCID: 0000-0003-2948-8727.

[**] Profesör Doktor, Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi, Yazılım Mühendisliği Bölümü, ensargul@maltepe.edu.tr, ORCID: 0000-0001-8753-6075.

Makale Gönderim Tarihi/Received: 18.05.2020.

Makale Kabul Tarihi/Accepted: 08.05.2021.

Atıf/Citation: Karaca, Muhammet, ve Gül, Ensar. "Kritik Altyapılara Yönelik Bilişim Suçları, Türkiye ve AB Uygulamaları." *Bilişim Hukuku Dergisi* 3, no: 1 (2021): 1-30.

karşı yapılan çalışmalardan ve alınan tedbirlerden bahsedilerek gerekli önerilerde bulunulmuş ve sonuçlar değerlendirilmiştir.

Anahtar Kelimeler: Kritik Altyapılar, Bilişim Güvenliği, Siber Suçlar, İnternet Hukuku, Avrupa Siber Suçlar Sözleşmesi.

Abstract

Critical infrastructures describe the physical and cyber systems which cause loss of lives, large scaled-economical damage, national security flaw or public order breakdown when their info/data confidentiality, integrity or accessibility is compromised. Although technological advances provide great convenience in many ways, they also bring various security problems. The increasing number of crimes committed in cyberspace reveal that goverments need to increase their security measures in this field. The Turkish Criminal Law, European Cyber-Crimes Contract have different laws and practices in this field. In this article cyber attacks on critical infrastructures and the measures taken against these attacks are discussed.

Keywords: Critical infrastructures, Information Security, Cyber Crimes, Internet Law, European Cyber-Crimes Contract.

GİRİŞ

Kritik altyapı, ülkeden ülkeye ve ülke birliklerine göre farklı farklı şekillerde tanımlanabilmektedir. Türkiye için kritik altyapı, işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar olarak ifade edilmektedir.[1]

[1] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi*, (Ankara: T.C. UDHB, 2016), 8, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf.

Bilişim sistemlerinin gün geçtikçe gelişmesi ve değişmesi, farklı şekillerde işlenen bilişim suç fiillerinin de artmasına neden olmaktadır. Her ne kadar teknoloji büyük bir kolaylık sunsa da hukuka aykırı olarak bu teknolojinin kullanıldığına ve siber saldırıların artarak devam ettiğine her geçen gün şahit olunmaktadır. Bu konuya hem Türk Ceza Kanunu'nda hem de Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi'nde önemli bir yer ayrılmıştır.[2]

765 sayılı Mülga Türk Ceza Kanunu'nda, bilişim suçlarına yönelik hükümler oldukça kısıtlıyken, 5237 sayılı yeni yasanın yürürlüğe girmesi ile daha geniş çaplı hükümlere yer verilmiştir. 5237 sayılı yasanın 243-246. maddelerinde bilişim alanında işlenecek suçlarla ilgili yeni düzenlemeler yapılmıştır. Bu bağlamda hem bilişim sistemleri ile işlenen suçlar hem de bilişim sistemlerine karşı işlenen suçlar, TCK'nın ilgili maddelerinde yerini almıştır.

Avrupa Konseyi Siber Suçlar Sözleşmesi de küreselleşmenin kaçınılmaz bir sonucu olan bilişim suçlarının küreselleşmesi sorununa bir çözüm üretilebilmesi için ortaya konmuş, birçok ülke tarafından kabul gören ve imzalanan bir sözleşme olmuştur. Bugün bu sözleşme kapsamında birçok bilişim suçu ile ilgili hükme yer verilmektedir.

Gelişen teknoloji hem birey bazında hem de kurumlar bazında olumlu ve olumsuz etkiler barındırmaktadır. Teknolojinin ilerlemesi, zaman, maliyet ve kalite konusunda büyük avantajlar sağlarken, yeni saldırı tiplerini de beraberinde getirmektedir. Bu saldırılar artık doğrudan fiziki bir saldırı olmaktan çıkmış, dolaylı yollardan bilişim sistemleri kullanılarak ve fark edilmesi imkânsız ya da uzun zaman alan bir saldırı tipine dönüşmüştür.

---

[2] Ebru Altunok ve Ali Fatih Vural, "Bilişim Suçları," *Denetişim,* no. 8 (2016): 76.

Bu makale dört bölümden oluşmaktadır. İlk bölümde, kritik altyapılara yönelik gerçekleştirilen bilişim suçları ve şekilleri ele alınmış ve kritik altyapıların tanımı yapılarak ve yapılara yönelik siber saldırı örnekleri verilerek durum analizi yapılmıştır. İkinci bölümde konu ile ilgili yayımlanmış eserlerden bahsedilmiştir. Üçüncü bölümde kritik altyapılarla ilgili ülkemizde ve Avrupa Birliği'nde yapılan çalışmalar incelenmiş, bu alanlarda yapılan siber saldırılarla ilgili yasal ve kurumsal düzenlemelere yer verilmiştir. Dördüncü bölümde kritik altyapılara yönelik siber saldırı istatistikleri verilmiş ve değerlendirmeler yapılmıştır. Son bölüme gelindiğinde çalışmamız ile ilgili sonuç ve değerlendirmeler yapılacaktır.

I. KRİTİK ALTYAPILAR VE KRİTİK ALTYAPILARA YÖNELİK SİBER SALDIRILAR

Teknolojinin gelişimi ve farklılığı, kritik altyapı sayılan sektörlerin de çeşitliliğini artırmıştır. Bu çeşitlilikle siber saldırılar artarak yükselmiş ve sektörlere göre çeşitlilik göstermiştir. Öyle ki bu saldırıların sayısı yıllık bazda milyonların üzerine çıkmıştır.

Kritik altyapılara yönelik siber saldırılar ulusal güvenliği tehlikeye atmaktadır.[3] Önce hangi altyapıların kritik altyapı olarak tanımlandığına bakmamız faydalı olacaktır.

A. Kritik Altyapı Sistemleri

Ülkelerin gelişmişlik oranı, değer kavramları ve teknolojik donanımlarına göre kritik altyapı olarak nitelendirilen sistemleri

[3] Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective*, no. 18 (2009): 1.

farklılaşmaktadır. Türkiye[4], AB[5] ve ABD[6] için belirlenen kritik altyapı sistemleri tablo şeklinde sunulmuştur:

Tablo 1: Türkiye, AB ve ABD' ye Göre Kritik Altyapılar

TÜRKİYE	AB	ABD
Enerji	Su ve Gıda	Ticari Tesisler
Su Yönetimi	Nakliye ve Ulaşım	Kimya Sektörü
Kritik Kamu Hizmetleri	Sağlık ve Finans	Kritik İmalat Sektörü
Ulaştırma	Kamu Düzeni ve Emniyet	İletişim Sektörü
Bankacılık ve Finans	Nükleer ve Kimyasal	Savunma Sanayi Baz Sektörü
Elektronik Haberleşme	Uzay ve Araştırmalar	Acil Servis Sektörü
	Bilgi ve İletişim Sektörü	Barajlar
		Enerji Sektörü
		Devlet Tesisleri
		Sağlık ve Halk Sağlığı
		Su ve Atık Su Sistemleri
		Bilgi Teknolojileri
		Ulaştırma Sektörü
		Nükleer Reaktörler, Malzemeler ve Atık Sektörü

Kritik altyapı sektörlerine ilişkin Tablo 1'e bakıldığında ABD'nin devlet endeksli ve ekonomik güvenliğe yönelik bir belirleme içinde olduğu görülmektedir. Kritik altyapı niteliğindeki işletmelerin birçoğunun özel şirketler tarafından yürütüldüğü ABD'de, devletin amaçlarından biri de bu şirketler arasında en yüksek seviyede iş birliğini sağlamaktır. Olası bir saldırıda ya da saldırı öncesinde bu şirketler arasında

4 T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. *2016-2019 Ulusal Siber Güvenlik Stratejisi*, 8.

5 "European Programme for Critical Infrastructure Protection-Summaries of EU Legislation", EUR-Lex, erişim tarihi: Aralık 26, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33260&from=EN.

6 The White House, "Presidential Policy Directive," erişim tarihi: Aralık 2, 2018, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience.

koordinasyon sağlanması ve bilgi paylaşımı yapılması hedeflenmektedir.

AB açısından kritik altyapılar, ABD'nin aksine, sadece güvenlik ya da savunmaya yönelik altyapılar değildir. Kritik altyapıların belirlenmesinde daha sivil bir anlayışın olduğu söylenebilecektir. AB, bu kapsamda siber alanda teşvikler sunmakta ve tedbirlerin alınmasını kolaylaştırıcı önlemler almaktadır.

Türkiye'deki kritik altyapı sistemleri ise ekonomik ve kamu güvenliği endeksli belirlenmiştir. Ülkemizde bu alanın tanımlanması ABD ve AB'ye göre çok daha yeni olduğu için belirlenen sektörlerin çeşitliliği de değişmektedir. Örneğin, bilişim alanının kritikliği ülkemiz açısından sonraki yıllarda ortaya çıkan bir durum olmuştur. Ülkemizde, son dönemlerde gerek siber alan gerekse kritik altyapılara ilişkin çalışmalara hız verilmiş ve yeni birtakım düzenlemelerin yapılmasına başlanmıştır.

Türkiye'nin, kritik altyapı sistemi olarak tanımladığı alanları genişletmesi gerektiği Tablo 1'den anlaşılmaktadır. Teknolojinin hızlı gelişimi ve yaygın kullanımından dolayı Bilgi Teknolojilerini, Türkiye Uzay Ajansının kurulmasının akabinde Uzay Araştırmalarını ve Sinop ile Mersin'de yapılmakta olan nükleer santrallerden dolayı Nükleer Reaktörleri kritik altyapı sistemlerine dahil etmesi gerekmektedir.

B. Kritik Altyapılara Yapılan Siber Saldırı Vakaları

Teknolojik donanımları bünyesinde ağırlıklı olarak barındıran kritik altyapı sistemleri aynı zamanda üzerinde büyük bir risk taşımaktadır. Gerek ülkeler arasındaki rekabetler gerek düşmanlık duyguları gerekse kişisel menfaatler bu sistemlere saldırıları ön plana çıkarmıştır.

Kritik altyapı sistemlerini hedef alarak yapılan siber saldırılara örnek vermek gerekirse; 2000 yılında Avustralya'da, atık kontrol sistemine izinsiz erişen eski bir çalışan, birçok atık istasyonunun komutasını ele geçirerek bir milyon litrelik bir

atığın nehir ve deniz sularına karışmasına sebebiyet vermiştir.[7] Yine 2016 yılında Türkiye, tarihindeki en kapsamlı siber saldırıya maruz kalmıştır. Gerek internet trafiğini gerekse de ".tr" alan adlarını hedef alan bir DDOS (*distributed denial of service attack*) saldırısı gerçekleşmiştir. 2015 yılında Black Energy 3 adlı kötü amaçlı yazılım Ukrayna elektrik sistemini saatlerce devre dışı bırakmıştır. Bu saldırılara benzer birçok örnekler bulunmaktadır.

İnternete bağlı olmayan altyapılara bile siber saldırı yapmak mümkündür. Bu saldırılara örnek olarak 2010 yılında İran nükleer enerji altyapısını hedef alan bir siber saldırıyı gösterebiliriz. Daha sonra bu zararlı yazılımın adı *Stuxnet* olarak açıklanmıştır. Öyle ki bu saldırıda kullanılan zararlı yazılımlar sadece bu saldırı yapmak için geliştirilmiştir ve İran ciddi manada zarar görmüştür.[8]

Kritik altyapıların güvenliği için önlemler alınsa da bu tek başına yeterli olmamaktadır. Teknoloji hızlı bir gelişim içerisinde olduğundan aynı hızla saldırı çeşitleri de çoğalmaktadır. Bundan dolayı devletler ve şirketler bu önlemleri güncel tutmak zorundadırlar. Güncel durumun teyidi ve gerekli önlemlerin ne ölçüde olduğunu görebilmek için kurum ya da şirketler sızma testleri yaptırmaktadır. Bu testler, ihtiyaca göre

---

[7] Kevin Curran, Kevin Concannon ve Sean McKeever, "Cyber Terrorism Attacks," iç. *Cyber Warfare and Cyber Terrorism*, ed. Lech J. Janczewski ve Andrew M. Colarik, (Hershey, PA: IGI Global, 2008): 2, http://doi:10.4018/978-1-59140-991-5.ch001.

[8] Dünyada kritik altyapılara karşı yapılan çeşitli siber saldırılar hakkında bkz. Mutsuo Noguchı ve Hirofumi Ueda, "An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures," *NEC Technical Journal* 12, no. 2 (2017), erişim tarihi: Kasım 16, 2020, https://www.nec.com/en/global/techrep/journal/g17/n02/pdf/170204.pdf.; Ana Kovacevic ve Dragana Nikolic, "Cyber Attacks on Critical Infrastructure: Review and Challenges," iç. *Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance*, ed. Maria Manuela Cruz-Cunha ve Irene Maria Portela, (Hershey, PA: IGI Global, 2015): 6, http://doi:10.4018/978-1-4666-6324-4.ch001.

açık sızma testi ya da kapalı sızma testi olarak yapılmaktadır. Açık sızma testi yapılırken testi yapan firmaya şirketle ilgili maksimum oranda bilgi verilmektedir. Kapalı sızma testinde ise testi yapacak firmaya şirketle ilgili hiçbir bilgi verilmeden test yaptırılmaktadır. Bu testler sonucunda şirketin içeriden ya da dışarıdan gelebilecek saldırılara karşı hangi konumda olduğu belirlenmekte ve eksiklikler giderilmeye çalışılmaktadır.

II. İLGİLİ ÇALIŞMALAR

Aydın, bilişim suçları ile ilgili hukuki düzenleme yapılmadan önce bu konuya dikkat çekmiş ve bilişim suçlarının toplum düzenine aykırı davranışlar olarak kabul edildiğini, fakat yasaların ihlal edilmesi olarak tanımlanmadığını belirtmiştir.[9] Erdoğan tarafından adli bilişimin bir bilim dalı olarak kabul edilmesi ve adli tıp benzeri bir yapılanma kurulması önerilmiştir.[10] Böylece nesnelerin de internete bağlanmasıyla çok daha büyüyecek olan bilgisayar ağlarına yönelik saldırılar ve işlenecek suçların tespiti yapılabilecektir. Özsoy Yargıtay kararları ışığında doğrudan bilişim suçlarını incelemiş, TCK 243. ve 244. maddeleri üzerine yorumlar yapmıştır.[11] Bilişim suçlarına yönelik Yargıtay kararlarının incelenmesi neticesinde yerel mahkemelerin suçun vasfını belirlemek konusunda zorluk yaşadığı görülmüştür.[12] Bilişim suçlarının hızla yöntem değiştirdiği ve kanuni düzenlemelerin

---

9 Emin Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenirlilik Mahremiyet ve Bilişim Suçları," *Marmara İletişim Dergisi* 1, no. 1 (1992): 113.

10 Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 12, (2010): 1427.

11 Nevzat Özsoy, "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları," *Yaşar Hukuk Dergisi* 1, no. 2 (2019): 296.

12 Metin Turan ve Özgür Külcü, "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi," *Türk Kütüphaneciliği* 28, no. 1 (2014): 19.

buna ayak uyduramadığı öne sürülmüştür.[13] Apiş, Bilişim Sistemlerine Girme Suçunu karşılaştırmalı hukuk açısından incelemiştir.[14] Erdağ, bu maddeler ile Alman Ceza Kanunu'nun ilgili düzenlemelerini incelemiş, Alman Ceza Kanunu'nda bilişim suçlarının Türk mevzuatında olduğu gibi ayrı bir başlıkta düzenlenmediği belirtmiştir.[15]

Kritik altyapılara yönelik Türkçe yayın sayısı yok denecek kadar azdır. Ak, iç güvenlik yönetimi açısından kritik yapıların korunmasına dair yeni bir iç güvenlik yaklaşımına ihtiyaç duyulduğunu belirtmiş, bu yapılara yönelik internet üzerinden de tehditlerin gelebileceğine dikkat çekmiştir.[16] Göçoğlu, akıllı şehirlerde kullanılan elektrik dağıtım sistemi, su ve atık su dağıtım sistemi ve ulaşım altyapısının, elektronik sistemlerle kontrol edildiğini, bu sistemlerin siber güvenliğinin sağlanması gerektiğini belirtmiştir.[17] Kritik altyapı operatörlerini kamera ile gözlemleyerek yorgunluk, uyku gibi davranışlar gösterdiklerinde uyarı veren bir sistem Osman Yeşil, Erdal Irmak ve Halil İbrahim Bülbül tarafından geliştirilmiştir.[18]

Von Solms, ülke içinde internete bağlı herhangi bir bilgisayarın kritik sistemler için risk oluşturabileceğini ve siber

---

13 Ercan Yılmaz, Serkan Gönen ve Halil İbrahim Ulus, "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme," *Bilişim Teknolojileri Dergisi* 9, no. 3 (2016): 229.

14 Özge Apiş, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama," *Yasama Dergisi*, no. 37 (2018): 52.

15 Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)," *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 14, no. 2 (2010): 285.

16 Tarık Ak, "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması," *ASSAM Uluslararası Hakemli Dergi* (2019): 46.

17 Volkan Göçoğlu, "Cyber Security of Critical Infrastructures in Smart Cities," *Uluslararası Yönetim Akademisi Dergisi* 2, no. 1 (2019): 56.

18 Osman Yeşil, Erdal Irmak ve Halil İbrahim Bülbül, "Kritik Altyapı Operatörleri İçin Görüntü İşleme Tabanlı Bir Yorgunluk Tespit ve Uyarı Sistemi," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 6, no. 1 (2020): 39.

saldırılara karşı bütüncül bir yaklaşımla mücadele edilmesi gerektiğini söylemiştir.[19] Kozik ve Choras kritik altyapılara yönelik siber saldırıların fiziksel saldırılar kadar önemli olduğunu ve stratejik analizlere dâhil edilmesi gerektiğini belirtmiştir.[20] Kritik altyapılarda kullanılan endüstriyel kontrol sistemleri bilinen standartlara uygun parçalar kullandığından diğer bilgisayar sistemleri gibi siber saldırılara maruz kalabilecektir.[21]

Günümüzde enerji sistemleri sayısal sistemler tarafından kontrol edildiğinden siber saldırı tehdidi bu sistemler için de geçerlidir. Bu sistemleri siber saldırılara karşı korumak için bilişim teknolojisi ve operasyonel konularda uzmanlık gereklidir.[22] SCADA sistemleri ile kontrol edilen elektrik şebekesinin DOS, ortadaki adam ve kötücül yazılımlardan nasıl etkileneceği ve elektrik şebekesinin bu saldırılar sonucu kesintiye uğrayabileceği gösterilmiştir.[23] Malezya'da internet alt yapısının bir kritik altyapı olarak değerlendirilmesi ve siber terör

---

19 Sebastiaan von Solms, "Critical information infrastructure protection: How comprehensive should it be?," *2013 International Conference on Adaptive Science and Technology*, (Pretoria: IEEE, 2013): 1, https://doi.org/10.1109/ICASTech.2013.6707516.

20 Rafal Kozik ve Michal Choraś, "Current cyber security threats and challenges in critical infrastructures protection," *2013 Second International Conference on Informatics & Applications*, (Lodz: IEEE, 2013): 93, https://doi.org/10.1109/ICoIA.2013.6650236.

21 Kovacevic ve Nikolic, "Cyber Attacks on Critical Infrastructure: Review and Challenges," 5.

22 Chee Kiong Gary Ang ve Utomo Nugroho, "Cyber Security in the Energy World," *2017 Asian Conference on Energy, Power and Transportation Electrification*, (Singapore: IEEE, 2017): 3, https://doi.org/10.1109/ACEPT.2017.8168583.

23 Ester Ciancamerla, Michele Minichino ve Silvia Palmieri, "Modeling cyber attacks on a critical infrastructure scenario," *IISA 2013*, (Piraeus: IEEE, 2013): 2, https://doi.org/10.1109/IISA.2013.6623699.

saldırılarına karşı korunması gerektiği tavsiye edilmiştir.[24] İtalya'da, kritik bilişim altyapısını korumak üzere Napoli Futura isminde bir proje başlatılmış, büyük veri analitiği kullanarak siber saldırıların önlenmesi için öneriler getirilmiştir.[25] ABD'de, Başkanlık Ulusal Altyapılar Tavsiye Kurulu kritik altyapıların siber saldırılara karşı korunması ile ilgili bir rapor yazmıştır.[26] Taylor ve Sharif, kritik altyapıların siber-fiziksel sistemler olduğunu belirtmiş ve bu sistemlerin siber saldırılara karşı savunmasının zayıf olduğunu dile getirmiş, siber güvenliğin sağlanması için karmaşık olmayan ve kullanımı kolay siber savunmanın bu sistemlerde uygulanması gerektiğini belirtmiştir.[27]

---

[24] Zahri Yunos et al., "Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework," *2010 Sixth International Conference on Information Assurance and Security*, (Atlanta, GA: IEEE, 2010): 25, https://doi.org/10.1109/ISIAS.2010.5604182.

[25] Stefano Avallone et al., "Napoli Futura: Novel Approaches for Protecting Critical Infrastructures from Cyber Attacks," *2014 IEEE International Symposium on Software Reliability Engineering Workshops*, (Naples: IEEE, 2014): 35, https://doi.org/10.1109/ISSREW.2014.53.

[26] The Cybersecurity and Infrastructure Security Agency, "National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report," erişim tarihi: Aralık 6, 2020, https://www.cisa.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final.

[27] James M. Taylor ve Hamid R. Sharif, "Security challenges and methods for protecting critical infrastructure cyber-physical systems," *2017 International Conference on Selected Topics in Mobile and Wireless Networking*, (Avignon: IEEE, 2017): 5, https://doi.org/10.1109/MoWNet.2017.8045959.

III. TÜRKİYE VE AVRUPA'DA KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNE YÖNELİK GERÇEKLEŞTİRİLEN YASAL VE KURUMSAL DÜZENLEMELER

A. Türkiye Çalışmaları

Bilişim suçlarının niteliği ve kapsamı göz önüne alınarak bu suçlar için farklı düzenleme yapılması gerekliliği ortaya çıkmıştır.[28] Türkiye'de siber suçları da kapsayan bilişim alanındaki suçlarla ilgili ilk düzenleme 1991 yılında, 765 sayılı TCK'nın 20. maddesine eklenen "Bilişim Alanında Suçlar" başlığı ile yapılmıştır.[29] 2004 yılında yürürlüğe giren 5237 sayılı TCK ile "Bilişim Alanında Suçlar" tanımı teknolojinin gelişimine paralel olarak genişletilmiştir. Bu kanunun 243. maddesi ile bilişim sistemine girme, 244. maddesi ile girilen sisteme müdahale, 245. maddesi ile kredi kartlarının ve banka kartlarının kötüye kullanımı ve 246. maddesiyle 243-245. maddelerde belirtilen suçları işleyerek haksız kazanç sağlayan tüzel kişinin durumuyla ilgili suçlar tanımlanmıştır.

Bilişim kavramının geçtiği bir alanda akla ilk gelen kelime internettir. İnternetin varlığı ve yaygınlaşmasıyla bu alanda yasal düzenlemelere ihtiyaç duyulmaya başlanmıştır. Ülkemizde internet ile ilgili ilk kapsamlı düzenleme 23 Mayıs 2007 yılında, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[30] ile yapılmıştır. Kanunla internet erişimlerinin kontrol altına alınması amaçlanmıştır.

5651 sayılı kanun tüm bu olumsuzlukları en düşük seviyeye indirmeyi amaçlayarak, hizmet veren kurumların, hizmet sundukları ve internette savunmasız bulunan kullanıcıları korumasını istemektedir. Bu sebeple, ücretli ya da ücretsiz

---

28 Berrin Bozdoğan Akbulut, "Bilişim Suçları," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 551.

29 RG. 14.06.1991, S. 20901.

30 RG. 04.05.2007, S. 26530.

birden çok kişiye internet erişim hizmeti sunan tüm kurum ve kuruluşlardan henüz kara listeye alınmamış web sayfasında işlenebilecek suçları sonradan takip edebilmek ve kim/kimler tarafından nasıl gerçekleştirildiğinin öğrenilmesi amacıyla web sayfalarına erişen tüm kullanıcıların kayıtlarının (*log*) zaman ve tarih mührü ile tutulması ve saklanması istenmektedir. Buna göre, internet sağlayıcı konumunda bulunan kurumlar ve kuruluşlar kendi ağları içerisinde dağıtılan IP adreslerinin bilgilerini, kullanıma başlanıp bitirilme saatlerini ve kullanılan IP adresleriyle bağlantı kuran bilgisayarların MAC adreslerini elektronik ortamda kayıt altına almak zorundadır. Ayrıca, bu kayıtların doğruluk ve bütünlüğü için elde edilen verileri, dosyanın oluşturulduğu zaman bilgisini ve dosyaların "*hash*" bilgilerini günlük olarak kayıt altına almalıdır. Erişim kayıtlarının 1 yıl ilâ 2 yıl arasında saklanması istenmektedir.

5846 Sayılı Fikir ve Sanat Kanunu[31] (FSEK) madde 2'de, 7 Haziran 1995 tarihinde 4110 sayılı kanunun eklenmesi ile değişikliğe gidilmiş ve "eser" kavramının tanımlaması yapılırken bilişim programları da koruma altına alınmıştır. Madde 2'de bahsi geçen eserler, dil ve yazı ile ifade edilen eserler, bilgisayar programları ve bunların hazırlıkları olarak ifade edilebilir.

FSEK madde 6'da ise yeni eklenen kanun maddesi yer almaktadır. 10 numaralı bende şu ibareler eklenmiştir: "Bir bilgisayar programının uyarlanması, düzenlenmesi ya da program üzerinde değişim yapılması da fikir ve sanat eseri sayılmaktadır." Yapılan bu değişiklikle madde Avrupa Konseyi ilkelerine uygun hale getirilmiştir.[32]

TBMM tarafından 15 Ocak 2004 tarihinde kabul edilen ve bundan altı ay sonra yürürlüğe giren 5070 sayılı Elektronik İmza

---

31 RG. 05.12.1951, S. 7981.

32 Ali Karagülmez, *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri*, (Ankara: Seçkin Yayıncılık, 2005), 154.

Kanunu[33], Avrupa Birliği direktifleri doğrultusunda hazırlanmıştır. Kanunda amaçlanan, elektronik imzanın hukuki ve teknik yönleri ile ilgili çeşitli yaptırımların sağlanabilmesidir. Bu madde ile elektronik araçlar kullanılarak oluşturulan rızasız, hukuka aykırı ve aynı zamanda da izinsiz şekilde düzenlenen elektronik imzaların yaptırımları net olarak ifade edilmektedir.

2006 yılında yapılan bir değişiklik ile 3713 sayılı Terörle Mücadele Kanunu[34]'nda siber suçların terör kapsamında değerlendirileceği durumlar belirtilmiştir. 2016 yılında, 6698 sayılı Kişisel Verilerin Korunması Kanunu[35] ile kişisel veriler kanun nezdinde koruma altına almıştır.

Ülkemizde siber saldırılarla ilgili en yüksek yetkili merci, Bilgi Teknolojileri ve İletişim Kurumudur. Kurumun amacı; Uluslararası sözleşmeler ile garanti altına alınan haberleşme ve mahremiyetin korunmasını sağlamak ve 2007 tarihli 5651 sayılı kanun gereği "… İnternet ortamında işlenen belirli suçlar ile içerik, yer ve erişim sağlayıcılar üzerinden mücadeleye ilişkin usul ve esaslar belirlemektir". Bilgi Teknolojileri ve İletişim Kurumu'nun yanında TÜBİTAK, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Merkezi (SOME), Afet ve Acil Durum Yönetim Başkanlığı (AFAD), Türk Silahlı Kuvvetleri (TSK), Emniyet Genel Müdürlüğü ve Millî İstihbarat Teşkilâtı da siber saldırılara karşı ülkemizin korunmasında etkin rol almaktadırlar.

Ülkemizde özellikle 2000'li yılların başından itibaren siber güvenlik alanında çalışmalar ve düzenlemeler yapılmıştır. Bunlar[36]:

2003/10 Sayılı Başbakanlık Genelgesi (2003)

---

33 RG. 23.01.2004, S. 25355.

34 RG. 12.04.1991, S. 20843 Mükerrer.

35 RG. 24.03.2016, S. 29677.

36 Hasan Çiftçi, *Her Yönüyle Siber Savaş*, (Ankara: TÜBİTAK, 2017).

2003/12 Sayılı Başbakanlık Genelgesi (e-Dönüşüm Türkiye Projesi)

e-Dönüşüm Türkiye Projesi 2005 Yılı Eylem Planı

Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010)

Ulusal Bilgi Güvenliği Programı (2007)

BOME 2008 Tatbikatı (İlk Siber Tatbikatımız) (2008)

Ulusal Sanal Ortam Güvenlik Politikası (2009)

Ulusal Siber Güvenlik Tatbikatı (2011)

Siber Güvenlik Çalıştayı (2011)

Siber Güvenlik Hukuku Çalıştayı (2012)

Siber Kalkan Tatbikatı (2012)

Türkiye Siber Güvenlik Organizasyonu ve Yol Haritası (2012)

Ulusal Siber Güvenlik Strateji Çalıştayı (2012)

TSK Siber Savunma Komutanlığı'nın Kurulması (2012)

TÜBİTAK Siber Güvenlik Enstitüsü'nün Kurulması (2012)

Siber Güvenlik Kurulu'nun Kurulması (2012)

Ulusal Siber Güvenlik Tatbikatı-2 (2013)

Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) (2013)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Kurumsal SOME'lerin Kurulması (2013)

2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi (AFAD)

Siber Güvenlik Faaliyetlerinin Yasalaşması (2014)

Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Sözleşmesi) (2014)

Uluslararası Siber Kalkan Tatbikatı (2014)

Bilgi Toplumu Stratejisi ve Eylem Planı 2015-2018

Elektronik Ticaretin Düzenlenmesi

Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı

TSK Siber Savunma Merkezi Projesi (SİSAMER)(2016)

Kamu Kurum ve Kuruluşlarının KamuNet'e Dahil Edilmesi (2016)

Ulusal Siber Savunma 2017 Tatbikatı

"Bilgi ve İletişim Güvenliği" Başlıklı 2019/12 Sayılı Cumhurbaşkanlığı Genelgesi[37],

Bilgi ve İletişim Güvenliği başlıklı Cumhurbaşkanlığı Genelgesinden bahsetmek faydalı olacaktır. Genelge, 6 Temmuz 2019 tarihli resmî gazetede yayınlanarak, kamu kurum ve kuruluşlarının bilgi ve iletişime yönelik uyması gereken birtakım kurallardan bahsetmiştir. Bu kurallardan özellikle bazıları çok önemli niteliktedir. Bu önemli maddeler incelenecek olursa;

* (Madde 1): *"Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurt içinde güvenli bir şekilde depolanacaktır***."** Söz konusu madde hayata geçirildiği takdirde; kritik bilgi ve verilerin yurt dışına çıkmasının ve yabancı devletlerin eline geçmesinin önünde büyük bir engel oluşturacaktır. Ülke içinde birçok kritik alanlara girişte güvenliğin genetik ve biyometrik verilerle sağlandığı göz önüne alınacak olursa bu maddenin hayata tez zamanda geçirilmesinin elzem olduğu da görülmektedir.

* (Madde 3): *" Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri ya da kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır."* Ülkemizde henüz yerli bulut depolama

[37] RG. 06.07.2019, S. 30823.

hizmeti verilmediği için bu madde ile kurum verilerinin yabancı menşeli bulut sağlayıcılarında tutulması engellenmiş olacaktır.

* (Madde 17): *"Milli güvenliği doğrudan etkileyen stratejik öneme haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak… personellerin güvenlik ve arşiv araştırması yapılacaktır."* Ülkemizin son dönemde yaşadığı olağanüstü olaylardan, özellikle de 15 Temmuz 2016'da yaşanan darbe girişiminden sonra kritik yerlerde çalışan insanların güvenilirliği daha da önemli bir hale gelmiştir. Öyle ki kritik yerlerdeki bir kişi ülkenin kaderini etkileyebilecek birtakım hamleler yapabilmektedir. Dolayısıyla söz konusu maddenin hayata geçirilmesi çok önemlidir.

Yine bu genelge ile, Cumhurbaşkanlığı Dönüşüm Ofisi'nin koordinasyonu ve kamu kurum ve kuruluşlarının katkısı ile "Bilgi ve İletişim Güvenliği Rehberi" oluşturulması hedeflenmiştir. Bu rehber ile kamu kurum ve kuruluşları ile kritik öneme haiz işletmelerin uyması zorunlu kurallar getirilmesi hedeflenmekte ve kurulacak denetim mekanizması ile her sene en az 1 kere denetlenmesi amaçlanmaktadır. Söz konusu bu rehber söylemden ibaret kalmayıp hayata geçirildiği takdirde olumlu sonuçlar verecektir.

Yapılan bu çalışmalar ve düzenlemeler ile kritik altyapı tanımlamaları ve bu alanın siber güvenliğine yönelik birtakım düzenlemeler hayata geçirilmiştir. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile birlikte artık ülkemiz için hangi sektörlerin kritik altyapı niteliğinde olduğu belirlenmiştir. Yine bu eylem planlarıyla birlikte siber alandaki mevzuat çalışmaları derinleşmiş ve siber güvenlik tatbikatlarından bahsedilmiştir.

Ülkemizde yapılan siber güvenlik tatbikatları ilk başlarda doğrudan kritik altyapılarla ilişkilendirilerek yapılmasa da 2011 yılında yapılan Ulusal Siber Güvenlik Tatbikatı ile birlikte doğrudan kritik altyapı sayılacak sektörleri içinde bulunduran tatbikatlar yapılmaya başlanmıştır. Yine, TSK Siber Savunma Komutanlığı'nın kurulması ve TÜBİTAK Siber Güvenlik

Enstitüsü'nün kurulması ile birlikte kritik alanlardaki siber savunma mekanizması güçlendirilmiştir.

SOME'lerin kurulmasıyla birlikte, kritik altyapılara yönelik yapılan siber saldırılara karşı USOM çatısı altında daha güçlü bir merkezi otorite oluşturulmaya çalışılmıştır. Kritik altyapı sektöründe de kurulan SOME'lerin birbirleriyle iletişimi artırılarak olası siber saldırılara karşı ortaklaşa önlem alınması amaçlanmıştır.

AFAD tarafından yayınlanan; 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi ile Türkiye'nin uzun vadede ulaşması gereken hedefler belirlenmiştir.[38] 2014 yılında Türkiye, Sanal Ortamda İşlenen Suçlar Sözleşmesi'ni (Budapeşte Sözleşmesi) imzalayarak uluslararası alandaki ilk siber anlaşmasını imzalamıştır.

B. Avrupa Çalışmaları

1. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa bilişim suçları ile mücadelede, bu alanda imzalanan ilk anlaşma olan Avrupa Konseyi Siber Suçlar Sözleşmesi'ni 23 Kasım 2001 tarihinde, Budapeşte'de imzaya açmış ve bu sözleşme 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Avrupa Konseyi'ne dâhil olmayan ülkelere de söz hakkı tanınan bu sözleşmeye bugüne kadar 46 tanesi Avrupa Konseyi üyesi olan toplamda 68 ülke sözleşmeye taraf olmuştur.[39] Sözleşme ülkemizde 10 Kasım 2010 tarihinde imzalanmış ve 2 Mayıs 2014'te yürürlüğe konmuştur. Sözleşme, Türkçe'ye "Sanal

[38] T.C. Başbakanlık Afet Acil Durum Yönetimi Başkanlığı, *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*, (Ankara: AFAD, 2014).

[39] İsa Başıbüyük, "Dijital Çağda Suçla Mücadele: Bir Avrupa Siber-Suç Merkezinin Kurulması," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 15, (2013): 1585.

Ortamda İşlenen Suçlar Sözleşmesi" biçiminde çevrilmiş olup, "Avrupa Siber Suçlar Sözleşmesi" ismiyle de anılmaktadır.[40]

Sözleşmede yer alan temel amaçlara, sözleşme açıklayıcı raporunda yer verilmektedir. Buna göre, bilişim suçları ile ilgili ulusal düzeyde bulunan yasal düzenlemeler ile bağlantılı hükümlerin uyumlu hale getirilmesi, bilişim suçları ve elektronik delillerin bulunduğu diğer klasik suçların soruşturması ve takibi ile ilgili olarak ulusal yetkilerin ve düzenlemelerin sağlanması, ayrıca uluslararası anlamda oluşturulacak iş birliğinin hızlı ve etkili olmasına çalışılması sözleşmenin temel amaçları olarak ifade edilmektedir. Sözleşme bazı yönlerden eleştiriler de almıştır, ancak yine de bilişim suçları ile mücadelede ciddi bir ilerleme sağladığı da inkâr edilemez bir durumdur.[41] Sözleşmede bu tür olumlu katkıların yanında, doğrudan kritik altyapılara yönelik bir hüküm bulunmaması ise bir eksiklik olarak nitelendirilmektedir. Sözleşmede belirsiz ifadelerin bulunması da yine bir eksiklik olarak tanımlanabilir. Örnek vermek gerekirse, Sözleşme'nin 14. maddesinde geçen "diğer suçlar" ifadesi açık değildir. Düzenlemeye göre, sözleşmeye taraf olan devletler bilgisayar aracılığıyla işlenen diğer suçlara uygulanacak usullere ve yetkilere ilişkin gerekli yasal ve diğer tedbirleri alacaklardır. Bu cümlede ve daha birçok maddede geçen ve tanımlanmayan

---

40 Türkiye Büyük Millet Meclisi, *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırma Komisyonu Raporu*, (Ankara: TBMM, 2012), https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf.; Cahit Aliusta ve Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 4, no. 2: (2018): 37.

41 Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri," (2015): 87, erişim tarihi: Ocak 12, 2019, https://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf.

"diğer" kavramının netleştirilmesi ve açık bir şekilde belirtilmesi gerekmektedir.

Avrupa Birliği tarafından bu alanda kapsamlı strateji geliştirme çalışmaları da devam ettirilmektedir. Avrupa Parlamentosu, internet altyapısına yönelik siber suçlarla mücadele için, üye ülkelerin kanun çıkarması ve mevcut kanunlara ek yapması için karar almıştır.[42] Buna ek olarak, Avrupa çapında bilişim suçlarının faillerinin takibi ve bilişim suçlarının soruşturması konusunda birtakım engeller bulunmaktadır. Yargı yetkisi, istihbaratın paylaşılması konusundaki yetersizlikler, bilişim suçlularının izlerinin sürülmesi önündeki teknik engeller, uzman personel sayısının az olması, hukuki imkânların uyumsuz olması bu engeller arasındadır. Bu gibi engeller, siber saldırganlara karşı caydırıcı cezalar verilmesine engel olmakla birlikte dolaylı yoldan saldırganlara açık kapı bırakmaktadır. Bu hususlar göz önüne alınarak Avrupa Komisyonu yeni kararlar almıştır. Avrupa Birliği ülkeleri mahkemeleri üye ülkelerden elektronik mesaj ve benzeri elektronik delilleri talep edebilecek, internet servis sağlayıcılardan ilgili verileri korumasını isteyebilecektir.[43]

III. KRİTİK ALTYAPILARA YÖNELİK GERÇEKLEŞEN SİBER SALDIRI İSTATİSTİKLERİ

Siber tehditlerin daha iyi gözlemlenmesi için birtakım istatistiki çalışmalar aşağıda sunulmuştur. 2017 yılında yapılan, endüstri ve organizasyon büyüklüğüyle ilgili bilişim

---

42 "Directive 2013/40/Eu Of The European Parliament And Of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," EUR-Lex, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

43 European Commission, "e-evidence," erişim tarihi Aralık 7, 2020, https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en.

saldırılarını incelendiğinde aşağıdaki tablodaki veriler elde edilmiştir.[44]

Tablo 2: 2017 yılı Küresel Siber Güvenlik Olay Sayısı

	Büyük	Küçük	Belirsiz	Toplam
Konaklama	40	296	32	368
İdari	7	15	11	33
Tarım	1	0	4	5
İnşaat	2	11	10	23
Eğitim	42	26	224	292
Eğlence	6	19	7.163	7.188
Maliye	74	74	450	598
Sağlık hizmeti	165	152	433	750
Bilgi	54	76	910	1.040
Yönetim	1	0	1	2
İmalat	375	21	140	536
Madencilik	3	3	20	26
Diğer servisler	5	11	46	62

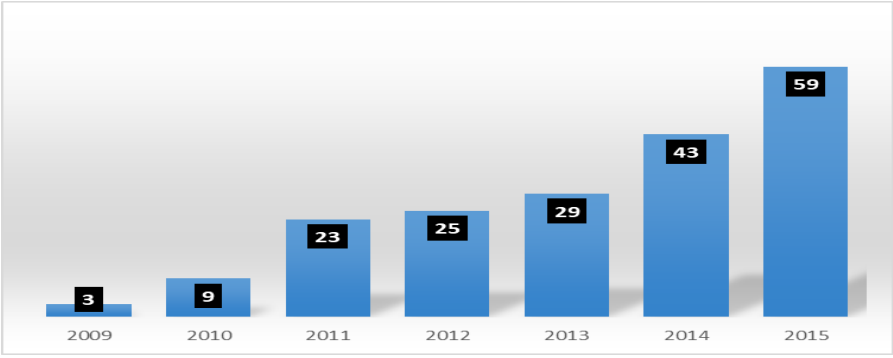
Saldırılar, konaklama sektöründe ağırlıklı olarak küçük sektörlere, imalatta ise büyük sektörlere karşı gerçekleşmiştir. Eğlence sektöründeki saldırıların ağırlığı ise büyüklük ya da küçüklük durumu belirlenemeyen sektörlere karşı yapılmıştır. Sektörler incelendiği zaman sağlık hizmeti, maliye ve bilgi teknolojileri gibi ülkeler için kritik altyapı niteliğindeki sektörlere de siber saldırılar yapıldığı ve toplam saldırı içindeki payının da yüksek olduğu gözlemlenmektedir.

Teknolojinin gelişimine paralel olarak kritik altyapı niteliğindeki bilgi teknolojileri alanına da siber saldırı sayısı

[44] Statistica, "Global number of cyber security incidents in 2017, sorted by victim industry and organization size," erişim tarihi: Ekim 6, 2018, https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/.

artmıştır. Aşağıdaki grafikte 2009 yılından 2015 yılına kadarki siber saldırı sayısı ile ilgili istatistiki veri paylaşılmıştır[45]:

Grafik 1. Dünya Genelinde Bilişim Teknolojilerine Yapılan Saldırı Sayısı (Milyon)



Grafik incelendiği zaman Bilgi Teknolojileri alanında yapılan siber saldırı sayısındaki artışın teknoloji gelişimiyle paralellik gösterdiği gözlenmektedir. Bu artışa teknolojinin gelişimi kadar teknoloji kullanımının yaygınlaşması da etki etmektedir. Yaygınlaşmak, beraberinde tedbirsizliği de getirmektedir. Bu durum saldırganlar için bir fırsat niteliğinde sayılmaktadır. Nihayetinde grafikteki artış da bu durumun sonucunu ortaya koymaktadır.

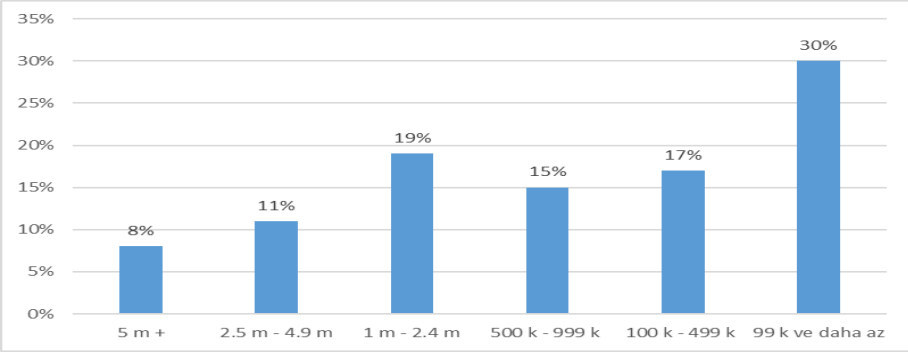
Nisan 2018'de yapılan istatistiki bir çalışmaya göre dünya çapındaki işletmelere yapılan siber saldırıların maliyetleri aşağıdaki gibi belirlenmiştir.[46]

---

[45] Statistica, "Global number of cyber security incidents from 2009 to 2015," erişim tarihi: Şubat 16, 2019, https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/.

[46] Statistica, "Average financial damages of cyber attacks caused to businesses worldwide as of 2018 (in U.S. dollars)," erişim tarihi: Şubat 19, 2019, https://www.statista.com/statistics/881158/average-financial-damages-via-cyber-attacks/.

Grafik 2. Siber Saldırıların Dünya Çapındaki İşletmelere Ortalama Finansal Zararı



Grafik incelendiği zaman, dünya çapında işlem gören işletmelere yönelik siber saldırıların %8'i 5 milyon doların üzerinde, %19'u 1 ilâ 2.4 milyon dolar arasında ve %30'unun ise 100 bin doların altında zarara sebep olduğu gözlenmektedir.

Bu grafiklerden görüldüğü üzere siber saldırılar ve bunun sonucunda ortaya çıkan zararlar eksponansiyel bir artış göstermektedir. Kritik altyapılara yönelik saldırılar ise sadece maddi zararlara değil toplum üzerinde psikolojik yıpranmaya da yol açabilecektir.

SONUÇ

Ülkemizde son yıllarda siber alanla ilgili birçok düzenleme, seminer ve çalıştay yapılmaktadır. Bu çalışmalar sonucunda bazı kararlar alınarak eksiklikler tespit edilmeye çalışılmıştır. Eksiklikler tespit edilmeye başlandığı halde gerek bürokratik engeller gerekse başka durumlardan ötürü yeterli düzeyde kanuni düzenlemeler yapılmamış ve yeterli önlemler alınmadığı tespit edilmiştir. Bu alanla ilgili düzenleme yalnızca 5237 sayılı TCK'nın 243-246. maddeleri ile genel çerçeveleri çizilerek belirtilmiştir. Bu maddelerin siber suçlara yönelik değil de doğrudan işlenen suçların bilişim alanına yansıması şeklinde düşünülerek hazırlanması bu alandaki ihtiyaca yeterince cevap verememektedir.

Bilişim suçları alanında TCK'da birçok yenilik yapılmış ve bu suçlar da çeşitli yaptırımlarla büyük oranda kontrol altına alınmıştır. Yeni Türk Ceza Kanunu aynı zamanda Avrupa Konseyi Siber Suçlar Sözleşmesi ile de büyük oranda uyum içinde geçerliliğini sürdürmektedir.

Belirtmek gerekir ki, bilişim alanında önlemler almış olsa da ne yazık ki ülkemizde henüz kritik altyapıları doğrudan ilgilendiren bir hukuki düzenleme yoktur. Kritik altyapılar için belirlenmiş strateji planı da henüz yoktur. Kanunlarımız siber saldırıların bireysel düzeyiyle ceza hukuku bazında ilgilenmiştir. Kurumları doğrudan ilgilendiren bir siber güvenlik yasası yoktur ve ihtiyaç duyulmaktadır. Bu yasa birtakım zorunluluklar getirmelidir. Kritik altyapıların herhangi birine yapılan siber saldırı hakkında diğer kritik altyapı işletmelerinin bilgilendirilmesi zorunlu hale getirilmelidir. Yasa kapsamında oluşturulan maddeler açık ve kesin olmalıdır. Kritik altyapılara yönelik siber saldırılar milyonlarca kişinin hayatını olumsuz yönde etkileyebilir hatta milli güvenliği tehlikeye düşürebilir. Bundan dolayı, kritik altyapılara yönelik saldırılara verilecek cezalar caydırıcı olmalıdır. Maddeler evrensel nitelikte lakin ülke menfaati ön planda tutulacak şekilde oluşturulmalı ve sürekli güncellenmelidir.

Ülkemizde eksikliği hissedilen durumlardan biri de ulusal bazda çıkarılan siber güvenlik strateji belgelerinin içinde belirtilen hususların çerçeve bir şekilde düzenlenmesidir. Örneğin, *2016- 2019 Ulusal Siber Güvenlik Strateji Belgesi* içinde belirlenen amaç ve eylemler başlığı altındaki 2. maddede belirtilen; "*Siber güvenlik alanında denetim yaklaşımını da içeren uluslararası standartlara uygun mevzuatın oluşturulması"* gerekliliği belirtilmiştir. Bu maddenin varlığına rağmen henüz böyle bir mevzuat oluşturulmamıştır. Belirlenen hedefler uygulamaya geçtiği takdirde ülkemiz açısından çok güvenli ve faydalı bir dijital alan oluşacaktır.

Her ne kadar bugün yaptırımlar ya da cezai hükümlerle ilgili birçok eleştiri ve eksik yön bulunuyor olsa da bu alanda

yapılan çalışmaların değişen dünya düzenine uyum sağlanması bakımından devam ettirildiği bilinmektedir. Bilişim suçlarına yönelik ceza hükümleri üzerinde gerekli olması halinde gerek ülke çapında gerekse Avrupa genelinde düzenlemeler ve kanunlarda yeniliklerin yapılacağı yahut yapılması gerektiği öngörülmektedir.

KAYNAKÇA

Ak, Tarık. "İç Güvenlik Yönetimi Açısından Kritik Altyapıların Korunması." *ASSAM Uluslararası Hakemli Dergi*, no. 1 (2019): 42-51.

Aliusta, Cahit ve Benzer, Recep. "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci." *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 4, no.2 (2018): 35-42.

Altunok, Ebru ve Vural, Ali Fatih. "Bilişim Suçları." *Denetişim*, no.8 (2016): 74-84.

Ang, Chee Kiong Gary ve Nugroho, Utomo. "Cyber Security in the Energy World." İç. *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*. (Singapore: ACEPT, 2017):1-5. https://doi.org/10.1109/ACEPT.2017.8168583.

Apiş, Özge. "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama." *Yasama Dergisi*, no.37 (2018): 49-86.

Avallone, Stefano, Carrozza, Gabriella, Cinque, Marcello, Della Corte, Raffaele, Marotta, Antonio, Pecchia, Antonio ve Savignano, Agostino. "Napoli Futura: Novel Approaches for Protecting Critical Infrastructures from Cyber Attacks." *2014 IEEE International Symposium on Software Reliability Engineering Workshops*. (Naples: IEEE, 2014): 33-36. https://doi.org/10.1109/ISSREW.2014.53.

Aydın, Emin. "Bilişim Sistemlerinde Güvenlik, Güvenirlilik Mahremiyet ve Bilişim Suçları." *Marmara İletişim Dergisi* 1, no. 1 (1992): 109-138.

Başıbüyük, İsa. "Dijital Çağda Suçla Mücadele: Bir Avrupa Siber-Suç Merkezinin Kurulması." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 15, (2013): 1583-1594.

Bozdoğan Akbulut, Berrin. "Bilişim Suçları." *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 545-550.

Ciancamerla, Ester, Minichino, Michele ve Palmieri, Silvia. "Modeling cyber attacks on a critical infrastructure

scenario." *IISA 2013*. (Piraeus: IEEE, 2013): 1-6. https://doi.org/10.1109/IISA.2013.6623699.

Curran, Kevin, Concannon, Kevin ve McKeever, Sean. "Cyber Terrorism Attacks." İç. *Cyber Warfare and Cyber Terrorism*. ed. Lech J. Janczewski ve Andrew M. Colarik. (Hershey, PA: IGI Global, 2008): 1-6. http://doi:10.4018/978-1-59140-991-5.ch001.

Çiftçi, Hasan. *Her Yönüyle Siber Savaş*. Ankara: TÜBİTAK, 2017.

Erdağ, Ali İhsan. "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)." *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 14, no. 2 (2010): 275-303.

Erdoğan, Yavuz. "Bilişim Sistemine Girme ve Kalma Suçu." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 12, (2010): 1363-1433.

EUR-Lex. "Directive 2013/40/Eu Of The European Parliament And Of The Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA." https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

EUR-Lex. "European Programme for Critical Infrastructure Protection-Summaries of EU Legislation." Erişim Tarihi: Aralık 26, 2018. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm#KeyTerms.

European Commission. "e-evidence." Erişim Tarihi: Aralık 7, 2020. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime/e-evidence_en.

Geers, Kenneth. "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Information Security Journal: A Global Perspective*, no. 18 (2009): 1-7.

Göçoğlu, Volkan. "Cyber Security of Critical Infrastructures in Smart Cities." *Uluslararası Yönetim Akademisi Dergisi* 2, no.1 (2019): 51-63.

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

Kovacevic, Ana ve Nikolic, Dragana. "Cyber Attacks on Critical Infrastructure: Review and Challenges." İç. *Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance*. ed. Maria Manuela Cruz-Cunha ve Irene Maria Portela. (Hershey, PA: IGI Global, 2015): 1-18. http://doi:10.4018/978-1-4666-6324-4.ch001.

Kozik, Rafal ve Choraś, Michal. "Current cyber security threats and challenges in critical infrastructures protection." *2013 Second International Conference on Informatics & Applications*. (Lodz: IEEE, 2013): 93-97. https://doi.org/10.1109/ICoIA.2013.6650236.

Noguchi, Mutsuo ve Ueda, Hirofumi. "An Analysis of the Actual Status of Recent Cyberattacks on Critical Infrastructures." *Nec Technical Journal* 12, no. 2 (2017): 19-24. Erişim Tarihi: Kasım 16, 2020, https://www.nec.com/en/global/techrep/journal/g17/n02/pdf/170204.pdf.

Özbek, Mücahid. "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri," (2015): 73-88. Erişim Tarihi: Ocak 12, 2019. https://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf.

Özsoy, Nevzat. "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları." *Yaşar Hukuk Dergisi* 1, no. 2 (2019): 295-352.

Statistica. "Average financial damages of cyber attacks caused to businesses worldwide as of 2018 (in U.S. dollars)." Erişim Tarihi: Şubat 19, 2019,

https://www.statista.com/statistics/881158/average-financial-damages-via-cyber-attacks/.

Statistica. "Global number of cyber security incidents from 2009 to 2015." Erişim Tarihi: Şubat 16, 2019. https://www.statista.com/statistics/387857/number-cyber-security-incidents-worldwide/.

Statistica. "Global number of cyber security incidents in 2017, sorted by victim industry and organization size." Erişim Tarihi: Ekim 6, 2018. https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/.

Taylor, James M. ve Sharif, Hamid R. "Security challenges and methods for protecting critical infrastructure cyber-physical systems." *2017 International Conference on Selected Topics in Mobile and Wireless Networking*. (Avignon: IEEE, 2017): 1-6. https://doi.org/10.1109/MoWNet.2017.8045959.

T.C. Başbakanlık Afet Acil Durum Yönetimi Başkanlığı. *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*. Ankara: AFAD, 2014.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. *2016-2019 Ulusal Siber Güvenlik Stratejisi*. Ankara: T.C. UDHB, 2019. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf.

The Cybersecurity and Infrastructure Security Agency. "National Infrastructure Advisory Council Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure Final Report." Erişim Tarihi: Aralık 6, 2020. https://www.cisa.gov/publication/niac-securing-cyber-assets-addressing-urgent-cyber-threats-critical-infrastructure-final.

The White House. "Presidential Policy Directive." Erişim Tarihi: Aralık 2, 2018. https://obamawhitehouse.archives.gov/the-

press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resilience.

Turan, Metin ve Külcü, Özgür. "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi." *Türk Kütüphaneciliği* 28, no. 1 (2014): 18-46.

Türkiye Büyük Millet Meclisi, *Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler İle İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırma Komisyonu Raporu*. Ankara: TBMM, 2012. https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss381.pdf.

Von Solms, Sebastiaan. "Critical information infrastructure protection: How comprehensive should it be?." *2013 International Conference on Adaptive Science and Technology*. (Pretoria: IEEE, 2013): 1-5. https://doi.org/10.1109/ICASTech.2013.6707516.

Yeşil, Osman, Irmak, Erdal ve Bülbül, Halil İbrahim. "Kritik Altyapı Operatörleri İçin Görüntü İşleme Tabanlı Bir Yorgunluk Tespit ve Uyarı Sistemi." *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* 6, no.1 (2020): 35-44.

Yılmaz, Ercan, Gönen, Serkan ve Ulus, Halil İbrahim. "Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme." *Bilişim Teknolojileri Dergisi* 9, no. 3 (2016): 229-236.

Yunos, Zahri, Ahmad, Rabiah, Suid, Syahrul Hafidz ve Ismail, Zuraini. "Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework." *2010 Sixth International Conference on Information Assurance and Security*. (Atlanta, GA: IEEE, 2010): 21-27. https://doi.org/10.1109/ISIAS.2010.5604182.

ELEKTRONİK ÇEK VE BONO KANUNU TEKLİFİ İLE YAPILMASI PLANLANAN DÜZENLEMELERE DAİR DÜŞÜNCELER *

Evaluations Regarding the Arrangements Planned to be Done with the Electronic Check and Bills Law Offer

Mete TEVETOĞLU**

Özet

Çek ve bono, ticaret hayatında en çok kullanılan kambiyo senetleridir. Bu senetler kredi pazarında önemli bir yere ve hacme sahiptir. Çek ve bononun tabi olduğu yasal düzenlemelerin temeli oldukça eskiye dayanmaktadır. Bu sebeple, çek ve bononun değişen ve gelişen ticaret hayatının ve teknolojinin gerekleriyle uyumlu hale getirilmesi ihtiyacı ortaya çıkmıştır. Çek ve bononun günümüzün ihtiyaçlarına, değişen mevzuata uyumlu hale getirilmesi, sahteciliğin önüne geçilmesi, kayıt dışılığın önlenmesi temel gerekçeleriyle Ticaret Bakanlığı

---

* Bu makale, 18-19-20 Şubat 2021'de düzenlenen "Ticaret Hukuku Kongresi"nde, 19.02.2021 tarihinde yazar tarafından sunulan "Elektronik Çek ve Bono Kanunu Teklifi ile Yapılması Planlanan Düzenlemelere Dair Düşünceler" başlıklı tebliğin makale olarak kaleme alınmış versiyonudur.

** Dr. Öğretim Üyesi, Maltepe Üniversitesi Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Anabilim Dalı, metetevetoglu@maltepe.edu.tr, ORCID: 0000-0002-2575-906X.

Makale Gönderim Tarihi/Received: 30.05.2021.

Makale Kabul Tarihi/Accepted: 17.06.2021.

Atıf/Citation: Tevetoğlu, Mete. "Elektronik Çek ve Bono Kanunu Teklifi ile Yapılması Planlanan Düzenlemelere Dair Düşünceler." *Bilişim Hukuku Dergisi* 3, no: 1 (2021): 31-75.

tarafından hazırlanan Elektronik Çek ve Bono Kanun Teklifi önemli değişiklikler öngörmektedir. Bu düzenlemeler, çek ve bono kullanımını ve ticaret hayatını derinden etkileyecek; elektronikleşmiş çek ve bonoyu, yeni nesil dijital ticaret araçları olarak kullanıma sunacaktır. Bu makalede, üzerinde uzun zamandır çalışılan ve artık son haline ulaşmış olduğu görülen Kanun Teklifi ile getirilmesi planlanan düzenlemeler incelenmektedir. Kısa bir süre içinde yasalaşması beklenen bu düzenlemelerin ve gerekçelerinin daha iyi anlaşılması ve analiz edilmesi çalışmanın amacıdır. Bu amacın temini için konu hem elektronik çek ve bononun teknolojik özellikleri hem de çek ve bononun tabi oldukları genel esasların ışığında ele alınarak değerlendirilmiştir.

Anahtar Kelimeler: Kambiyo Senedi, Çek, Bono, Elektronik Çek, Elektronik Bono

Abstract

Checks and bills are the most used bills of exchange in business life. These securities also have an important place and volume in the loan market. On the other hand, the basis of the legal regulations governing checks and bills is very old. For this reason, the need to adapt checks and bills to the needs of the changing and developing trade life and technology has emerged. The Electronic Check and Bills Law Proposal prepared by the Ministry of Commerce for the main reasons of adapting checks and bills to today's needs, changing legislation, preventing counterfeiting of checks and bills, preventing informality, anticipates important changes regarding checks and bills. These regulations will deeply affect the use of checks and bills and trade life, and will make electronicized checks and bills available. In this article, the regulations planned to be brought by the Law Proposal, which has been worked on for a long time and are now in its final form, will be evaluated in the light of both their technological features and the principles to which the

checks and bills are subject, in order to better understand and analyze them and their reasons.

Keywords: Bills of Exchange, Check, Bond, Electronic Check, Electronic Bills.

GİRİŞ

Ticaret hayatında en yaygın şekilde kullanılan senetler kambiyo senetleridir. TTK gereği hukukumuzda kambiyo senetleri, sınırlı sayıda olmak üzere poliçe, bono ve çekten oluşur. Çek, kimi ülkelerde kısa ibraz sürelerinden ve ödeme aracı özelliğinden ötürü kambiyo senetlerinden kabul edilmese de hukukumuzda TTK. m. 780 vd. hükümleriyle açıkça bir kambiyo senedi olarak düzenlenmiştir. Kambiyo senetlerinden çek ve bono, pratik şekilde kullanılabilmelerinden ötürü, uygulamada poliçeye göre çok daha fazla tercih edilmektedir.[1] Bu senetler, kredi pazarının önemli bir kısmını oluşturdukları için ülkemizdeki genel ekonomik ve ticari faaliyetlere doğrudan etki etmektedir. Öte yandan bono ve çekte sahtecilik, kayıt dışılık, çekte karşılıksızlık gibi durumlar bu senetlerin kullanımını ve potansiyellerini arzu edilenin aksine azaltmaktadır.[2] Bu durum, genel kredi havuzunun derinliğini kaybetmesine yol açmaktadır. Buna mukabil, halka açık anonim ortaklıkların hisse senetleri, internet bankacılığı, ödeme hizmetleri gibi ürün ve servisler teknolojinin sağladığı olanaklarla tamamen dijitalleşmiştir. İlaveten, teknolojiyle ortaya çıkan kredi kartları, ön ödemeli kartlar, elektronik para, kripto varlıklar, elektronik akreditif, elektronik mutabakat sistemleri gibi finansal enstrümanlar, çek ve bononun tercih

---

1 Oğuz İmregün, *Kıymetli Evrak Hukuku* (İstanbul: Filiz Kitabevi, 1995), 35-36; Hüseyin Ülgen et. al., *Kıymetli Evrak Hukuku*, (İstanbul: Vedat Kitapçılık, 2019), 260.

2 Alev Deniz Dursun, *Karşılıksız Çek Keşide Etmenin Hukuki ve Cezai Sorumluluğu* (Ankara: Seçkin Yayıncılık, 2019), 40.

edilirliğini olumsuz etkilemekte; bu ürün ve servisleri düzenleyen mevzuatla uyumsuz bir konuma sürüklemektedir. Bu sebeplerle, çek ve bononun teknoloji ile uyumlu hale getirilmesi gereksinimi belirgin bir şekilde meydana çıkmaktadır.

Öte yandan, ticaret hayatındaki konumları nedeniyle çek ve bononun diğer finansal araçların yaşadığı dijital uyum ve dönüşümün ortaya çıkarttığı rekabete karşı korunmaları gerekmektedir. Bu amaçlarla, elektronik çek ve bonoya dair yapılması planlanan değişikliklerin üzerinde uzun bir süreden bu yana çalışılmaktadır. Bu çalışmaların son aşamaya geldiğini söylemek hatalı olmayacaktır. Söz konusu düzenlemeler oldukça dikkat çekicidir. Buna göre bir yandan klasik kambiyo senetleri olan çek ve bono modernize edilmekte, teknolojiyle donatılmakta gibi görünmektedir. Oysa diğer yandan, Kanun Teklifi ile öngörülen değişiklikler, elektronik işlemler ve tamamen dijitalleştirilen yapı ile aslında yepyeni dijital finansal enstrümanların ortaya çıkartıldığını söylemek mümkündür. Elektronik Çek ve Bono Kanun Teklifinin yakın zamanda yasalaşması beklenmektedir. Teklifin, yasalaşmasından evvel, içerdiği tamamı yeni ve teknoloji odaklı düzenlemelerin, kıymetli evrak hukukunun genel ilkelerinin ışığında ele alınmasında, daha iyi anlaşılması bakımından açık bir fayda vardır. İlaveten, elektronik çek ve bononun dayandıkları teknolojinin, günümüzdeki mevcut teknolojiyle ve diğer finansal teknoloji enstrümanlarıyla uyumluluk açısından mukayese edilerek ele alınması, daha iyi anlaşılmalarını, daha doğru uygulanmalarını sağlamak bakımından bu çalışmanın temel gayesi olarak tespit edilmiştir.

I. ELEKTRONİK ÇEK VE BONOYA OLAN İHTİYAÇ

Elektronik Çek ve Bono Kanun Teklifi çeşitli sebeplerin etkisiyle, kimi hukuki kimi teknolojik gerekçelere dayanan bir

arka plana sahiptir. Fakat bu konudaki çalışmalar yeni değildir.[3] Ülkemizde olduğu gibi yabancı ülkelerde de elektronik kambiyo senetleri hakkında birçok yasal ve teknik alt yapı çalışması söz konusudur.[4] Ticaret eski Bakanı Ruhsar Pekcan'ın elektronik çek ve bono kanununun önce 2020, sonra 2021'de yürürlüğe gireceğini net bir şekilde ifade etmesi üzerine konu hakkındaki çalışmalar yoğunlaşmış ve hızlanmıştır.[5] Kanun Teklifinin hazırlanması, 2015'ten itibaren Ticaret Bakanlığının gözetiminde Türkiye Bankalar Birliği nezdinde yapılan çalışmalara dayanmaktadır.[6] Bu teklifin ortaya çıkmasının ve çek ve bononun elektronik olarak düzenlenmesinin birtakım hukuki, ekonomik ve teknolojik sebepleri vardır. Kanun teklifini, kabul edilmesi ve yürürlüğe girmesi halinde Kanuna dönüşecek olan bu düzenlemeleri tam ve sağlıklı bir şekilde anlayabilmek ve doğru uygulayabilmek için bu sebeplerin her zaman göz önünde

---

3 Örneğin, çeklerin elektronik ortamda takas edilmesi 1993'ten beri Bankalararası Takas Odaları Merkezinde elektronik ortamda yapılmaktadır.

4 ABD, Hindistan, Avustralya, Hong Kong, Kanada, Ürdün örnekleri için bkz. Deniz Baytemür, *Elektronik Kambiyo Senetleri* (Yayımlanmamış Yüksek Lisans Tezi, Ankara Hacı Bayram Veli Üniversitesi, Lisansüstü Eğitim Enstitüsü, Ankara, 2020), 73-80. Almanya'daki yasal düzenlemeler için bkz. Murat Can Atakan, "Kıymetli Evrak Hukuku'nda Yeni Bir Öneri: Elektronik Çek. Alman Elektronik Kıymetli Evrak Kanunu Tasarısı (Ewpg-E) Işığında Bir İnceleme," *Yargıtay Dergisi* 47, no. 2 (Nisan 2021): 541-580.

5 "2021'de çek-bonoya elektronik sistem getirilmesi planlanıyor," Bloomberg, erişim tarihi: Mayıs 10, 2021, https://www.bloomberght.com/2021-de-cek-bonoya-elektronik-sistem-getirilmesi-planlaniyor-2269211.

6 Emre Çotuksöken, "Dijitalleşme, Elektronik Çek ve Blockchain İlişkisi," *Finans Hukuku Gündemi Dergisi*, no. 4: (Temmuz 2020), erişim tarihi: Şubat 15, 2021, http://212.58.27.19/XXXX/FinansHDergi44/Dijitallesme,-Elektronik-Cek-ve-Blockchain-Iliskisi1_xxcid12679838#.YJ_z4ZMzbOQ; "Çekler Çalışma Grubu," TBB, erişim tarihi: Mart 12, 2021, https://www.tbb.org.tr/tr/hakkimizda/kurumsal/calisma-gruplari/surekli-calisma-gruplari/cekler-calisma-grubu/158.

tutulması gerekir. Fakat öncesinde söylemek gerekir ki 2015 yılında bu konuyla ilgili çalışmalara başlanırken, ilk etapta planlanıp üzerinde çalışılan konu sadece elektronik çekten ibarettir.[7] Daha sonra, buna elektronik bono da eklenmiştir.[8] Bononun eklenmesiyle, kapsam genişlemiştir. Bu durum, önemini çek ve bononun iki farklı statüde ürünler olmasında gösterir. Zira çek bir banka ürünüdür. Bono ise değildir. Teklif yasalaştığında hem çek hem de bono bir arada bir banka ürünü olacaktır. Böylece bu iki kambiyo senedi birlikte elektronikleştirilecek, her ikisi de banka ürünü olacak, finansal teknoloji aracı olarak kullanıma sunularak; kredi kartı, internet bankacılığı, elektronik para gibi rakipleri olarak sayabileceğimiz diğer finansal teknoloji araçlarıyla rekabete dâhil edilecektir.

Çek ve bononun ortak özelliği olarak bu iki senet de kambiyo senedidir. Çek; üç taraflı, muhatabın her zaman banka olması zorunlu olan nitelikli bir havaledir. Buna karşılık bono bir banka ürünü değildir.[9] Bono, iki taraflı mücerret bir borç ödeme taahhüdü veya vaadi olmasına karşın, yapılan ön hazırlık çalışmalarında kambiyo senetlerinden poliçe dahil edilmeksizin, çek için başlatılan çalışmaya, bononun dahil edilmesinin bir diğer ve asıl önemli nedeni uygulamadaki kullanım

---

7 "Çek koçanı tarihe karışacak," İTO, erişim tarihi: Nisan 8, 2021, https://www.itohaber.com/haber/guncel/204360/cek_kocani_tarihe_karisacak.html.

8 "Bakan Pekcan: Karekodlu bono, elektronik çek ve bono uygulamasını başlatıyoruz," Ticaret Bakanlığı, erişim tarihi: Nisan 14, 2021, https://www.ticaret.gov.tr/haberler/bakan-pekcan-karekodlu-bono-elektronik-cek-ve-bono-uygulamasini-baslatiyoruz.

9 Çek, 6102 sayılı TTK m. 780'den 823'e kadar sevk edilen maddelerinde, 5941 Sayılı Çek Kanununda ve Karekodlu Çek örneğinde olduğu gibi çok sayıda ikincil düzenlemeye konu edilmiştir. TTK m. 818 gereği poliçeye dair bazı düzenlemeler de çeke uygulanmaktadır. Çekin hukuki niteliği ve ekonomik yönü hakkında detaylı açıklamalar için bkz. Abuzer Kendigelen, *Çek Hukuku* (İstanbul: XII Levha Yayınları, 2019), 7- 18.

yaygınlığıdır.[10] Sadece çekle sınırlı kalınması halinde; bu durum bonoya olan ihtiyacı ve ilgiyi artıracak, kayıt dışılık gereksinimi bonoya odaklanacaktır. Bunu öngören kanun koyucu bonoyu da çekle aynı veya benzer kurallara dâhil ederek elektronikleştirme gereği duymuştur. Kanun teklifinin dayandığı gerekçeler bu perspektiften bakılarak, mevzuatın teknoloji ile uyumunun sağlanması, güvenin temini, sahteciliğin önlenmesi, kayıt dışılığın önüne geçilmesi, tedavülün kayıt altına alınması sayesinde ödeme ve kredi fonksiyonlarının temin edilmesi şeklinde ifade edilebilir. Burada, hukuki nitelik bakımından, yepyeni bir çek ve bonodan bahsetmemekteyiz. Daha ziyade, klasik kambiyo senetleri olan çek ve bononun; teknolojinin nimetlerinden yararlanılarak elektronik ortamda düzenlenebilen, devredilebilen ve ödenen bir şekilde yorumlanması söz konusu olmaktadır.[11] Teklifte yer alan, aşağıda incelediğimiz, kimi hükümler dikkate alındığında, elbette klasik anlamdaki çek ve bonoya ana hatlarıyla benzemekle beraber, diğer yandan, elektronik çek ve bononun birçok yönüyle tamamen yeni finansal teknoloji enstrümanları olduklarının söylenmesi de mümkündür.

---

[10] Bono, TTK. m.776-779'da düzenlenmiştir. Ticaret hayatımızda uygulamasına en sık rastlanan kambiyo senedidir. Buna mukabil kanun koyucu, bonoya sadece dört madde sevk etmiştir. Aynı durum elektronik çek ve bono için yapılan kanun çalışmasında da gözlemlenmekte olup yapılan çalışmanın ağırlık noktasını çek oluşturmaktadır. TTK'da bono için yer verilen dört maddede bonoya dair özel hükümler yer almış ve bonoya da uygulanacak olan poliçe hükümlerine atıf yapılmıştır. Bu durum elektronik bono için de zaman zaman gözlemlenmektedir.

[11] Bkz. Elektronik Çek ve Kanunu Teklif Genel Gerekçesi (Kısaca: Teklif Genel Gerekçesi); Ayşegül Karabıyık, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-2," *Muhasebe ve Finansman Dergisi*, no. 39 (Temmuz 2008): 156ff.

A. Teknoloji ile Uyumun Sağlanması

Teknolojideki gelişmeler, elektronik para, kripto para, blok zinciri, dijital mutabakat sistemleri gibi yeni ürün ve servisler ortaya çıkarmakta, bazen de mevcut bir ürün veya servisi dijitalleştirerek dönüştürmektedir. Özellikle Almanya'da yapılan çalışmalar ve kripto varlıklar alanında rüştünü ispat eden blok zincir teknolojisi elektronik çek ve bono için uygun bir teknolojik altyapıdır[12]. Her yeni teknolojinin mevzuat üzerinde, bu yeni teknolojilere dair yeni yasal düzenlemeler yapılması yahut dönüşüme uğrayan ürün ve servislere dair mevzuat değişikliklerine gidilmesi şeklinde etkisi olmaktadır.[13] Hem Dünya'da hem de ülkemizde bu şekilde, son yıllarda sayıları giderek artan pek çok mevzuat çalışması yapılmıştır. Böylece teknolojik gelişmeleri esas alan, piyasa ihtiyaçlarını karşılayan hukuk kuralları oluşturulmaktadır. 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun[14] ve Elektronik Ticaretin Düzenlenmesi Hakkında Kanun[15] bunlara örnek gösterilebilir. Teknoloji ile uyumlu olan bu yeni yasalar yeni ürün ve servislerin kullanımını kolaylaştırmakta ve bunları öne çıkartmaktadır. Finansal ürün ve servisler, bu şekilde dijital ve yasal bir dönüşüm yaşarken, çek ve bononun bununla uyumlu olmaması, bu durumdan etkilenmemesi mümkün değildir. En klasik kredi ve ödeme araçları olan çek ve bononun, reel sektörün birbirini fonlaması açısından taşıdıkları önem ve fayda dikkate alınarak, uygulamada yaşanan sakıncalardan arındırılarak teknolojiyle uyumlu bir şekilde yeniden ele

12 Atakan, "Kıymetli Evrak," 547.

13 Serdar Demirci, "Türk Hukukunda Elektronik Çeke Doğru, Dünü̈ ve Bugünüyle Çek," *Ankara Barosu Dergisi* 78, no. 3 (2020): 3-4.

14 Kabul Tarihi: 20.06.2013, RG. 27.06.2013, S. 28690.

15 Kabul Tarihi: 23.10.2014, RG. 05.11.2014, S. 29166.

alınması açık bir ihtiyaçtır.[16] Aslında bu ihtiyaç ilk etapta daha ziyade çek için gündeme gelmiştir. Zira çek, piyasada hacim bakımından bankacılık sektörünün piyasaya sağladığı toplam ticari kredi büyüklüğünün yaklaşık üçte birine denktir. Ortalama 20 milyon çekin ibrazının söz konusu olduğu ülkemiz piyasasında, ciro ile beraber bu çeklerin birden fazla ticari işin finansmanına katkı sağladığı görülmektedir.[17] Çek için elektronik çek enstrümanını yasal olarak düzenleme gayesiyle başlayan çalışmalara daha sonra önemine ve yaygınlığına binaen bono da dahil edilmiştir. Böylece çekin ve bononun yoğun ve yaygın kullanıldığı ticaret hayatında, işlem güvenliğinin teknolojiden yararlanılarak sağlanması ve bu ödeme ve kredi araçlarının fonksiyonlarını etkin şekilde yerine getirmesi amacıyla, uzun zamandır devam eden çalışmaların ışığında bir yasa teklifi hazırlandığı görülmektedir.

---

16 Baytemür, "Elektronik Kambiyo," 81; Teklif Genel Gerekçesinde, öncelikli bir gerekçe olarak, uluslararası mevzuatla uyumun sağlanması gösterilmektedir. Ancak bununla kastedilen çok net değildir. Zira, Kanada, Amerika Birleşik Devletleri ve Hindistan gibi bazı ülkelerde elektronik çekin yasal olarak düzenlendiği görülmekte, uygulamanın ilerlediği tespit edilmektedir. Bunların dışında uluslararası seviyede elektronik çek ve bononun yaygın bir şekilde düzenlendiğini ve kullanıldığını söylemek şu an için mümkün görünmemektedir.

17 Çek ve bono reel sektörde fonlama etkisine sahip olan senetlerdir. Çekin bir kredi aracı olmadığı baskın görüşüne mukabil ülkemizde kredi pazarının üçte biri çeklerden oluşmaktadır. Çek Kanunu Geçici 3. maddenin de etkisiyle, çekin uygulamada vadeye tabi tutulan, kredi aracı etkisi gösteren bir kambiyo senedi olduğunu iddia edenlerin sayısı artmıştır. Ülkemizde 20 milyonun üzerinde çek ibrazı söz konusudur. Bu çekler, ciro ile birlikte birden fazla ticari işlemin finanse edilmesinde kullanılmaktadır. Bu sebeple, son yıllarda çekin uğradığı güven kaybının ortadan kaldırılması ve bononun güvenli bir şekilde kullanılmasını sağlamak ulusal ekonomi bakımından önem arz etmektedir.

B. Güvenin Temini, Sahteciliğin Önlenmesi

Ticaret hayatında, çek ve bonoda sahtecilikle, sahte imza, yetkisiz temsil gibi durumlarla sık sık karşılaşılmaktadır. Bu durum çeke ve bonoya olan güveni sarsmaktadır. Bu noktada, güveni arttırmak için karekodlu çek[18] gibi teknolojik çözümlere[19] başvurulmuştur.[20] Teknoloji, sahteciliğin engellenmesi, çek ve bonoya güvenin arttırılmasında önemli bir katkı sağlayabilir.[21] Böylece, elektronik çek ve bono ile aynı zamanda ödemelerde kayıt dışılığın önüne geçilmesi ve teknolojik gelişmeler kapsamında çek ve bononun tedavül sürecinin tüm ilgililer tarafından takip edilebilmesi mümkün olacaktır. Bu, çek ve bono aracılığıyla yapılan kredilendirme mekanizmasının etkin şekilde çalışmasına katkı sağlayacak bir potansiyel anlamına gelmektedir.[22]

---

18 09.08.2016 tarihinde Resmî Gazetede yayımlanarak yürürlüğe giren 15.07.2016 tarihli ve 6728 Sayılı Yatırım Ortamının İyileştirilmesi Amacıyla Bazı Kanunlarda Değişiklik Yapılmasına İlişkin Kanun (Bkz. RG. 09.08.2016, S. 29796) TTK'ya karekodlu çek düzenlemesini eklemiştir. Buna göre, 6728 sayılı Kanunun m. 70 hükmüyle TTK m. 780'e yapılan ekleme ile çekin şekil şartları yönünden yeni düzenlemeler getirilmiştir. Bu yenilikler çekin seri numarası ve karekodun çekte zorunlu şekil şartı olduğudur. Buna göre, çekin seri numarası ve karekodun ancak bankalar tarafından basılan çek yapraklarında yer alacağı; çek sözleşmesi olmadan düzenlenen çekin geçerli olmayacağı açıktır. Öte yandan, yabancı bankalar tarafından basılan çeklere ise istisna getirilmiştir (Bkz. 6728 sayılı Kanun m. 71. maddesi ile değişik TTK. m. 781/4).

19 Bu amaçla başvurulan bir diğer teknolojik tedbir düzenlemesi de çek takas sistemidir. Bu sistem 02.07.2018 tarihinde yürürlüğe giren Çek Takas Faaliyetleri Hakkında Yönetmelik (Bkz. RG. 09.06.2018, S. 30446) ile düzenlenmiştir.

20 Reha Poroy ve Ünal Tekinalp, *Kıymetli Evrak Hukuku Esasları* (İstanbul: Vedat Kitapçılık, 2019), 318-320.

21 Atakan, "Kıymetli Evrak," 549.

22 Teklif Genel Gerekçesinde bu durum şu şekilde ifade edilmiştir: "Güvenin temini ve tercih edilirliğin arttırılması için çek ve bononun elektronik ortamda oluşturulması yoluyla, sahte çek düzenlenmesi, imza taklidi vb.

C. Tedavülün Takip Edilmesi

Çek ve bononun fiziksel olarak tedavülünün takip edilmesi güçlükler arz etmektedir. Bu durum ödemelerde kayıt dışılıkla mücadelede zaaflar ve tereddütler yaratan bir durumdur. Elektronik çek ve bono ile tedavül ve ciro sürecinin adeta adım adım elektronik ortamda izlenebilmesi mümkündür.[23] Bu elektronik izleme elektronik para ve internet bankacılığında hâlihazırda mevcuttur. Böylece, çek ve bononun kayıt dışı ekonomide kullanılmasıyla etkin mücadele için, dijital izleme ve kayıt teknolojileri aracılığıyla kolay ve doğru bir şekilde veri toplanabilecektir.[24] Veri toplama, Elektronik Çek ve Bono Sistemi ve bu Sistemin İşleticisi için hayati önemdedir. Bu sebeple, sisteme entegre olan tüm bankaların, kendi sistemleri kanalıyla gerçekleştirilen elektronik kambiyo taahhüdü, onay ve ibraz işlemleri ile kendi kayıtlarında bulunan ve sistemde işlem yapan kişilerin, daha önce sisteme tanımladıkları veriler ile bunlarda meydana gelen değişiklikleri ve güncel iletişim bilgilerini işletici kuruluşa iletmekle, işleticinin ise bunları sürekli güncellemek ve periyodik şekilde Hazine Bakanlığına raporlamakla yükümlü tutulmaları söz konusudur.[25]

---

dolandırıcılıklar ile çek ve bononun çalınması, kaybedilmesi gibi durumlar engellenebilecektir."

23 Elektronik çek ve bononun sadece elektronik ortamda düzenlenen ve ciro edilen senetler olmasından ötürü, düzenleme tarihi ve ciro tarihi, bunların elektronik ortamda yapıldığı andır.

24 Tedavülün takibi, kayıt dışılığın önlenmesi, suçun finansmanı ile mücadele edilmesi, müracaat hakkının etkin kullanılmasının sağlanması gibi amaçlarla, Kanun Teklifi çalışmalarında, hamiline elektronik çekin kabul edilmediğini ifade etmek gerekir. Tıpkı hamiline senetler için getirilen bildirim mükellefiyetinde olduğu gibi burada da merkezi bir kayıt takip sistemiyle bu senetlerle yapılan işlemlerin takip edileceği, yani kayıt altına alınmasının hedeflendiği anlaşılmaktadır.

25 Sistem işleticisinin Karekodlu Çekler için aynı yönde bir diğer raporlama yükümlülüğü için bkz. Çeklerde Karekod Uygulamasına İlişkin Tebliğ m. 11/3.

Tedavülün elektronik olarak kaydedilmesi ve takip edilmesi, lehine çek ve bono düzenlenen ve ciro edilenler ile bunlar lehine aval verecek olanların, bu çek ve bono ile kendisinden önce kambiyo taahhüdü altına girenlerin geçmiş ödeme bilgilerine çok kolay şekilde erişebilmeleri, çeki ya da bonoyu kabul edip etmeme kararını sağlıklı şekilde vermelerine de yardımcı olması beklenen bir olanaktır.[26] Elektronik tedavül ve takibin, ödemelerin etkin ve düzenli şekilde yapılması halinde, çek ve bononun ödeme ve kredi fonksiyonlarının etkin şekilde çalışmasını desteklemesi olasıdır. Yine, elektronik çek ve bononun ciro edilebilmesi için fiziken teslim zorunluluğunun bulunmaması da taraflara gerek maliyet gerekse zaman tasarrufu sağlayacaktır.[27] Öte yandan, bu durum beraberinde

[26] Bkz. Teklif Genel Gerekçesi.

[27] Elektronik çek ve bononun ikincil bir faydası olaraksa, fiziksel çek ve bono için kullanılan kağıtların üretim, saklama ve taşıma maliyetleri gösterilmektedir. Uygulamada, bankalar çek yapraklarının basımı için özel olarak üretilen kâğıtları yurt dışından yüksek bedellerle ithal edilmektedir. Bu kağıtlar kullanılarak toplu şekilde basılan çek koçanları bankaların stoklarında saklanmaktadır. Elektronik çekin, çek koçanı basılması gerekliliğini ve stok maliyetini ortadan kaldırması umulmaktadır. Yine bankalar tarafından tahsil ya da teminata alınan çeklerin şubeler, bölge müdürlükleri ve genel müdürlüklere taşınmasına veya buralarda saklanmasına gerek kalmayacaktır. Bu durumun bankalar tarafından, müşterilere yüklenen maliyetleri ortadan kaldırması tali bir fayda olarak dikkate alınabilir. Bu hedefler ve araçlar ile stok, basım, taşıma ve saklama maliyetleri gibi bazı maliyetlerden çek ve bononun dijitalleştirilmesiyle sakınılması öngörülmektedir. Gerçekten de bu yan maliyetler çek hesap sahiplerine ve banka müşterilerine yansıtılan maliyetler olarak karşımıza çıkmaktadır. Lakin bu maliyetlerin yerine Teklifte öngörülen sistem işleticisinin, işletim hizmetleri dolayısıyla birtakım maliyetleri ve ücretleri sistemin kullanıcılarına yansıtması olasılığı söz konusudur. Bu sistem işleticisi ücretleri ise yeni düzenlemeyle bertaraf edileceği düşünülen maliyetlerin yerini almaya adaydır. Teklifte sistem işleticisi olarak 19.10.2005 tarihli ve 5411 sayılı Bankacılık Kanunu uyarınca kurulan Türkiye Bankalar Birliği Risk Merkezi kabul edilmiştir. Elektronik Çek ve Bono Sistemini kurma ve işletme yükümlülüğü sistem işleticisindedir.

elektronik ortamda finansal veri mahremiyeti tartışmalarını getirecektir.

Özellikle çeklerde, çek defteri çek hesabı sahibine teslim edildikten sonra çek yaprakları ödeme, tahsil ya da teminata verme amacıyla bankalara gelmediği sürece, keşidecinin kaç adet çek keşide ettiğini tespit etmek mümkün değildir. Bir diğer önemli sorun ise çek hesabı sahibi hakkında, bir mahkeme tarafından çek düzenleme ve çek hesabı açma yasağı kararı verildiği hallerde, hakkında yasaklılık kararı verilen kişinin elindeki boş çek yapraklarını bankaya iade yükümlülüğü söz konusu olmasına karşın, kişiyi bunları iade etmeye zorlayan bir mekanizmanın bulunmamasıdır. Çek yasaklısı birinin buna rağmen elindeki çek yapraklarını keşide etmeye devam etmesi fiilen mümkündür. Uygulamada da bu tür örneklerle karşılaşılmaktadır. Bu durum ise hem keşideci, hem lehtar ve hem de cirantalar bakımından ödeme, güven, takip işlemleri bakımından zorluklara, kayıplara yol açmaktadır.[28] Bu somut sorun Kanun Teklifi çalışmalarında doğrudan dikkate alınmıştır. Böylece, Kanun Teklifi ile kurulması önerilen Elektronik Çek ve Bono Sistemi[29] üzerinden, keşidecinin tüm çeklerinin sayı ve

[28] Poroy ve Tekinalp, "Kıymetli Evrak Hukuku Esasları," 389 ve 396ff.

[29] Elektronik Çek ve Bono Sistemi, bu iki kambiyo senedine yönelik olarak beklenen yasal düzenlemede ele alınacak olan düzenleme, ciro, aval, ödeme gibi işlemlerin gerçekleştirilmesi amacıyla kurulacak olan banka sistemlerinin ve ilgili diğer sistemlerin birbirleri ile ilişkisini mümkün kılacak olan ana sistemi ifade edecektir. Elektronik çek ve bono düzenlenmesi, ciro edilmesi vb. bütün işlemlerin mutlaka bir banka üzerinden yapılması zorunlu tutulacaktır. Elektronik Çek ve Bono Sisteminin, 5411 sayılı Kanunun ek 1. maddesi hükmü uyarınca kurulan Türkiye Bankalar Birliği Risk Merkezi tarafından kurulması ve işletilmesi beklenmektedir. Bilindiği gibi, Türkiye Bankalar Birliği Risk Merkezi, Kanunlarla kendisine verilen benzer yetkileri Hazine ve Maliye Bakanlığının görüşü ve Bakanlığın onayı ile 5411 sayılı Kanunun ek 1.

tutarının, lehtar ve cirantalarca görülebilmesi, keşidecinin bir çeki karşılıksız kaldığında bankaların o kişinin henüz keşide etmediği diğer tüm çek kayıtlarını anında iptal etmelerine olanak sağlanması, bu suretle alacaklıların tahsilat risklerinin azaltılması hedeflenmektedir.[30]

Çekin elektronik tedavülü, müracaat hakkının kullanılmasını tam ve etkin şekilde desteklemesi yönüyle de önem arz etmektedir. Zira bir çekin hamilinin, müracaat borçlularının tamamını tespit etmesi ve bu kişilere erişerek alacağını tahsil etmesi uygulamada hiç de kolay değildir.[31] Kanun Teklifinde, Elektronik Çek ve Bono Sistemi üzerinden, ciro silsilesine girenlerin kayıt altına alınması yoluyla müracaat borçlularına ulaşmayı kolaylaştırma fonksiyonu önerilmektedir.[32] Tabi bu öneri, veri kayıt takip sistemi, diğer yanıyla başka bir dijital–finansal veri mahremiyeti sorunu ve tartışması anlamına gelmektedir.

Teklifte bononun tedavül güvenliği içinse karekod uygulamasına başlanılması önerilmektedir. Karekodlu bononun uygulamasında, alacaklıya, düzenleyenin geçmiş ödeme

maddesinin 11. fıkrası uyarınca kurulmuş şirketler veya 5941 sayılı Kanunun 8. maddesi uyarınca yetkilendirilmiş kuruluş aracılığıyla kullanabilmektedir. Buna göre, elektronik çek ve bono hizmeti veren bankaların, sistemlerini Elektronik Çek ve Bono Sistemine entegre etmeleri zorunlu olacaktır. Ancak bir bankanın elektronik çek ve bono hizmeti vermesi zorunluluğu öngörülmemektedir. İşletici kuruluşun sistemin kullanımını kolaylaştıracak ve güvenliği artıracak geliştirmeleri zaman içinde yapması olasıdır ve açıkçası gereklidir. Bunların arasında öncelikle, işletici kuruluşun, lehine çek, bono düzenlenen ve ciro edilen kişiler ile bunlar lehine aval verenlerin erişimine sunacağı veri ve bilgileri kullanarak ilave istatistiki bilgiler içeren servis ve ürünler geliştirmesi, sayılanlara sunması orta vadedeki hedefleri arasında sayılabilir.

30 Bkz. Teklifin Genel Gerekçesi ve Madde Gerekçeleri.

31 Hayri Bozgeyik, *Poliçede Müracaat Hakkı* (Ankara: Seçkin Yayıncılık, 2003), 154; Dursun, *Karşılıksız Çek Keşide Etmenin*, 49.

32 Aynı sayede imza itirazı, çek ve bononun rıza hilafına elden çıkması yönündeki ihtilafların da azalması umulmaktadır.

performansına erişme ve bonoyu kabul edip etmeme kararını bu bilgi ışığında verme olanağının karekodlu çekte olduğu şekilde sunulması, böylece bonoya olan güvenin pekiştirilmesi planlanmaktadır.[33]

II. ELEKTRONİK ÇEK VE BONO İÇİN ÖNGÖRÜLEN DÜZENLEMELER

A. Genel Olarak

Elektronik çek ve bonoya duyulan ekonomik ve hukuki ihtiyaca istinaden hazırlanan Kanun Teklifinin genel dayanak ve gerekçelerini göz önünde bulundurduğumuzda, Kanun Teklifi ile öngörülen düzenlemelerin kapsamı, ana hatlarıyla ortaya çıkmaktadır. Genel gerekçelerin ötesinde maddelerin detayları incelendiğinde ise yapılacak düzenlemelerin ticaret hayatını derinden değiştireceği görülmektedir. Diğer bir ifadeyle, çek ve bononun teknolojiyle modernize edilmesi, bu iki klasik kredi ve ödeme aracının karakteristik yapısında kalıcı ve derin tesirler meydana getirecektir.[34] Bu noktada, elektronik ortamda yapılacak düzenleme, ciro, ibraz, ödeme gibi işlemlerde imza,

---

[33] Bonoda karekodun kabul edilmesi ve zorunlu kılınması halinde, bundan önceki karekodsuz bonoların akıbetinin ne olacağının da açıkça düzenlenmesi önem arz eder. Teklifte, belirli bir tarihten (Teklifin kanunlaşması halinde yürürlük tarihi) evvel düzenlenen bonolarda karekod olmamasının bunların geçerliliğini etkilemeyeceği yerinde bir şekilde ifade edilmiş, yine belirli bir tarihten sonra ise karekod olmaksızın düzenlenmesi halinde bono vasfının söz konusu olmayacağı öngörülmüştür. Bu durumun, yasalaşması halinde yürürlük tarihi itibarıyla karekodsuz bono düzenleme yasağı olarak yorumlanması hatalı olmayacaktır. Türkiye'de yerleşik olmayan kişiler tarafından yurt dışında düzenlenen veya düzenlendiği yer gösterilmeyen bonolarda ise karekodun bulunmamasının bir istisna ile bu geçersizliğin haricinde bırakılması söz konusudur.

[34] Öte yandan, Kanun Teklifinde terim birliği noktasında bir kararsızlık veya dikkatsizlik olduğunu gözlemlemekteyiz. Zira Teklifte, elektronik ortamda düzenlenen çek, elektronik düzenlenen çek, elektronik çek gibi birbirinden farklı ibareler kullanılarak birtakım tereddütlere yol açılmaktadır.

ibraz, teşhis gibi işlemlerin mümkün hale getirilmesi ve elektronik ortama uyarlanması gerekmektedir. Bu durum, Türk Borçlar Kanunu, Türk Ticaret Kanunu, HMK, İİK gibi bazı temel kanunlarda değişiklikler yapılmasını gündeme getirecektir.[35]

Bilindiği gibi, Türk Borçlar Kanunu m. 15 ve 16'ya göre kural, imzanın, sahibi tarafından el yazısı ile atılmasıdır. Temel kural elle imza olsa da teknoloji imzayı da elektronikleştirmiş ve kanun koyucu bu sebeple her şeyden evvel imzaya dair teknolojileri dikkate almış ve düzenlemiştir. Kanun koyucu, elektronik imzanın, güvenlik açısından gerekli özelliklerini sağlamak şartıyla, sadece ispat gücü açısından değil, prensip itibariyle tüm sonuçları bakımından elle atılan imza ile aynı hukuki etkiyi doğuracağını kabul ve tanzim etmiştir. Öte yandan, TTK. m. 1526/1 gereği, poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetlerin güvenli elektronik imza ile düzenlenmesine izin verilmemiştir.[36] Bahse konu senetlere ilişkin kabul, aval ve ciro gibi senet üzerinde gerçekleştirilen işlemler de güvenli elektronik imza ile yapılamamaktadır. Bir tek konşimentonun imzasının[37] elle, faksimile baskı, zımba, ıstampa, sembol şeklinde mekanik veya elektronik herhangi bir araçla da atılabileceği TTK. m. 1526/2 ile kabul edilmiştir.[38] Ticaret hayatı ve ticari işlemlerin biçimleri

---

35 Demirci, "Türk Hukukunda," 6-8.

36 TTK. m.1526/1 ile kambiyo senetleriyle makbuz senedi ve varantın elektronik imza ile düzenlenmesini kabul etmemiştir. Bu senetlerin mutlaka ıslak imza ile imzalanmasını geçerlilik şartıdır. Buna karşın, adi senetlerin elektronik imza ile düzenlenebilmesinin önünde bir engel bulunmamakta, adi senetler elektronik imzayla tanzim edilebilmektedir.

37 Ahmet Said Ber, *Elektronik Konişmento* (Ankara: Seçkin Yayıncılık, 2018), 95.

38 Kıymetli evrak, teknolojik gelişmeler ve bu gelişmelerin meydana getirdiği hukuki ve fiili sonuçların ışığında yeniden yorumlanmaya gereksinim duymaktadır. Örneğin, el ile atılan imza başta olmak üzere kıymetli evrakın çeşitli unsur ve uygulamaları reforma açıktır. Bunun en eski ve kabul edilmiş örneği Sermaye Piyasası Kanunu m.13'e dayanan varakasız

değişip elektronikleşirken ticaret araçlarının, ticaret senetlerinin ve para senetlerinin bu değişime uyum sağlamaması mümkün değildir. Detaylarını aşağıda ele alacağımız üzere, gündemdeki Kanun Teklifi ile ana hatlarıyla yapılmak istenen düzenlemeler; sahte çek düzenlenmesinin ve imza taklidinin önüne geçilmesi, dolandırıcılıkların azaltılması, çalınma ve kaybetme hallerinin engellenmesi, haciz ve iptal işlemlerinin basitleştirilmesi[39], tek tip ibraz süresi, elektronik tedavül ve bono bakımından tek vade uygulamasına geçilmesi şeklinde sıralanabilir.

1. Fiziksel Çek ve Bononun Durumu

Elektronik çek ve bononun yasal bakımdan düzenlenmesinden sonra, fiziksel çek ve bononun bundan ne şekilde etkileneceği akla ilk gelen sorulardandır. Acaba bu olası yeni yasal düzenleme, fiziki çek ve bonoyu ortadan kaldıracak mı? Yoksa aynı anda hem fiziksel hem de elektronik türleri olan senetler mi söz konusu olacak? Açıkçası, elektronik çek ve bono yasa ile düzenlendiğinde, bunun fiziksel çeki ve bonoyu hemen ortadan kaldırması, bunların hâlihazırda yaygın şekilde kullanılmakta olmasından ötürü mümkün değildir. Yapılan çalışma incelendiğinde, Kanun Teklifinin, elektronik çek ve

kıymetli evraktır. Varakasız kıymetli evrak, kıymetli evrakın zorunlu senet unsurunda yarattığı istisna ile elektronik çek ve bononun mümkün olmasının yolunu açan öneme sahip bir öncüdür. Bkz. Fırat Öztan, *Kıymetli Evrak Hukuku* (Ankara: Yetkin Yayınları, 1997), 324. Böylece kıymetli evrak senetten bağımsız maddi olmaktan çıkartılan bir kıymet hakkına dönüşmüştür. Ayrıca bkz. Asuman Turanboy, *Varakasız Kıymetli Evrak* (Ankara: Banka ve Ticaret Hukuku Araştırma Enstitüsü, 1998), 42.

39 Elektronik çek ve bononun haczi, dijital bir haciz işlemi olarak alacak haczi vasfında olmak üzere mümkün ve pratik olmalıdır. Bu durumda, Elektronik Çek ve Bono Sisteminde hacze ilişkin bir kayıt konulması mümkün ve yeterli olacaktır. Haczedilmiş bir çek veya bono miktarının, haciz bildiriminden evvel veya sonra şu veya bu şekilde tahsil edilmesi halinde, bu meblağ tahsilatı alan banka tarafından haczi uygulayan icra mercii hesabına aktarılarak haciz dışına çıkartılmasının önüne de kolayca geçilebilir. Haczedilen çek ve bono, ciro ve iptal edilemez.

bonoyu kapsadığı, fiziksel çek ve bonoyu ortadan kaldıran bir düzenleme içermediği, böyle bir hedefinin olmadığı görülmektedir.[40]

Beklenen yeni düzenlemenin kapsamı ve gayesi çek ve bononun elektronik ortamda düzenlenmesi ile ciro edilmeleri, devredilmeleri ve ödenmelerine ilişkin kuralların belirlenmesidir. Bu bakımdan Kanun Teklifi, elektronik ortamda düzenlenen çek ve bonoyla ilgili işlemleri kapsamaktadır. Bu durumda, Türk Ticaret Kanunu ve Çek Kanununun, çek ve bono hakkındaki ilgili düzenlemeleri yürürlüğünü koruyacaktır. Hatta elektronik çek ve bonoya dair yasada hakkında hüküm bulunmayan hallerde TTK ve Çek Kanunu hükümleri kıyasen uygulanacaktır.[41]

Bu noktada üzerinde tereddüt yaşanan, henüz karar verilememiş görünen öncelikli bir diğer konu, belirli bir rakamın üzerindeki çek ve bonoların mutlaka elektronik olarak düzenlenip düzenlenmeyeceğidir. Şu an için bu konuda verilmiş net veya nihai bir karar bulunmamakla beraber, bu ihtimalin yüksek olduğunu, yani elektronik çek ve bono yasalaşırsa belirli bir miktarın üzerindekiler için sadece elektronik olarak düzenlenme şartının konulacağını ön görmekteyiz. Teklifte bu konuda karar verme yetkisinin Cumhurbaşkanlığına tanınmış olması da kanaatimizi pekiştirmektedir. Bu uygulama, hem elektronik çek ve bononun kullanımını yaygınlaştırmaya hem de bir anda değilse bile zamanla fiziksel çek ve bono kullanımını sonlandırmaya yönelik bir geçiş sağlayacaktır. Böylece, fiziksel çek ve bonodan tamamen vazgeçilip geçilmeyeceği sorusu da cevaplanmış olmaktadır. Tekrar etmek gerekirse, geçiş

---

40 Bkz. Teklif Genel Gerekçesi.

41 Örnek vermek gerekirse yapılan Kanun Teklifi defilere dair özel bir düzenleme içermemektedir. Bu durumda, defiler için genel hükümler elektronik çek ve bonoda da kıyasen uygulama alanı bulur. Defiler hakkında detaylı açıklama için bkz. Lerzan Yılmaz, *Kambiyo Senetlerinde Def'iler* (İstanbul: Aristo Yayınevi, 2007).

sürecinden sonra elektronik çek ve bono sistemi ve uygulaması oturduğunda, fiziksel çek ve bono kullanımını önce meblağ bakımından sınırlandırmaya gidilmesi, bundan sonra ise tamamen yasaklama yoluyla fiziksel çek ve bononun mazide kalması olasılığı oldukça yüksektir. Kanun Teklifinin son halinde, sadece belirli bir rakamın altındaki çek ve bononun fiziki olarak kullanımına izin verecek şekilde bu rakamı belirleme yetkisi Cumhurbaşkanlığına tanınarak bu olasılığa işaret edilmektedir. SPK'da yaşanan değişim ve dönüşümün sonucunda borsada işlem gören tüm hisse senetlerinin kaydileştirilerek fiziki hisse senetlerinin kullanımının sona erdiği[42] dikkate alınırsa aynı durumun çek ve bono için de oldukça yüksek bir olasılık olduğu sonucuna varılabilir.

Bu bahiste cevap aranması gereken son soru, elektronikleşen çek veya bononun, daha sonra herhangi bir şekilde tekrar fiziki formda kullanılmasının mümkün olup olmayacağıdır. Teknik olarak bu mümkünse de böyle bir yolun açılması elektronik çek ve bono ile varılmaya çalışılan düzen ve amaçtan sapılması anlamına gelir. Bu sebeple, Kanun Teklifinde yer verildiği üzere, elektronik çek ve bonolar, çıktısı veya görüntüsü alınarak fiziki ortamda kambiyo senedi olarak kullanılamamalıdır.

Teklife göre elektronik çek, seri numarası belirtilerek, fiziken yapılacak başvuruyla bankaya ibraz edilebilir. Bu durumda kimlik doğrulaması yapılacağı ve fiziksel ibraz yahut tedavül söz konusu olmayacağı için bu elektronik çek veya bononun fiziki dönüşüme tabi tutulması olarak yorumlanmamalıdır.

---

42 Mücahit Ünal, *Sermaye Piyasası Araçlarının Kaydileştirilmesi* (Ankara: Adalet Yayınevi, 2011), 76-77.

2. Yeni Kavramlar

Elektronik çek ve bono düzenlemesinin temelini yeni kavramlar ve bunların ne şekilde anlaşılacağına dair düzenlemeler ile tanımlar oluşturacaktır. O sebeple bu yeni kavramların, bunların unsurlarının kısaca ele alınmasında fayda bulunmaktadır.

a. Elektronik Çek ve Bono Kavramları

Hukukumuzda mevcut bir kavramın ve enstrümanın elektronik ortamda keşide edilecek ve kullanılacak olan versiyonuna dair yapılacak yeni düzenleme bakımından temel kavramlar "elektronik çek" ve "elektronik bono"dur. Bir tanıma göre elektronik çek, kağıt çeklerle birlikte yapılandırılan, geliştirilmiş yasal altyapısı ve iş süreçleriyle, benzer bütün elektronik işlemlerin verimliliğini, hızını ve güvenliğini birleştiren yeni bir ödeme aracıdır. Bu anlamda elektronik çek, kağıt olmaksızın, ödemenin sayısal imza ile taahhüt edildiği bir banka ödeme aracı olarak tanımlanabilir.[43] Bu tanım daha ziyade çekin kâğıt olmadan düzenlenmesine ve fonksiyonuna odaklanmıştır. Hukuki bakımdan ise ne elektronik çeki ne de bonoyu yeniden tanımlamaya gerek bulunmadığı akla gelebilir. Buna göre elektronik çek ve bono, bildiğimiz çekin ve bononun teknolojiden yararlanılarak elektronik ortamda düzenlenmesi, devredilmesi, ödenmesi şeklinde ortaya çıkan halidir.[44]

Teklifte elektronik çek ve bono için, yukarıdaki yaklaşımımıza paralel bir şekilde, kısa ve sade tanımlara yer verilmiştir.[45] Buna göre elektronik çek, elektronik ortamda

---

[43] Ayşegül Karabıyık, "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-1," *Muhasebe ve Finansman Dergisi*, no. 38 (Nisan 2008): 81.

[44] Baytemür, "Elektronik Kambiyo," 78.

[45] Yapılan Kanun çalışmasının bir önceki halinde yer verilen elektronik çek tanımı, "fiziken düzenlenmeyen, elektronik kimlik doğrulama veya güvenli elektronik imza yöntemiyle elektronik ortamda çek hesabının

düzenlenen, devredilen ve ödenen çek şeklinde tanımlanmışken, elektronik bono ise elektronik ortamda düzenlenen, devredilen ve ödenen bono olarak tarif edilmiştir. Her iki tanımın ortak özelliği çek veya bonoya tanım bakımından başka bir unsur eklemeksizin bunların elektronik ortamda düzenlenebileceklerini, devir ve ödeme işlemlerine konu edileceklerine işaret edilmekle yetinilmesidir.

Elektronik çekin unsurları belirlenirken esas alınacak hükümler TTK m. 780 ve 5491 sayılı Çek Kanununun 2. maddesidir. Bu maddelerde çek için öngörülen zorunlu unsurlardan, niteliği itibarıyla elektronik çek için zorunlu ve uygun olanların dikkate alınması gerekir. Bu zorunlu unsurlara "Elektronik ibraz başlangıç tarihi" ve "Çek hesap sahibinin güvenli elektronik imzası veya elektronik kimlik doğrulama yöntemiyle oluşturulan kaydı" unsurlarının eklenmesi söz konusudur. Yöntem olarak, elektronik çekin unsurlarının belirlenmesinde bu yaklaşım isabetli olmuştur.[46]

Elektronik bono için ise aynı durum TTK m. 776'da yer bulan zorunlu unsurlardan bu yeni nesil bonoya uygun olanların tespiti ve dikkate alınması şeklindedir. Diğer yandan, elektronik bono banka sistemi aracılığıyla elektronik ortamda düzenlenip, yetkili hamilin banka hesabına ödeneceği için TTK'da bono için yer alan "düzenleme yeri" ve "ödeme yeri" gibi zorunlu unsurlar elektronik bononun unsurlarının arasında yer almayacaktır. Böylece elektronikleşme, bono bakımından

bulunduğu muhatap bankanın sisteminden Elektronik Çek sistemine erişim sağlanarak düzenlenen emre yazılı, tam ciro ile devredilebilen kayıtsız ve şartsız belirli bir bedelin ödenmesi hususunu içeren havaleyi ve elektronik kambiyo senedi" şeklindeydi. Devam eden çalışmalarda bu uzun ve unsurlara odaklanan tanım yerine, kısa bir tanımın tercih edildiği tespit edilmektedir.

46 Karabıyık, "Alternatif Ödeme," 89.

fiziki mekân kayıtlarını kullanmaya olan ihtiyacı sona erdirecektir.[47]

b. Elektronik Çek ve Bono Sistemi

Elektronik Çek ve Bono Sistemi'ni açıklamak gerekirse bu sistemin banka sistemleriyle diğer sistemlerin birbiriyle olan ilişkisini sağlayan bir sistem olarak Bankalar Birliğinin sistem işleticisi pozisyonunda olacağı bir çek ve bono sistemi üzerinden kurgulanması öngörülmekte ve beklenmektedir.[48] EÇBS olarak kısaltabileceğimiz bu sistem, elektronik çek ve bono için yeni düzenlemelerle yapılması mümkün hale gelecek olan tüm kambiyo senedi işlemlerinin gerçekleştirilmesi amacıyla kurulacak olan banka sistemleri ve ilgili diğer sistemlerin birbirleriyle ilişkisini sağlayan bir sistem şeklinde kurgulanacaktır.[49]

Sistem, tedavül ve ciro sürecinin her adımının elektronik ortamda izlenebilmesini mümkün kılmak amacıyla

---

47 Baytemür, "Elektronik Kambiyo," 174.

48 Çotuksöken, "Dijitalleşme," 4: "Bu sistem elektronik çeklerin keşide edilmesi (düzenlenmesi), ciro edilmesi, avali, elektronik ibrazı, iptali, haczi, karşılıksız çıkması ve bunlara ilişkin bütün onaylar ile taslakta düzenlenen tüm işlemlerin gerçekleştirileceği, tüm bankalar ve ortak çek platformu işleticisi nezdinde kurulu sistemleri de içeren bir sistemler bütününü ifade etmektedir."

49 Bu sistemin gerek içereceği veriler ve gerekse sunacağı hizmetler bakımından güvenli şekilde işlemesi son derece önemli bir konumdadır. Buna göre sistemin güvenli şekilde işletilebilmesi için uyulması gereken asgari unsurlar sistemin işlemeye başlamasından evvel belirlenmeli ve uygulanmalıdır. Bu yapılırken, işletici kuruluş tarafından BDDK'nın bankacılık hizmetlerinin sunulduğu sistemlerin güvenliğine dair uyguladığı standartları belirleyen ilgili mevzuatının dikkate alınacağını öngörüyoruz. Günün sonunda, sistemin hem kurulması hem de işletilmesinin sorumluluğu işletici kuruluşta kalacağı için işletici, güvenliğe ilişkin asgari unsurlara uyulmasıyla ve sistemin güvenliği hususunda gerekli önlemleri almakla mükellef kılınacaktır.

öngörülmüştür.[50] Böylece kayıt dışı ekonomiyle etkin mücadele edilebilir, bu amaçla gerek duyulan veriye ulaşılabilir. Öte yandan, uygulamada önemli bir sorun olan lehine çek ve bono düzenlenen ve ciro edilenler ile bunlar lehine aval verecek olanların, bu çek ve bono ile kendisinden önce kambiyo taahhüdü altına girenlerin geçmiş ödeme bilgilerine ulaşamamaları da bu sistem ile çok kolay şekilde çözüme kavuşturulacaktır. Böylece, çeki ya da bonoyu kabul edip etmeme kararı daha sağlıklı bir şekilde verilebilecektir. Tabi tüm bu bireysel faydaların asıl nihai toplu hedefi çek ve bono ile gerçekleştirilen kredi mekanizmasının etkin şekilde çalışması, kredi kartının ve diğer finansal çözümlerin gölgesinde kalan çek ve bononun teknoloji ile donatılarak rekabet gücüne sahip kılınmasıdır.[51] Sistem, açık bankacılık uygulama ve teknolojileriyle de uyumludur.[52]

c. Elektronik İbraz ve Elektronik İbraz Başlangıç Tarihi

Diğer bir yeni kavram, elektronik ibrazdır. Çekin ödemek için muhatap bankaya, 5941 sayılı Çek Kanununun 8/1 hükmü çerçevesinde işletilen çek takas sistemiyle[53] iletilmesi elektronik

---

50 Sistemin bir diğer yasal bileşeni olarak; Açık Bankacılık kavramını da tanımlayan Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik, 15.03.2020 tarihinde Resmî Gazete'de yayımlanarak 01.07.2020 tarihinde yürürlüğe girmiştir.

51 Demirci, "Türk Hukukunda," 38.

52 Bertaç Şakir Şahin ve Barış Cihan Cantürk, "Türkiye'deki Hukuki Altyapı ve Ödeme Hizmetleri Yönergesi 2 Bağlamında API Teknolojisi ve Açık Bankacılık," *Maliye ve Finans Yazıları*, no. 114 (2020), 168-170.

53 Çek Takas Sistemi, 02.07.2018 tarihli Çek Takas Faaliyetleri Hakkında Yönetmelik uyarınca, Takasbank nezdinde yürütülmekte olan takas sistemiyle, fiziki çekler şu anda kullanılıyor olmakla beraber, e-çek sistem altyapısının ilk ve en önemli kısmını oluşturmaktadır.

ibraz olarak kabul edilmektedir.[54] Elektronik ibrazla bağlantılı olarak üzerinde durulması gereken bir diğer kavram ise elektronik ibraz başlangıç tarihidir. Elektronik çek için çek düzenlenirken düzenleyen tarafından belirtilen ve hamilin çeki bankaya ibraz edebileceği en erken tarih elektronik çekin elektronik olarak ibraz işlemini yapmaya başlayabileceği ilk andır. Buna göre, hamil söz konusu çeki, düzenleyen tarafından çek tanzim edilirken belirtilen tarihten daha evvel bankaya ibraz edemeyecektir. Bu durumda, aslında yeni bir tip elektronik vadeli senetten bahsetmek mümkündür. Diğer bir görüşe göre ise çekin bu şekilde elektronik ortamda, elektronik ibraz başlangıç tarihine tabi tutulması, ileri tarihli çek düzenlenememesi demektir.[55]

Elektronik çekte ibraz süresi, elektronik ibraz başlangıç tarihini takip eden 10 gün olarak öngörülmektedir. Elektronik ibraz süresini ise düzenleyen belirlemektedir. Bu halde düzenleyenin hangi tarihten itibaren 10 gün içinde ödeme yapacağını belirleyeceği şekilde bir vade oluşturması dolaylı da olsa mümkün olabilmektedir.

d. Onay ve Teslim

Elektronik kambiyo taahhüdü[56] yapılması ciro ve devir işlemlerini kapsarken, Teklifte karşımıza çıkan bir diğer kavram "Onay"dır. Onay, çek ve bononun lehtar tarafından veya ciro

---

[54] Karabıyık, "Alternatif Ödeme," 83; Yürürlükteki düzenlemeye göre ve Kanun Teklifinden evvel elektronik ortamda düzenlenmesi halinde bunun çekte ileri tarihli çek sorununu sona erdireceği hakkında bkz. Mehmet Bahtiyar, "5941 Sayılı Çek Kanunu Açısından İleri Tarihli Çek," *Kadir Has Üniversitesi Hukuk Fakültesi Dergisi* 1, no. 2 (2013): 53.

[55] Bahtiyar, "5941 Sayılı," 54.

[56] Teklife göre, çek ve bononun elektronik ortamda düzenlenmesi, ciro edilmesi ve aval verilmesi elektronik kambiyo taahhüdü işlemlerini oluşturur.

edilen tarafından elektronik ortamda teslim alınmasını ifade etmektedir.[57]

Öngörülen sistem ve işlem sırasına göre; düzenleyen, çeki elektronik ortamda tanzim ettiğinde bu çek ancak lehtar tarafından onaylanmak kaydıyla zilyetlik lehtarın kendisine geçer. Bu şekilde çek düzenlendiği tarihten itibaren hüküm doğurmaya başlar. Aynı durum ciro bakımından da söz konusudur. Böylece fiziki çek ve bonodan farklı olarak ciro alan veya devir alan iradesini onay ile aktif bir irade şeklinde göstermektedir.[58]

B. İbraz

Kanun Teklifinde, çek bakımından 10 günlük tek bir ibraz süresi, bono bakımından ise tek bir vade olarak belirli vade öngörülmektedir. Bu durumun sebebi çek ve bononun kullanımını basitleştirmektir.[59] Bu düzenleme yapılırken her iki senedin hem kredi hem de ödeme fonksiyonları göz önünde tutulmuştur.

Elektronik ortamda keşide, saklama, ödeme gibi sebeplerle fiziksel çek veya bonoda olduğu gibi çok sayıda farklı ibraz süresine veya vadeye gereksinim duyulmayacaktır. Tek vade tipi ve bir adet kısa ibraz süresinin benimsenmesi, çekin elektronikleştirilmesi yaklaşımıyla ve dayanak teknolojiyle uyumlu ve makul bir düzenlemedir.

İbraz süresinin, klasik anlamdaki ibraz süreleri arasında en kısa olan sürenin, tek süre olarak belirlenmesi çekin ödeme aracı karakterinin ön planda tutulduğunu işaret ederken bono için de

---

57 Elektronik zilyetliğin şartları için bkz. Ahmet Said Ber, "Elektronik Olarak Devredilebilir Kayıtlara İlişkin UNCITRAL Model Kanunu (Çeviri), m. 10 ve 11," *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi* 1, no. 2 (Aralık 2019): 449.

58 Baytemür, "Elektronik Kambiyo," 133, 140 ve 195.

59 Bkz. Kanun Teklifi Genel Gerekçesi.

bu fonksiyonun ağırlık kazanacağını söylemek mümkündür. İbraz anında, tıpkı fiziki çekte olduğu gibi, çek hesabında yeterli karşılığın bulunması halinde muhatap banka tarafından hamil hesabına çek bedeli aktarılacaktır.[60] Yani çek ve bononun kaydî araçlar olmasında olduğu gibi bunların ödeme işlemleri de kayden yapılacaktır. Kayden ödemenin yerine fiziken ödemenin mümkün olup olmadığına dair Kanun Teklifinde açık bir hüküm bulunmamaktadır. Öyleyse, açıkça yazılmasa ve kayden ödeme esas ödeme şekli olsa bile lehtar, isterse, en azından aksine bir hüküm konulmadıkça, ödemeyi kayden veya fiziken talep edebilir.

C. Etkin ve Kolay İptal Mekanizması

Elektronik çek ve bononun ciro edilebilmesi için fiziken teslim şartına tabi olmaktan çıkartılması bir diğer önemli yeniliktir. Yukarıda değindiğimiz gibi, fiziki çeklerde, çek defteri çek hesabı sahibine teslim edildikten sonra çek yaprakları ödeme, tahsil ve teminata verme amacıyla bankalara gelmediği sürece hangi çek yaprağının keşide edildiğinin bilinmemesi bir problem olarak tespit edilmektedir. Bu durumun yarattığı risklerin önüne elektronik kayıt ve takip sistemiyle geçilebilir. Nitekim elektronik çek ile kaç çek yaprağının ne zaman düzenlendiğinin, keşide edildiğinin ve kimde bulunduğunun kolayca takip edilebilmesinin hedeflendiğini görmekteyiz.[61]

Birden fazla çek yaprağına sahip kullanıcının bir çekinin ödenmemesi halinde geri kalan çeklerin iade edilmesine yönelik taleplere riayet etmemesi olası ve riskli bir durumdur. Aksine bu durumdaki kişinin geriye kalan çek yapraklarını keşide edip tedavüle sokması birçok kişi ve kurum için çığ gibi büyüyen sorunlara yol açabilmektedir. Oysa elektronik olarak düzenlenen ve takip edilen bir çekin ödenmemesi durumunda, geri kalan çekler bakımından bankanın devreye girip söz konusu

60 Baytemür, "Elektronik Kambiyo," 175.

61 Demirci, "Türk Hukukunda," 39.

çekleri iptal edip kullanımlarını engellemesi teknik olarak mümkündür. Bu iptal hukuki değil teknik bir iptaldir. Bu iptal işlemiyle, çek yasağının etkin bir biçimde uygulanması mümkün olabilir.

Teklifte başka bir iptal hali daha öngörülmüştür. Buna göre, elektronik çekin ibraz edilene kadar hamil tarafından; elektronik bononun ise bedelin tamamı ödeninceye veya tahsil edilinceye kadar hamil tarafından iptal edilebilmesi önerilmektedir. Çek ve bononun bu şekilde iptal edildiği hallerde, bu durum, Elektronik Çek ve Bono Sistemi üzerinden düzenleyene, cirantalara ve aval verenlere iletilerek, şeffaflık ve bilgilendirmede teknik altyapıdan istifade edilmesi, yerinde ve doğru bir uygulama olarak, ödeme planlaması ve kredilendirme işlevleri bakımından fayda sağlayacaktır.[62]

D. Müracaat Hakkının Kullanılmasında Kolaylık

Uygulamadaki bir diğer güçlük müracaat hakkının kullanılmasında yaşanan zorluklardır. Zira fiziki kambiyo senetlerinde müteselsil sorumluların, yani müracaat hakkı kapsamındaki müracaat borçlularının tamamının yetkili hamil tarafından saptanması, bu kişilere ulaşılıp ödeme talep edilmesi ve takip işlemlerinin yapılması birtakım güçlükler arz etmektedir. Bu güçlüklerin önüne elektronik sistemle geçilebilir. Bu sistemle kambiyo taahhüdünde bulunanların, fiziki kambiyo senetlerindekinin aksine, imza itirazında bulunmalarına imkân bulunmamaktadır. Senedin rıza hilafına elinden çıktığına yönelik itirazlar da sistem kayıtları ve elektronik imza kullanımıyla mümkün olmayacaktır. Bu iki çözümün sağlayacağı katkıyla müracaat hakkının daha etkin ve başarılı şekilde kullanılması mümkün olabilir. Bono bakımındansa karekodlu bononun, elektronik çek gibi, şimdi olmasa da bir süre sonra zorunlu hale getirileceği öngörülmektedir. Bunun, belirli

[62] Karabıyık, "Alternatif Ödeme-2," 165.

bir tarihten sonra belirli bir rakamın üzerindeki bonolar için mutlaka karekodla düzenlenme şartının kabul edilmesi veya meblağ sınırı olmaksızın sadece karekod şartına tabi olarak bononun düzenlenebilmesi şeklinde olması mümkündür. Böylece, bono bakımından belirli bir tarihte vade şartına tabi tutulan elektronik bono karşısında diğer bono türlerinin ve vadelerinin önemini ve varlığını kaybedeceği öngörülmektedir.[63] Tek vade, karekod gibi unsurlar bono bakımından müracaat hakkının etkin şekilde kullanılmasına katkıda bulunacaktır.[64]

E. Elektronik Çek ve Bononun Düzenlenmesi, İmza, Ciro, Ödeme

1. Elektronik Çek ve Bononun Düzenlenmesi

Kabul edilmesi halinde elektronik çekin ve bononun tamamen elektronik ortamda üretilebilen ve kullanılabilecek senetler olması sebebiyle ancak ve sadece bir bankanın sistemi üzerinden düzenlenmesi mümkün olabilecektir. Bu sistemde,

---

63 Teklifte yer alan bir diğer hükme göre, kambiyo mevzuatı saklı kalmak kaydıyla, Türk lirası ve yabancı para cinsi üzerinden düzenlenecek çek ve bonolara elektronik ortamda düzenlenme zorunluluğu getirmeye, elektronik ortamda düzenlenmesi zorunlu olan çek ve bonoların tutarlarını belirlemeye, bu tutarları artırma ve azaltmaya Cumhurbaşkanı yetkili kılınmaktadır. Aynı hükme göre, Cumhurbaşkanınca belirlenen tutarların üzerinde bir bedelle elektronik ortam dışında düzenlenen çek ve bonolar, kıymetli evrak vasfını kazanamaz. 5411 sayılı Kanun uyarınca Türkiye'de faaliyet göstermeyen yurt dışında kurulu bankalarca bastırılan çekler ile yabancı ülke mevzuatı uyarınca yurt dışında düzenlenen bonolar ise bu hükümden istisnadır. Söz konusu düzenleme önerisi, çeklerin elektronikleşmesinin zorunlu kılınabileceğini, bunun meblağla belirlenebileceğini öngörmektedir. Ancak yabancı banklarca bastırılan çeklerin bu kuralların dışında kalması kredibilite rekabetinde bir dezavantaj oluşturma riskine yol açmamalı, meblağa dair olası düzenlemede bu husus ve piyasa verileri dikkate alınmalıdır.

64 Yürürlükteki düzenlemeye göre bankanın çeki elektronik ortamda düzenlemesi ihtimalinde hamilin müracaat hakkını kullanamayacağına dair bkz. Ülgen et. al., *Kıymetli Evrak Hukuku*, 280.

çek hesabı sahibinin talebiyle, banka tarafından sınırlı sayıda çek sayfasının veya bonoyu düzenleyenin talebiyle banka sisteminde elektronik bononun, kaydi bir şekilde oluşturulması; tedavül, takip ve iade yahut iptal işlemlerini mümkün kılacak ve kolaylaştıracaktır. Böylece, ilgililerin, sistemde düzenlenen çeki ve bonoyu, bunların sayısını ve miktarını görmeleri, ödeme için gerekli karşılığı ayırmaları mümkün olacaktır.

Elektronik Çek ve Bono Sistemi'nde dikkat çeken bir diğer düzenleme ve kavram ise lehtarın adına düzenlenen çeke veya bonoya onay vermesidir.[65] Elektronik sistemde bu onay verme, fiziki çekteki ve bonodaki zilyetliği devralmaya benzetilebilir. Onay verilmesi ister istemez bir süreye bağlanmak durumundadır. Bunun için çekte en geç elektronik ibraz başlangıç tarihine ve bonoda vadeye[66] kadar onay verilebilir. Zira bu tarihlerden evvel bu senetler ibraz olunmayacağı, ödenmeyeceği için onayın pratik bakımdan etkisi ancak bu andan itibaren başlayacaktır. Onayla beraber çek ve bono, düzenlendikleri andan itibaren hüküm doğurmaktadır. Onay, bunların hukuki etkisini başlatan bir ön şart değildir.[67] Hem düzenleme hem de onay elektronik ortamda yapılacak işlemler olup, bunların elektronik kayıtları da ispat hukuku bakımından

---

65 Elektronik ortamda çek ve bonoya dair yapılacak işlemlerin, unsurları bakımından TTK'ya uygunluğunun temini için lehine çek düzenlenen ve ciro edilenler ile aval verenler; çekte elektronik ibraz süresinin sonuna kadar, bonoda ise vadeye kadar, çek hesabı sahibinin, kendisinden önceki cirantaların ve aval verenlerin TTK'nın 776 ve 780. maddelerinin ikinci fıkraları uyarınca ulaşılan bilgilerine bunların rızası olmaksızın erişim sağlayabilmesi öngörülmektedir. Bu düzenlemenin KVKK açısından çeşitli eleştirilere yol açacağı, veri koruma hukukunda büyük bir istisna olan bankacılık uygulamalarının kapsamının genişletilmesine yol açacağı görüşündeyiz.

66 Bankalar Birliğinin teklifine ve Bakanlığın Kanun Teklifine göre elektronik bono, sadece belirli bir günde ödenmek üzere düzenlenebilir. Vade, gün, ay ve yıl şeklinde açıkça belirtilir.

67 Baytemür, "Elektronik Kambiyo," 195.

yeni tür dijital delillerdir. Üzerinde çalışılan sisteme göre şayet henüz lehtar tarafından onaylanmamış ise düzenleyen, çeki veya bonoyu düzenleme tarihinden üç gün geçtikten sonra değiştirebilecek veya geri alabilecektir. Geri alınan veya elektronik ibraz başlangıç tarihine kadar onaylanmayan çek ve bono düzenlenmemiş kabul edilecektir. Onay, çekin veya bonoyla ödemenin lehtar tarafından kabulünü sağlayan bir işlem olduğu gibi, onay anından itibaren elektronik çek ve bono değiştirilemezlik özelliği kazanmaktadır.

2. Elektronik İmza

Bilindiği üzere, TTK. m. 1526/1 uyarınca poliçe, bono, çek, makbuz senedi, varant ve kambiyo senetlerine benzeyen senetlerin güvenli elektronik imza ile düzenlemesine izin verilmemiştir. Ayrıca, bu senetlere ilişkin kabul, aval ve ciro gibi senet üzerinde gerçekleştirilen işlemler de güvenli elektronik imza ile yapılamamaktadır.[68] Bu sebeple, elektronik çek ve bonoda imza meselesi ilk akla gelen ve nasıl düzenleneceği merak edilen konuların başında yer almaktadır. Teklifte, elektronik çek ve bonoda, 5070 sayılı Elektronik İmza Kanunu'nda tanımlanan güvenli elektronik imzanın veya elektronik kimlik doğrulama yöntemlerinin kullanılabilmesi öngörülmektedir. Yani Teklif, TTK'nın çek ve bono bakımından elektronik imza ile düzenlenememe kuralını değiştirmektedir.[69]

---

[68] Atakan, "Kıymetli Evrak," 544.

[69] Elektronik imzayla ve hatta uzaktan kimlik doğrulama yöntemleri ile çek ve bono keşide edilmesine dair ortaya konan cesur yaklaşım vekalet ve temsil bakımından korunamamıştır. Yapılan çalışmalarda varılan sonuca göre, Kanun teklifinde bunun tam olarak kabul edilmediğini, gerçek kişiler bakımından temsille veya vekâletle düzenlemenin uygun bulunmadığını fakat tüzel kişiler bakımından sadece sisteme kayıtlı olan temsilci veya temsilciler tarafından işlem yapılmasına olanak verilmesine olumlu yaklaşıldığını belirtmek gerekir. Elektronik çek ve bonoda avale dair bunların bedelinin tamamı veya bir kısmı için banka sistemi üzerinden aval verilmesinin mümkün olması beklenmektedir. Burada aval verme işlemi,

Getirilecek olan aksi yöndeki düzenleme ile elektronik çek ve bono bakımından hem güvenli elektronik imzanın hem de elektronik kimlik doğrulama yöntemlerinin kullanılmasıyla işlemlerin yapılması (keşide, devir ve diğer işlemler) mümkün hale gelecektir.[70]

Güvenli elektronik imzanın ötesinde elektronik kimlik doğrulama yöntemlerinin ne olacağı hakkında da bir yönetmelik yapılması için Bakanlığa yetki verilmesi planlanmaktadır. Bankacılık hizmetlerinde bir süredir uygulanan bu yöntemlerin elektronik çek ve bono bakımından da uygulanması beklenmektedir. Bahse konu kimlik doğrulama uygulamalarında kişi, yer ve cihaz temelli doğrulama uygulamalarının, yazılımlarının ve operasyonunun söz konusu olacağına işaret etmek gerekir. Mevcut uzaktan kimlik doğrulama uygulamalarında zaman zaman hileli işlemlerin, dolandırıcılıkların, kopyalamaların ve benzer dijital yönlendirmelerle kişilere işlem yaptırılmasının söz konusu olduğunu nazara aldığımızda, elektronik çek ve bono bakımından bu uygulamanın çeke ve bonoya özgü tedbirlerle oluşturulmasının ve uygulanmasının önemi açıktır. Bu noktada önce güvenli elektronik imzayla başlatılacak olan uygulamanın, bir süre sonra uzaktan kimlik doğrulama yöntemleri de dâhil edilerek geliştirilmesi, sistemin güvenliğinin temini ve yeni olmasının risklerini daha doğru yönetmek için tercih edilmesi daha yerinde olur. Nitekim elektronik çek ve bono bakımından

çek ve bononun seri numarasına kimin lehine aval verildiğinin ve aval verenle ilgili bilgilerin belirtilmesiyle mümkün olacaktır. Eklemek gerekir ki TTK ile uyumun sağlanması için TTK m. 77, 780, 1526 gibi birçok hükümde değişiklik yapılması gerekecektir.

70 Hasan Pulaşlı, *Kıymetli Evrak Hukukunun Esasları* (Ankara: Adalet Yayınevi, 2019), 4.

uzaktan kimlik doğrulama yöntemlerinin[71] ikincil bir düzenleme ile belirlenecek olması bu geçiş için uygun zamanın ve makul tedbirlerin temin edilmesine olanak sağlayabilir.[72] Diğer yandan, elektronik takas alt yapısının mevcut ve faal olmasının yanı sıra, elektronik imzanın kullanılmasıyla kâğıttan elektronik çeke geçişin kolayca yapılabileceğini düşünüyoruz.[73]

3. Elektronik Çek ve Bonoda Ciro

Elektronik çekte ve bonoda cironun, lehine ciro edilen kişi ve cironun türü belirtilmek suretiyle, ciro edenin hesabının bulunduğu bankanın sistemi üzerinden yapılması söz konusudur.[74] Böylece, tüm bilgilerin girilmesi gereğinden ötürü bu sistemde sadece tam cironun kabul ve tatbik olunması beklenmekte, hamiline çek ve bonoya, beyaz ciroya yer verilmemektedir.[75] Cironun türünün belirtilmemesi durumunda ise amacına göre temlik cirosu yapılmış sayılacaktır.

Tıpkı keşide işleminde olduğu gibi ciroda da fiziki teslim mümkün olmayacaktır. Bunun sonucu olarak, lehine ciro edilen, ciroya hesabının bulunduğu herhangi bir bankanın sistemi üzerinden ve en geç elektronik ibraz başlangıç tarihine kadar onay vererek zilyetliği teslim almış gibi değerlendirilecektir. Bu

---

71 Öte yandan, uygulamada, uzaktan elektronik kimlik doğrulama yöntemleriyle ilgili teknik altyapının çoğunlukla yurtdışı kaynaklı şirketler tarafından sunulan yazılım altyapılarıyla sağlandığının, bu şekilde temin edilen verilerin genellikle yurt dışına aktarıldığının da göz önünde bulundurması gerekir. Finansal kişisel verilerin hem kişisel veriler hem de finansal işlem güvenliği bakımından, uzaktan kimlik doğrulama yazılımlarında işlenecek verilerin işlenmesi ve aktarılması noktasında ayrı bir hassasiyet konusu olacağını şimdiden öngörmek mümkündür. Ayrıca bkz. Demirci, "Türk Hukukunda," 39.

72 Bu durumda örneğin keşidecinin, hamile ödeme hakkını saklı tutmak suretiyle çeki hamiline tanzim etmesi de söz konusu olmayacaktır. Bkz. Şaban Kayıhan, *Kıymetli Evrak Hukuku* (Ankara: Seçkin, 2018), 48-49.

73 Karabıyık, "Alternatif Ödeme-2," 161.

74 Demirci, "Türk Hukukunda," 38.

75 Baytemür, "Elektronik Kambiyo," 123-124.

onay, zilyetliğin elektronik şekilde devralınması niteliğinde olacağı için, onay ciro tarihindeki cironun onayı yani zilyetliğin bu anda devri vasfındadır. Dolayısıyla onaylanmış ciro, cironun tarihinde yapılmış cirodur.

Keşidede olduğu gibi geri alma kurumu ciroda da ciro tarihinden itibaren üç gün geçtikten sonra ve ancak onaylanana kadar ciro edenin tek taraflı tasarrufuyla mümkündür. Onaylandıktan sonra ise fiziksel senetler için de mümkün olduğu gibi hamil ve ona ciro edenin anlaşmaları üzerine elektronik çek veya bono iptal edilebilir. Geri alınması veya iptal edilmesi halinde ilgili ciro yapılmamış addolunur.[76] Tüm bu hükümler işlem basamaklarının elektronik takip ve kayıtlarına dayanmasını sağlamaktadır.

4. Elektronik Çek ve Bonoda Ödeme

Elektronik çek için ödeme, hamilin hesabının bulunduğu herhangi bir bankanın sistemi üzerinden çek takas sistemine sunularak veya Elektronik Çek ve Bono Sistemi aracılığıyla doğrudan muhatap bankaya ibraz üzerine yapılacaktır. Elektronik çekin, seri numarası belirtilerek, bankaya fiziken yapılacak başvuruyla ibraz edilmesi ve banka sisteminden seri numarası kontrolü ile kayden teyit edilerek ödenmesi de mümkündür. Aynı şekilde bono bedeli, hamilin sisteme tanımladığı banka hesabına, bononun seri numarası belirtilerek kolayca ödenebilir. Elektronik bonoda ise vadeden önce, düzenleyenin veya cirantanın banka sistemi üzerinden ileteceği talep ve hamilin onayı ile ödemenin mümkün olacağı anlaşılmaktadır. Burada hamilin onayı, bononun Elektronik Çek

[76] Demirci'nin belirttiği üzere; bu noktada öncelikle elektronik ortamda çekin düzenlenmesi, tedavülü, cirosu ile ödenmesine ilişkin her türlü işlem ve sürecin gerçekleştirileceği elektronik çek transfer sisteminin tanımlanmasına ihtiyaç duyulmuş olup, Kanun teklifi ile bu süreçler tanımlanmıştır. Bkz. Demirci, "Türk Hukukunda," 37.

ve Bono Sistemi tarafından ödemeye açılmasını sağlayacaktır.[77] Bono bakımından da bono bedeli, hamilin sisteme tanımladığı banka hesabına, bononun seri numarası belirtilerek ödenecektir. Uygulamada, ödeme çoğunlukla ya banka aracılığıyla ya da takasa ibraz yoluyla olacaktır.[78] Öte yandan, çekten farklı olarak vadede bono bedelinin tamamı ödenmemesi halinde, bakiye miktarı vadeyi takip eden ilk iş günü faizi ile birlikte sırasıyla; düzenleyenin, varsa düzenleyen lehine aval verenin, yine varsa ilk cirantanın, ilk ciranta lehine aval verenin, ikinci cirantadan başlamak üzere ciro sırasına göre her bir ciranta ve sonrasında onun lehine aval verenin, sisteme tanımladıkları hesaplarından doğrudan tahsil edilmesi öngörülmektedir.[79] Buna göre, lehtar, ciranta ve aval sisteme hesap tanımlamak zorundadır. Bu suretle bonoya güvenin, ödemenin kolaylaştırılması, desteklenmesi suretiyle pekiştirilmesi hedeflenmektedir.[80] Ayrıca, sistem üzerinden kimin hesabından ödeme yapılırsa bu durum kayıt

---

77 Karabıyık, "Alternatif Ödeme-2," 158.

78 Ömer Cem Aksoy, "Türkiye'de Çek Takası ve Çek Takası Verileri Işığında Çek Kullanımının İncelenmesi" (Türkiye Cumhuriyet Merkez Bankası, Uzmanlık Tezi, Ankara 2016), 14.

79 Karekodlu çek sisteminde Findeks üzerinde tüm bu verilerin kayıtlı olduğu düşünüldüğünde, sistem işleticisinin bu verileri kullanarak ve bunlara ödeme bilgilerini ekleyerek hizmet sunacağı, bu suretle sistem işleticisinin karekod ve Findeks hizmetlerini sunan kurumla aynı olacağı anlaşılmaktadır.

80 Topaloğlu, elektronik çeki ve elektronik çekle ödemeyi 2005 yılında yaptığı çalışmasında şu şekilde ele almış ve ifade etmiştir; "elektronik çek kâğıt tabanlı çekin e-imza ile oluşturulmuş elektronik versiyonudur. Borçlu müşteri kendi ekranında beliren elektronik çeki formunun unsurlarını tekemmül ettirdikten sonra e-imzası ile imzaladıktan sonra alacaklısına gönderir. Alacaklısı da bu çeki elektronik ortamda ulaştırır. Alacaklının bankası, söz konusu elektronik çeki muhatap bankadan tahsil ederek alacaklının hesabına aktarır. Bu şekilde ödeme veya ifa tamamlanmış olur." Bkz. Mustafa Topaloğlu, *Bilişim Hukuku* (Adana: Karahan Kitabevi, 2005), 208. Oysa Atakan'ın haklı olarak işaret ettiği üzere fiziki çekin elektronik suretini oluşturmakla sınırlı bir uygulamaya elektronik çek demek oldukça güçtür. Bkz. Atakan, "Kıymetli Evrak," 546.

altına alınarak, ödemeyi yapan, ödeme miktarı vb. bilgiler o bononun düzenleyeni, cirantaları ve ilgili diğer kişilere sistem üzerinden duyurulup bildirilmekle şeffaflık ve takip kolaylığı temin edilebilecektir. Bu uygulamada, bonoda protesto ve ihbar mükellefiyetini ortadan kaldırmak mümkün olabilir.[81]

Elektronik çek ise elektronik ibraz başlangıç tarihinden önce ibraz edilemezken; elektronik çek için tek bir ibraz süresi kabul edilerek, bu ibraz süresi, elektronik ibraz başlangıç tarihinden itibaren on gün şeklinde benimsenmiştir.[82] Çekin düzenlenmesi mutlaka muhatap banka sistemi üzerinden gerçekleştirilmelidir. Muhatap banka ancak düzenlenen çek bakımından kısıtlamaya tabidir. Lehtar kendi adına düzenlenen çeklere, hesabının bulunduğu bir banka sistemi üzerinden en geç elektronik ibraz başlangıç tarihine kadar onay verebilir ve onay vermesi halinde zilyetliği devralmış olur. Onaylayanın bu şekilde yaptığı onay işlemi ile çek düzenleme tarihinden itibaren hüküm doğuracak şekilde tedavüle geçmiş olur. Fakat düzenleyenin, onayladığı çeki düzenleme tarihinden 3 gün geçtikten sonra değiştirebilmesi veya geri alabilmesi yönünde bir düzenlemenin olduğu görülmektedir. Geri alınan ve elektronik ibraz başlangıç tarihine kadar onaylanmayan çeklerin düzenlenmemiş sayıldığının hükme bağlandığını söyleyebiliriz. Benzer düzenlemeler ciro bakımından da geçerli olup ciro için sadece tam ciro esas alınmıştır. Açık ciro mümkün değildir. Cironun türünün belirtilmediği durumlarda temlik cirosunun yapılmış olacağı Teklifle ortaya konmuştur. Onay işlemi tıpkı düzenlemede olduğu gibi ciro bakımından da onaya bağlı

[81] Öngörülen sistemde kayıtlı bono ve ödeme bilgilerinin kaydı sistem üzerinden UYAP'a aktarılarak alacak davalarında yargılamanın hızla tamamlanmasına destek sunulması planlanmaktadır.

[82] Elektronik ibraz ve takas sisteminin entegre şekilde çalışması beklenmektedir. Bkz. Karabıyık, "Alternatif Ödeme," 83.

şekilde zilyetliğin devri sistemi üzerinden elektronik olarak gerçekleştirilebilecektir.[83]

Çekin hamilin hesabının bulunduğu herhangi bir banka sistemi üzerinden ibraz edilmesi mümkündür. Seri numarası ile beraber fiziken ibraz edilmesi de Teklife göre mümkündür. Bundan seri numarasına sahip herkesin fiziki ibraz gerçekleştirerek ödeme isteyebileceği anlaşılmamalıdır. Seri numarasını ibraz eden kişinin bankanın sisteminde kimlik doğrulamasının gerçekleşmesi ve sistemdeki kayıt ve verilere göre meşru hamil olduğunun tespit edilebilmesi halinde bu ibraza karşılık bir ödeme talep edilebileceğine işaret edilmektedir.

Elektronik ibraz başlangıç tarihinden önce ibraz mümkün değildir. İbraz başlangıç tarihinden itibaren 10 günlük tek bir süre öngörülmüştür. Fiziki bir çek söz konusu olmadığı için, klasik anlamda çek için öngörülmüş diğer ibraz sürelerinin bir kenara konulması söz konusudur.[84]

F. Karşılıksızlık

Elektronik çekin kısmen veya tamamen karşılıksız çıkması mümkündür.[85] Karşılıksızlık riski teknolojinin azami seviyede kullanıldığı bu elektronik senetlerde dahi yok edilememektedir. Bu durumda Çek Kanununun 3. maddesinin 1. fıkrası ile 5. ve 6. maddeleri hükümlerinin uygulanması gündeme gelecektir. Bu halde, karşılıksızlık işlemi, çek yasaklılığı ve pişmanlık durumunda belirtilen 3., 5. ve 6. maddelerdeki düzenlemeler uygulama alanı bulacaktır. Çekin adli bir işleme konu edilmesi durumunda ise bir mahkeme ya da icra dairesince elektronik çek ve bono sistemi üzerinden bu talebin belirtilmesinin mümkün olması beklenmektedir. Ticaret ve Adalet Bakanlıkları

---

83 Karabıyık, 83.

84 Baytemür, "Elektronik Kambiyo," 174.

85 Kendigelen, *Çek Hukuku*, 350.

nezdindeki çalışmalarda UYAP'a[86] bu şekilde aktarılacak olan elektronik çek ve bono, çek ve bono aslı olarak kabul edilerek işlem yapılması hususunda mutabakata varıldığı görülmektedir.

G. Cayma

İlk bakışta elektronik çekin geri alınamaz olduğu sanılabilir. Ancak fiziksel senetlerin tam aksine, kullanılan teknoloji çekte değişiklik yapmaya ve geri almaya olanak vermektedir. Buna göre, düzenleyenin elektronik ibraz süresinin sona ermesinden itibaren 7 gün içerisinde elektronik çekten cayabilmesi Teklifte kabul edilen önemli bir düzenlemedir. Bu durumda elektronik ibraz süresinin sona ermesi ve 7 günlük süre içerisinde cayma hakkının kullanılması gerekecektir. Çekin ibraz süresinin geçmesinden sonra çekin ibraz edilmesi durumunda muhatap banka, elektronik çekten cayılmamışsa ve karşılığı varsa çek bedelinin tamamını, kısmi karşılığı varsa bu kısmi tutarı hamiline ödemekle mükellef olacaktır. Çekin ibraz süresinden sonraki sürede düzenleyenin ve hamilin işlemleri, yani ödeme talebi veya cayma işlemleri bu noktada birbirleri ile adeta bir yarışa sokulmuştur.

H. Elektronik Bono Bakımından Özellik Arz Eden Durumlar

Bono bakımından TTK m. 766 ve devamı hükümlerine ek olarak, elektronikleşmesinden ötürü bu durumun gerektirdiği unsurlar, elektronik bononun unsurlarına eklenmek durumundadır. Bunlar, elektronik bono ibaresi ve elektronik çek ve bono sisteminden bono için verilen seri numarasıdır. Elektronik olması ve diğer düzenlemelerin ışında, elektronik bononun da elektronik çek gibi sadece banka sistemi üzerinden düzenlenebileceği anlaşılmaktadır. Böylece banka bonosu olarak adlandırılabilecek bir tek tipleşme söz konusu olacaktır.

---

86 Adalet Bakanlığı Ulusal Yargı Ağı Bilişim Sistemi.

Elektronik çekte olduğu gibi elektronik bonoda da lehtar kendi lehine düzenlenmiş olan bir bonoyu banka sistemi üzerinden en geç vadeye kadar onay vererek kabul edip zilyetliğini devralmaktadır. Bu durumda onaylanan bono, düzenlendiği tarihten itibaren hüküm doğuracak şekilde tedavüle girmiş kabul edilecektir. Düzenleyenin onaylanmamış bir bonoyu düzenleme tarihinden 3 gün geçtikten sonra değiştirmesi veya geri alması tıpkı çekte olduğu gibi mümkündür. Düzenleyen bunu sıklıkla lehtarla arasındaki temel borç ilişkisinden kaynaklanan bir sebeple yapacaktır. Bu durum, senetlerin mücerretlik tesirinin ortaya çıkması için bir süre öngörüldüğü şeklinde yorumlanabilir.[87] Ayrıca elektronik bono sadece belirli bir günde ödemek üzere tek bir vadeye bağlanmakta, tam ciro şartına tabi tutulmakta; tam cirolar dışındaki cirolar kabul edilmemektedir. Buna göre, cironun kabulünün, ciro lehtarının sistem üzerinden onayına tabi tutulduğu bir uygulamanın devreye sokulması planlanmaktadır.[88]

Bonoda ödeme ancak bankaya ibraz edilerek ve bankaya seri numarası belirtilerek yapılacak olan bir işlemle gerçekleştirilecektir. Fakat bu hususta enteresan bir hüküm mevcuttur. Eğer vadede bono bedelinin tamamı ödenmemişse bu durumda kalan borç miktarı vadeyi takip eden ilk iş günü faiziyle birlikte sırasıyla düzenleyenin, düzenleyen lehine aval verenin, ilk cirantanın, ilk ciranta verenin lehine aval verenin veya ikinci cirantadan başlamak suretiyle ciro sırasına göre her bir cirantanın ve sonrasında onların lehine aval verenlerin elektronik çek ve bono sistemine tanımladıkları hesaplardan doğrudan tahsil edilecektir. Yani bir elektronik bonoda

---

87 Çotuksöken, "Dijitalleşme," 8.

88 Elektronik çekte beyaz cironun mümkün olabileceğine ve elektronik senetlerde beyaz cironun kabul edilmemesinin bu çeklerin fiziki çeke göre dezavantajlı bir pozisyona sokulmasına yol açacağına dair bir görüş için bkz. Baytemür, "Elektronik Kambiyo," 141.

düzenleyen, lehtar (ilk ciranta), sonraki ciranta veya aval olmak için bankaya tanımlı hesabınız olması gerektiği anlaşılmaktadır. Bononun vadesinde ödenmemesi veya eksik ödenmesi halinde ise Teklifin öngördüğü sırayla bu kimselerin ilgili hesaplarının herhangi birindeki bakiye üzerinden doğrudan tahsilat yapılması söz konusu olacaktır.

Elektronik çekten farklı olarak bonoda, düzenleyen, ciro eden ve aval veren; tahsilatta kullanılmak üzere en az bir banka hesabını kambiyo taahhüdünde bulunduğu bankanın sistemine tanımlamakla mükellef kılınmıştır. Tabii ki birden fazla hesap tanımlanması da mümkündür. Bu durumda sıraya göre işlem yapılabilir. Bu tanımlama için müşterek hesap kullanılması ise riskli olacağı için Teklif hazırlanırken kabul edilmemiştir.

Yine, lehtar ve lehine ciro edilenler, ödemenin yapılacağı bir banka hesabını onay işlemini gerçekleştirdikleri bankanın sistemine tanımlamakla mükellef kılınmıştır. Şüphesiz herhangi bir hesabın tanımlanması yeterli değildir. Aksi halde bu tanımlama basit bir prosedür olur ve ödemeye katkı sunmaz. Bu sebeple, ilgili hesabın tanımlayana ait olup olmadığı, tahsil ve ödemeye uygun bir hesap olup olmadığı gibi hususların doğrulanması gerekir. Banka, hesap kendisine aitse bunu kolayca yapabilecektir. Başka bankaya ait bir hesap varsa bu durumda devreye Elektronik Çek ve Bono Sistemi girecektir. Kural olarak hesap doğrulamasının yapılamadığı hallerde kambiyo taahhüdü ve bunların onaylanması işlemlerinin gerçekleştirilememesi gerekir.[89]

[89] Hesabın para cinsi ve içeriği bakımından uygunluğu da sağlanmalıdır. Yine, zamanla değişecek şartlara uyumun temini gayesiyle, bu işlemler sırasında tanımlanan hesaplar, yeni hesap bilgisinin tanımlanması suretiyle sonradan değiştirilebilmelidir.

SONUÇ

Elektronik Çek ve Bono'nun hukukumuzda düzenlenmesine dair yapılan çalışmalar ve hazırlanan Kanun Teklifi bugünün ticaret hayatının ihtiyaçlarıyla teknolojisinin sunduğu imkânları bir arada ele alan, gelecek vadeden çalışmalardandır. Bu düzenlemenin ve uygulamanın altyapısı, 2016 yılındaki Çeklerde Karekod Uygulamasına İlişkin Tebliğ[90] ve 2018 yılındaki Çek Takas Faaliyetleri hakkında Yönetmelik[91] ile hazırlanmıştır. Elektronik çek ve bono, değişen ve dönüşen ticaret hayatının, elektronik ticaretin; çek ve bononun kredi kartı, elektronik para gibi dijital ödeme araçlarının gölgesinde kalmasının etkisiyle bir ihtiyaç haline gelmiştir. İlaveten, elektronik çek ve bononun, kayıt dışılıkla mücadele, sahteciliğin önlenmesi, çek yaprağı üretme, taşıma ve saklama maliyetlerinin önüne geçilmesi, teknolojinin sunduğu imkânlardan yararlanılması, yasaların teknoloji ile uyumlu hale getirilmesi, ödemelerde güvenliğin temini gibi her biri son derece somut ve haklı gerekçeleri mevcuttur. Elektronik çek ve bononun yasal olarak düzenlenmesine dair çalışmalarda son aşamaya gelinmiş olup yasanın kısa bir süre içinde yürürlük kazanması beklenmektedir. Fakat bu düzenlemenin, TTK ve Çek Kanunu hükümlerinin yürürlüğüne tesiri olmayacaktır. Aksine, Elektronik Çek ve Bono Kanunu Teklifinin yasalaşması halinde, burada hüküm bulunmayan hallerde elektronik çek ve bono hakkında, genel hüküm olarak, niteliğine uygun düştüğü ölçüde 6102 sayılı Kanun ile 5941 sayılı Kanun hükümleri uygulanacaktır. Bu durum, çek hakkında üç, bono hakkında iki ayrı yasal düzenlemenin aynı zamanda yürürlükte olması anlamına gelmektedir. Hem bu düzenlemelerin birbirine uyumunun sağlanması, hem de elektronik çek ve bononun zorunlu hale getirilmeleri ihtimallerine istinaden, elektronik çek

90 RG. 31.12.2016, S. 29935 (3. Mükerrer).

91 RG. 09.06.2018, S. 30446.

ve bono için ayrı bir yasal düzenlemeye gitmek yerine, mevcut TTK ve Çek Kanunu içinde düzenleme yapılması değerlendirilebilirdi.

Hem elektronik çek hem de elektronik bono için sistemsel bir zorunluluk olarak, Türkiye Cumhuriyeti Kimlik Numarası veya yabancı kimlik numarası veya mavi kart numarası bulunmayan kişiler, kimlik bilgilerinin doğrulanması sağlıklı şekilde yapılamayacağı için çek düzenleyemeyecek veya çeke onay veremeyecektir. Bu sebeple elektronik çek ve bononun en azından şimdilik yerel bir uygulama olması, yabancı banka çeklerinin, yabancı ülkelerde düzenlenen bonoların kapsam dışında kalması uygulamada kimi karışıklıklar ve adil olmayan sonuçlar yaratma riski taşımaktadır.

Kanun Teklifi ile önerilen düzenlemeler, 6493 sayılı Elektronik Para Kanunu karşısında elektronik çek ve bononun statüsünün belirlenmesi noktasında tereddütler yaratmaktadır. Zira yasalaşması beklenen Kanun Teklifi ile çek ve bono neredeyse tüm işlem basamakları bakımından elektronikleşirken elektronik paraya, kaydî paraya, kredi kartına oldukça yaklaşmaktadır. Oysa her bir finansal enstrüman kendine özgü yönleriyle farklı ihtiyaçları karşılamaya aday olabilir.

Elektronik çek ve bono sisteminin kurulmasında, blok zincir teknolojisin kullanılmasının mümkün, uyumlu ve faydalı olabileceğini gözlemlediğimizi de ifade etmeliyiz. Blok zincir üzerinde olmayan çek ve bononun kriptografik varlıklarla uyum ve rekabet gücünün kısa ve orta vadede sorunlar yaratması gündeme gelebilir. Kaldı ki blok zincir sisteme üye olacak kurumlar, bankalar ve Bankalar Birliği bakımından da uygun çözümler sunabilir.

Kısaca ifade etmek gerekirse, Kanun Teklifi yasalaşırsa çek ve bono önemli bir evrim geçirecektir. Bir yanıyla çek ve bono sadece elektronik ortama taşınmış gibi görünecektir. Diğer

yanıyla elektronik çek ve bononun sürekli gelişen teknolojiyle uyumluluğunun sağlanması devamlılık arz edecek ve Teklifte öne çıkan yenilikçi düzenlemelerin ışığında aslında tamamen yeni finansal teknoloji enstrümanlarının hayatımıza girdiklerini söylemek mümkün olacaktır. Her halükârda, elektronik çek ve bononun hem geleneksel anlamda hem de yenilikçi bir bakış açısıyla çok sayıda hukuki tartışmayı beraberinde getireceği açıktır.

KAYNAKÇA

Aksoy, Ömer Cem. "Türkiye'de Çek Takası ve Çek Takası Verileri Işığında Çek Kullanımının İncelenmesi." Uzmanlık Tezi, Ankara: Türkiye Cumhuriyet Merkez Bankası, 2016.

Atakan, Murat Can. "Kıymetli Evrak Hukuku'nda Yeni Bir Öneri: Elektronik Çek. Alman Elektronik Kıymetli Evrak Kanunu Tasarısı (Ewpg-E) Işığında Bir İnceleme." *Yargıtay Dergisi* 47, no. 2 (Nisan 2021): 541-580.

Bahtiyar, Mehmet. "5941 sayılı Çek Kanunu Açısından İleri Tarihli Çek." *Kadir Has Üniversitesi Hukuk Fakültesi Dergisi* 1, no. 2 (2013): 47-58.

Baytemür, Deniz. "Elektronik Kambiyo Senetleri." Yayımlanmamış Yüksek Lisans Tezi, Ankara: Ankara Hacı Bayram Veli Üniversitesi Lisansüstü Eğitim Enstitüsü, 2020.

Ber, Ahmet Said. *Elektronik Konişmento*. Ankara: Seçkin Yayıncılık, 2018.

Ber, Ahmet Said. "Elektronik Olarak Devredilebilir Kayıtlara İlişkin UNCITRAL Model Kanunu (Çeviri), m. 10 ve 11." *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi* 1, no. 2 (Aralık 2019): 445-452.

Bozgeyik, Hayri. *Poliçede Müracaat Hakkı*. Ankara: Seçkin Yayıncılık, 2003.

Çotuksöken, Emre. "Dijitalleşme, Elektronik Çek ve Blockchain İlişkisi." *Finans Hukuku Gündemi Dergisi*, No. 4 (Temmuz 2020). Erişim Tarihi: Şubat 25, 2021. http://212.58.27.19/XXXX/FinansHDergi44/Dijitallesme,-Elektronik-Cek-ve-Blockchain-Iliskisi1_xxcid12679838#.YJ_z4ZMzbOQ.

Demirci, Serdar. "Türk Hukukunda Elektronik Çeke Doğru, Dünü ve Bugünüyle Çek." *Ankara Barosu Dergisi* 78, no. 3 (2020): 1-47.

Dursun, Alev Deniz. Karşılıksız Çek Keşide Etmenin Hukuki ve Cezai Sorumluluğu. Ankara: Seçkin Yayıncılık, 2019.

İmregün, Oğuz. *Kıymetli Evrak Hukuku*. İstanbul: Filiz Kitabevi, 1995.

Karabıyık, Ayşegül. "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-1." *Muhasebe ve Finansman Dergisi*, no. 38 (Nisan 2008): 80-94.

Karabıyık, Ayşegül. "Alternatif Ödeme Aracı Olarak: Elektronik Çek Sistemi (E-Çek)-2." *Muhasebe ve Finansman Dergisi*, no. 39 (Temmuz 2008): 155-166.

Kayıhan, Şaban. *Kıymetli Evrak Hukuku*. Ankara: Seçkin Yayıncılık, 2018.

Kendigelen, Abuzer. *Çek Hukuku*, İstanbul: XII Levha Yayınları, 2019.

Öztan, Fırat. *Kıymetli Evrak Hukuku*. Ankara: Yetkin Yayınları, 1997.

Poroy, Reha ve Ünal Tekinalp Ünal. *Kıymetli Evrak Hukuku Esasları*. İstanbul: Vedat Kitapçılık, 2019.

Pulaşlı, Hasan. *Kıymetli Evrak Hukukunun Esasları*. Ankara: Adalet Yayınevi, 2019.

Şahin, Bertaç Şakir ve Barış Cihan Cantürk. "Türkiye'deki Hukuki Altyapı ve Ödeme Hizmetleri Yönergesi 2 Bağlamında API Teknolojisi ve Açık Bankacılık." *Maliye ve Finans Yazıları,* no. 114 (2020): 149-178.

Topaloğlu, Mustafa. *Bilişim Hukuku*. Adana: Karahan Kitabevi, 2005.

Turanboy, Asuman. *Varakasız Kıymetli Evrak*. Ankara: Banka ve Ticaret Hukuku Araştırma Enstitüsü, 1998.

Ülgen, Hüseyin, Helvacı, Mehmet, Kaya, Arslan ve Ertan, Füsun Nomer. *Kıymetli Evrak Hukuku*. İstanbul: Vedat Kitapçılık, 2019.

Ünal, Mücahit. *Sermaye Piyasası Araçlarının Kaydileştirilmesi*. Ankara: Adalet Yayınevi, 2011.

Yılmaz, Lerzan. *Kambiyo Senetlerinde Def'iler*. İstanbul: Aristo Yayınevi, 2007.

Web Siteleri

Bloomberg. "2021'de çek-bonoya elektronik sistem getirilmesi planlanıyor." Erişim Tarihi: Mayıs 10, 2021. https://www.bloomberght.com/2021-de-cek-bonoya-elektronik-sistem-getirilmesi-planlaniyor-2269211.

İTO. "Çek koçanı tarihe karışacak." Erişim Tarihi: Nisan 8, 2021. https://www.itohaber.com/haber/guncel/204360/cek_kocani_tarihe_karisacak.html.

Ticaret Bakanlığı. "Bakan Pekcan: Karekodlu bono, elektronik çek ve bono uygulamasını başlatıyoruz." Erişim Tarihi: Nisan 14, 2021. https://www.ticaret.gov.tr/haberler/bakan-pekcan-karekodlu-bono-elektronik-cek-ve-bono-uygulamasini-baslatiyoruz.

TBB. "Çekler Çalışma Grubu." Erişim Tarihi: Mart 12, 2021. https://www.tbb.org.tr/tr/hakkimizda/kurumsal/calisma-gruplari/surekli-calisma-gruplari/cekler-calisma-grubu/158.

Kanun Gerekçesi:

Elektronik Çek ve Kanunu Teklif Genel Gerekçesi (Kısaca: Teklif Genel Gerekçesi)

BELGEDE SAHTECİLİK SUÇLARININ KONUSU OLARAK ELEKTRONİK/DİJİTAL BELGE*

Electronic/Digital Document as the Subject of Document Forgery Crimes

Gülfer AKIN**

Özet

Bilimsel gelişmeler, belge kavramına birtakım yenilikler getirmiştir. Bu yeniliklerden biri de elektronik belgedir. Teknolojinin hayatın birçok alanına girmesiyle birlikte kamusal alanda ve özel sektörde birçok işlem gittikçe artan bir oranda elektronik ortamda yapılmaktadır. Klasik anlamda kâğıt ya da maddi bir nesne üzerine yazılan belgelerin yerini son dönemde elektronik belgeler almaya başlamıştır.

Bu gelişmeler sebebiyle TCK'nın sahtecilik suçunu düzenleyen hükümlerinin elektronik belgeyi de kapsayıp kapsamadığına, elektronik bir belgede sahtecilik yapılması durumunda hukuksal sorumluluk ve cezai yaptırımın nasıl belirleneceğine dair tartışmalar yaşanmaya başlamıştır. Makalede, belgede sahtecilik suçlarının konusu olarak elektronik (dijital) belge teknik ayrıntılara girilmeden ve

* Bu makale, Ankara Sosyal Bilimler Üniversitesi Sosyal Bilimler Enstitüsünde yazılmakta olan "Resmi Belgede Sahtecilik Suçu" isimli doktora tezinden üretilmiştir.

** Yargıtay Cumhuriyet Savcısı, akingulfer@gmail.com, ORCID: 0000-0003-0436-1666.

Makale Gönderim Tarihi/Received:

Makale Kabul Tarihi/Accepted:

Atıf/Citation: Akın, Gülfer. "Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/Dijital Belge." *Bilişim Hukuku Dergisi* 3, no:1 (2021): 76-138.

sahtecilik suçunun diğer unsurlarına değinilmeden incelenmiştir.

Anahtar Kelimeler: Sahtecilik, belge, veri, dijital/elektronik belge, elektronik imza.

Abstract

Scientific developments have brought some innovations to the document concept. One of these innovations is the electronic document. With the introduction of technology in many areas of life, many transactions in the public and private sector are increasingly carried out in electronic environment. In the classical sense, documents written on paper or a material object have recently started to be replaced by electronic documents.

Due to these developments, discussions have started about whether the provisions of the Turkish Penal Code regulating the crime of forgery also include the electronic document, and how to determine legal liability and criminal sanctions in case of forgery of an electronic document. In the article, the electronic (digital) document as the subject of the crime of forgery has been examined without technical details and without mentioning the other elements of the forgery crime.

Keywords: Forgery, document, data, digital/electronic document, electronic signature.

Giriş

Belgeler, bir durumu tespit etmeleri ve ispat vasıtası olmaları nedeniyle hukuki sonuç doğuran, toplumun da bu nedenle doğruluk ve geçerliliklerine güven duyduğu araçlardır.[1] Belgeler üzerinde gerçekleştirilen sahtecilik fiillerinin kamu

[1] Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* (Ankara: Adalet Yayınevi, 2020), 761.

güvenini sarstığı kabul edilerek bu tür fiiller tarihi süreç içerisinde ceza kanunlarıyla yaptırım altına alınmıştır.[2]

Değişen ve gelişen toplumsal hayat, sosyo-ekonomik ilişkiler, teknolojik gelişmeler nedeniyle özel ve resmi iş ve işlemler, sayı, çeşit ve içerik bakımından artmıştır. Buna bağlı olarak da belgeler, toplumsal hayatta gittikçe daha fazla önem kazanmıştır. Bu gelişmeler elektronik belge kavramının doğmasına neden olmuştur.[3]

Günümüzde resmi ve özel birçok iş ve işlem elektronik ortamda yapılmaktadır. Yakın gelecekte, klasik anlamdaki maddi bir şeyin üzerine yazılı bulunan belgelerin yerini tamamen elektronik belgelerin alacağı öngörülmektedir. Bu şekilde düzenlenen ve maddi bir varlığı haiz olmayan elektronik belgelerde gerçekleştirilen değişikliklerin ceza hukukunda hangi suçu oluşturacağı tartışma konusudur.[4]

Doktrin ve uygulamada konuya ilişkin tartışma ve tereddütler devam etmektedir. Bu belirsizlik, elektronik ortamda işlenen sahtecilik fiillerinin çoğu zaman cezasız kalması veya karşılığı olandan daha hafif bir yaptırıma tabi tutulması sonucunu doğurmaktadır. Çalışmada konuya bir nebze de olsa katkı sağlamak amaçlanmıştır.

I. BELGE KAVRAMI

A. Genel Olarak

Belgede sahtecilik suçlarının maddi konusu belgedir. Yazıda yapılan sahtecilik fiilinin kamunun güvenini sarstığının kabulü ve bu nedenle de belgede sahtecilik suçu isnadıyla cezalandırılabilmesi için sahteciliğin konusunu oluşturan

---

2 Erol Çetin ve İsmail Malkoç, Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat, (Ankara: Adalet Yayınevi, 1995), 128.

3 Kubilay Taşdemir, *Açıklamalı-İçtihatlı Belgelerde Sahtecilik Suçları*, (Ankara: R24 Medya Ltd. Şti., 2019), 293.

4 Taşdemir, *Belgelerde Sahtecilik*, 247.

yazının hukuksal olarak "belge"den sayılabilmesi zorunludur.[5] Ayrıca ceza hukuku anlamında bir belgenin varlığının kabulü için bunun, hukuki hüküm ifade etmesi de gerekmektedir.[6] Bu kavram Türk Dil Kurumu sözlüğünde, "*Bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb. vesika, doküman*" olarak tanımlanmaktadır.[7]

Belge kavramı, ilk kez 5237 sayılı Türk Ceza Kanunu'nda (TCK) kullanılmıştır. Bu terim, 765 sayılı TCK'daki "evrak" ve "varaka" terimleri karşılığında kullanılmaktadır. 5237 sayılı TCK m.204'ün gerekçesinde bu duruma dikkat çekilmiştir.[8] Evrak terimi Arapça bir terim olan varak kelimesinin çoğulu olan "*kâğıt yaprakları, kitap sayfaları, yazılmış kitaplar, mektuplar ve yazılar*"[9] anlamlarına gelmektedir. Belge kavramı, varak terimini de içeren daha geniş bir kavramdır. Birçok yasada klasik anlamdaki maddi varlığı olan kâğıt, metal, deri vb. şeyler üzerindeki yazının yanında, dijital ortamdaki verilerle videokaset gibi şeylerin de belge kavramının kapsamında değerlendirildiği görülmektedir. Bu nokta da irade açıklamalarını içeren hangi yazıların yasal anlamda belge olarak

---

5 Sahir Erman, "Evrakta Sahtekârlık Suçlarında 'Varaka' Mefhumu," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 15, no. 1(1949), 167; Sahir Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku,* Cilt III, (İstanbul: İstanbul Üniversitesi Fen Fakültesi Döner Sermaye İşletmesi Prof. Dr. Nazım Terzioğlu Basım Atölyesi, 1987), 302.

6 Yar. 11. CD. E. 2016/9261, K. 2017/1057, 16.02.2017.

7 http://www.tdk.gov.tr, erişim tarihi:21.05.2020.

8 Madde gerekçesinde; *"Belge, eski dilimizdeki "evrak" kelimesi karşılığında kullanılmakta olup, yazılı kâğıt anlamına gelmektedir. Bu bakımdan, yazılı kâğıt niteliğinde olmayan şey, ispat kuvveti ne olursa olsun, belge niteliği taşımamaktadır."* şeklindeki açıklama yer almaktadır.

9 *Türk Dil Kurumu Sözlüğü,* http://www.tdk.gov.tr, erişim tarihi:*04.06.2020.*

kabul edildiğinin tespiti önemli bir sorun olarak karşımıza çıkmaktadır.[10]

765 sayılı TCK'da olduğu gibi 5237 sayılı TCK'da da belgenin tanımı yapılmamıştır. TCK'nın yapım çalışmaları sırasında bu kavramla ilgili olarak yapılacak herhangi bir tanımın uygulamayı daraltabileceği belirtilerek kavramın tanımlanmasından vazgeçilmiştir.[11] Her ne kadar TCK'da belge kavramı tanımlanmamışsa da, Türk hukuk mevzuatında belgeyi tanımlayan kanunlar bulunmaktadır. Örneğin 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 3. maddesinin d bendine göre belge; "*Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film, fotoğraf, teyp ve videokaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını*" ifade eder. Uygulama ve doktrinde belge kavramının ortak bir tanımına ulaşılamamış olup farklı tanımlamalar ortaya konulmuştur.

Doktrinde belge kavramına ilişkin farklı tanımlar bulunmakla birlikte, bunlardan hareketle ortak bir tanım olarak hukuki terminolojide belgeyi; "*Bir olayı nakleden veya bir irade beyanını içeren, bir kimse tarafından oluşturulup delil değeri bulunan ve hukuki açıdan değer taşıyan her türlü yazı*" şeklinde tanımlamak mümkündür[12].

---

[10] Arif Gözel, "Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge," *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 5, no. 1(2015),147.

[11] TBMM Adalet Komisyonu'nda 5237 sayılı Türk Ceza Kanunu'nun görüşülmesi esnasında, belgenin tanımına ilişkin tartışmalar yapılmış, ancak kavramın tanımlanmasının bir süre sonra uygulamaya dar gelebileceği düşüncesi ile tanımı yapılmamıştır. (**Bkz. Meclis tutanakları**)

[12] Sahir Erman, *Sahtekârlık Suçları Ticari Ceza Hukuku* - III, (İstanbul: Nazım Terzioğlu Matematik Araştırma Enstitüsü Baskı Atölyesi, 1981), 308; Faruk Erem, *Türk Ceza Hukuku Hususi Hükümler,* Cilt II. (Ankara: Ajans-Türk Matbaası, 1962),555; Koca ve Üzülmez, *Özel Hükümler*, 763; Mustafa Ekinci,

Yargıtay'ın, belgeyi farklı şekillerde tanımladığı görülmektedir.[13] Yargıtay 11. Ceza Dairesi belgeyi; "*taşınabilen bir şey üzerine yazılıp da hukuki hüküm ifade* eden bir olayı kanıtlamaya yarayan yazı" şeklinde tanımlamaktadır.[14] Yargıtay Ceza Genel Kurulu ise; "*belirli bir düşünce, hukuki ilişki veya vakayı yansıtan, başka deyişle hukuki sonuç doğurmaya elverişli bir irade beyanını içeren ve düzenleyicisinin kim olduğunu da gösteren yazılı evrak*"[15] şeklinde belgeyi tanımlanmaktadır. Yargıtay bazı kararlarında, belgeyi tanımlamadan yalnızca özelliklerinden

Sinan Esen, *Anlatımlı ve Gerekçeli 5237 sayılı Türk Ceza Kanununda Yer Alan Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar*, (Ankara: Adalet Yayınevi, 2005), 245-246; Abdullah Pulat Gözübüyük, *Türk Ceza Kanunu Gözübüyük Şerhi*, 3. Cilt, (İstanbul: Kazancı Yayınları, 1988), 278; Nevzat Toroslu, *Ceza Hukuku Özel Kısım*, (Ankara: Savaş Yayınevi, 2019), 226; Durmuş Tezcan, Mustafa Ruhan Erdem ve Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku, (*Ankara: Seçkin Yayınevi, 2020), 1037; Doğan Soyaslan, *Ceza Hukuku Özel Hükümler*, (Ankara: Yetkin Yayınları, 2020), 511; Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Özel Hükümler*, (Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020), 829; Mehmet Emin Artuk, Ahmet Gökcen, Mehmet Emin Alşahin ve Kerim Çakır, *Ceza Hukuku Özel Hükümler,* (Ankara: Adalet Yayınevi, 2019),708; Devrim Güngör,*Resmi Belgelerde Sahtecilik Suçu*, (Ankara: Yetkin Yayınları, 2010), 45; Hasan Tahsin Gökcan, "Resmi Belgede Sahtecilik Suçu," *Ankara Barosu Dergisi,* 67, no. 3.(2009), 96; Taşdemir, *Belgelerde Sahtecilik*, 6.

13 "Ceza hukukunda belge; belirli bir düşünce, hukuki ilişki veya vakayı yansıtan, başka deyişle hukuki sonuç doğurmaya elverişli bir irade beyanını içeren ve düzenleyicisinin kim olduğunu da gösteren yazılı evrak olarak tanımlanabilir." Yar. CGK, E. 2016/21-1065, K. 2017/27, 24.01.2017, (UYAP);"Resmi belgede sahtecilik suçlarının konusunu oluşturan belgenin, taşınabilen bir şey üzerine yazılıp da hukuki hüküm ifade eden bir olayı kanıtlamaya yarayan yazı olduğu," Yar. 11. CD, E. 2017/4804, K.2018/623, 30.01.2018, (UYAP); "Belge; içeriği olan, hak doğurucu, kaldırıcı ve kanıt aracı olan yazıdır." Yar. 15.CD, E. 2014/2517, K. 2016/5863, 06.06.2016, (UYAP).

14 Yar. 11. CD, E. 2013/13549, K. 2014/17326, 23.10.2014, (UYAP).

15 Yar. CGK, E. 2015/15-393, K. 2017/74, 21.02.2017, (UYAP).

bahsetmekle yetinmiştir.[16] Kanaatimizce belge; "*Hukuken hüküm ifade eden, düzenleyicisi belirlenebilir olan, bir hakkın doğmasına, sona ermesine veya değiştirilmesine ve bir olayı ispata elverişli olan her türlü yazı*" olarak tanımlanabilir. Bu bağlamda öğretideki tanımlamalar bakımından ortak unsurlar olarak ele alınan, hukuki açıdan bir değer içeren irade beyanının bulunması, yazının delil değerini ihtiva etmesi ve belirli bir kimse tarafından oluşturulması hususlarının belgenin tanımında yer alması gerektiği ifade edilebilir.

B. Belgenin Unsurları

1. Yazılı Olması

Hukuksal anlamda bir belgenin varlığının kabulü için bulunması gereken ilk unsur, yazılı olmasıdır. Bu bağlamda ancak yazılı olan şeyler belge olarak kabul edilebilir.[17] Yazılılık şartı gerçekleşmediği takdirde hukuki anlamda bir belgenin varlığından söz edilmesi olanaklı değildir. Üzerinde yazının mevcut olması hâlinde koşulları varsa bir levha, deri veya plastik de belge olarak kabul edilebilecektir.[18] Yargıtay'ın istikrar kazanmış uygulaması da bu yöndedir.[19]

---

[16] "Belgede sahtecilik suçunun oluşabilmesi için, suçun maddi unsuru ve konusunun belge niteliğini taşıması gerekmektedir. Kanunda belge tanımlanmamış, kavramın tanımı ve açıklanması doktrin ve uygulama ile belirlenmiştir. Buna göre belgenin, yazılı olması, hukuki değer ihtiva etmesi, düzenleyicisinin belli ve imzalı olması gerekir." Yar. 11. CD, E. 2017/2237, K. 2019/531, 16.01.2019, (UYAP).

[17] Soyaslan, *Özel Hükümler*,512; Remzi Gündüz ve Veysel Gültaş, *Belgelerde ve Faturalarda Sahtecilik Suçları*, (Ankara: Bilge Yayınevi, 2013), 20; Faruk Erem, *Ümanist Doktrin Açısından Türk Ceza Hukuku Özel Hükümler,* Cilt IV, (Ankara: Seçkin Kitabevi, 1985), 40.

[18] Erman, "Evrakta Sahtekârlık Suçlarında 'Varaka' Mefhumu,"174.

[19] "Resmi belgede sahtecilik suçlarının konusunu oluşturan belgenin, taşınabilen bir şey üzerine yazılıp da hukuki hüküm ifade eden bir olayı kanıtlamaya yarayan yazı olduğu, 5237 sayılı TCK'nın 204. maddesinin gerekçesinde de belirtildiği üzere, belgenin varlığının kabulü için yazılı

Yazının anlaşılabilir bir içeriğinin bulunması gerekmektedir. Başka bir ifadeyle yazının içerdiği irade beyanının açıkça anlaşılabilecek nitelikte olması gerekmektedir.[20]Bu şartı gerçekleştiren yazının mevzuatta belirli bir dilde yazılmış olması şartı bulunmadığı takdirde hangi dilde yazılmış olduğunun bu yazının belge olarak kabul edilmesi açısından önemi bulunmamaktadır.[21]Yazının aynı zamanda taşınabilir nitelikte olması gerekmektedir.[22] Dolayısıyla kâğıdın yanısıra deri, metal, plastik vb. gibi taşınabilir maddi varlıklar üzerine yazı yazılması halinde de yazılılık koşulu gerçekleşir. Yargıtay'da belgenin taşınabilir olması gerektiğini benimsemektedir.[23]

kağıdın bulunmasının zorunlu olmadığı, bir metal levha üzerine yazı yazılması halinde de diğer unsurların varlığı durumunda, belgeden söz edilebileceği, bu bakımdan araç plakalarının da resmi belge olarak kabulü gerekeceği," Yar. 11. CD, E. 2016/963, K. 2018/3540, 16.04.2018, (UYAP).

[20] Erman, "Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu," 173; Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku,* 1987, 309; Sahir Erman ve Çetin Özek, *Ceza Hukuku Özel Bölüm, Kamu Güvenine Karşı İşlenen Suçlar TCK 316-368,* (İstanbul: Globus Dünya Basımevi, 1996), 314.

[21] Faruk Erem ve Nevzat Toroslu, *Türk Ceza Hukuku Özel Hükümler,* (Ankara: Savaş Yayınevi, 1994), 252; Soyaslan, *Özel Hükümler*, 512.

[22] Erman, "Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu," 173; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*,314; Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku, 1987*, 31; Nihat Bozkurt Çam, "Evrakta Sahtekârlık Suçları," *Ankara Barosu Dergisi,* no. 3 (1989): 455; Ekinci ve Esen, *Bilişim Alanında Suçlar*, 247.

[23] "Resmi belgede sahtecilik suçlarının konusunu oluşturan belgenin, taşınabilen bir şey üzerine yazılıp da hukuki hüküm ifade eden bir olayı kanıtlamaya yarayan yazı olduğu, 5237 sayılı TCK'nın 204. maddesinin gerekçesinde de belirtildiği üzere, belgenin varlığının kabulü için yazılı kağıdın bulunmasının zorunlu olmadığı, bir metal levha üzerine yazı yazılması halinde de diğer unsurların varlığı durumunda, belgeden söz edilebileceği, bu bakımdan araç plakalarının da resmi belge olarak kabulü gerekeceği cihetle" Yar. 11.CD, E. 2016/963, K. 2018/3540, 16.04.2018; E. 2018/1686, K. 2018/1857, 01.03.2018, (UYAP).

2. Belgeyi Düzenleyen Kişinin Teşhis Edilebilir Olması

Belgenin zorunlu unsurlarından bir diğeri de belirli bir kişiye izafe edilebilmesidir.[24] Bu husus, TCK'nın 204. madde gerekçesinde de vurgulanmıştır.[25]

Belgede sahtecilik suçundan bahsedilebilmesi için yalnızca yazı muhtevasında bir irade beyanının bulunması değil bu irade beyanının kime ait olduğunun belgeden anlaşılabilmesi de gerekmektedir.[26] Başka bir ifadeyle, yazının kim tarafından yazılmış olduğunun bizzat yazının içeriğinden anlaşılabilmesi gerekmektedir.[27]Kime ait olduğunun anlaşılamadığı hallerde, yazı, hukuki açıdan bir hüküm ifade etmediğinden belge olarak nitelendirilemez.[28]

3. Hukuki Değeri Haiz Olması

Belgenin mevcudiyetinden söz edilebilmesi için bulunması gereken son unsur, yazı içeriğinin hukuki bir değeri haiz olması, yani hukuki sonuç doğuracak nitelikte olmasıdır.[29] Yazı

---

[24] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1038; Erman, "Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu," 174; Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku*, 1987, 311; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*, 315;Gökcan, "Resmi Belgede Sahtecilik Suçu," 99; Gözübüyük, *Türk Ceza Kanunu Gözübüyük Şerhi*, 278.

[25] Bkz. Madde gerekçesi.

[26] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1038.

[27] Erman, "Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu," 174; Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku,* 1987, 311; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*,315; Gökcan, "Resmi Belgede Sahtecilik Suçu," 99; Gözübüyük, *Türk Ceza Kanunu Gözübüyük Şerhi*, 278; Koca ve Üzülmez, *Özel Hükümler*, 766.

[28] Erem, *Ümanist Doktrin*, 42; Gökcan, "Resmi Belgede Sahtecilik Suçu," 99; Çetin ve Malkoç, *Sahtekârlık Suçları*, 132.

[29] Gözübüyük, Türk Ceza Kanunu Gözübüyük Şerhi, 279.

içeriğinin hukuki olarak önemli olması gerekir.[30] Dolayısıyla yazı, kanıt olma özelliğini haiz olmalıdır.[31] Bu suretle belge kavramının yazı kavramından çok daha dar bir anlam taşıdığı anlaşılmaktadır. Dolayısıyla her belge bir yazı olduğu halde her yazı belge değildir.[32] Özetle, TCK'nın aradığı anlamda bir belgeden bahsedilebilmesi için; belgenin taşınabilir birşey

---

30 İsmail Malkoç, Sahtecilik Suçları ve Mala Karşı Suçlar, (Ankara: Seçkin Yayınevi, 1995), 132; "Suç tarihinde ...Köyü muhtarı olarak görev yapan sanığın, köy karar defterinin 20, 21, 22 ve 23. sayfalarını ihtiyar heyeti azası T. Ş. adına sahte olarak imzaladığının iddia ve kabul olunduğu olayda; 2972 sayılı Mahalli İdareler İle Mahalle Muhtarlıkları Ve İhtiyar Heyetleri Seçimi Hakkında Kanun'un 30/a maddesinde, köy ihtiyar meclisine seçilecek aza sayısının en az dört kişiden oluşacağının belirtilmesi; 442 sayılı Köy Kanunu'nun 23.maddesinde, "Köyün imamı ile muallimi veya başmuallimi ihtiyar meclisinin her zaman azasıdırlar" şeklinde düzenleme bulunması; Köy Kanunu'nda toplantı ve karar yeter sayısından bahsedilmemesi ile muhtarın oyunun ağır basmasını öngören bir hüküm de mevcut olmaması karşısında; suç tarihlerinde köyde imam ve öğretmenin bulunup bulunmadığının İlçe Milli Eğitim Müdürlüğü ve İlçe Müftülüğünden araştırılması, bulunması durumunda; ihtiyar meclisinin muhtar dâhil en az 7 kişiden oluşacağı ve üye tam sayısının salt çoğunluğuyla toplanıp, toplantıya katılanların da salt çoğunluğuyla karar alınabileceği, köy karar defterinin suça konu sayfalarında muhtar ve 2 aza olmak üzere toplam 3 imza bulunduğu, toplantı yeter sayısının en az 4 olması gerekirken 3 kişiyle karar alındığı, bu nedenle alınan kararların hukuki sonuç doğurmaya elverişli olmadığı, aksi durumda ise atılı suçun unsurlarının oluşacağı gözetilmeden, 16.10.2018 tarihli Kaymakamlık yazısıyla yetinilerek eksik araştırma ve inceleme ile sanık hakkında mahkûmiyet hükmü kurulması…" Yarg. 11. CD, E. 2019/1545, K. 2019/3569, 08.04.2019, (UYAP).

31 Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku, 1987*, 316; Erman, "Evrakta Sahtekârlık Suçlarında "Varaka "Mefhumu," 176; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*, 324; Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1039; Soyaslan, *Özel Hükümler*, 515; Erem ve Toroslu, *Özel Hükümler*,253; Koca ve Üzülmez, *Özel Hükümler*,765.

32 Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku, 1987*, 316; Erman, "Evrakta Sahtekârlık Suçlarında "Varaka "Mefhumu," 176; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*,324.

üzerine yazılı olması, yazanının bilinebilir olması ve hukuki hüküm ifade etmesi gerekmektedir.

Belgeyi sadece klasik anlamdaki kâğıt ya da maddi varlığı olan şeyler üzerine yazılan yazıyla sınırlandırmamak gerekir. TCK'nın 204. maddesinin gerekçesine göre;*"Her ne kadar belgeden söz edilen durumlarda yazılı bir kâğıdın varlığı gerekli ise de bazı durumlarda belgenin varlığını kabul için yazının kâğıt üzerinde bulunması aranmaz. Bir metal levha üzerine yazı yazılması hâlinde de belgenin varlığını kabul etmek gerekir. Bu itibarla araç plakalarının da resmi belge olarak kabul edilmesi gerekir".* Kanaatimizce, bu açıklamalardan kanun koyucunun belge kavramını kâğıt üzerine yazılmış olan yazıyla sınırlandırmak, daraltmak istemediği sonucu çıkartılabilir.[33] Böylece başka şeyler üzerine yazılan ve başka ortamlara kaydedilmiş bulunan yazıların da koşulların varlığı hâlinde belge olarak kabul edilebileceği ifade edilebilir.

C. Belge Türleri

Türk Ceza Kanunu'na göre belgeler; resmi, özel ve resmi belge hükmündeki belgeler olmak üzere üç gruba ayrılmıştır.[34] Resmi belge, bir kamu görevlisi tarafından, görev ve fonksiyonu sebebiyle düzenlenen yazıdır.[35] Burada dikkat edilmesi gereken husus, bir belgenin resmi belge olarak kabul edilebilmesi için kamu görevlisi tarafından düzenlenmesinin zorunlu olmadığıdır. Daha açık bir anlatımla, kamu görevlisi tarafından düzenlenmesi gereken resmi bir belgenin, onun tarafından görevi gereği düzenlenmesi durumunda eylem TCK' nın 204. maddesinin ikinci fıkrasındaki kamu görevlisinin resmi belgede sahteciliği suçunu oluşturur. Buna karşın bu nitelikteki bir belgenin kamu görevlisi dışındaki kişiler tarafından düzenlenmesi durumunda, eylem TCK'nın 204. maddesinin

[33] Bkz. Madde gerekçesi

[34] Gözel, *Elektronik Belge*,148.

[35] Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku,* 1987, *356.*

birinci fıkrasındaki sivil kişiler tarafından işlenen resmi belgede sahtecilik suçunu oluşturur. 204. maddenin birinci fıkrasındaki suç bakımından failin kamu görevlisi olması koşulu bulunmamaktadır. Burada, aslında kamu görevlisi tarafından düzenlenmesi gereken bir belge kamu görevlisi olmayan kişiler tarafından sahte olarak düzenlenmektedir.[36] Kamu görevlilerinin görevleri gereğince düzenledikleri dışında kalan ancak belge olmanın diğer unsurlarını taşıyan yazılar özel belgedir.[37] Başka bir ifadeyle belge kavramına girmekle birlikte resmi belgeden sayılmayan bütün yazılar, özel belge olarak kabul edilmektedir. TCK'nın 210/1. maddesi bazı özel nitelikteki belgeleri resmi belgeye eş değer olarak kabul etmiştir. Bunlar, resmi belge hükmündeki belgelerdir. Emre veya hamile yazılı kambiyo senetleri, emtiayı temsil eden belge, hisse senedi, tahvil ve vasiyetname bu tür belgelerden sayılmıştır.[38]

II. ELEKTRONİK VERİ (DATA) VE ELEKTRONİK BELGE KAVRAMLARI

A. Genel Olarak

Dijital ortamda yapılan iş ve işlemlerin fazlalığı ve bunların zaman içinde daha da artacağı göz önüne alındığında yakın gelecekte işlemlerin büyük bir çoğunluğunun, hatta tamamının elektronik ortamda yapılabileceğini söylemek olanaklı görünmektedir. Kanun koyucunun da elektronik belgenin hukuk sistemimiz içinde yaygınlaştırılmasını amaçladığı ifade edilebilir. Nitekim 6100 sayılı Hukuk Muhakemeleri Kanunu'nun 445. maddesinin gerekçesinde, kâğıtsız sisteme

---

36 Koray Doğan, "Ceza Hukukunda Belge Kavramı," *Ceza Hukuku Dergisi 5*, no. 14 (Aralık 2010):55.

37 Ahmet Öztel, "Adli Belge İncelenmesinde Karşılaşılan Sorunlar ve Çözüm Önerileri", *Türkiye Barolar Birliği Dergisi*, no. 50 (Ocak- Şubat 2004):154.

38 Doğan, "Ceza Hukukunda Belge Kavramı," 57; Erman, *Sahtekârlık Suçları-Ticari Ceza Hukuku, 1987*, 393; Sahir Erman, *Sahtekârlık Cürümleri*, (İstanbul: İsmail Akgün Matbaası, 1952), 394.

geçmenin amaçlandığı ifade edilmektedir.[39] Hukuk düzeni ve uygulamasının, herhangibir tereddüt ve adaletsizliğe yol vermemek amacıyla, değişen ihtiyaçlara olabildiğince hızlı bir şekilde cevap vermesi gerektiği hususu da gözetilerek "*elektronik veri*"lerin belgede sahtecilik suçlarına konu olan belge kavramının kapsamına dâhil olup olmadığı net bir şekilde ortaya konulmalıdır.

B. Elektronik Veri (Data) Kavramı

Elektronik veri (data) kavramı, Bilişim Terimleri Sözlüğünde; "*Olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi*"[40] şeklinde tanımlanmıştır. Başka bir tanıma göre elektronik veri; "*Sistem ve uygulama yazılımları, sabit disk veya flopi diskler, CD-ROM'lar, bantlar, sürücüler, hücreler, veri işleme cihazları ya da elektronik olarak kontrol edilen ekipmanla kullanılan herhangi diğer araçlar dâhil olmak üzere bilgisayar yazılımında veya üzerinde depolanan, oluşturulan veya kullanılan veya bu yazılımlara aktarılan ya da yazılımlardan aktarılan bilgiler, olgular veya programlar*"[41] anlamına gelir. Anılan kavram; "*Bilgisayarın bir sonuca ulaşmak amacıyla bilgi işleme süreci içinde, üzerinde işlem yaptığı rakamlar, sözcükler ve cümleler*"[42] şeklinde de tanımlanmaktadır.

Bu kavram TCK'da tanımlanmamış ancak "*Bilişim sistemine girme*" başlıklı 243. maddenin gerekçesinde; "*Sistem içindeki bütün soyut unsurlar veri teriminin kapsamındadır.*" şeklindeki ifadelerle kavrama açıklık getirilmeye çalışılmıştır. 5070 sayılı Elektronik İmza Kanunu'nun 3/a maddesine göre elektronik veri; "*elektronik, optik veya benzeri yollarla üretilen, taşınan ve saklanan*

---

[39] Bkz. madde gerekçesi.

[40] https://sozluk.gov.tr/?kelime= Bilişim Terimleri Sözlüğü, erişim tarihi: 19.06.2020.

[41] https://www.lawinsider.com/dictionary/electronic-data, erişim tarihi: 13.03.2021.

[42] Ayşe Saadet Arıkan, "Bilgisayar Programlarının Korunması AB. ve Türkiye," *Türkiye Barolar Birliği Dergisi*, no. 3 (1996): 326.

kayıtlardır". 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 2/1-k maddesinde, *"Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"*veri olarak tanımlanmıştır. Avrupa Siber Suçlar Sözleşmesi'nin 1/b maddesine göre elektronik veri; "*bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dâhil olmak üzere, bir bilgisayar sistemindeki işlenmeye uygun nitelikteki her türlü bilgi ve kavramı ifade eder*". Elektronik veriler klasik anlamdaki belgelerden farklı olarak bilgisayar veya makine tarafından işlenip depolanabilmektedirler. Hukuk sistemimiz nazarında, dijital ortamda bulunan elektronik verilerin belgenin varlığı için aranan birtakım koşulları sağlamaları durumunda elektronik belge olarak kabul edildiklerini söyleyebiliriz.[43] Kanaatimizce bu tanımlama ve açıklamalardan hareketle elektronik veri kavramı; " *elektronik cihazlarla üretilen, bu cihazlara kaydedilebilen ve bunlar aracılığıyla algılanabilen her türlü kayıtlar*" olarak ifade edilebilir.

C. Elektronik Belge

Elektronik belge, "*Elektronik ortamda sayısal olarak kodlanmış şekilde bulunan elektronik veriler*"; "*elektronik verilerin hukuki hüküm ifade edecek şekilde bir araya gelerek bir bütün oluşturması*";[44] "*bilgi sisteminde kullanılmak üzere elektronik biçimde sunulan dijital imza ve elektronik imza ile onaylanan bir belge*"[45]olarak tanımlanabilir. Başka bir tanıma göre ise "*Bir bilgisayar sistemi veya başka bir benzer cihaz içinde, herhangi bir ortama kaydedilen veya depolanan ve bir kişi veya bilgisayar sistemi ya da diğer benzer cihazlar tarafından okunabilen veya algılanabilen veriler anlamına gelir*".[46] 213 sayılı

[43] Gözel, *Elektronik Belge*,159.

[44] Mine Erturgut, Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi, (Ankara: Yetkin Yayınları, 2004),30.

[45] https://tr.wikipedia.org/wiki/Elektronik_belge, erişim tarihi:20.03.2021.

[46] https://www.lawinsider.com/dictionary/electronic-document, erişim tarihi: 13.03.2021.

Vergi Usul Kanunu m.242/2'ye göre elektronik belge; *"Şekil hükümlerinden bağımsız olarak bu Kanuna göre düzenlenmesi zorunlu olan belgelerde yer alan bilgileri içeren elektronik kayıtlar bütünüdür*." Yargıtay Ceza Genel Kurulu'na göre elektronik belge; *"Elektronik ortamda sayısal olarak kodlanmış bulunan elektronik verileri ifade etmektedir"*.[47] Bu tanımlardan elektronik belgelerin ayırt edici özelliklerinin, bilgisayar veya makine tarafından işlenmeleri ve depolanabilmeleri olduğu sonucuna ulaşılmaktadır.[48]Elektronik belgeler kodlanmış ve/veya kodlanmamış bilgi yığınını içerir.[49]

Elektronik verilerin bir araya gelip hukuken anlamlı bir bütünü oluşturmaları durumunda, elektronik belge yoluyla görünür olmaları söz konusu olmaktadır. Dolayısıyla elektronik belgenin, elektronik verilerden oluşan ve hukuksal açıdan anlam ifade eden bir bütünün taşıyıcısı olduğu ifade edilebilir. Elektronik belgeyi oluşturan verilerin algılanabilir olması zorunludur. Bu belgelerin, maddi varlığı bulunan şeyler üzerine yazılı olan klasik anlamdaki belgelerden farkları, doğrudan algılanabilmelerinin olanaklı olmamasıdır. Bunların algılanabilmeleri ancak bir veri taşıyıcısının yardımıyla olanaklı olmaktadır. Anılan kavram, dijital ortamda[50] yapılan hukuki işlemler, e-mailler, bir irade açıklamasını ihtiva eden elektronik veriler gibi elektronik ortamda gerçekleştirilen iş ve işlemleri kapsamaktadır[51].Elektronik sertifikayı ihtiva eden elektronik belge hukuksal anlamda sonuç doğurmaya elverişli belge niteliğini elde eder.[52]

---

47 Yar. CGK. E. 2017/11-46, K. 2017/211, 04.04.2017.

48 Gözel, *Elektronik Belge*,156.

49 Mine Erturgut, "Elektronik İmza Kanunu Bakımından E-Belge ve E-İmza," *Bankacılar Dergisi, no.* 48(2003): 66.

50 Dijital ortam; "verilerin üzerine kaydedilip saklandığı ortamların genel adıdır. https://tr.wikipedia.org/wiki/Dijital_ortam, erişim tarihi: 20.03.2021.

51 Erturgut, *Medeni Usul*, 29 vd.

52 Taşdemir, Belgelerde Sahtecilik**,** 248.

1. Elektronik Belgenin Unsurları

Elektronik ortamda kayıtlı bir yazının TCK anlamında belge olarak kabul edilebilmesi için klasik belgenin mevcudiyeti için gerekli olan tüm unsurları içermesi gerekmektedir. Kanaatimizce, elektronik belge, taşınabilir bir şey üzerine yazılı olmak, yazanı bilinebilinir olmak (imza unsuru) ve hukuki hüküm ifade edecek bir içeriğe sahip olmak unsurlarını taşıması durumunda TCK anlamında belge olarak kabul edilebilecektir.[53]

a. Yazılılık Unsuru

Klasik anlamda belge; irade beyanının kâğıt, metal vb. maddi varlığı olan cisimler üzerine yazılmasıyla oluşmaktadır.[54] Ancak, elektronik ortamda yazı kavramı klasik anlamından farklıdır. Elektronik ortamda, kişi iradesinin sayısal olarak saklanabilecek şekilde girilmesi de yazı olarak kabul edilmiştir.[55]

Kâğıt, metal, deri gibi maddi varlığı olan şeyler, üzerlerindeki yazı ve işaretlerin; elektronik belgelerse dijital ortamda oluşturulan verilerin taşıyıcısıdır. Bu belgelerin klasik belgelerden farkları doğrudan algılanamamalarıdır. Bunlar, ancak yardımcı teknik araçlar vasıtasıyla örneğin bilgisayar kullanılarak algılanabilmektedirler.[56]

Ayrıca elektronik ortamda oluşturulan belgelerin de veri taşıyıcılarına aktarılmaları durumunda, anılan ekipmanlar aracılığıyla taşınabilmeleri nedeniyle bu belgeler bakımından da

---

53 Gözel, *Elektronik Belge*,163; Taşdemir, *Belgelerde Sahtecilik*, 252.

54 Erem ve Toroslu, *Özel Hükümler*,252; Gökcan, "Resmi Belgede Sahtecilik Suçu,"96; Gözübüyük, *Türk Ceza Kanunu Gözübüyük Şerhi*, 278; Koca ve Üzülmez, *Özel Hükümler*, 763; Ekinci ve Esen, *Bilişim Alanında Suçlar*, 245246.

55 Memduh Aslan, "Vergilendirmede Elektronik Belgelerin Hukuki Geçerliliklerinin Değerlendirilmesi," *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi* 2, no. 3 (2014): 27.

56 Gözel, *Elektronik Belge*,157.

taşınabilir şekilde yazılılık koşulunun gerçekleşmiş olduğu kabul edilebilir.[57] El yazısıyla imzayla eşdeğer olduğu birçok yasal düzenlemeyle benimsendiğine göre güvenli elektronik imzayla imzalanmış olan elektronik belgelerin de istenildikleri zaman ibraz edilmek üzere saklanabilmeleri şartıyla yazılılık koşulunu taşıdıklarının kabulü gerekmektedir.[58] Kanaatimizce, fikri içeriği olan açıklamaların elektronik ortamdaki verilerden oluşması hâlinde de bunların taşınmaya ve devredilmeye elverişli oldukları gözetildiğinde, yazı koşulunun gerçekleşmesi için aranan taşınabilirlik unsurunun bulunduğunun kabulü gereklidir.

b. Belgeyi Düzenleyen Kişinin Teşhis Edilebilir Olması (İmza Unsuru)

Belgede sahtecilik suçundan bahsedilebilmesi için yalnızca yazı muhtevasında bir irade beyanının bulunması yeterli olmayıp bu irade beyanının kime ait olduğunun belgeden anlaşılabilmesi de gerekmektedir.[59] Klasik anlamdaki belgelerde

---

[57] Bazı yazarlara göre yazının mutlaka kağıt veya bez gibi taşınır şeyler üzerine yazılması zorunludur; Vincenzo Manzını, *Trattato Di Diritto Penale*, C.VI, (Torino: 1962), 93. (nakleden Toroslu, *Özel Kısım*,227); Faruk Erem, *Türk Ceza Kanunu Şerhi Özel Hükümler*, Cilt II. (Ankara: Seçkin Yayınevi, 1993), 1676; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*,314. Diğer bir görüşe göre ise, belgenin varlığı için aranan diğer unsurların mevcudiyeti durumunda taşınmazlar da, örneğin bir evin duvarındaki yazı da belge sayılmalıdır. Antolisei, Par. spec, II, 92, nakleden ve aynı düşüncede, Toroslu, *Özel Kısım*, 227.

[58] Fatih Önder, "Borçlar Hukuku Açısından Elektronik İmza" (Yüksek Lisans Tezi, Kırıkkale Üniversitesi, 2007), 30.

[59] Tezcan, Erdem ve Önok, *Ceza Özel Hukuku*, 1038; Erman, "Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu," 174; Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku, 1987*, 311; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*, 315; Gökcan, *Resmi Belgede Sahtecilik Suçu*, 99; Gözübüyük, *Türk Ceza Kanunu Gözübüyük Şerhi*, 278; Koca ve Üzülmez, *Özel Hükümler*, 766.

düzenleyenin kimliği genellikle üzerindeki imzadan anlaşılmaktadır.[60]

Güvenli elektronik imzayla imzalanmış belgelerdeyse belgeyi düzenleyenin kimliği elektronik imza sertifikasından tespit edilebilmektedir.[61] Güvenli elektronik imza, imzalama işlemi sırasında imzalayan kişinin kimliğinin doğrulanmasını sağlamaktadır.[62] Bu nitelikteki bir imzayla imzanmış bir belge, 5070 sayılı Elektronik İmza Kanunu'nun 4. maddesindeki münhasıran imza sahibine bağlı olma, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracıyla oluşturulma, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlama ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlama hususlarını içermektedir. Dolayısıyla, düzenleyen kişinin kimliğinin teşhisine olanak tanıyacaktır. Sonuç olarak; güvenli elektronik imzanın, belgenin düzenleyicisinin daha doğru bir ifadeyle, imza sahibinin tespitine güvenilir bir şekilde olanak tanıdığı söylenebilir.[63]

c. Hukuki Değeri Haiz Olması

Belgenin mevcudiyetinden söz edilebilmesi için yazı içeriğinin hukuki bir değeri haiz olması, hukuki sonuç doğuracak nitelikte olması gerektiği ifade edilebilir. Yasal anlamda belge olarak kabul edilebilmesi için güvenli elektronik imzayla oluşturulmuş olan belgenin de klasik belgeler gibi hukuki sonuç doğurması gerekmektedir.[64]

---

60 Erman," *Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu,"* 175; Erman, *Sahtekârlık Suçları, Ticari Ceza Hukuku, 1987,* 312; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar,316.*

61 Ayşe Ece Acar, *Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Değeri,* (İstanbul: XII Levha Yayınları, 2013), 96.

62 Gözel, *Elektronik Belge*,180.

63 Acar, *Elektronik İmzalı Belgelerin Delil Değeri*, 96.

64 Gözübüyük, *Türk Ceza Kanunu Gözübüyük Şerhi*, 279.

Özetle ifade etmek gerekirse; güvenli elektronik imzayla imzalanmış bir elektronik belge, klasik anlamdaki belgenin tüm unsurlarını haizdir. Elektronik belge, yazılı olmak, yazanı bilinebilir olmak ve hukuki hüküm ifade edecek bir içeriğe sahip olmak unsurlarını taşıyacak şekilde oluşturulabilir. Bunların yanında, dijital veri taşıyabilen hafıza kartları vb. birçok donanım aracıyla taşınabilir olmak unsurunu da içermektedir. Elektronik belgenin aslı, teknik araçlarda kayıtlı olanıdır. Bunların yazıcı ekipmanlar yardımıyla kâğıda dökülen suretleri hukuki hüküm doğurmamaktadır.[65] Islak imza içermeyen elektronik belge çıktıları yasal anlamda belge olarak kabul edilmemektedir.[66]Başka bir ifadeyle, elektronik imzalı belgenin fiziki çıktısı tek başına hukuki sonuç doğurmaz. Elektronik belge, yalnızca dijital yollardan teyit edildiğinde bir anlam ifade eder. E-imzalı belgenin çıktısı üzerinden elektronik imzanın kontrol edilmesi olanaklı değildir. Örneğin UYAP'tan alınıp "*elektronik imzayla imzalanmıştır*" ibaresini içeren bir belgenin ispat gücü bulunmamaktadır. Ancak ıslak imzayla onaylanmış olan belgelerin hukuki hüküm ifade etmeye elverişli oldukları kabul edilmektedir. Dolayısıyla bu nitelikteki belgelerin, TCK'da düzenlenmiş bulunan sahtecilik suçunun konusunu oluşturan belge kavramına dâhil oldukları kabul edilmektedir.[67]

Elektronik imza, belgeye yapılan her türlü müdahaleyi kaydederek gösterdiğinden belgenin gerçek olup olmadığı elektronik imza aracılığıyla belirlenebilmektedir. Kanaatimizce, bunların orijinalliği ancak elektronik ortamda denetlenebildiğinden çıktıları belge niteliğinde kabul

---

65 Taşdemir, *Belgelerde Sahtecilik*, 253.

66 Nurullah Tekin, "Resmi Belgede Sahtecilik Suçunda Bazı Özel Durumlar," *Türkiye Adalet Akademisi Dergisi*, no. 19 (Ekim 2014): 935; Güngör, *Resmi Belgelerde,*48; Erturgut, *Medeni Usul*, 47.

67 Taşdemir, *Belgelerde Sahtecilik***,** 298.

edilemez.[68]Ancak bu çıktılar vasıtasıyla anılan belgelerin algılanmaları sağlanmaktadırlar.[69]

2. Elektronik Belgenin Niteliği

Elektronik belgenin, TCK bakımından belge olarak kabul edilip edilmeyeceği hususu tartışmalıdır. Doktrindeki görüş farklılıkları esas itibariyle maddi varlığı olmayan yazıların TCK anlamındaki belge kavramının kapsamında bulunup bulunmadığı noktasında toplanmaktadır.

Doktrinde bazı yazarlara göre, belgenin mevcudiyeti için gerekli olan unsurları içermeleri durumunda, elektronik belgeler de ceza hukuku anlamında belge olarak kabul edilmelidir[70].

Bazı yazarlar ise, yalnızca maddi varlığı bulunan yazıların ceza hukuku anlamında belge olarak kabul edilebileceğini savunmaktadırlar[71].

Diğer bir kısım yazarlar ise kanunilik ilkesi gereğince elektronik ortamdaki verilerin ceza hukuku korumasından yararlanabilmeleri için bu ortamda yapılan sahtecilik fiillerinin

---

68 Bkz. Aynı görüşte Gözel, *Elektronik Belge*,157; Taşdemir, *Belgelerde Sahtecilik*, 298.

69 Erturgut, *Medeni Usul*, 34.

70 Ahmet Gökcen, *Belgede Sahtecilik Suçları*, (Ankara: Adalet Yayınevi, 2018), 52.(Bkz. 23 nolu dipnot); Dülger, Murat Volkan. "Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik Belge." *Belgede Sahtecilik Ve Vergi Suçları Sempozyumu*, TOBB ETÜ Sosyal Tesisleri Ankara 21-23 Ekim 2019, *Melek Metbaa&Promosyon Hizmetleri, Ankara 2020*: 175; Taşdemir, *Belgelerde Sahtecilik*,252-253; Gözel, *Elektronik Belge*,189; Tekin,"Resmi Belgede Sahtecilik," 935; Erturgut, *Medeni Usul*, 32-33.

71 Güngör, *Resmi Belgelerde*,50-51; Fahri Gökçen Taner, "Özel Belgelerde Sahtecilik Suçları Bağlamında Maddi Hasarlı Trafik Kazası Tespit Tutanakları (Kağıt Ve Elektronik) Ve Ortaya Çıkan Sorunlar," *Ceza Hukuku Dergisi,* no.35 (Aralık 2017):124.

mevzuatta açıkça suç olarak tanımlanmış olması gerektiğini savunmaktadırlar[72].

Güvenli elektronik imzayla imzalanmış belgelerin yasal anlamdaki niteliğiyle ilgili olarak Yargıtay'ın yerleşik bir uygulaması söz konusu değildir. Konuya ilişkin olarak çok az sayıda içtihada rastlanmaktadır. Bunların da soruna açıklık getirdiğini ifade etmek olanaklı görünmemektedir. Bu bağlamda Yargıtay tarafından özellikle elektronik ortamda oluşturulan elektronik işe giriş bildirgelerinde sahtecilik yapılması hâlinde durumun ne olacağı konusu üzerinden elektronik belgenin TCK anlamında belge olarak kabul edilip edilemeyeceği hususu tartışılmaktadır. Yargıtay 11. Ceza Dairesi'nin bu konuda muhalefet şerhleriyle çıkmış kararları mevcut olup[73]anılan

---

[72] Çetin Arslan ve İhsan Baştürk, "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler," *Erciyes Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 2 (2013): 208.

[73] "Akyol İnşaat isimli şirketin sahibi ve yetkilisi olan sanığın, gerçekte bu işyerinde çalışmayan şahısları çalışıyormuş gibi göstererek sahte işe giriş bildirgesi düzenlemek suretiyle resmi belgenin düzenlenmesinde yalan beyanda bulunma suçunu işlediğinin iddia olunması, sanığın suçlamaları kabul etmemesi, suça konu edilen işe giriş bildirgelerinin dosya kapsamında bulunmaması ve suça konu işe giriş bildirgesi üzerindeki imzaların aidiyetine ilişkin herhangi bir inceleme yaptırılmamış olması karşısında, maddi gerçeğin kuşkuya yer bırakmayacak şekilde belirlenmesi bakımından; öncelikle suça konu işe giriş bildirgelerinin kim tarafından verildiği, e-bildirge veya ıslak imzalı olarak verilip verilmediği Sosyal Güvenlik Kurumu'ndan sorulması, fiziki olarak verildiğinin, tespiti durumunda; suça konu belge asılları dosya arasına alınıp, belgelerde sahtecilik suçlarında aldatma niteliğinin bulunup bulunmadığının takdiri hakime ait olduğundan, suça konu belge asılları incelenmek suretiyle, özelliklerinin duruşma tutanağına yazılması ve aldatıcılık niteliğinin olup olmadığının değerlendirilmesi, belge üzerindeki imzaların ve yazıların sanığa ait olup olmadığı hususunun sanıktan sorulması, kabul etmemesi durumunda, konusunda uzman bir kurum veya kuruluştan rapor alınması, adlarına işe giriş bildirgesi düzenlenen kişilerin idari soruşturma sırasında vermiş oldukları beyanları hatırlatılarak çelişkilerin giderilmesinden sonra,

kararlarda elektronik ortamda güvenli imzayla oluşturulmasına rağmen e-işe giriş bildirgesinin resmi belge olarak kabul edilmediği anlaşılmaktadır. Yargıtay bazı karalarında elektronik işe giriş bildirgesinin TCK'nın 244. maddesinin 2. fıkrasındaki sisteme veri yerleştirme suçunu oluşturduğunu kabul etmiştir.

"*Sanığın Sosyal Güvenlik Kurumuna e-bildirge ile bilgisayar ortamında sahte işe giriş bildirgesi düzenleyerek işyerinde çalışmayan kişileri sigortalı olarak gösterdiği iddiasıyla açılan kamu davasında; e-bildirge, imza ve şifre ile bilgisayar ortamında işe giriş bildirgelerinin verilmesi eyleminde, sahte oluşturulmuş maddi varlığa haiz, somut bir belge olmadığı, eylemin bu hali ile TCK'nın 244. maddesi 2. fıkrasında yazılı sisteme veri yerleştirme suçunu oluşturduğu gözetilmeden suç vasfında yanılgı ile yazılı şekilde resmi belgede sahtecilik suçundan hüküm kurulmuş olması…*".[74]

sonucuna göre, fiziki olarak verilen işe giriş bildirgelerinin içeriğinde sahtecilik bulunması ya da belgelerin e-bildirge şeklinde verilmesi durumunda, kurum tarafından bu bildirimlere istinaden düzenlenmiş belgelerin varlığı halinde eylemin TCK'nin 206/1. maddesinde düzenlenen resmi belgenin düzenlenmesinde yalan beyanda bulunma suçunu oluşturacağı; fiziki olarak verilen işe giriş bildirgelerinin imza kısımlarında sahtecilik bulunması halinde eylemin TCK'nin 207. maddesinde düzenlenen "özel belgede sahtecilik" suçunu oluşturacağı da nazara alınarak sanığın hukuki durumunun belirlenmesi gerektiği gözetilmeden eksik araştırma ile hüküm kurulması..." Yar. 11. CD, E. 2018/4004, K. 2019/2115, 28.02.2019, (UYAP).

74 Yar. 11. CD, E. 2017/13703, K. 2017/5542, 13.09.2017; "*Fikir ve eylem birliği içinde hareket eden sanıkların D. S. Ü. Ticaret Ltd. Şti'nde fiilen çalışmayan kişileri sigortalı olarak gösterdikleri iddiasıyla açılan kamu davasında, gerçeğin kuşkuya yer vermeyecek şekilde ortaya çıkarılması bakımından; A. K. ile adı geçen şirket arasında suç tarihlerinden önce düzenlenen hizmet sözleşmesi bulunup bulunmadığının araştırılması, bulunması halinde getirtilip incelenerek, sözleşme kapsamının ve sözleşmenin şirket adına kim tarafından imzalandığının tespit edilmesi; gerçekte çalışmadıkları halde sigortalı olarak gösterilen kişiler ile aynı dönemde fiilen çalışan kişilerin tespit edilerek, fiilen çalışan kişilerin tanık sıfatıyla dinlenmesi; şirketin gerçek yetkilisinin kim olduğunun, idari ve mali işlemler ile*

Kanaatimizce, güvenli elektronik imzayla imzalanmış sahte elektronik işe giriş bildirgesine istinaden elektronik ortamda resmi veriler ve kayıtlar oluşturulduğundan anılan işe giriş bildirgeleri resmi belge mahiyetindedir. Bunun yanında ayrıca 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun "*Bilgi ve belge isteme hakkı, bilgi ve belgelerin Kuruma verilme usûlü*" başlıklı 100. maddesindeki; "*Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir*." şeklindeki özel düzenleme gereğince de elektronik işe giriş bildirgelerinin resmi belge olarak kabulü gerekmektedir. Bu nedenlerle Yargıtay'ın aksi yöndeki kararlarına iştirak etmediğimizi ifade etmek isteriz. Yargıtay'ın, bazı kararlarında bu yasal düzenlemeyi gözeterek suç vasfının yanlış tayin edilmiş olması nedeniyle ilk derece mahkemesi kararlarını bozduğu görülmektedir.

"5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 100. maddesinde yer alan ''Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir.'' şeklindeki düzenleme karşısında sanığın bir başkasına ait şifreyi kullanarak çalışmayan kişilerin çalışmaya başladıkları yönünde e-bildirge hazırlaması şeklindeki eyleminin resmi

kimin ilgilendiğinin, bildirgelerin kimin talimatı ile düzenlendiğinin araştırılması; bildirgenin maddi varlığı haiz, somut bir belge olarak düzenlenip kuruma verilmesi eyleminin sübutu halinde, TCK'nın 207. maddesinde düzenlenen "özel belgede sahtecilik" suçunun oluşacağı, bildirgelerin e-şifre ile elektronik ortamda düzenlenip kuruma iletilmesi eyleminin sübutu halinde, TCK'nın 244/2, 43/1. maddelerinde düzenlenen "zincirleme olarak sisteme veri yerleştirme" suçunun oluşacağı, sahtecilik ve sisteme veri yerleştirme suçlarının oluşması için saik ve maksat aranmadığından genel kastın yeterli olduğu gözetilip, toplanan deliller birlikte değerlendirilerek sonucuna göre sanıkların hukuki durumunun belirlenmesi gerekirken, eksik araştırma ve yetersiz gerekçeyle yazılı şekilde karar verilmesi, Yasaya aykırı…" Yar. 11. CD, E. 2017/4157, K. 2018/973, 07.02.2018; Aynı yönde Yar. 11. CD, E. 2014/9737, K. 2016/726, 28.01.2016; Yar. 11. CD, E. 2013/10595, K. 2015/31550, 03.12.2015, (UYAP).

evrakta sahtecilik suçunu oluşturup oluşturmayacağı tartışılmadan yazılı şekilde karar verilmesi Yasaya aykırı…".[75]

Yargıtay Ceza Genel Kurulu'nun 04.04.2017 gün ve 2017/11-46 E., 2017/211 K. sayılı içtihadına göre; "*E-imza sahibinin imza doğrulama verisinin ve kimlik bilgilerini birbirine bağlayan elektronik kayıt yani elektronik sertifikanın da yer almasıyla e-belge hukuken sonuç doğurmaya elverişli belge niteliğini kazanacaktır*". Yargıtay Ceza Genel Kurulu, 2016/1065 E., 2017/27 K. 24.01.2017 tarih ve sayılı kararında da benzer şekilde; *"Gerçeğe aykırı olarak düzenlenen ödeme listelerinin elektronik imza ile imzalanmamış olması nedeniyle bu belgelerin gerçeğe uygun şekilde düzenlenerek maliyeye gönderilen ödeme listelerinin içeriğini sahteleştirecek nitelikte bulunmadığının kabulü gerekmektedir."* şeklindeki açıklamalarda bulunmuştur. Kanaatimizce, bu içtihatlarından, Genel Kurul'un, güvenli elektronik imzayı el yazısıyla atılan imzaya eşdeğer gördüğü ve bu imzayla oluşturulmuş olan elektronik belgeyi resmi belge olarak kabul ettiği sonucuna ulaşılabilir.

Ancak Genel Kurul, yeni tarihli bir kararıyla, anılan içtihatlarıyla çelişki oluşturacak nitelikte bir sonuca ulaşmıştır. Yargıtay Ceza Genel Kurulu'nun, 29.09.2020 tarih, 2017/11-1122 esas, 2020/381 karar sayılı kararına göre;

"5237 sayılı TCK'da 765 sayılı mülga TCK'dakine benzer biçimde elektronik verilerin "belge" olarak kabul edilebileceklerine ve sahtecilik suçunun konusunu oluşturabileceklerine ilişkin bir norm mevcut değildir. Bu nedenle kanunilik ilkesi gereğince elektronik belgelerin sahtecilik suçuna konu olabilmesi ve ceza hukuku korumasından yararlanabilmesi için yasa hükmüyle "belge" olarak nitelenmesi zorunludur". Yargıtay bu kararıyla *"*kanunilik ilkesi"ni gerekçe göstererek elektronik belgelerin sahtecilik suçunun konusunu oluşturabilmeleri için bu konuda yasal bir düzenleme yapılmış olmasının zorunlu olduğu hususunu benimsemiştir. Yargıtay,

[75] Yar. 8. CD, E. 2012/31922, K. 2013/29069, 12.12.2013, (UYAP).

anılan kararında ayrıca, gerçeğe aykırı elektronik işe giriş bildirgesi düzenlenmesi hâlinde eylemin Sosyal Sigorta İşlemleri Yönetmeliği'nin 11 ve 15. maddeleri gereğince elektronik ortamda düzenlenmesi gereken işe giriş bildirgelerinin 5510 sayılı Kanun'un 100. maddesi gereğince TCK'nın 204/1. maddesinde düzenlenen resmî belgede sahtecilik suçu ile birlikte TCK'nın 244/2. maddesinde düzenlenen sisteme veri yerleştirme suçunu da oluşturacağını kabul etmiştir. Bu bağlamda, TCK'nın 244. maddesinin ikinci fıkrasındaki düzenlemenin elektronik belgelerde yapılacak sahtecilik eylemlerine ilişkin özel norm niteliğinde olduğunu, özel normun önceliği ilkesi gereğince de sanık hakkında genel normun değil özel normun uygulanması gerektiğini belirtmiştir. Yargıtay bu kabullerden hareketle, sanığın eyleminin TCK'nın 204. maddesinin birinci fıkrasında yer alan resmî belgede sahtecilik suçuna göre özel norm niteliğinde olduğu gerekçesiyle aynı Kanun'un 244. maddesinin ikinci fıkrasındaki bilişim sistemine veri yerleştirme suçunu oluşturduğu sonucuna ulaşmıştır.[76]

---

[76] *"Mali müşavir olan şikâyetçi Y. H.'in bürosunda çalışması nedeniyle mükelleflere ait elektronik bildirge şifrelerini öğrenen sanık S. E.'ın, iş yerinden ayrıldıktan sonra katılan Ç. K.'e ait şifreyi onun bilgisi dışında kullanarak Y. K. isimli iş yerinde gerçekte çalışmayan M. F. Y., A. M., F. K., Ö. A., Ö. A. ve H. E. isimli kişileri sanki bu iş yerinde çalışıyorlarmış gibi gösterip haklarında gerçeğe aykırı elektronik işe giriş bildirgeleri düzenlediği olayda; suç tarihinde yürürlükte bulunan Sosyal Sigorta İşlemleri Yönetmeliği'nin 11 ve 15. maddeleri gereğince elektronik ortamda düzenlenmesi gereken işe giriş bildirgelerinin 5510 sayılı Kanun'un 100. maddesi gereğince adli ve idari makamlar nezdinde resmî belge niteliğinde olacağı ve elektronik ortamda düzenlenecek bu belgeler üzerinde yapılacak sahtecilik eylemlerinin de resmî belgede sahtecilik suçunu oluşturacağı öngörülmüş ve Yerel Mahkemece sanık hakkında TCK'nın 204. maddesinin birinci fıkrasında düzenlenen resmî belgede sahtecilik suçundan mahkûmiyet hükmü kurulmuş ise de aynı Kanun'un 244. maddesinin ikinci fıkrasındaki "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" şeklindeki düzenleme karşısında sanığın eyleminin*

Mevzuatta, ceza kanunundaki sahtecilik suçlarını düzenleyen maddelerin elektronik belgelere uygulanamayacağını gösteren herhangi bir düzenleme bulunmamaktadır. Kanaatimizce, elektronik belgeler, belge kavramının bütün unsurlarını haiz olduklarından bunların resmi belge olduklarını özel olarak düzenleyen herhangi bir yasal düzenlemeye gerek kalmaksızın TCK anlamındaki belge kavramına dâhildirler. Güvenli elektronik imzayla imzalanmış olan elektronik veriler bütün unsurlarını içerdiğinden, bunları belge olarak değerlendirdiğimizde ne kıyas yasağı ne de suç ve cezada kanunilik ilkesi ihlal edilmektedir.[77] Ceza Genel Kurulu'nun yukarıda anılan 29.09.2020 tarih, 2017/11-1122 esas, 2020/381 karar sayılı kararındaki kabul doğrultusunda düşünüldüğünde, resmi belge olduklarına dair özel bir yasal düzenlemeye konu edilmeyen tüm elektronik belgelerin kanuni anlamda resmi belge olarak kabul edilmemeleri gerektiği sonucuna ulaşılmaktadır. Başka bir ifadeyle, aksi görüşün kabulü halinde, yasal bir düzenlemeyle resmi belge oldukları özel olarak belirtilmediği takdirde UYAP'ta kayıtlı belgeler örneğin mahkeme ilamları da dâhil olmak üzere birçok kamu kurumunun resmi sistemlerinde kayıtlı elektronik belgelerin, TCK anlamda belge olmadıkları sonucuna ulaşılır. Zira örneğin UYAP'ta kayıtlı mahkeme ilamlarının resmi belge olduklarına

aynı zamanda bilişim sistemine veri yerleştirme suçunu da oluşturduğu, TCK'nın 244. maddesinin ikinci fıkrasındaki bu düzenlemenin elektronik belgelerde yapılacak sahtecilik eylemlerine ilişkin özel norm niteliğinde olduğu ve özel normun önceliği ilkesi gereğince de sanık hakkında genel normun değil özel normun uygulanması gerektiği hususları göz önünde bulundurulduğunda, sanığın eyleminin TCK'nın 204. maddesinin birinci fıkrasında yer alan resmî belgede sahtecilik suçuna göre özel norm niteliğinde olan aynı Kanun'un 244. maddesinin ikinci fıkrasındaki bilişim sistemine veri yerleştirme suçunu oluşturduğu kabul edilmelidir". Yar. CGK, E. 2017/11-1122, K. 2020/381, 29.09.2020, (UYAP).

77 Aynı görüşte Tekin, "Resmi Belgede Sahtecilik," 94-95; Taşdemir, *Belgelerde Sahtecilik*, 252-253; Gözel, *Elektronik Belge*,189.

dair herhangi bir açık yasal düzenleme bulunmamaktadır. Oysaki bunların resmi belge olarak kabul edilmeleri yönünde bir uygulama gelişmiştir.

III. ELEKTRONİK İMZA

A. Elektronik İmza Kavramı

İmzanın sözlük anlamı; "*Bir kimsenin herhangi bir belgeyi yazdığını veya onayladığını belirtmek için her zaman aynı biçimde kullandığı işaret*"[78]tir. Bu tanımlama gözetildiğinde, imzanın varlığının kabulü için yazılı kâğıt ve kalemin mevcudiyeti şartı bulunmamaktadır. Bir sembolün varlığı ve belgenin muhtevasıyla anılan belgeyi düzenleyen kişinin iradesinin örtüşmesi yeterli kabul edilmelidir. Bu bakımdan elektronik bir kayıt ya da verideki sembol veya kodların da imza olarak kabul edilmelerinin önünde herhangi bir engel bulunmamaktadır. Elektronik ortamda (dijital ortam) yapılan işlemlerde en önemli ihtiyaç güvenliktir. Bu güvenliği sağlayıp gizlilik, işlem emniyeti ve bunun yanında dijital ortamdaki iş ve işlemleri gerçekleştiren kişilerin hüviyetlerinin gerçekliğini garanti edebilmek başka bir ifadeyle belgeyi düzenleyen kişinin tespit edilebilmesi ve belgeyle bunu düzenleyen arasındaki bağın inkârının önüne geçilmesi amacıyla elektronik imza tekniği geliştirilmiştir. Elektronik imzanın, dijital ortamda gerçekleştirilen hukuki işlemler bakımından gerekli olan güvenlik, işlemi yapan kişinin kimliğinin belirlenmesi, yapılan işlemin inkârının önlenmesi unsurlarını sağlamaya yönelik olarak ortaya çıkarıldığı söylenebilir. Bu tekniğin yasal olarak geçerliliğinin sağlanması bakımından da gerekli düzenlemeler yapılmaktadır. Ülkemizde bu yöndeki düzenleme 5070 sayılı Elektronik İmza Kanunu'yla ortaya konulmuştur.[79] 5070 sayılı Kanun m.3/b'deki düzenlemede elektronik imza; "*başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik*

---

78 https://sozluk.gov.tr/, erişim tarihi:20.03.2021.

79 Önder, "Borçlar Hukuku Açısından Elektronik İmza," 29-31.

doğrulama amacıyla kullanılan elektronik veri" şeklinde tanımlanmıştır. 1999/93 sayılı Avrupa Birliği Direktifi m.2'de elektronik imza; "*diğer elektronik verilere eklenen veya bunlarla mantıksal olarak ilişkilendirilen ve bir kimlik doğrulama yöntemi işlevi gören elektronik biçimdeki veriler*"[80] şeklinde tanımlanmıştır. Elektronik imza, bu tanımlamaların yanında; "*Elektronik ortamda oluşturulmuş bir mesajın bütünlüğünü ve değişmemişliğini ifade eden, aynı zamanda mesaj sahibinin kimliğini tanımlamaya yarayan her türlü elektronik işaret*",[81] *"başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir. E-imza olarak da bilinir. Elektronik ortamlarda imza yerine kullanılabilen yasal kimlik doğrulama sistemi*"[82]şeklinde de tanımlanmaktadır. Anılan kavram Amerika Birleşik Devletleri Küresel ve Ulusal Ticarette Elektronik İmza Kanunu'nun (Electronic Signatures in Global and National Commerce Act) tanımlar bölümünde; "*Bir sözleşmeye veya başka bir kayda iliştirilmiş veya mantıksal olarak ilişkilendirilmiş ve kaydı imzalama niyetiyle bir kişi tarafından yürütülen veya benimsenen elektronik bir ses, sembol veya işlem*"[83] şeklinde tanımlanmaktadır.

Elektronik iletişimde beş güvenlik unsurunun sağlanmış olması gerekmektedir. Bunlar, güvenilirlik, veri bütünlüğü, yetkili şahsın belirlenebilirliği, inkâr edilememe ve giriş korumasıdır. Elektronik imzayla oluşturulmuş olan belgeler üzerinde yapılacak her türlü değiştirme ve silme işlemlerinin elektronik araçlarla yapılacak kontroller yoluyla tespiti olanaklıdır. Dolayısıyla, bu belgeler üzerinde yapılan sahtecilik

---

80 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093, erişim tarihi:15.03.2021.

81 Önder, "Borçlar Hukuku Açısından Elektronik İmza," 3.

82 https://tr.wikipedia.org/wiki/Elektronik_imza, erişim tarihi:20.03.2021.

83 https://en.wikipedia.org/wiki/Electronic_Signatures_in_Global_and_National_Commerce_Act#Definitions, erişim tarihi:21.03.2021.

fiillerinin ortaya çıkartılması klasik anlamdaki belgeler üzerinde gerçekleştirilen fiillere oranla daha kolaydır. Bu sebeple değiştirilemez bir belgenin belgeyi gizli anahtarıyla imzalayan kişiden sâdır olduğunu kabul etmek gerekmektedir.[84]

Kural olarak imza elle atılır.[85] 6098 sayılı Türk Borçlar Kanunu m.15'te imzanın elle atılmasının zorunlu olduğu belirtilmiştir. İmzanın el dışında bir araçla atılması, aynı yasanın 15 inci maddesinin ikinci fıkrasında belirtilen durumlarda geçerli kabul edilir. Bu maddede güvenli elektronik imzanın da el yazısıyla atılmış imzanın bütün hukuki sonuçlarını doğuracağı ifade edilmiştir. Bu düzenlemeyle nitelikli elektronik imza, el yazısı imzanın eşdeğeri kabul edilmiştir.[86] Elektronik imzanın, elle atılan imzayla eşdeğerde kabul edilebilmesi için imzalayan şahsın hüviyetinin tespiti ve imzalanan irade beyanıyla imza arasında bağlantı (sonuçlandırma) işlevlerini içermesi gerekmektedir. Bu unsurları içeren bir elektronik imzanın, ispat fonksiyonunu da haiz olduğu kabul edilecektir.[87]

Elektronik İmza el yazısıyla imzanın bir istisnası değildir. El yazısıyla imzanın istisnaları mevzuatta buna izin verilmesi şartıyla, fiziki belge üzerinde şahıslardan kaynaklanan sebeplerle ıslak imza atma olanağının bulunmadığı durumlarda söz konusu olur. Fiziki belge üzerine yasanın öngördüğü şekillerde oluşturulur. Elektronik imzaysa elle atılan imzanın dijital ortamdaki karşılığı olup işlev ve doğurduğu sonuçlar itibariyle elle atılan imzanın alternatifidir.[88]

---

84 Erturgut, *Medeni Usul*, 55-58.

85 Erman, "Evrakta Sahtekârlık Suçlarında "Varaka "Mefhumu," 172; Erman ve Özek, *Kamu Güvenine Karşı İşlenen Suçlar*, 311; Soyaslan, *Özel Hükümler*, 486.

86 İnci Biçkin,"Elektronik İmza Kanunu ve Getirdiği Düzenlemeler," *Yargıtay Dergisi* 30, no. 3 (2004): 358.

87 Erturgut, *Medeni Usul*, 104.

88 Önder, "Borçlar Hukuku Açısından Elektronik İmza", 25.

Elektronik imzanın el yazısıyla atılan imzayla eşit kabul edilebilmesi için iki şartın gerçekleşmesi gerekir. Bu şartlar; belgeyi imzalayanın kimliğinin tespiti ve imzalanan metinle imza arasında bağlantı, yani sonuçlandırma işlevidir. Bu iki şartın gerçekleşmesi durumunda imzanın ispat fonksiyonu da sağlanmış olacaktır.[89]Mevcut mevzuat gözetildiğinde ancak nitelikli elektronik imzayı içeren belgeler hukuken ıslak imzayla eşdeğerde kabul edilebilmektedir.[90] Bu husus 5070 sayılı Kanun m.5'te; *"Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur."* şeklinde ifade edilmiştir.

Güvenli elektronik imzanın yanında basit elektronik imza olarak adlandırılan imzalar da bulunmaktadır. Bu tür imzalara örnek olarak kişilerin biyometrik özelliklerini esas alarak kullanılan örneğin ses, parmak izi ya da göz retinası taranmasının söz konusu olduğu imzalar, elle atılıp tarayıcıdan bilgisayara (elektronik ortama) aktarılanlar, kredi kartları için kullanılan PIN, bilgisayara ve cep telefonlarının ekranlarına doğrudan bu iş için özel olarak yapılmış kalemlerle atılanlar ve çift anahtarlı kriptografi tekniğiyle üretilmiş bulunan dijital (sayısal) imzalar gösterilebilir. Bu bağlamda elektronik imzanın, bir belgenin elektronik ortamda imzalanması için kullanılabilen yöntemlerin tümünü ifade bir üst kavram olduğu söylenebilir.[91] Şimdilik basit elektronik imzalı belgelerin yasal anlamda belge olarak kabul edildiğini söylemek olanaklı görünmemektedir.[92] Ancak Avrupa Birliği Direktifi m.5'te güvenli elektronik imza içeren yazılar dışında kalıp diğer elektronik imzalarla imzalanmış yazıların da hukuki etki doğurmasına veya

89 Erturgut, *Medeni Usul,* 104.

90 İnci Biçkin, "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler." *Türkiye Barolar Birliği Dergisi,* no. 63 (2006): 23.

91 Erturgut, *Medeni Usul*, 61; Önder, "Borçlar Hukuku Açısından Elektronik İmza," 31.

92 Güngör, Resmi Belgelerde, 47.

yargılamada caiz delil olarak kullanılmasına engel olunmaması gerektiği ifade edilmiştir.[93] Kanaatimizce, Avrupa Birliği direktifinde belirtildiği üzere diğer elektronik imzalarla imzalanmış olan yazıların da güvenli elektronik imzadaki kadar güçlü olmasa dahi hukuki anlamda sonuç doğurduklarının kabulü gerekmektedir. Başka bir ifadeyle, "*delil serbestisi ilkesi*"nin bir sonucu olarak dijital deliller de yargılama sürecinde kullanılabilmelidirler.[94]

1. İstisnai Durumlar

5070 sayılı Kanun m.5/2'ye göre; "*Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemler ile banka teminat mektupları dışındaki teminat sözleşmeleri, güvenli elektronik imza ile gerçekleştirilemez*." Bu düzenlemeyle elektronik imzanın uygulama alanını daraltılmaktadır. Düzenlemeyle banka teminat mektupları maddedeki sınırlama kapsamının dışında bırakılmıştır. Bu maddede belirtilen hukuksal işlemlerin öngörülen usulde yapılması zorunlu şekil şartı olup bunların elektronik imzayla imzalanması olanağı bulunmamaktadır. Aksi durumda anılan işlemler geçersiz olacaktır. Ancak bu sınırlama, resmi belgelerin tamamını kapsamayıp yalnızca mevzuatın özel usuller öngördüğü hukuki işlemlere ilişkin belgeler ve teminat sözleşmeleri bakımından geçerlidir. Dolayısıyla diğer tüm resmi belgeler nitelikli elektronik imza kullanılarak imzalanabilir[95]. Kanunların resmi şekle veya özel bir merasime tabi tuttuğu hukuki işlemlere örnek olarak; noterlerde yapılan işlemler, resmi vasiyetname, kefalet sözleşmeleri, evlenme akdi, tescil zorunluluğu bulunan işlemler örneğin gayrimenkul ve motorlu

---

93 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093,erişim tarihi:15.03.2021; Erturgut, *Medeni Usul*, 61.

94 Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi," *Ceza Hukuku ve Kriminoloji Dergisi 3, no. 2 (2015)*: 257.

95 Güngör, *Resmi Belgelerde,* 48; Önder, "Borçlar Hukuku Açısından Elektronik İmza," 65.

araç alım satımı gibi işlemler gösterilebilir. Ancak teknolojik gelişmeler gözetilerek getirilecek yasal düzenlemelerle elektronik ortamda yapılabileceklerinin belirtilmesi halinde, bunlarında elektronik belge olarak düzenlenmesi söz konusu olabilecektir. Bu bağlamda 6572 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6. maddesiyle Noterlik Kanunu'na eklenen 198/A maddesinde, Kanunda öngörülen noterlik işlemlerinin elektronik ortamda güvenli elektronik imza kullanılarak da yapılabileceği belirtilmiştir. Dolayısıyla Noterlerde yapılan işlemlerin Noterlik Kanunu'na eklenen 198/A maddesi kapsamında kalması halinde bunların elektronik olarak yapılabilmeleri mümkün olmaktadır. Bunların dışında, 5070 sayılı Kanun m.5/2'deki hüküm kapsamında kalan işlemlerin şimdilik elektronik yollarla yapılamayacağı ve elektronik imza kullanılarak bu işlemlerin yapılması durumunda da geçersiz olacakları anlaşılmaktadır.[96]

Maddede belirtilen istisnalardan biri kambiyo senetleridir. Kambiyo senetleriyle ilgili olarak 6102 sayılı TTK. "İmzalar" başlıklı 756. maddesine göre (mülga TTK. md.668) *"Poliçe üzerindeki beyanların el ile imza edilmesi gerekir. El ile atılan imza yerine, mekanik herhangi bir araç veya elle yapılan veya onaylanmış bir işaret veya resmi bir şahadetname kullanılamaz."*Bu hükmüyle Kanun, kambiyo senetlerinin mutlaka elle imzalanmasını şart koşmuş olup değişik gerekçelerle imza atamayan kişilerin Borçlar Kanunu'nun 16. maddesindeki istisnalardan yararlanmalarına da olanak tanımamıştır.[97] Kambiyo senetlerinin yürürlükteki mevzuat gereğince elle imzalanması zorunlu şekil şartıdır. Yasal düzenlemeler değişmedikçe bunların elektronik imzayla imzalanmaları hâlinde ortada

[96] Önder, "Borçlar Hukuku Açısından Elektronik İmza," 65.

[97] Ahmet M. Kılıçoğlu, *Borçlar Hukuku Genel Hükümler*, (Ankara: Turhan Kitabevi, 2018), 200.

geçerli bir kambiyo senedinin bulunduğunun kabulü mümkün olmayacaktır.[98]

B. Güvenli Elektronik İmza

5070 sayılı Elektronik İmza Kanunu'nun "*Güvenli Elektronik İmza*" başlıklı 4. maddesinde elektronik imzanın unsurları olarak;

* Münhasıran imza sahibine bağlı olma,

* Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulma,

* Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlama,

* İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlama hususları sayılmıştır.

Bu düzenlemeye göre güvenli elektronik imzanın varlığı; kişiye hasredilmiş olmasına, nitelikli elektronik sertifikayı içeren imzayla oluşturulmasına, meydana getiren kişinin hüviyetinin belirlenebilmesi olanaklarını içerip içermediğine bağlıdır. Güvenli elektronik imzanın, bu sayılanların yanında ayrıca imzalandıktan sonra bu belgeye herhangi bir müdahalede bulunulup bulunulmadığının tespitine olanak tanıyan teknik imkânları da barındırması gerekmektedir.

Aynı yasanın güvenli elektronik imzanın hukuki sonucu ve uygulama alanı başlıklı 5. Maddesinde; güvenli elektronik imzanın ıslak imzayla aynı hukuki sonucu doğuracağı vurgulandıktan sonra kanunların resmi şekil veya özel bir usule tabi tuttuğu hukuki işlemler ve banka teminat mektupları dışındaki teminat sözleşmelerinin güvenli elektronik imzayla gerçekleştirilemeyeceği belirtilmiştir.

---

98 Erturgut, *Medeni Usul*, 124.

Güvenli elektronik imza, el yazısı (ıslak) imzanın işlevlerini yerine getirebilmektedir. Yani ıslak imzayla güvenli elektronik imza hukuki ve fonksiyonel anlamda eşittir. Elle atılan imzayla yapılabilecek her türlü işlem güvenli elektronik imza yoluyla da yapılabilir.[99]Elektronik imzada veri güvenliğinin, el yazısıyla imzaya nazaran daha yüksek olduğu göz önünde bulundurulmalıdır. Dijital imzada verinin bütünlüğünün sonraki müdahalelere karşı korunması, belgeyi imzalayanın kimliğinin tespitine olanak sağlanması, imzayla metin arasındaki irtibatın kolaylıkla ve güvenilir bir şekilde belirlenebilmesi ve imzanın kontrolünün tamamen elektronik ortamda ve otomatik olarak yapılması hususları gözetildiğinde nitelikli elektronik imza içeren belgelerin el yazısıyla atılan imzayı içeren klasik anlamdaki belgelerden daha güvenli olduğu açıkça anlaşılacaktır.[100]

Güvenli elektronik imza, elle atılan imzadaki gibi belgenin bunu imzalayandan sadır olduğuna dair işlevi yerine getirmesinin yanı sıra elektronik verileri her türlü müdahaleye karşı da korumaktadır. Dolayısıyla bu imzayı içeren belgeler üzerinde sahtecilik fiillerinin gerçekleştirilmesi kâğıt ya da maddi varlığı bulunan bir şey üzerine yazılan yazılara oranla daha zordur.[101]

5070 sayılı Kanunu'nun 5. maddesinin gerekçesinde de vurgulandığı üzere güvenli elektronik imzanın ıslak imzayla hukuken aynı hüküm ve sonuçları doğurabilmesi için öncelikli olarak Elektronik İmza Kanunu başta olmak üzere yasal düzenlemelere uygun olması zorunludur. Dolayısıyla güvenli elektronik imzanın mevzuata aykırı olması hâlinde ıslak imzayla

99 Önder, "Borçlar Hukuku Açısından Elektronik İmza," 44.

100 Erturgut, *Medeni Usul*, 55.

101 Güngör, Resmi Belgelerde,47.

aynı nitelikte kabul edilmesi olanaklı değildir.[102] Yasanın aradığı şartları taşımayan bir elektronik imza güvenli elektronik imza vasfını haiz olamayacaktır. Bütün bu özellikleri ve yasal düzenlemeler gözetildiğinde, güvenli elektronik imzanın, ıslak imzanın tüm işlevlerini tamamen yerine getirdiği, bunların hukuki ve fonksiyonel anlamda eş değer olduğu görülmektedir.[103] Yürürlükteki mevzuat gözetildiğinde, elektronik imza çeşitleri arasında yalnızca güvenli elektronik imza içeren yazılar yasal anlamda belge olarak kabul edilebilir.[104]

IV. ELEKTRONİK İMZALI BELGELERİN BENZER DÜZENLEMELER BAKIMINDAN DEĞERLENDİRİLMESİ

Elektronik belgeler üzerinde gerçekleştirilen eylemlerin 5070 sayılı yasanın 16 ve 17. maddeleri ve 5237 sayılı TCK'nın 244. maddesi kapsamında değerlendirilip değerlendirilemeyeceği hususları da tartışılmaktadır.[105]

5070 sayılı Kanun'un "*İmza oluşturma ve verilerin izinsiz kullanımı*" başlıklı 16. maddesine göre; "*Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılırlar. Bu suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır*.";

Aynı kanunun "*Elektronik sertifikalarda sahtekârlık" başlıklı 17. maddesine göre ise; "Tamamen veya kısmen sahte elektronik sertifika*

---

[102] Mehmet Ertan Yardım, "Elektronik İmza ve Elektronik İmzanın Medeni Usul Hukukumuza Etkileri" (Yayınlanmış Yüksek Lisans Tezi, İstanbul Üniversitesi, 2006), 77.

[103] Taşdemir, *Belgelerde Sahtecilik*, 248 vd.

[104] Güngör, *Resmi Belgelerde*, 47.

[105] Taşdemir, *Belgelerde Sahtecilik*, 251.

oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adli para cezasıyla cezalandırılır. Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."

Görüldüğü gibi 5070 sayılı Kanun'un 16 ve 17. maddelerinde elektronik ortamda düzenlenen sahte belgelerden değil izinsiz imza oluşturulması ve sertifikada sahtecilik yapılması gibi eylemlerden bahsedilmektedir. Bu bağlamda, anılan Kanunun 16. maddesindeki suçun oluşması için elektronik imza oluşturmak maksadıyla ilgili kişinin rızası dışında, imza oluşturma verisi ya da imza oluşturma aracının elde edilmesi, üçüncü şahıslara verilmesi, kopyalanması ve bu araçların yeniden oluşturulmasıyla izinsiz elde edilen imza oluşturma araçlarının kullanılması suretiyle izinsiz elektronik imza oluşturulması şeklindeki hareketlerin gerçekleştirilmesi gerekmektedir. Kanunun 17. maddesindeki suçun oluşması için ise elektronik sertifikaların tamamen veya kısmen sahte oluşturulması veya geçerli olarak oluşturulan elektronik sertifikaların taklit veya tahrif edilmesi ve bu elektronik sertifikaların bilerek kullanılması şeklindeki hareketlerin yapılması gerekmektedir. Dolayısıyla bu kanun maddelerinin sahte elektronik belge düzenlenmesi ve kullanılması hâlinde uygulanamayacağı kanaatindeyiz.[106] Bunun gibi TCK'nın "*Sistemi engelleme, bozma, verileri yok etme veya değiştirme*" başlıklı 244/2. maddesinin de e-belgede yapılan sahtecilik eylemlerinde uygulanabileceği düşünülebilir. Anılan maddeye göre;

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

[106] Aynı görüşte bkz. Taşdemir, *Belgelerde Sahtecilik*, 297.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur."

Maddenin ikinci fıkrasıyla, *"verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi, mevcut verilerin başka bir yere gönderilmesi"* fiilleri yaptırım altına alınmıştır. Bu fıkrada düzenlenen suçun konusunu bilişim sistemindeki veriler oluşturmaktadır[107]. Başka bir ifadeyle fıkradaki düzenlemenin, belge özelliğini haiz olmayan elektronik veriler üzerinde gerçekleştirilen eylemlere ilişkin olduğu ve elektronik belge niteliğini kazanmış olan veri bütününü kapsamadığı ifade edilebilir. Zira elektronik belgelerin, elektronik verilerin bir araya gelip anlamlı bir bütün oluşturması sonucunda oluştuğu gözetildiğinde elektronik bir belgede sahtecilik fiili, bu belgeyi oluşturan verilere müdahale edilmesi, bu bağlamda anılan verilerin değiştirilmesi, bozulması, yok edilmesi yoluyla ya da bilişim sistemine veri yerleştirilmesi suretiyle gerçekleştirilebileceği sonucuna ulaşılmaktadır[108]. Dolayısıyla eylemin, belge niteliğini haiz veriler bütünü üzerinde gerçekleştirilmesi durumunda TCK'nın belgede sahteciliği düzenleyen 204 vd. maddeleri hükümlerinin; aksi durumdaysa aynı Kanunun 244/2. fıkrasının kapsamında kalacağı kanaatindeyiz. Konuya örnek vermek gerekirse Sosyal

[107] Koca ve Üzülmez, *Özel Hükümler*, 914.

[108] Dülger, *Elektronik Belge*,178.

Güvenlik Kurumunda çalışan bir kamu görevlisinin bir kişiye ait sigortalılık bilgilerini kurumun elektronik sistemi üzerinden gerçeğe aykırı olarak değiştirmesi durumunda TCK'nın 244. maddesinin 2. fıkrasındaki suç söz konusu olur. Çünkü sistem üzerinde önceden mevcut olan ve belge niteliğini taşımayan veriler değiştirilmiştir. Ancak aynı görevlinin dijital ortamda elektronik belge meydana getirmesi durumunda, örneğin sistemde sahte elektronik işe giriş bildirgesi düzenlemesi durumunda kamu görevlisinin sahte resmi belge düzenlemesinden bahsedilir. Bu ikinci durumda fail elektronik verileri kullanarak dijital ortamda belge özelliklerini taşıyan bir veri bütünü meydana getirmiştir. Her iki durumda da sisteme veri girilmektedir. Ancak birinci durumda sisteme yerleştirilen veriler bir belgeye vücut vermemekte, ikinci haldeyse sisteme yüklenen veriler birleşerek sahte bir belgeyi meydana getirmektedirler.[109]

Sisteme veri yerleştirilmesi suretiyle sahte belge oluşturulması durumunda eylem, TCK'nın 204 vd. maddeleri ile 244/2. fıkralarındaki suçlara temas etmektedir. Burada TCK'nın 212. maddesi gereğince her iki suçtan ayrı cezaya hükmedilmesi gerektiği ileri sürülebilir. Kanaatimizce, ortada belge niteliğini kazanmış veriler bütününün bulunması durumunda eylemin belgede sahtecilik suçları bakımından özel norm olan TCK m.204 vd. maddeleri kapsamında değerlendirilmesi gerekmektedir. Ancak ortada belge özelliklerini taşıyan bir yazının bulunmaması durumunda TCK'nın 244/2. maddesi gündeme gelebilir. Doktrinde, TCK'nın 244. maddenin 4. fıkrasındaki; "*Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suçu oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur*." şeklindeki düzenleme gereğince eylemin ancak başka bir suçu

[109] Taşdemir, Belgelerde Sahtecilik, 253.

oluşturmaması halinde TCK m.244'ün uygulama olanağı bulacağı ileri sürülmektedir[110]. Yukarıda da belirttiğimiz gibi Yargıtay bazı kararlarında bu tür eylemlerin TCK'nın 244. maddesi kapsamında kaldığını kabul etmektedir.[111]

---

[110] Dülger, *Elektronik Belge*,178-179.

[111] "*Mali müşavir olan şikâyetçi Y.H.'in bürosunda çalışması nedeniyle mükelleflere ait elektronik bildirge şifrelerini öğrenen sanık S. E.'ın, iş yerinden ayrıldıktan sonra katılan Ç.K.'e ait şifreyi onun bilgisi dışında kullanarak Y. K. isimli iş yerinde gerçekte çalışmayan M. F. Y., A. M., F. K., Ö. A., Ö. A. ve H. E. isimli kişileri sanki bu iş yerinde çalışıyorlarmış gibi gösterip haklarında gerçeğe aykırı elektronik işe giriş bildirgeleri düzenlediği olayda; suç tarihinde yürürlükte bulunan Sosyal Sigorta İşlemleri Yönetmeliği'nin 11 ve 15. maddeleri gereğince elektronik ortamda düzenlenmesi gereken işe giriş bildirgelerinin 5510 sayılı Kanun'un 100. maddesi gereğince adli ve idari makamlar nezdinde resmî belge niteliğinde olacağı ve elektronik ortamda düzenlenecek bu belgeler üzerinde yapılacak sahtecilik eylemlerinin de resmî belgede sahtecilik suçunu oluşturacağı öngörülmüş ve Yerel Mahkemece sanık hakkında TCK'nın 204. maddesinin birinci fıkrasında düzenlenen resmî belgede sahtecilik suçundan mahkûmiyet hükmü kurulmuş ise de aynı Kanun'un 244. maddesinin ikinci fıkrasındaki "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" şeklindeki düzenleme karşısında sanığın eyleminin aynı zamanda bilişim sistemine veri yerleştirme suçunu da oluşturduğu, TCK'nın 244. maddesinin ikinci fıkrasındaki bu düzenlemenin elektronik belgelerde yapılacak sahtecilik eylemlerine ilişkin özel norm niteliğinde olduğu ve özel normun önceliği ilkesi gereğince de sanık hakkında genel normun değil özel normun uygulanması gerektiği hususları göz önünde bulundurulduğunda, sanığın eyleminin TCK'nın 204. maddesinin birinci fıkrasında yer alan resmî belgede sahtecilik suçuna göre özel norm niteliğinde olan aynı Kanun'un 244. maddesinin ikinci fıkrasındaki bilişim sistemine veri yerleştirme suçunu oluşturduğu kabul edilmelidir*". Yar. CGK, E. 2017/11-1122, K. 2020/381, 29.09.2020; "*Sanığın Sosyal Güvenlik Kurumuna e-bildirge ile bilgisayar ortamında sahte işe giriş bildirgesi düzenleyerek işyerinde çalışmayan kişileri sigortalı olarak gösterdiği iddiasıyla açılan kamu davasında; e-bildirge, imza ve şifre ile bilgisayar ortamında işe giriş bildirgelerinin verilmesi eyleminde, sahte oluşturulmuş maddi varlığa haiz, somut bir belge olmadığı, eylemin bu hali ile TCK'nın 244. maddesi 2. fıkrasında yazılı sisteme veri yerleştirme suçunu oluşturduğu gözetilmeden suç vasfında yanılgı ile yazılı şekilde resmi belgede sahtecilik suçundan hüküm kurulmuş olması…*" Yar. 11. CD, E. 2017/13703, K. 2017/5542, 13.09.2017, (UYAP).

Kişiye ait elektronik imzanın, onun rızası dışında kullanılarak düzenleyeni imza sahibiymiş gibi sahte elektronik belge oluşturulması da söz konusu olabilir. Bu durumda, EİK m.17 ve TCK'nın 204 vd. maddeleri gündeme gelmektedir. Uygulamada bu husus özellikle elektronik işe giriş bildirgeleri üzerinden yapılan tartışmalara konu olmaktadır. Örneğin mali müşavir olan şikâyetçi Y.'ye ait büroda çalışan ve daha sonra bu iş yerinden ayrılan sanık S.'ın, haksız olarak elde ettiği şifreyi kullanarak büronun müşterilerinden olan Y. Kuyumculuk isimli iş yerinde gerçekte çalışmamasına rağmen çalışıyormuş gibi H. E. isimli kişi hakkında işe giriş bildirgesi (elektronik bildirge) düzenlediği olayda eylemin hangi madde kapsamında değerlendirilmesi gerektiği tartışmalara konu olmaktadır. Burada kişiye ait elektronik imzanın onun rızası dışında kullanılması nedeniyle EİK m.17 hükmünün uygulanabileceği düşünülse de imzanın kullanılması sonucunda sahte bir belge meydana getirildiğinden (işe giriş bildirgesi) özel norm niteliğindeki TCK m.204'ün uygulanması gerektiği kanaatindeyiz. Aynı eylem kapsamında hem başkasına ait elektronik imzanın rıza dışında kullanılması hem de belgede sahtecilik yapılmış olması nedeniyle belgede sahtecilik suçları bakımından özel bir içtima kuralı getiren TCK'nın 212. maddesi gereğince EİK m.17 ile TCK m.204/1'in bir arada tatbiki gerektiği düşünülebilir. Ancak doktrinde, m.212 hükmünün, ancak TCK'da düzenlenen suçlar yönünden geçerli olduğu, bu hükmün TCK dışındaki kanunlarda uygulanamayacağı, özel ceza kanunları ve ceza içeren diğer kanunlarda açık bir düzenleme bulunmadıkça TCK m.212 hükmüne dayanılarak cezaların içtima ettirilemeyeceği hususu savunulmaktadır[112]. Yargıtay uygulaması da bu doğrultudadır[113]. Uygulama ve doktrindeki bu kabul gözetildiğinde özel yasa niteliğindeki EİK

[112] Gökcen, *Belgede Sahtecilik Suçları*, 353.

[113] Yar. CGK, E. 2010/7-38, K. 2010/79, 06.04.2010, (UYAP).

m.17'deki bu düzenleme nedeniyle ayrı cezaya hükmedilemeyeceği sonucuna ulaşılabilir.

Yargıtay Ceza Genel Kurulu, yukarıda da değinilen bir kararında, başkasının elektronik imzasının izinsiz olarak kullanılması suretiyle sahte elektronik işe giriş bildirgesi düzenlenmesi olayında eylemin TCK'nın 204/1 ve 244/2. fıkralarındaki suçlara temas ettiğini belirtmiştir. Yargıtay, anılan kararında, elektronik belgelerde yapılacak sahtecilik eylemlerine ilişkin özel norm niteliğinde olduğu gerekçesiyle TCK'nın 244/2. fıkrasının uygulanması gerektiğine hükmetmiştir[114].

V. 765 VE 5237 SAYILI TCK'DAKİ DURUM

Avrupa Konseyi Siber Suç Sözleşmesinin "*Bilgisayarlara İlişkili Sahtecilik Fiilleri*" başlıklı 7. maddesine göre; *"Taraflardan her biri, söz konusu verilerin doğrudan doğruya okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilmez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiilinin, söz konusu farklı verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasıtlı olarak ve haksız şekilde yapıldığında kendi ulusal mevzuatı kapsamında cezai birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar, bu gibi durumlarda cezai sorumluluğun ortaya çıkmasını, hile veya benzeri bir sahtekârlık niyetinin mevcut olması şartına bağlayabilirler.*"

Anılan sözleşmenin açıklayıcı raporunda,[115] maddenin amacının fiziki belgelerle ilgili sahteciliğe paralel bir suç tesis etmek olduğu belirtilmiştir. Sözleşmenin bu maddesi, elektronik verilere ilişkin sahtecilik eylemlerine ilişkin olarak taraf devletlere, ulusal mevzuatları bakımından belirtilen fiillerin suç

[114] Yar. CGK, E. 2017/11-1122, K. 2020/381, 29.09.2020, (UYAP).

[115] Bkz. Explanatory Report to the Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, erişim tarihi: 19.06.2020.

sayılarak cezai yaptırıma tabi tutulması için gereken her türlü işlemin yapılması yönünden yükümlülük getirmektedir. 765 sayılı TCK'nın 525/c maddesine göre; "*Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir*." Bu hükmün getiriliş amacı, fiziki belgelerde yapılan sahteciliğe paralel bir suç tipini elektronik ortamda yapılabilecek sahtecilik fiilleri için de tesis etmek idi.[116]

Madde gerekçesinde bu düzenlemeye ilişkin olarak; "*Düzenlemeyle bilgileri otomatik olarak işleme tabi tutan bir sistem marifetiyle sahtecilik yapılmasının cezalandırıldığı ve suçun maddi unsurunun gerçeğe uygun olmayan bilgi veya diğer unsurları sisteme yerleştirmek veya var olan verileri ve diğer unsurları tahrif etmek, tahrif edilmiş olanları bilerek kullanmak olduğu*" belirtilmiştir. Gerekçede ayrıca; suçun seçimlik hareketli olduğu, failin bu eylemi sahte bir belgeyi oluşturmak üzere gerçekleştirmesi gerektiği hususu yani özel bir kast aranacağı belirtildikten sonra suçun oluşması için gerçeğe aykırı bilgi ve unsurları sisteme yerleştirmek veya var olan veri veya unsurları tahrif etmenin yeterli olduğu ve tahrif edilmiş bilgi ve unsurları kullanmanın da suç teşkil ettiği belirtilmiştir. 765 sayılı TCK'daki bu düzenlemenin karşılığına 5237 sayılı TCK'da yer verilmemiştir. Ayrıca madde gerekçesinde ve meclis tutanaklarında, yeni TCK'da bu tür bir düzenlemeye yer verilmeme nedenine ilişkin bir gerekçeye de rastlanılmamaktadır.

---

116 Arslan ve Baştürk, "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler," 195-218-219.

VI. ELEKTRONİK BELGE İLE İLGİLİ MEVZUATIMIZDA YER ALAN DÜZENLEMELER

5070 sayılı Kanun'un "*Güvenli elektronik imzanın hukuki sonucu ve uygulama alanı*" başlığını taşıyan 5. maddesinde; "*güvenli elektronik imzanın elle atılan imzayla aynı sonucu doğuracağı*" hükmü yer almaktadır. Belge kavramının tanımının yapıldığı Hukuk Muhakemeleri Kanunu'nun 199. maddesinde; "*Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanun'a göre belgedir*." hükmü düzenlenmiştir. Anılan Kanunun 205 inci maddesindeyse "*Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler, senet hükmündedir. Hâkim, mahkemeye delil olarak sunulan elektronik imzalı belgenin, güvenli elektronik imza ile oluşturulmuş olup olmadığını resen inceler*." şeklindeki düzenleme yer almaktadır. HMK'nın 445/2. maddesine göre; "*Elektronik ortamda, güvenli elektronik imza kullanılarak dava açılabilir, harç ve avans ödenebilir, dava dosyaları incelenebilir. Bu Kanun kapsamında fiziki olarak hazırlanması öngörülen tutanak ve belgeler güvenli elektronik imzayla elektronik ortamda hazırlanabilir ve gönderilebilir. Güvenli elektronik imzayla oluşturulan tutanak ve belgeler ayrıca fiziki olarak gönderilmez, belge örneği aranmaz*". Bu hükümlerden hareketle, imza doğrulama verisini ve imza sahibinin hüviyetine ilişkin bilgileri birbirine bağlayan elektronik sertifikaya dayanan elektronik verilerin hukuki hüküm ifade eden belge niteliğini haiz olacağı ifade edilebilir.[117] Başka bir ifadeyle, bu düzenlemeler gözetildiğinde, güvenli elektronik imzayla imzalanmış elektronik belgelerin de yasal anlamda belge olarak kabul edildiği sonucuna ulaşılmaktadır.

---

[117] Erturgut, *Medeni Usul*, 123-124; Taşdemir, *Belgelerde Sahtecilik*, 248; Gözel, *Elektronik Belge*,197.

Türk Ticaret Kanunu'na göre, tacirler güvenli elektronik imza vasıtasıyla e-fatura düzenleyebilmektedirler.[118] Aynı Kanunda, tacirler arasındaki bazı işlemlerin güvenli elektronik imza vasıtasıyla kayıtlı elektronik posta (KEP) sistemiyle yapılacağı düzenlenmiş ve bu verilere belge vasfı verilmiştir.[119] 5271 sayılı Ceza Muhakemesi Kanunu'nun 38/A-1 maddesinde, *"Her türlü ceza muhakemesi işlemlerinde Ulusal Yargı Ağı Bilişim Sistemi (UYAP) kullanılır. Bu işlemlere ilişkin her türlü veri, bilgi, belge ve karar, UYAP vasıtasıyla işlenir, kaydedilir ve saklanır."* şeklindeki hüküm yer almaktadır. Maddenin 5. fıkrasında ise elektronik imzalı belgenin elle atılan imzayı içeren belgeyle çelişmesi durumunda güvenli elektronik imzalı belgenin geçerli kabul edileceği hususu vurgulanmak suretiyle elektronik imzalı belgelere üstünlük tanınmıştır.[120]

213 sayılı Vergi Usul Kanunu'nun *"Elektronik ortamdaki kayıtlar ve elektronik cihazla belge düzenleme"* başlığını taşıyan mükerrer 242.maddesine göre (Ek:28.08.1991-3762/3); *Elektronik cihazlarla düzenlenen belgeler ile özel cihazlardan çıkarılan pulları ihtiva eden belgeler, bu Kanun hükümlerine uygun olarak düzenlenmiş belge hükmündedir."* Aynı maddenin ikinci fıkrasındaysa elektronik defter, elektronik belge ve elektronik kayıt kavramları tanımlanmıştır. Bu maddenin son fıkrasıyla verilen yetki uyarınca da Maliye Bakanlığı, çıkarmış olduğu tebliğlerle bu belgelerin güvenli elektronik imzayla imzalanmaları zorunluluğunu getirmiştir.[121]

6572 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 6. maddesiyle Noterlik Kanunu'na eklenen 198/A

---

118 Gözel, *Elektronik Belge*,196.

119 Arslan ve Baştürk, "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler," 213.

120 Gözel, *Elektronik Belge*,195.

121 Arslan ve Baştürk, "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler," 213.

maddesinde; Kanunda öngörülen noterlik işlemlerinin elektronik ortamda güvenli elektronik imza kullanılarak da yapılabileceği ve güvenli elektronik imzayla imzalanmış belgenin elle atılan imzalı suretiyle çelişmesi hâlinde noterlerin kullandığı bilişim sisteminde kayıtlı olan güvenli elektronik imzalı belgenin esas alınacağı belirtilmek suretiyle güvenli elektronik imzayla imzalanmış belgenin ıslak imzalı belgeyle eşdeğerde olduğu kabul edilmiştir.

5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun "*Bilgi ve belge isteme hakkı, bilgi ve belgelerin Kuruma verilme usulü*" başlıklı 100. maddesine göre; "*Elektronik ortamda hazırlanacak bilgi ve belgeler adli ve idari makamlar nezdinde resmi belge olarak geçerlidir*". 4982 sayılı Bilgi Edinme Hakkı Kanunu'nun 3. maddesinin d bendine göre belge; "*Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film, fotoğraf, teyp ve videokaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını*" ifade eder. Kanaatimizce tüm bu yasal düzenlemeler bağlamında, güvenli elektronik imzayla imzalanmış elektronik ortamdaki veriler belge olarak kabul edilmiş olup bu verilerde yapılacak olan sahtecilik fiilleri ayrı bir düzenlemeye gerek kalmadan TCK anlamında belge olarak kabul edilebileceklerdir.

Yukarıda yer verilen mevzuattaki düzenlemeler uyarınca elektronik imzayla imzalanmış elektronik ortam verilerinin belge olarak kabul edilmesi**,** hatta 6352 sayılı Kanun'un 95. maddesiyle 5271 sayılı Ceza Muhakemesi Kanunu'na eklenen 38/A maddesinde UYAP ortamındaki elektronik imzalı belgenin elle atılan imzayı içeren belgeyle çelişmesi hâlinde UYAP'ta kayıtlı olan güvenli elektronik imzalı belgenin geçerli kabul

edileceğinin vurgulanması[122]ve kanun koyucunun e-belgede sahtecilik konusunda özel bir düzenlemeye gitmemesi hususları birlikte değerlendirildiğinde elektronik ortamdaki verilerin TCK anlamında belge olarak kabul edilmesi gerektiği ve sahtecilik suçunu düzenleyen ceza maddelerinin e-belgede sahtecilik hâlinde de uygulanabileceği sonucuna ulaşılır.[123] Kanaatimizce kanun koyucu, bilinçli olarak kavramı sınırlandırmamak ve ortaya çıkacak yeni durumlarında her defasında ayrı bir düzenlemeye gerek kalmaksızın bu kapsamda değerlendirilmesini temin amacıyla belgenin tanımını yapmamıştır. Bu durum da kanun koyucunun belge kavramını daraltmak istemediğini göstermektedir.

---

122 "Yukarıda mahkemesi ve esas/karar sayıları yazılı dava dosyasının temyiz incelemesi sırasında fiziki dosyada ıslak imzalı gerekçeli kararın hüküm fıkrasındaki " …harç, vekalet ücretleri ve masraflara ilişkin paragraflarda miktar yazıldığının, ancak Uyap ortamında kayıtlı elektronik imzalı gerekçeli kararda " …harç, vekalet ücretleri ve masraflara ilişkin paragraflarda miktar yazılmadığının anlaşılması üzerine mahkemenin Uyap ortamında kayıtlı gerekçeli kararının yazıya dökülmesi suretiyle yapılan incelemede; Mahkemece fiziki dosyada bulunan ıslak imzalı gerekçeli kararın hüküm fıkrasındaki " …harç, vekalet ücretleri ve masraflara ilişkin paragraflarda miktar yazıldığı, ancak Uyap ortamında kayıtlı elektronik imzalı gerekçeli kararda " …harç, vekalet ücretleri ve masraflara ilişkin paragraflarda miktar yazılmadığı anlaşılmıştır. HMK.nun 445. Maddesi ile HMK.nun uygulanmasına ilişkin yönetmeliğe göre elektronik ortamda saklanan UYAP kayıtları asıldır. Mahkemece fiziki dosyada ıslak imzalı gerekçeli kararın hüküm fıkrasındaki " …harç, vekalet ücretleri ve masraflara ilişkin paragraflarda miktar yazıldığı halde Uyap ortamında kayıtlı elektronik imzalı gerekçeli kararda " …harç, vekalet ücretleri ve masraflara ilişkin paragraflarda miktar yazılmaması HMK.nun 445. Maddesi ile HMK.nun uygulanmasına ilişkin yönetmeliğe aykırı olup, belgelendirmeyi bozucu nitelikte olup, bu şekilde oluşturulan kararın bozulması gerekmiştir."Yar. 9. HD, E. 2014/22770, K. 2015/33762, 30.11.2015, (UYAP).

123 Taşdemir, Belgelerde Sahtecilik, 296.

VII. ELEKTRONİK BELGELERDE SAHTECİLİK SUÇUNUN KANUNİLİK İLKESİ AÇISINDAN DEĞERLENDİRİLMESİ

A. Kanunilik ve Belirlilik İlkeleri

Suçta ve cezada kanunilik ilkesi, suç sayılan fiillerin ve bunların işlenmesi halinde uygulanacak yaptırımların kanun tarafından önceden açık olarak belirlenmesini ifade etmektedir.[124] 1982 Anayasasının 38. maddesi ve TCK'nın 2. maddesinde bu ilkeye yer verilmiştir. Anayasa'nın 38. maddesine göre; "*Kimse, işlendiği zaman yürürlükte bulunan kanunun suç saymadığı bir fiilden dolayı cezalandırılamaz; kimseye suçu işlediği zaman kanunda o suç için konulmuş olan cezadan daha ağır bir ceza verilemez. Suç ve ceza zamanaşımı ile ceza mâhkumiyetinin sonuçları konusunda da bu hüküm uygulanır. Ceza ve ceza yerine geçen güvenlik tedbirleri ancak kanunla konulur.*" TCK'nın 2. maddesindeki düzenlemeye göre ise "*Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolunamaz.*" Bu ilke uyarınca "kanunsuz suç ve ceza olmaz. Fiil önceden kanunda suç olarak düzenlenmemişse bunun suç olarak kabulü olanaklı değildir. Ayrıca suçun cezası ve türünün de kanunda açıkça yazılmış olması gereklidir.[125] Bu suretle "*kanunilik ilkesi*", bireyin hak ve özgürlüklerinin korunmasının güvencesini oluşturmaktadır.[126]

Ceza hukukunun güvence fonksiyonunu yerine getirebilmesi için kanunda yer alan suç tanımlarının açık olması

---

[124] Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020), 65-66; Mahmut Koca ve İlhan Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020), 55; İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020), 122-123.

[125] Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 122-123; Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 66.

[126] Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 55.

gerekmektedir. Bu durum, belirlilik ilkesi olarak adlandırılmaktadır. Bunun anlamı hangi insan davranışlarının suç olarak kabul edildiğinin ve bu fiiller için öngörülen yaptırımların kanunda açıkça ve hiçbir tereddüde yer vermeyecek şekilde gösterilmesidir.[127] Bu ilke TCK'nın 2. maddesinde, "*Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilmez ve güvenlik tedbiri uygulanmaz*" ifadeleriyle yer bulmuştur. Anılan ilke uyarınca belirli bir kanuna sadece atıf yapıp soyut ifadeler kullanılarak suç ve ceza ihdası kabul edilemez. Kanun koyucunun suçları düzenleyen hükümlerin tanımlarını açıkça göstermesi gerekmektedir. Tereddüde yer verecek şekilde farklı anlamlar içeren, belirsiz ve gereğinden kapsamlı ifadeler kullanılmamalıdır.[128]

Bu iki ilke çerçevesinden resmi belgede sahtecilik suçuna baktığımızda, anılan suçun, TCK'nın 204. maddesinde[129] suçta ve cezada kanunilik ve belirlilik ilkelerine uygun bir şekilde düzenlendiği anlaşılmaktadır. Zira bir fiilin anılan suçu oluşturması için gerçekleştirilmesi gereken hareketlerin ve bu hareketlere uygulanacak yaptırımların maddede açıkça ve tereddüde yer bırakmayacak şekilde gösterildiği görülmektedir. Bu bağlamda kâğıt ya da herhangi bir maddi varlığı bulunan

---

127 Özbek, Doğan ve Bacaksız, Türk *Ceza Hukuku Genel Hükümler*, 70; Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 132-133; Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 58.

128 Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 58.

129 TCK Madde 204"*(1) Bir resmi belgeyi sahte olarak düzenleyen, gerçek bir resmi belgeyi başkalarını aldatacak şekilde değiştiren veya sahte resmi belgeyi kullanan kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

(2) Görevi gereği düzenlemeye yetkili olduğu resmi bir belgeyi sahte olarak düzenleyen, gerçek bir belgeyi başkalarını aldatacak şekilde değiştiren, gerçeğe aykırı olarak belge düzenleyen veya sahte resmi belgeyi kullanan kamu görevlisi üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır.

(3) Resmi belgenin, kanun hükmü gereği sahteliği sabit oluncaya kadar geçerli olan belge niteliğinde olması hâlinde, verilecek ceza yarısı oranında artırılır."

nesne üzerinde gerçekleştirilebilen seçimlik hareketlerin dijital ortamda elektronik veriler yoluyla gerçekleştirilmesi halinde de kanaatimizce sayılan ilkelere uygun bir fiil söz konusu olmaktadır. Zira maddede belirlenen seçimlik hareketlerin bu kez elektronik ortamda gerçekleştirilmesi söz konusudur. TCK'nın 204. maddesinde, "*Resmi bir belgenin sahte olarak düzenlenmesi, gerçek bir belgenin başkalarını aldatacak şekilde değiştirilmesi, belgenin gerçeğe aykırı olarak düzenlenmesi veya sahte resmi belgenin kullanılması*" fiillerinden bahsedilmiş, ancak bu hareketlerin üzerinde gerçekleştirileceği resmi belgenin maddi cisimlerle sınırlandırılması yoluna gidilmemiştir. Dolayısıyla, Kanunda belirtilen seçimlik hareketlerin üzerlerinde gerçekleştirildiği unsurlar anılan kanun maddesinde sınırlandırılmamış olduğundan bu hareketlerin elektronik ortamda elektronik belgeler üzerinde gerçekleştirilmesi durumunda da suçun oluştuğunun kabulü gerektiği kanaatindeyiz. Örneğin daha önce kâğıt üzerinde düzenlenen işe giriş bildirgesi, bu kez aynı tipiklik içeren hareketlerle elektronik ortamda düzenlenmektedir. Bu durumda elektronik işe giriş bildirgesinin, salt kâğıt ya da maddi varlığı bulunan bir cisim üzerine değil de elektronik ortamda aynı bilgileri içerir ve aynı hukuki sonucu doğuracak mahiyette düzenlenmesi fiilinin kanunilik ve belirlilik ilkelerine uygun bulunmadığını ileri sürmek yerinde bir kabul değildir. Buradaki tek fark bu hareketlerin kâğıt ya da maddi varlığı bulunan bir nesne üzerinde değil de elektronik ortamda elektronik verilerin kullanılması yoluyla gerçekleştirilmesidir. Kanaatimizce güvenli elektronik imzayla imzalanmış belgelerin yasal anlamdaki belge kavramına dâhil olduğu kabul edildiğinde bunların sahtecilik suçlarının konusu olarak değerlendirilmesi halinde açıklanan bu ilkelere aykırılık söz konusu olmamaktadır. Gerçekten de unsur, işlev ve doğurduğu hukuki sonuçlar itibariyle klasik anlamdaki belgelerden farkı bulunmayan elektronik belgeler üzerinde gerçekleştirilen sahtecilik fiillerinin, TCK'daki belgede sahtecilik suçlarının

konusunu oluşturduğunun kabulünün ne kanunilik ne de belirlilik ilkesine aykırılığı söz konusu olur.[130]

B. Yorum ve Kıyas Yasağı

TCK'nın 2. maddesinin 3. fıkrasında kıyas yasağı ve yorum düzenlenmiştir. Buna göre; "*Kanunların suç ve ceza içeren hükümlerinin uygulanmasında kıyas yapılamaz. Suç ve ceza içeren hükümler, kıyasa yol açacak biçimde geniş yorumlanamaz.*"

Yorum, "*bir kanun hükmünün anlamını, kanun koyucunun gerçek iradesini ortaya koymaya yönelik fikri bir faaliyettir*".[131] Burada kanunda mevcut olan bir kuralın ne anlama geldiğine[132] ve kanun koyucunun bu kuralı ihdas etmekteki iradesinin ne olduğuna ilişkin düşünsel bir faaliyet söz konusu olmaktadır. Ceza hukukunda kıyas yasağı bulunmasına karşın yorum kabul edilmektedir. Başka bir ifadeyle ceza hukukunda, bir kanun hükmünün ne anlama geldiği ve kapsamının tayini bakımından yorum yapılabilir. Yorumlama sırasında; kanun hükmünün lafzından, kanunun hazırlık çalışmalarından, sistematiğinden, düzenlenen hukuk kurumunun tarihçesinden, mukayeseli hukuktaki düzenlemeler ve hukukun genel ilkelerinden yararlanılabilir[133].

Yorum sonucunda kanun metninin anlamı açıklığa kavuşturuluyorsa açıklayıcı yorum, anlam daraltılıyorsa daraltıcı yorum, genişletiliyorsa genişletici yorum söz konusu olmaktadır[134].Ayrıca yorum, kanunun kelime ve ifadelerine göre

---

130 Tekin, "Resmi Belgede Sahtecilik," 94-95; Taşdemir, *Belgelerde Sahtecilik*, 252-253; Gözel, *Elektronik Belge*,189.

131 Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 134.

132 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 69.

133 Özgenç, *Türk Ceza Hukuku Genel Hükümler*, 135.

134 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 117-118; Doğan Soyaslan, *Ceza Hukuku Genel Hükümler*, (Ankara: Yetkin Yayınevi, 2016), 119 vd.

yapılan mantıki yapıcı metod ve kanun metninin önemini kabul etmekle birlikte kanunun amacına önem veren amaçsal (teleolojik) metod kullanılarak yapılabilir.[135] Yorumlama yapılırken kanun koyucunun iradesini göz önüne alan yoruma sübjektif teori, kanunun iradesini göz önünde tutarak yorumlama yapılmasına ise objektif teori denilmektedir.[136]Çoğu zaman kanunun, kanun koyucunun öngöremediği durumlara da uygulanması gerekebilmektedir. Bu durumlar kanunun yürürlüğe girmesinden sonra ortaya çıkmaktadırlar. Bu nedenle kanaatimizce, kanunun sonradan ortaya çıkacak durumlar açısından da uygulanabilirliğini sağlamak açısından objektif teori esas alınarak yorum yapılması gerekmektedir.[137]

Kıyas, *"bir olaya ilişkin hukuk kuralının, kanun tarafından düzenlenmemiş benzer bir olaya uygulanması"*[138] demektir. Başka bir ifadeyle kanunda açık bir yazılı hüküm bulunmayan yani suç olarak düzenlenmemiş bir fiil hakkında kanunda suç olarak düzenlenmiş bulunan benzer başka bir fiile ilişkin hükmün uygulanmasıdır".[139] Bu şekilde, kanunun bir normuna dayanılarak kanununda düzenlenmemiş bulunan başka bir norm meydana getirilmektedir.[140] Bu tanımlardan da anlaşılacağı üzere, kıyas; kanunda hakkında düzenleme yapılmamış olan bir eylemin cezalandırılmasına yönelik olup bunun kanunilik ilkesine aykırılık içerdiği söylenebilir. Medeni hukuk uygulamasının aksine ceza hukukunda, hâkime kanunda bulunan boşlukları doldurma yetkisi, kanunu tamamlama yetkisi verilmemiştir. Kıyas yasağı kanunların sadece ceza içeren

---

135 Soyaslan, *Ceza Hukuku Genel Hükümler*, 122.

136 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 117; Soyaslan, *Ceza Hukuku Genel Hükümler*, 119.

137 Aynı görüşte; Soyaslan, *Ceza Hukuku Genel Hükümler*, 120.

138 Soyaslan, *Ceza Hukuku Genel Hükümler*, 123; Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 61.

139 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 69.

140 Koca ve Üzülmez, *Türk Ceza Hukuku Genel Hükümler*, 61.

hükümleri bakımından söz konusu olabilir.[141] Yorumla kıyas farklı kavramlardır. Yorum mevcut olan kuralın anlamının ortaya çıkarılması, kıyas ise norm boşluğunun başka normlara bakarak doldurulmasıdır.[142] Kanunilik ilkesi karşısında, elektronik ortamdaki belgelerin ceza hukuku korumasından yararlanmalarının ancak onlara *"belge"* niteliğin tanınmasıyla mümkün olabileceği açıkça ortaya çıkmaktadır.

Bilindiği gibi TCK'da düzenlenmiş bulunan belgede sahtecilik suçlarının konusunu "*belge*" oluşturmaktadır. Bu bağlamda, elektronik belgenin TCK anlamındaki belge kavramının kapsamına girip girmediğinin belirlenmesi gerekmektedir. Kanun koyucu tarafından belgenin tanımı yapılmamış ve kapsamı da belirlenmemiştir. Yargıtay'ın genişletici yorum yöntemini kullanarak benzer olaylara ilişkin çözüm getirdiği durumlar bulunmaktadır. Örneğin 765 sayılı TCK döneminde enerjinin hırsızlık suçu bakımından mal sayılıp sayılmayacağı konusu uzun süre tartışılmıştır. Bu tartışmalar özellikle elektrik enerjisi üzerine yoğunlaşmıştır. 765 sayılı TCK'da hırsızlık suçunun düzenlenmiş olduğu 491 vd. maddelerinde enerjinin taşınabilir mal kavramına dâhil olup olmadığına ilişkin bir hüküm bulunmamaktaydı. Elektrik enerjisi ilk kez 1991 yılında 3756 sayılı yasa ile 765 sayılı TCK'da yapılan değişiklik sonrasında mal sayılmıştır. Ancak enerjinin açıkça hırsızlık suçuna konu olabileceğine ilişkin 1991 yılındaki bu yasal düzenleme yapılmadan evvel de Yargıtay'ın elektrik hırsızlığı ve telefon hattından saplama yaparak konuşma yapılması şeklindeki eylemleri genişletici yorum metoduyla hırsızlık suçu kapsamında değerlendirdiği görülmektedir.

"*Görüşmeler sırasında Ceza Hukukunda kıyasın caiz olmadığı toplumun değer yargılarına göre, yasada açıklık olmadığı halde bir*

141 Özbek, Doğan ve Bacaksız, *Türk Ceza Hukuku Genel Hükümler*, 70.

142 Soyaslan, *Ceza Hukuku Genel Hükümler*, 123.

eylemin suç sayılamayacağı ileri sürülmüşse de çoğunluk olayda kıyas yoluna başvurulmadığı yukarıda da açıklandığı üzere genişletici yorum yapıldığı, buna da ceza da cevaz bulunduğu, genişletici yorum yoluna başvurulurken toplumun değer yargılarından yararlanılabileceği gerekçesiyle bu görüşlere katılmamıştır.

Burada genişletici yorum, T.C.Y.'nın 491. maddesinin kapsamı dışında bir eylemi madde kapsamına dâhil etmek değil, esasen maddenin içinde mündemiç bulunan ve zamanın teknolojik gelişmeleri ile ekonomik değeri olan her türlü şeyin sahibinin rızası dışında kullanılması eylemlerinin de T.C.Y.'nın 491. maddesinin kapsamında olduğunu açıklığa kavuşturmaktan ibarettir."[143]

---

[143] Yar. 6. CD, 7080/8497, 06.11.1990; "*Türk Ceza Kanunu'nun 491. maddesinin 1. fıkrasında hırsızlık şöyle tarif edilmiştir: "Her kim, diğerinin taşınabilir malını rızası olmaksızın faydalanmak için bulunduğu yerden alırsa, altı aydan üç seneye kadar hapsolunur." Bu tanım açısından içtihadı birleştirmenin konusu (taşınabilir mal) ve (bulunduğu yerden alma) kavramları yönünden özellik kazanmaktadır. Bu sözler değerlendirilirken kuşkusuz (zilyetlik) ve (mamelek) kavramlarının dikkate alınmaları zorunludur. İçtihadı birleştirmeye esas tutulan kararlarda sözü edilen olayların ortak özelliği, herhangi bir kişiye ait telefon hattından saplama yapmak suretiyle hat alıp sanığın kendisine ait telefon makinası ile rıza olmaksızın konuşma sağlaması keyfiyetidir. Ceza Genel Kuruluna intikal eden diğer bir olayda ise sanıkların kendi evlerinde kurdukları özel telefon santralleri ile Tarabya santrallerini kullanarak kaçak milletlerarası konuşmalar yapılmasını sağlamaları söz konusu edilmiştir. Bu olayların Türk toplumunun değer yargılarına tamamen ters düştüğü, ahlâka ve hukuka aykırı sonuçlar doğurduğu tartışmasızdır. Türk Ceza Kanununun 491. maddesinin ilk fıkrasındaki unsurlar genişletici yoruma tabi tutulduğunda yukarıda özetlenen eylemleri kapsamına aldığının kabulü gerekli görülmüştür. Zira yorumda toplumun değer yargıları ve teknolojinin gerisinde kalınamaz.*

Görüşmeler sırasında Ceza Hukukunda kıyasın caiz olmadığı toplumun değer yargılarına göre, yasada açıklık olmadığı halde bir eylemin suç sayılamayacağı ileri sürülmüşse de çoğunluk olayda kıyas yoluna başvurulmadığı yukarıda da açıklandığı üzere genişletici yorum yapıldığı, buna da ceza da cevaz bulunduğu, genişletici yorum yoluna başvurulurken toplumun değer yargılarından yararlanılabileceği gerekçesiyle bu görüşlere katılmamıştır.

Burada genişletici yorum, T.C.Y.'nın 491. maddesinin kapsamı dışında bir eylemi madde kapsamına dâhil etmek değil, esasen maddenin içinde mündemiç bulunan

Kanaatimizce, belge kavramının kapsamının belirlenmesi hususu da bir yorum sorunudur. Başka bir ifadeyle bu sorunun çözümü için yorum müessesesinden yararlanılması gerekmektedir[144]. Bunun için maddenin yapım çalışmalarına bakıldığında ilk olarak meclis tutanaklarından kanun koyucunun belge kavramını tanımlamamasının nedeninin kavramın daraltılmasından imtina etmek olduğu anlaşılmaktadır.[145] Yine madde gerekçesine göre; "*Her ne kadar belgeden söz edilen durumlarda yazılı bir kâğıdın varlığı gerekli ise de bazı durumlarda belgenin varlığını kabul için yazının kâğıt üzerinde bulunması aranmaz."* Gerekçedeki bu ifadelerden de kanun koyucunun bu kavramı geniş yorumlama eğiliminde olduğu anlaşılmaktadır.[146] 5237 sayılı TCK'da, mülga 765 sayılı TCK'daki "*yazılı kâğıt*" anlamına gelen "*varaka*" ve "*evrak*" kavramlarının yerine bu terimleri de ihtiva eden ve daha kapsamlı olan "*belge*" kavramının kullanılması suretiyle yapılan değişikliğin de elektronik belgelerin belgede sahtecilik suçları kapsamında değerlendirilmesi yolunda bir düzenlemeye yol

ve zamanın teknolojik gelişmeleri ile ekonomik değeri olan her türlü şeyin sahibinin rızası dışında kullanılması eylemlerinin de T.C.Y.'nın 491. maddesinin kapsamında olduğunu açıklığa kavuşturmaktan ibarettir.

Sonuç: Yukarıda açıklanan nedenle, telefon hizmetinden çeşitli usul ve yöntemlerle saplama yapmak suretiyle bedelsiz ve kaçak yararlanmanın, Türk Ceza Kanunu açısından hırsızlık fiilini oluşturacağına, ilk görüşmede üçte ikiyi geçen çoğunlukla karar verildi." Yar. İç. Bir. K. 06.04.1990, 2/3. (Kubilay Taşdemir ve Ramazan Özkepir, *Belgelerde Sahtecilik Mala Karşı Suçlar ve Bilişim Alanında Suçlar,* (Ankara: Adil Yayınevi, 1999), 340-341; Yar. 6. CD, 11622/2870, 5.4.1983; Yar. 6. CD, 2676/3603, 25.4.1983. (Kubilay Taşdemir ve Ramazan Özkepir, *Mala Karşı Suçlar,* (Ankara: Gen Matbaacılık, 1993), 133.

144 Bkz. Aynı görüşte Dülger, *Elektronik Belge*,175.

145 TBMM Adalet Komisyonu'nda 5237 sayılı Türk Ceza Kanunu'nun görüşülmesi esnasında, belgenin tanımına ilişkin tartışmalar yapılmış, ancak kavramın tanımlanmasının bir süre sonra uygulamaya dar gelebileceği düşüncesi ile tanımı yapılmamıştır. (**Bkz. Meclis tutanakları**)

146 Gözel,*Elektronik Belge*,145; Gökhan Güler, "Resmi Belgede Sahtecilik Suçu" (Yüksek Lisans Tezi, ÇankayaÜniversitesi, Ankara, 2018), 21.

açtığı ifade edilebilir[147]. 765 sayılı TCK'nın 525/c maddesine benzer bir düzenlemeye 5237 sayılı TCK'da yer verilmemiş olmasının nedeninin de mevcut düzenlemelerin elektronik belgelerin TCK anlamında belge sayılması için yeterli görülmesi olduğu ileri sürülebilir. Bunların yanında belgede sahtecilik suçlarının ihdas amacı kamu güvenine mazhar olan belgeleri, yapılacak her türlü hukuka aykırı saldırıya karşı korumaktır.[148] Klasik anlamdaki belgelerle aynı unsurları içeren ve aynı fonksiyonu ifa eden elektronik belgelere de kamunun güven duyduğu ifade edilebilir. Tüm bu hususlar gözetildiğinde, kanaatimizce, elektronik belgelerin TCK anlamındaki belge kavramının kapsamına dâhil olduğu sonucuna ulaşılabilir.[149] Hukukun genel ilkeleri ve sosyolojik gerçekler gözetildiğinde de ayrıca yasal bir düzenlemeye ihtiyaç duyulmaksızın genişletici yorum metoduyla elektronik belgelerin, belgede sahtecilik suçlarına konu olan belge kavramına dâhil olarak değerlendirilmesi bakımından engel bir durumun olmadığı kanaatindeyiz[150].

SONUÇ

Belgeler; sosyal, ekonomik ve hukuki açıdan oldukça büyük bir önemi haizdirler.Bunlar üzerinde gerçekleştirilen sahtecilik fiillerinin kamunun güvenini sarstığı kabul edilerek bu fiiller tarihin her aşamasında ceza kanunlarıyla yaptırım altına alınmıştır. Belgenin, taşınabilir birşey üzerine yazılı olmak, yazanının bilinebilinir olması ve hukuki hüküm ifade edecek bir içeriğe sahip olmak unsurlarını içermesi gerekmektedir. Ancak bunu, sadece bilinen anlamıyla kâğıt ya da maddi varlığı olan

147 Dülger, *Elektronik Belge*,168-169.

148 Kubilay Taşdemir ve Ramazan Özkepir, *Belgelerde Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar*, (Ankara: Adil Yayınevi, 1999), 98.

149 Tekin,"Resmi Belgede Sahtecilik," 935; Gözel, *Elektronik Belge*, s.188; Taşdemir, *Belgelerde Sahtecilik*, 247 vd.

150 Dülger, *Elektronik Belge*,175.

şeyler üzerine yazılan yazıyla sınırlandırmamak gerektiği ifade edilmelidir.

Elektronik belge, elektronik ortamda sayısal olarak kodlanmış olarak bulunan elektronik verileri ifade etmektedir. Elektronik sertifikayı içeren elektronik yazı, hukuken sonuç doğurmaya elverişli belge niteliğini kazanacaktır. Yalnızca güvenli elektronik imza içeren yazılar yasal anlamda belge olarak kabul edilebilir. "*Elektronik İmza*" el yazısıyla imzanın (ıslak imza) istisnası olmayıp alternatifidir. Mevzuatta belirtilen istisnai durumlar dışında ıslak imzayla gerçekleştirilebilecek her türlü işlem güvenli elektronik imzayla da gerçekleştirilebilir.

Elektronik belgenin TCK bakımından belge olarak kabul edilip edilmeyeceği hususu tartışmalıdır. Konuya ilişkin olarak Yargıtay uygulamaları da yerleşmiş değildir. 5070 sayılı Kanun'un 16 ve 17. maddelerinde elektronik ortamda düzenlenen sahte belgelerden değil izinsiz imza oluşturulması ve sertifikada sahtecilik yapılması eylemlerinden bahsedilmektedir. Dolayısıyla bu kanun maddeleri sahte e-belge düzenlenmesi ve kullanılması hâlinde uygulanamayacaktır. TCK'nın 244. maddesinin 2. fıkrasıysa, verinin sahte olarak oluşturulmasına ilişkin olmayıp bu madde, "*elektronik verilerin bozulması, yok edilmesi, erişilmez hale getirilmesi veya değiştirilmesi*" gibi fiilleri düzenlemiştir. Burada veri olarak tanımlanan elektronik belge niteliğine sahip olmayan elektronik veriler olduğundan maddenin e-belgede yapılan sahtecilik eylemlerinde uygulanabilmesi olanaklı değildir.

Güvenli elektronik imzayla imzalanmış bir belgenin TCK'nın aradığı anlamda belge olarak kabul edilmesine engel hiçbir durum yoktur. Güvenli e-imzayla imzalanıp nitelikli sertifikayla "onaylanmış" bulunan elektronik veri, bütün unsurlarını içerdiğinden bunları belge olarak değerlendirdiğimizde ne kıyas yasağının ne de suç ve cezada kanunilik ve belirlilik ilkelerinin ihlal edilmesi gibi bir durumun

söz konusu olmadığı açıktır. Yürürlükteki mevzuat gözetildiğinde, yalnızca güvenli elektronik imzalı elektronik belgelerin TCK'da düzenlenmiş bulunan belgede sahtecilik suçlarına konu olması olanaklıdır. Kanaatimizce, unsur, işlev ve doğurdukları hukuki sonuçlar itibariyle klasik anlamdaki belgelerden farkı bulunmayan elektronik belgeler üzerinde gerçekleştirilen sahtecilik fiillerinin, TCK'daki belgede sahtecilik suçlarının konusunu oluşturduğunun kabulü gerekmektedir.

Yukarıda yaptığımız açıklamalar, bu bağlamda yer verdiğimiz yasal düzenlemelerle içtihatlar gözetildiğinde nitelikli elektronik imzayla imzalanmış elektronik belgenin, belgenin mevcudiyeti için aranan tüm unsurları haiz olduğundan yeni bir yasal düzenlemeye gerek kalmaksızın TCK anlamındaki belge kavramı içinde değerlendirilmesi ve korunması gerektiğini düşünmekteyiz. Aksi durumda e-belgede yapılan sahtecilik eylemlerinin cezai müeyyidelerinin olmadığı kabul edilmiş olacaktır. Ayrıca belirtmek gerekir ki, hernekadar yasal düzenlemeye gerek kalmadan bu tür verilerin TCK anlamında belge olarak kabulü gerektiğini savunsak da doktrin ve uygulamadaki bu tereddüt ve tartışmaların uzun süre devam etmesi durumunun, uygulamada ıslak imzalı belgelerle aynı sonucu doğurmalarına rağmen elektronik belgeler üzerinde yapılan sahtecilik fiillerinin cezasız kalmasına neden olacağı ya da TCK'da belgede sahtecilik suçlarının tabi tutulduğu yaptırımlara oranla daha hafif bir yaptırıma tabi tutulmak suretiyle adaletsizliklere yol açacağı anlaşılmaktadır. Dolayısıyla, ivedilikle bu tür belgelerin de TCK anlamında belge olarak kabulü gerektiği yönünde yasal düzenleme yapılması suretiyle bu konudaki tereddüt ve tartışmaların bir an önce sonuçlandırılması yerinde bir çözüm olarak görülebilir.

KAYNAKÇA

Acar, Ayşe Ece.*Medeni Muhakeme Hukukunda Elektronik İmzalı Belgelerin Delil Değeri*.İstanbul: XII Levha Yayınları, 2013.

Arıkan, Ayşe *Saadet*."Bilgisayar Programlarının Korunması AB. ve Türkiye."Türkiye Barolar *Birliği Dergisi*, no. 3 (1996): 309-381.

Arslan, Çetin ve İhsan Baştürk. "Belgede Sahtecilik Suçunun Konusu Olarak Elektronik Ortamdaki Veriler." *Erciyes Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 2(2013): 195-219.

Arslan, Çetin."Dijital Delil ve İletişimin Denetlenmesi."*Ceza Hukuku ve Kriminoloji Dergisi 3, no. 2 (2015*): 253 – 266.

Aslan, Memduh. "Vergilendirmede Elektronik Belgelerin Hukuki Geçerliliklerinin Değerlendirilmesi."*Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi 2*, no. 3 (2014): 2-39.

Artuk, Mehmet Emin, AhmetGökcen, Mehmet EminAlşahin ve KerimÇakır.*Ceza Hukuku Özel Hükümler.* Ankara: Adalet Yayınevi, 2019.

Biçkin, İnci. "Elektronik İmza Kanunu ve Getirdiği Düzenlemeler." *Yargıtay Dergisi* 30, no. 3(2004): 351-361.

Biçkin, İnci. "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler." *Türkiye Barolar Birliği Dergisi,* no. 63(2006): 109-126.

Çam, Nihat Bozkurt. "Evrakta Sahtekârlık Suçları."*Ankara Barosu Dergisi*, no. 3(1989): 450-471.

Çetin, Erol ve Malkoç, İsmail. Sahtekârlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat. Ankara: Adalet Yayınevi, 1995.

Doğan, Koray. "Ceza Hukukunda Belge Kavramı."*Ceza Hukuku Dergisi 5*, no. 14(Aralık 2010): 51-66.

Dülger, Murat Volkan. "Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik Belge." *Belgede Sahtecilik Ve Vergi Suçları Sempozyumu*, TOBB ETÜ Sosyal Tesisleri Ankara 21-23 Ekim 2019, *Melek Metbaa&Promosyon Hizmetleri*, Ankara 2020:155-182.

Ekinci, Mustafa ve Sinan Esen. Anlatımlı ve Gerekçeli 5237 sayılı Türk Ceza Kanunu'nda Yer Alan Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar. Ankara: Adalet Yayınevi, 2005.

Erem, Faruk.*Türk Ceza Hukuku Hususi Hükümler.* Cilt II. Ankara: Ajans-Türk Matbaası, 1962**.**

Erem, Faruk. Ümanist Doktrin Açısından Türk Ceza Hukuku Özel Hükümler. Cilt IV, Ankara: Seçkin Kitabevi, 1985.

Erem, Faruk. *Türk Ceza Kanunu Şerhi Özel Hükümler*. Cilt II. Ankara: Seçkin Yayınevi, 1993.

Erem, Faruk ve Nevzat Toroslu. *Türk Ceza Hukuku Özel Hükümler.* Ankara: Savaş Yayınevi, 1994.

Erman, Sahir. "Evrakta Sahtekârlık Suçlarında "Varaka" Mefhumu." *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,* 15, no. 1(1949): s.167-197.

Erman,Sahir.*Sahtekârlık Cürümleri*.İstanbul: İsmail Akgün Matbaası, 1952.

Erman,Sahir.*Sahtekârlık Suçları Ticari Ceza Hukuku – III*.İstanbul: Nazım Terzioğlu Matematik Araştırma Enstitüsü Baskı Atölyesi, 1981.

Erman, Sahir. *Sahtekârlık Suçları, Ticari Ceza Hukuku Cilt III.* İstanbul: İstanbul Üniversitesi Fen Fakültesi Döner Sermaye İşletmesi Prof. Dr. Nazım Terzioğlu Basım Atölyesi, 1987.

Erman, Sahir ve Çetin Özek. Ceza Hukuku Özel Bölüm, Kamu Güvenine Karşı İşlenen Suçlar TCK. 316-368.İstanbul: Globus Dünya Basımevi,1996.

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

Erturgut, Mine. Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi. Ankara: Yetkin Yayınları, 2004.

Gökcan, Hasan Tahsin. "Resmi Belgede Sahtecilik Suçu." *Ankara Barosu Dergisi,* 67, no. 3.(2009): 92-127.

Gökcen, Ahmet.*Belgede Sahtecilik Suçları*.Ankara: Adalet Yayınevi, 2018.

Gözel, Arif. "Belgede Sahtecilik Suçlarının Konusu Olarak Belge ve Elektronik Belge." *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi 5*, no. 1(2015): 147-154.

Gözübüyük, Abdullah Pulat. *Türk Ceza Kanunu Gözübüyük Şerhi*, 3. Cilt. İstanbul: Kazancı Yayınları, 1988.

Güler, Gökhan."Resmi Belgede Sahtecilik Suçu."Yüksek Lisans Tezi, Çankaya Üniversitesi, 2018.

Gündüz, Remzi ve Veysel Gültaş. *Belgelerde ve Faturalarda Sahtecilik Suçları.*Ankara: Bilge Yayınevi, 2013.

Güngör, Devrim. *Resmi Belgelerde Sahtecilik Suçu.* Ankara: Yetkin Yayınları, 2010.

Kılıçoğlu, Ahmet M. *Borçlar Hukuku Genel Hükümler*. Ankara: Turhan Kitabevi, 2018.

Koca, Mahmut ve İlhan Üzülmez.*Türk Ceza Hukuku Genel Hükümler*.Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020.

Koca, Mahmut ve İlhan Üzülmez. *Türk Ceza Hukuku Özel Hükümler*.Ankara: Adalet Yayınevi, 2020.

Malkoç, İsmail. *Sahtecilik Suçları ve Mala Karşı Suçlar*. Ankara: Seçkin Yayınevi, 1995.

Önder, Fatih. "Borçlar Hukuku Açısından Elektronik İmza."Yüksek Lisans Tezi, Kırıkkale Üniversitesi, 2007.

Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız.*Türk Ceza Hukuku Genel Hükümler*.Ankara: Seçkin Yayınevi, 2020.

Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız.*Türk Ceza Hukuku Özel Hükümler*.Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020.

Özgenç, İzzet. *Türk Ceza Hukuku Genel Hükümler*. Ankara: Seçkin Akademik ve Mesleki Yayınlar, 2020.

Öztel, Ahmet."Adli Belge İncelenmesinde Karşılaşılan Sorunlar ve Çözüm Önerileri."*Türkiye Barolar Birliği Dergisi*, No. 50(Ocak- Şubat 2004): 152-161.

Soyaslan, Doğan.*Ceza Hukuku Genel Hükümler*.Ankara: Yetkin Yayınları, 2016.

Soyaslan, Doğan. *Ceza Hukuku Özel Hükümler.*Ankara: Yetkin Yayınları, 2020.

Taner, Fahri Gökçen. "Özel Belgelerde Sahtecilik Suçları Bağlamında Maddi Hasarlı Trafik Kazası Tespit Tutanakları (Kağıt Ve Elektronik) Ve Ortaya Çıkan Sorunlar." *Ceza Hukuku Dergisi*,no.35(Aralık 2017):117-148.

Taşdemir, Kubilay ve Ramazan Özkepir.Belgelerde Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar.Ankara: Adil Yayınevi, 1999.

Taşdemir, Kubilay.*Açıklamalı-İçtihatlı Belgelerde Sahtecilik Suçları*.Ankara: R24 Medya Ltd. Şti.,2019.

Taşdemir, Kubilay ve Ramazan Özkepir, *Mala Karşı Suçlar*, Gen Matbaacılık, 1993.

Taşdemir, Kubilay ve Ramazan Özkepir. Belgelerde Sahtecilik Mala Karşı Suçlar ve Bilişim Alanında Suçlar, Adil Yayınevi, 1999.

Tekin, Nurullah. "Resmi Belgede Sahtecilik Suçunda Bazı Özel Durumlar."*Türkiye Adalet Akademisi Dergisi*, no. 19(Ekim 2014):903-941.

Tezcan, Durmuş, Mustafa Ruhan Erdem ve Murat Önok. *Teorik ve Pratik Ceza Özel Hukuku.* Ankara: Seçkin Yayınevi, 2020.

Toroslu, Nevzat.*Ceza Hukuku Özel Kısım*. Ankara: Savaş Yayınevi, 2019.

Yardım, Mehmet Ertan. "Elektronik İmza ve Elektronik İmzanın Medeni Usul Hukukumuza Etkileri."Yayınlanmış Yüksek Lisans Tezi, İstanbulÜniversitesi, 2006.

WEB KAYNAKLARI

https://en.wikipedia.org/wiki/Electronic_Signatures_in_Global_and_National_Commerce_Act#Definitions, erişim tarihi:21.03.2021.

https://www.lawinsider.com/dictionary/electronic-document, erişim tarihi: 13.03.2021.

https://www.lawinsider.com/dictionary/electronic-data, erişim tarihi: 13.03.2021.

https://sozluk.gov.tr/?kelime= Bilişim Terimleri Sözlüğü, erişim tarihi: 19.06.2020.

Türk Dil Kurumu Sözlüğü, http://www.tdk.gov.tr, Erişim Tarihi:*04.06.2020.*

https://sozluk.gov.tr/, erişim tarihi:20.03.2021.

Explanatory Report totheConvention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, erişim tarihi: 19.06.2020.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31999L0093,erişim tarihi:15.03.2021.

https://tr.wikipedia.org/wiki/Elektronik_imza, erişim tarihi:20.03.2021.

https://tr.wikipedia.org/wiki/Elektronik_imza, erişim tarihi:20.03.2021.

https://tr.wikipedia.org/wiki/Elektronik_belge, erişim tarihi:20.03.2021.

https://tr.wikipedia.org/wiki/Dijital_ortam, erişim tarihi:20.03.2021.
UYAP Bilgi Sistem

IS INSISTING ON SPECIFIC PERFORMANCE UNDER SMART CONTRACTS DESIRABLE UNDER ENGLISH CONTRACT LAW? INFLEXIBILITIES OF SMART CONTRACTS AND POTENTIAL SOLUTIONS

İngiliz Hukukunda Akıllı Sözleşmelerde Borcun İfasında Israr Etmek Gerekir mi?: Olası Sorunlar ve Çözüm Önerileri

Eyüp KUN*

Abstract

Smart contracts, as written by computer code, would secure the performance of the contract. It is believed that this feature of smart contracts is marketed as the solution to traditional contracts, which can be easily breached. The potential benefits of automated performance, such as predictability and certainty, would bring benefits to all parties. However, this idea of automated performance would not be desirable all the time. Not allowing for a breach by insisting on the specific performance required by a smart contract would be considered practically and economically inefficient, and which might deter their widespread use. As an illustration of this inflexibility, "efficient

* Doctoral Researcher, KU Leuven Center for Information Technology and Intellectual Property Law (CiTiP), eyup.kun@kuleuven.be, ORCID: 0000-0002-4766-5101.

Makale Gönderim Tarihi/Received: 27.05.2021.

Makale Kabul Tarihi/Accepted: 19.06.2021.

Atıf/Citation: Kun, Eyüp. "Is Insisting On Specific Performance Under Smart Contracts Desirable Under English Contract Law? Inflexibilities of Smart Contracts And Potential Solutions." *Bilişim Hukuku Dergisi* 3, no: 1 (2021): 139-175.

breach theory" will be used to prove that insisting on the specific performance of the obligation secured by a smart contract would not be desirable for the contractual parties. After showing this inflexibility, a feasible solution for this concern will be presented within the design of contracts. Before discussing this issue, in the second section, the definition of smart contracts and, and its potential benefits, will be explained. In the third section, as the main issue, how automated performance can cause inflexibilities, the difficulty of predicting future events, and the impossibility of a breach will be analysed. After detecting these problems, whether the design of a smart contract can help to alleviate these inflexibilities will be discussed. This article discusses the validity of smart contracts and the specific performance of obligations according to the English contract law.

Keywords: Smart Contracts, Law and Economics, Efficient Breach Theory, Specific Performance, English Contract Law.

Özet

Bilgisayar koduyla yazılan akıllı sözleşmeler, sözleşmenin ifasını güvence altına alacaktır. Akıllı sözleşmelerin bu özelliği, kolayca ihlal edilebilen geleneksel sözleşmelere alternatif olarak önerilmektedir. Sözleşmenin ifasının otomatikleştirilerek teminat altına alınması taraflara öngörülebilirlik ve kesinlik gibi faydalar sağlayacaktır. Bununla birlikte, bu otomatik ifa fikri her zaman arzu edilmeyecektir. Akıllı bir sözleşmenin gerektirdiği belirli bir borcun ifası üzerinde ısrar etmek ve bir ihlale izin vermemek, pratik ve ekonomik olarak verimsiz kabul edilebilir ve bu da akıllı sözleşmelerin geniş çaplı kullanımlarını engelleyebilir. Bu verimsiz durumu tasvir etmek ve akıllı sözleşmede aynen ifa konusunda ısrar etmenin sözleşme tarafları için arzu edilmeyeceğini kanıtlamak için "etkin ihlal teorisi" kullanılacaktır. Bu verimsiz durum gösterildikten sonra, akıllı sözleşmelerin tasarımında bu sorunun çözümü için uygulanabilir bir çözüm sunulacaktır. Bu konuyu tartışmadan

önce, ikinci bölümde akıllı sözleşmelerin tanımı ve potansiyel faydaları açıklanacaktır. Üçüncü bölümde, esas mesele olan, akıllı sözleşmelerde borcun ifasının otomatik olarak gerçekleşmesindeki olası sorunlar ele alınacak ve gelecekteki olayları tahmin etmenin zorluğu ve sözleşmeyi ihlalin imkansızlığı halleri analiz edilecektir. Bu sorunları tespit ettikten sonra, akıllı bir sözleşmenin tasarımının bu sorunların çözümünde nasıl bir rolü olacağı tartışılacaktır. Bu makalede, akıllı sözleşmelerin geçerliliğine ve aynen ifaya ilişkin tartışmalarda İngiliz sözleşme hukuku esas alınmış ve tartışmalar bu çerçevede yapılmıştır.

Anahtar Kelimeler: Akıllı Sözleşmeler, Hukuk ve Ekonomi, Etkin İhlal Teorisi, Aynen İfa, İngiliz Sözleşme Hukuku.

INTRODUCTION

Smart contracts, as written by computer code, would secure the performance of the contract. It is believed that this feature of smart contracts is marketed as the solution to traditional contracts,[1] which can be easily breached. The potential benefits of automated performance, such as certainty, would bring benefits to all parties. However, this idea of automated performance would not be desirable all the time. Not allowing for a breach by insisting on the specific performance required by a smart contract would be considered practically and economically inefficient, and which might deter their widespread use. As an illustration of this inflexibility, "efficient breach theory" will be used to prove that insisting on the specific performance of the obligation secured by a smart contract would not be desirable for the contractual parties. After showing this inflexibility, a feasible solution for this concern will be presented within the design of contracts.

[1] Traditional contracts as a term describes the contractual relations which do not secure the performance of the contracts technically.

Before discussing this issue, in the second section, the definition of smart contracts and its relationship with blockchain technology, and its potential benefits, will be explained. In the same section, whether a variety of smart contracts fall within the scope of English contract law will be assessed. In the third section, as the main issue, how automated performance can cause inflexibilities, the difficulty of predicting future events, and the impossibility of a breach will be analysed. After detecting these problems, whether the design of a smart contract could help alleviate these inflexibilities will be discussed.

I. SMART CONTRACTS: DEFINITION, GOALS AND LEGAL ASPECTS

A. The Definition of Smart Contracts: Is It Smart or Mere Automation?

The definition and scope of the smart contract have been discussed extensively in the literature. Szabo defined "smart contract" by saying that contractual terms into the software to execute and enforce them without any intermediary intervention by the trusted parties.[2] From Szabo's perspective, this concept hinges on the ensured execution of the contractual terms, which means it is related to the "performance of the contract". Cuccuru considered the concept of smart contracts as "a channel of online agreements", which means that they are not themselves truly contracts in a legal sense.[3] Smart contracts are constructed as an autonomous execution of a piece of code "whose input or output

---

[2] Nick Szabo, "Smart Contracts: Building Blocks for Digital Markets," accessed March 20, 2020, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html/.

[3] Pierluigi Cuccuru, "Beyond bitcoin: an early overview on smart contracts," *International Journal of Law and Information Technology* 25, no. 3 (Autumn 2017): 179–195, https://doi.org/10.1093/ijlit/eax003.

can include money".[4] The definition of a smart contract is sometimes broadly understood as an if-then relationship, without taking into account the broader context.[5] In this essay, even if it is conceded that smart contracts sometimes refer to mere code executing pre-determined instructions[6], it will be regarded as computer codes ensuring the automated execution of the contract. This feature differentiates smart contracts from traditional contracts.[7] This definition includes agreements directly concluded by codes[8] and algorithms. Admittedly the use of "smart" as an adjective, can be considered misleading since being smart in the context of contracts are more likely to reflect autonomous contracting, which is surely more than mere automated process. Due to the broad and vague definition of smart contracts, Scholz coined "algorithmic contracts" for contracts concluded by algorithms which would be legally enforceable.[9] This article will analyse these types of contracts under the definition of smart contract, that is, where contractual performance is secured by code. It is believed that coining

4 Ari Juels, Ahmed Kosba and Elaine Shi, "The Ring of Gyges: Using Smart Contracts for Crime," accessed March 29, 2020, http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf.

5 Michèle Finck, "Smart contracts as a form of solely automated processing under the GDPR," *International Data Privacy Law* 9, no. 2 (May 2019): 80, https://doi.org/10.1093/idpl/ipz004.

6 Marco Dell'Erba, "Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation," (2018): 22, http://dx.doi.org/10.2139/ssrn.3228445.

7 Primavera De Filippi and Aaron Wright, *Blockchain and the law: the rule of code*, (Cambridge, Massachusetts: Harvard University Press, 2018): 74.

8 Michael Bacina, "When Two Worlds Collide: Smart Contracts and the Australian Legal System," *Journal of Internet Law* 21, no. 8 (2018): 17.

9 Lauren Henry Scholz, "Algorithmic Contracts and Consumer Privacy," in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms,* eds. Cristina Poncibò, Larry A. DiMatteo and Michel Cannarsa, (Cambridge: Cambridge University Press, 2019): 256.

different terms for each example would exacerbate concerns related to the definition of the contract.

B. The Relationship Between Smart Contracts and Blockchain Technologies: Is It Indispensable?

The use of the blockchain has positively influenced how the smart contract has been developed. The network, the ledger and the consensus are three main elements of blockchain. To add a new block into the chain, the consensus model requires users to prove themselves by solving the extreme computational mathematical problems requiring high energy and computing power. Solving these problems to add the new block into the chain is called mining. When a majority of notes confirms this solution and consensus is reached, the block is added into the blockchain and becomes immutable due to the impracticability of the modification of blocks.[10] The immutable nature of the blockchain ensures the transfer of digital assets between parties without any intermediation. This nature of blockchain enhances the secured performance of smart contracts. Due to this relation with blockchain, Greenspan defines the concept of a smart contract by specifically referring to the role of blockchain.[11] He states that "A smart contract is a piece of code which is stored on a Blockchain, triggered by Blockchain transactions, and which reads and writes data in that Blockchain's database."[12] Similarly, Savelyev suggests that the definition of a smart contract must be limited by the use of blockchain.[13] He argues that smart contracts will be innovative only if complete self-enforcement and trust

---

10 Alexander Savelyev, "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law," *Information & Communications Technology Law* 26, no. 2 (2017): 118-119, https://doi.org/10.1080/13600834.2017.1301036.

11 Gideon Greenspan, "Beware of the Impossible Smart Contract," accessed April 23, 2020, https://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract.

12 Greenspan, "Beware."

13 Savelyev, "Contract law 2.0," 127.

are ensured by blockchain technology.[14] In conclusion, due to the positive impact of blockchain, smart contracts seem to be inextricably associated with it, according to some authors.

Nevertheless, a smart contract can be designed without blockchain technologies. Blockchain is not a requirement for the implementation of these contracts because other technologies can maintain automatic execution.[15] Mik points out that smart contracts are not synonyms with blockchain transactions and smart contracts involve running code on top of blockchain technologies to ensure the self-enforceability of these transactions.[16] Besides, in the example of the vending machine, Dell'Erba challenged the automatic association of smart contracts with blockchain-enabled contracts by considering the vending machine as such.[17] It is conceded that blockchain enhances self-execution; however, it is possible to have automatic execution of a transaction embedded in codes without the use of blockchain technology. However, blockchain technology facilitates the transfer of digital assets on a "peer-to-peer basis in the digital realm, just as they do offline."[18] The added value of blockchain technologies would not be disregarded. Thus, defining smart contracts as a transactional layer on top of blockchain would be an appropriate construction of the relationship between blockchains with smart contracts. To

---

14 Savelyev, 131.

15 Florian Möslein, "Legal Boundaries of Blockchain Technologies: Smart Contracts as Self-Help?," in *Digital Revolution - New challenges for Law (Forthcoming),* eds. Alberto Franceschi et. al., (2019): 3, accessed April 25, 2020, https://ssrn.com/abstract=3267852.

16 Eliza Mik, "Smart contracts: terminology, technical limitations and real world complexity," *Law, Innovation and Technology* 9, no. 2 (2017): 281, https://doi.org/10.1080/17579961.2017.1378468.

17 Dell'Erba, "Demystifying Technology," 12.

18 Tatiana Cutts, "Smart Contracts and Consumers," *LSE Legal Studies Working Paper,* no. 1 (2019): 15, accessed April 28, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354272.

conclude, if the automated execution is embedded in code, this would be sufficient to make it a smart contract.

C. The Validity of Smart Contracts in the Current Legal Framework: Are Smart Contracts Compatible with English Contract Law?

The flexible nature of contract law allows the application of the current legal system to smart contracts as long as they can be qualified as a "contract" under the applicable law of disputes. Under English law, there must be a meeting of minds (agreement), consideration, and legal intention to have a legally enforceable contract.[19] If these requirements are met, smart contracts fall within the scope of contract law. Conceiving smart contracts outside contract law is no more than a fiction.[20] When smart contracts are legally binding under contract law will be discussed below.

Meeting of minds under contract law can occur explicitly through offer and acceptance or implicitly by conduct. If a smart contract is constructed only to provide automated execution, this means that a contract is concluded *a priori* between the parties. In such an instance, a smart contract would not call into question the existence of legal contract since the parties have an underlying contractual relationship where the terms are embedded in the code after the conclusion of the contract.[21]

---

19 Robert Duxbury, *Contract Law: Textbook Series*, (London: Sweet & Maxwell, 2014): 1.008.

20 Andrew Murray, Information technology law: the law & society (Oxford, United Kingdom : Oxford University Press, 2019), 435; European Commission, Study on Blockchains. Legal, governance and interoperability aspects (SMART 2018/0038) (Luxembourg: Publications Office of the European Union, 2020), 60, https://op.europa.eu/s/pi6i; Savelyev, "Contract law 2.0", 123.

21 Kristian Lauslahti, Juri Mattila and Timo Seppala, "Smart Contracts – How Will Blockchain Technology Affect Contractual Practices?" *ETLA Reports*, no. 68 (2017): 21, accessed April 21, 2020, https://ssrn.com/abstract=3154043.

When it comes to smart contracts which are concluded and enforced within the code, the autonomous negotiation can be used in the conclusion phase might cause uncertainty concerning the agreement between the parties. Scoca illustrates the autonomous negotiation process by considering a fictive dynamic Service Level Agreement (SLA).[22] In this example, the negotiation algorithm determines the provider which is most compatible with customer requests. Assume that both parties use these algorithms to not only negotiate but also to conclude the contract. In this case, how the meeting of minds occurs can cause uncertainty as algorithms conclude and execute the contract without the parties' intervention. Lord Hodge points out a similar example in which computers with machine learning capabilities autonomously interact with each other to generate transactions.[23] It could certainly be argued that there is no meeting of minds in these transactions as the parties do not explicitly or implicitly agree on the conclusion of the contract. They would be outside the scope of contract law as they are fully concluded by computers.[24] Nonetheless, the flexibility of contract law can accommodate this scenario on the basis that these autonomous structures are delegated by parties to form these contracts, and the parties must then agree on what these autonomous structures agree. Dell'Erba appropriately observes that a fully automated process initially triggered by the parties

[22] Vincenzo Scoca, Rafael Brundo Uriarte and Rocco De Nicola, "Smart Contract Negotiation in Cloud Computing," *2017 IEEE 10th International Conference on Cloud Computing,* (Honololu, HI, USA: IEEE, 2017): 596, https://doi.org/10.1109/CLOUD.2017.81.

[23] The Right Honourable Lord Hodge, "The Potential and Perils of Financial Technology: Can the Law Adapt to Cope?" *The First Edinburgh FinTech Law Lecture*, (Edinburgh Law School, South Bridge, Edinburgh, March 14, 2019), 12, accessed April 24, 2020, https://www.law.ed.ac.uk/sites/default/files/2020-09/speech-190314%20-%20Acc.pdf.

[24] Savelyev, "Contract law 2.0", 121.

can be constructed as a contract in the legal sense.[25] Triggering the autonomous structure for the conclusion of the contract can be constructed as a tacit agreement to the terms the machines agree. The use of these agents should not change the occurrence of the meeting of minds. In conclusion, as long as the smart contracts are triggered by the parties, and these codes agree on the same terms of the agreement, the requirement for a meeting of minds will be met. It must be noted that this form of a contract might be a truly smart contract as the autonomous conclusion of contracts reflects the notion of smartness.

Intention to be legally bound is another requirement for an enforceable contract under the English law. This requirement is concerned with whether the parties intend to be bound by the agreement legally. Even parties can agree on certain terms and conditions; they do not want to be legally bound by their agreements.[26] For commercial transactions, there is a strong presumption that the parties intend to be bound by their agreements.[27] Dell'Erba gives an example of the use of smart contracts concerning the "Internet of Things".[28] The intention to be legally bound would not be so problematic in smart contracts provided that they are designed to engage commercially with others. However, having smart contracts might imply that the parties chose an "alternative regulatory system",[29] as the nature of smart contracts ensures the enforceability of the contract without the support of the courts, thus, there is no intention to be legally bound with the conclusion of smart contracts. Similarly, Werbach and Cornell state that transacting through smart contracts would mean that parties are not intended to have

25 Dell'Erba, "Demystifying Technology," 39.

26 Duxbury, Contract Law: Textbook Series, 3-012.

27 Duxbury, 3-020.

28 Dell'Erba, "Demystifying Technology," 37-38.

29 Savelyev, "Contract law 2.0," 123.

a legally enforceable contract as legal enforcement is not needed.[30] They detect the misleading nature of that thinking by underlying that the intention of the parties to use smart contracts as a means of self-execution does not mean that they do not want to enforce their contract legally.[31] In light of the strong presumption of intention to be bound in commercial transactions, preferring the use of a smart contract does not directly lead to the conclusion that the parties have chosen another regulatory system. Therefore, inasmuch as the intention of the parties is derived from smart contracts, they would create legally binding contracts regardless of the autonomous nature of smart contracts.

According to English law, the consideration must be present to have an enforceable contract. This requirement ensures that only bargains are enforceable under English law rather than mere promises.[32] Smart contracts in the commercial context do not challenge the notion of consideration as they generally include mutual bargains. It can be stated that as enforceability is ensured by a smart contract, there is no need to analyse whether the requirement of consideration is met. However, in the case of total failure of consideration, the claimant is entitled to recover what he pays based on unjust enrichment. In *Fibrosa Spolka Ackyjna v Fairbairn Lawson Combe Barbour Ltd*, the Polish company paid a deposit for goods ordered.[33] However, it did not receive anything in return. The Court held that the claimant is entitled to recover what it pays on the basis of total failure of consideration. In the case of smart contracts, after the

30 Kevin Werbach and Nicolas Cornell, "Contracts ex machina," *Duke Law Journal* 67, no. 2 (2017): 339, accessed May 4, 2020, https://scholarship.law.duke.edu/dlj/vol67/iss2/2.

31 Werbach and Cornell, "Contracts ex machina," 340.

32 Duxbury, Contract Law: Textbook Series, 4.001.

33 Fibrosa Spolka Ackyjna v Fairbairn Lawson Combe Barbour Ltd, [1943] A.C. 32.

performance of the contract, the claimant might seek recovery as grounded on unjust enrichment due to the failure of consideration. Therefore, it must be concluded that smart contracts should include the consideration to be legally enforceable.

II. THE AIMS OF SMART CONTRACTS: REMOVING TRUSTED INTERMEDIARIES AND THE DECREASE IN TRANSACTION COSTS

A. Removing Trusted Intermediaries: Are Blockchain Miners, New Intermediaries?

The idea behind smart contracts is the removal of trusted intermediaries such as courts or financial institutions by putting a piece of code in place as an alternative. Intermediaries record the transaction and solve disputes if such arise from the contract. Since smart contracts aim to allow for the self-execution of a contract, the need for an intermediary might be removed. Blockchain technology helps smart contract replace trusted third parties.[34] Cutts insightfully points out that the blockchain technology provides disintermediation in digital asset sales.[35] This disintermediation is provided by miners who solve "the cryptographic puzzles based on the transaction in a proposed new block on the blockchain."[36] Due to the role of miners in the smart contracts hosted on blockchain, they can be considered part of any intermediation considering the reward they gain for their role. It is stated that the concept of disintermediation stems from the fact that verifiers and users constitute the same group.[37]

---

[34] Werbach and Cornell, "Contracts ex machina," 329; Daniel Macrinici, Cristian Cartofeanu and Shang Gao, "Smart contract applications within blockchain technology: A systematic mapping study," *Telematics and Informatics* 35, no. 8 (2018): 2338, https://doi.org/10.1016/j.tele.2018.10.004.

[35] Cutts, "Smart Contracts and Consumers," 20.

[36] Mik, "Smart contracts," 276.

[37] Cutts, "Smart Contracts and Consumers," 19.

However, even if users transact between themselves, other nodes in the blockchain will continue to verify such transaction. For this reason, it may be noted that there is no actual disintermediation in the case of blockchain-enabled smart contracts. Nevertheless, the distributed nature of intermediation in blockchain removes the need for central intermediation.

B. Reducing Transaction Cost: Does It Reduce Transaction Cost or Move the Cost Upfront?

Smart contracts might reduce transaction costs as there is no litigation or enforcement procedures in the case of a breach as the code ensures the performance of the contract. Giancaspro states that smart contracts reduce transaction costs related to enforcement procedures before courts as the performance of the obligations is guaranteed by a piece of software.[38] This argument seems compatible with the goal of a smart contract targeting self-execution. In contrast to this idea, while decreasing the enforcement and litigation costs, the design process of the smart contract would inflict a much higher cost on the parties. It is contended that the smart contractware design must be carried out meticulously to ensure that the wills of the parties are genuinely incorporated into the software.[39] Furthermore, the designed system must be secure from the malicious attack,[40] which requires additional financial resources to increase its robustness. Considering design costs, Murray notes that the

---

38 Mark Giancaspro, "Is a 'smart contract' really a smart idea? Insights from a legal perspective," Computer Law & Security Review 33, no. 6 (2017): 827, https://doi.org/10.1016/j.clsr.2017.05.007; For same view: Savelyev, "Contract law 2.0," 127.

39 Jeremy M. Sklaroff, "Smart Contracts and The Cost of Inflexibility," *University of Pennsylvania Law Review* 166, no. 1 (2017): 277, accessed April 21, 2020, https://scholarship.law.upenn.edu/penn_law_review/vol166/iss1/5.

40 Amritraj Singh et. al., "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities," *Computers & Security* 88, (2020): 2, https://doi.org/10.1016/j.cose.2019.101654.

costs people incur are merely reallocated to the design phase in smart contracts.[41] Design and negotiation costs in the smart contract show that the total cost would not be decreased but allocated to the preparation phase rather than the enforcement phase.

III. AUTOMATIC EXECUTION AS A DISTINCT FEATURE OF SMART CONTRACTS

Smart contracts differ from traditional ones by their automatic enforcement as provided by their software protocols. This automatic performance is the consequence of embedding the required performance into the code.[42] However, this performance can be halted by a cyberattack, which makes this code vulnerable in this regard. Additionally, one party would control the execution of the code, which would cause the alteration of the smart contract unless both parties mutually control the code. In blockchain-enabled smart contracts, the immutability is enhanced as code is inserted into the blockchain technology by which the whole network is dispersed, and the underlying software ensures that the copies are updated as and when there is a new connection to the network.[43] Additionally, when the code is executed in the blockchain, it is highly resistant to alteration. However, this is not impossible if a majority of the miners in the blockchain "collectively decide to unwind previously recorded transactions or to block certain accounts or smart contracts."[44] Considering this potential for alteration,

41 Murray, Information technology law, 432.

42 Mik, "Smart contracts," 274.

43 De Filippi and Wright, *Blockchain and the law*, 35-36.

44 De Filippi and Wright, 36; Grimmelmann mentioned that how the forks are coming out in the case of disagreement about the upgrade in the blockchain result in forks. For a detailed explanaton, see: James Grimmelmann, "All Smart Contracts Are Ambiguous," *Journal of Law & Innovation* 2, no. 1 (2019): 17, accessed April 21,2020,h ttps://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1006&conte xt=jli.

parties should take these features into account while using blockchain-enabled transactions. Consequently, the idea is that the distinct feature of a smart contract is securing performance, despite the potential alteration. This feature is also considered a positive feature of the smart contracts as it allegedly reduces transaction cost and removes trusted intermediaries. However, this would bring inflexibilities to smart contracts which would deter parties from using them.

On the other hand, it must be noted that the modification in smart contracts are possible. As described in the previous section, smart contracts exist on top of blockchain technologies. Interestingly, Marino and Juels underline the difference between "contract states" and "code" in Etherum platforms.[45] They stated that 'contract states' on the blockchain are not immutable. They further noted that nodes "run contract code and maintain and adjust contract states in a virtual machine they all host, the Etherum Virtual Machine." By this virtual machine, it is possible to modify contracts or to rescind or to terminate them.[46] Also, oracles can be used to adopt contracts to changing circumstances. How these features can alleviate the inflexibilities of the contract will be discussed for the inflexibilities mentioned.

A. The Inflexibility of Smart Contracts: Are They Unsolvable?

1. The Incompleteness of Contract: The Unpredictability of Future Events

The problem of the incompleteness of contracts should be discussed in the context of smart contracts to show their

---

45 Bill Marino and Ari Juels, "Setting Standards for Altering and Undoing Smart Contracts," in *Rule Technologies. Research, Tools, and Applications*, eds. Jose Julio Alferes et. al., (Cham: Springer International Publishing, 2016): 158, https://doi.org/10.1007/978-3-319-42019-6_10, 158.

46 Marino and Juels, "Setting Standards," 162.

inflexibility. Aderlini and Felli define incomplete contracts by saying "a contract is incomplete if and only if it does not incorporate some information about the state of nature that it would have been optimal for the contracting parties to include."[47] In other words, it is not plausible to predict all future events in the contractual relations even in traditional contracts to have an optimal contractual relation. Even though parties foresee a contingency, they rationally prefer not to negotiate to reduce transaction costs.[48] This incompleteness will cause gaps and ambiguities.[49] Parties would renegotiate the contract after the unforeseen contingency occurs or the courts would adjudicate if a dispute arises from the unforeseen contingency. This characteristic reflects how traditional contracts adapt to changing circumstances. When it comes to smart contracts, it is accepted that blockchain-enabled smart contracts accommodate highly complex contractual relations.[50] However, this complexity would not encapsulate the prediction of all events in the future. Sklaroff points out that modelling the potential behaviours of the contractual parties is too complex to be designed.[51] Additionally, the immutable nature of smart contracts exacerbates the problem of the incomplete contract as the terms and conditions of these contracts cannot be modified as a rule. This might cause a more rigid application of smart contracts which would deter people from using them.

---

47 Luca Anderlini and Leonardo Felli, "Bounded rationality and incomplete contracts," *Research in Economics* 58, no. 1 (2004): 11.

48 Richard A. Posner, "The Law and Economics of Contract Interpretation," *Texas Law Review* 83, (2005): 1583.

49 Oliver Simon D'Arcy Hart, *Firms, Contracts, and Financial Structure*, (New York: Oxford University Press, 1995), 30

50 Eric Tjong Tjin Tai, "Force Majeure and Excuses in Smart Contracts," *European Review of Private Law* 26, no. 6 (2018): 790.

51 Sklaroff, "The Cost of Inflexibility," 279-280.

On the other hand, this inflexibility arising from the structure of smart contracts would be alleviated by a modification mechanism embedded in the code. Contractual parties can write renegotiation clauses into their smart contracts[52] to solve this rigidity. Marino and Juels discuss how the contract can be modified in smart contracts on Etherum platforms.[53] They describe three ways by which the parties can undertake such modification: 'modification of variable-captured terms, deletion of function-captured terms, and addition or alteration of function-captured terms.'[54] These modification mechanisms would also provide renegotiation mechanisms.

These modification mechanisms, with the secured self-execution of the performance, would solve the problems arising from the flexibility of traditional contracts. Having the possibility of modification after the conclusion of a traditional contract might be threateningly used by one party to gain an increased benefit from another without reciprocity if the other party makes a "sunk, relationship-specific investment."[55] This problem has been coined the 'hold-up' problem.[56] The possibility of this problem would render flexibility of renegotiations inefficient as one of the parties gets benefits unfairly without offering any associated value.[57] Smart contracts with a modification mechanism would solve the hold-up problem as the self-execution of the main performance is secured in

---

52 Richard T. Holden and Anup Malani, "Can Blockchain Solve the Hold-up Problem in Contracts?" *The National Bureau of Economic Research Working Papers*, no. 25833 (2019): 32.

53 Marino and Juels, "Setting Standards," 162.

54 Marino and Juels, 162.

55 Benjamin E. Hermalin and Michael L. Katz, "Information and the Hold-Up Problem," *The RAND Journal of Economics* 40, no. 3 (2009): 405. accessed April 22, 2021, http://www.jstor.org/stable/25593717.

56 Hermalin and Katz, "Information," 405.

57 For many cases illustrating the hold-up problem, see: Holden and Malani, "Can Blockchain Solve," 7.

advance. Based on the self-execution of the contract, Holden and Malani perceptively argue that the secured performance and designing the modification mechanism under the smart contract would prevent the hold-up problem since smart contracts would not then allow opportunistic modifications to be imposed by one party on another.[58] Therefore, the possibility of modification and renegotiation of a smart contract would be considered more secure flexibility since it is more likely to solve the hold-up problem arising from the elastic nature of contract law.

Contracts include a variety of clauses to govern the relations between parties to facilitate their transaction and to remove uncertainties, at least insofar as this is possible. Smart contracts would not be desirable in the case of a complex transaction if there is no connection between the smart contract and the real world. For instance, parties prefer to stipulate the condition precedent, which triggers the performance of the contract. In traditional contracts, these conditions can be easily incorporated into the contract, but even so, how the parties react to the occurrence of the condition bears a degree of uncertainty. When it comes to smart contracts, the relation with the real world must be maintained to have self-execution even in complicated contracts. Therefore, other contingencies foreseen by the parties must be incorporated; otherwise, mere secure performance would not be sufficient to allow for the extensive use of smart contracts.

Uncertainties about real-world incidents in smart contracts could be alleviated by using oracles.[59] Having a trusted oracle may soften these limitations by using external data to trigger specific conditions in smart contracts. These oracles can be divided into three types: automated, trusted third party, and

---

58 Holden and Malani, 28.

59 Grimmelmann, "All Smart Contracts," 15.

expert oracles.[60] As an illustration of automated oracles, signals from a self-driving car in a car accident would be considered the input for a smart contract.[61] Trusted third party and expert oracles can incorporate human views into smart contracts.[62] Lamberti proved the complex and flexible use of smart contracts in the initial coin offerings by incorporating different variables into these transactions.[63] Incorporating the human viewpoint into smart contracts by way of oracles can make these contracts more flexible. Responding to the changes in near real-time led some authors to think that smart contracts were more dynamic than traditional contracts.[64] Having objective inputs from the automated oracles will contribute to the flexibility of smart contracts. However, having a subjective view from experts would prejudice securing performance since the perspective of a third party would be wrong or biased. Therefore, contracting parties must consider this issue while drafting a smart contract.

2. Not Allowing A Breach Of Contract

The appealing characteristic feature of smart contracts has been determined as their automatic execution. It has been described that this characteristic of smart contracts acts as a form of self-help to get the specific performance agreed under the contract. This view hinges on the idea that this type of contract is a private action by the parties to resolve disputes without any

---

60 Tjong Tjin Tai, "Force Majeure," 791; All type of oracles are defined as getting information from trusted third party source, See for this definition: De Filippi and Wright, *Blockchain and the law*, 75.

61 Tjong Tjin Tai, "Force Majeure," 791.

62 Tjong Tjin Tai, 791.

63 Valentina Gatteschi, Fabrizio Lamberti and Claudio Demartini, "Technology of Smart Contracts," in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms,* eds. Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò, (Cambridge: Cambridge University Press, 2019), 45.

64 De Filippi and Wright, *Blockchain and the law : the rule of code*, 75

further assistance of third parties.[65] As stated below, this is a distinguishing feature of smart contracts from traditional contracts and other forms of electronic legal agreements.[66] This feature can be a mere manifestation of *pacta sund servanda*[67] and can be applauded as a proper solution and deterrent to post-opportunistic behaviours by the parties. On the other side of the coin, a strict application of the no-breach idea might be considered stringent. Allowing a breach by the parties in contract law allows business life to be more flexible to accommodate contingencies. The occurrence of a breach itself does not mean that parties will go to litigation to seek a remedy. Before the litigation phase, parties can have an informal dialogue to restore their contractual relationship. Sklaroff emphasises on how this informal dialogue solves the dispute arising from opportunistic behaviours of one party at a low cost, proposing more business in the future.[68] Levy underlines that non-enforcement of the contract would have the same benefits as enforcement in the courts.[69] Self-enforcement, as secured by smart contracts, deprives parties of recourse to informal dialogue or other ways to ensure a more efficient solution to their dispute(s). Even if informal dialogue does not end with an efficient compromise, traditional contract law would offer other ways to restore the relationship via remedies, which would be

---

65 Cristina Poncibò and Larry A. Dimatteo, "Smart Contracts: Contractual and Noncontractual Remedies," in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms,* eds. Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò, (Cambridge: Cambridge University Press, 2019), 126.

66 Werbach and Cornell, "Contracts ex machina," 331.

67 Savelyev, "Contract law 2.0," 130.

68 Sklaroff, "The Cost of Inflexibility," 277-278; For similar view, see Karen E. C. Levy, "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law," *Engaging Science, Technology, and Society* 3, (2017): 9.

69 Levy, "Book-Smart," 10.

more effective than the self-execution of a contract after a change in circumstances. Therefore, not allowing a breach of the contract reflects the inflexible side of smart contracts.

IV. IS INSISTING ON SPECIFIC PERFORMANCE BY AUTOMATIC EXECUTION DESIRABLE UNDER ENGLISH CONTRACT LAW

As smart contracts do not allow breach of contract, this feature can be regarded as a strict persistence of the main obligation under the agreed contract. In other words, the design of smart contracts presumes the desirability of specific performance under the contract. Thus, the essential question related to the practicality of smart contracts is whether their automatic execution is always desirable by the contractual parties. It must be acknowledged that smart contracts provide contractual parties commercial and legal certainty by their self-executing nature. Mik justifiably contends that the legal and economic certainty is guaranteed technically with the unbiased and objective nature of the code.[70] In most instances, this will attract businesses' attention to the use of smart contracts.

On the other hand, after the agreement, circumstances surrounding contracts might change, which may alter parties' views in terms of performing their obligations under the contract. Such a change in view is not limited to an opportunistic move by one of the parties, it might occur due to unforeseen circumstances beyond the parties' control, such as force majeure[71] or a more valuable offer from a third party. Due to these changes, parties would prefer to breach the contract instead of performing it.

---

70 Mik, "Smart contracts," 280; For similar view, see: Dell'Erba, "Demystifying Technology," 20.

71 For a detailed analysis of how the force majure can be incorporated into the smart contract, see: Tjong Tjin Tai, "Force Majeure," 787.

Breach of contract is one of the possibilities foreseen in contract law systems in contrast to the idea of a smart contract. Werbach and Cornell identify contract law as "remedial institution."[72] These remedies contain paying a variety of damages or insisting on specific performance. The party who breached the contract will pay the expectation damages[73] instead of fulfilling specific performance if a breach of contract has occurred in English law. Seeking damages is considered a primary remedy, as opposed to the civil law countries in which specific performance as a primary remedy persists.[74] The possibility of paying expectation damages in traditional contracts instead of performing the contract would prove how contractual parties have a right to change their minds. It should be noted that this change would not completely prejudice the expectation of the other party as they can be satisfied with damages. By contrast, the idea of self-execution of a smart contract would be incompatible with people's right to change their minds. Mik points out that self-enforcement does not allow the parties to deviate from the conditions of the contract, which hinders changing one's mind.[75] This lack of discretion might well be considered an inflexible side of the idea of a smart contract.

---

72 Werbach and Cornell, "Contracts ex machina," 106.

73 Expectation damages aims at putting the innocent party in the same position as if the contract had been performed.

74 Liao, Wenqing, *The Application of the Theory of Efficient Breach in Contract Law: A Comparative Law and Economics Perspective*, (Cambridge: Intersentia, 2015), 298; For the reasons why specific performance is not primary remedy, see: Tareq Al-Tawil, "English Contract Law and the Efficient Breach Theory: Can They Co-Exist?" Maastricht Journal of European and Comparative Law 22, no. 3 (2015): 414, https://doi.org/10.1177%2F1023263X1502200305; For the risk of disproportionate consequences of specific performance, see: Henrik Lando and Caspar Rose, "On the enforcement of specific performance in Civil Law countries," *International Review of Law & Economics* 24, no. 4 (2004): 483-484, https://doi.org/10.1016/j.irle.2005.01.005.

75 Mik, "Smart contracts," 280.

A. Efficient Breach Theory as an Illustration of the Inflexibility of Smart Contracts

In this section, voluntary breach of a contract in the expectation of increasing welfare will be discussed to show that insisting on securing performance would not be the mere choice the parties want; sometimes, breach of contract can be efficient for the parties. Before delving into the concept of efficient breach, the law and economics approach to contract law must be briefly analysed to make this theory intelligible.

According to law and economics theory, enforcing contracts enables people to cooperate to "maximise the gain" when the contract law "creates efficient incentives for performance and reliance."[76] The function of law is to facilitate people's capacity to maximise their welfare, thus incentivising people to behave appropriately.[77] Therefore, this theory assumes that people expect to gain benefit from a contract. If a contract does not produce a total efficiency for the parties, contract law should not enforce a requirement for these parties to perform their contractual obligations. Why should a party breach a contract if he/she anticipates economic gain from the contract? Liao gives three reasons for a breach of the contract: "uncertain risks, opportunistic behaviours and alternative to paying damages."[78] When people enter into a contract, the conditions of their performance in the future might not be certain. After the

---

[76] Robert Cooter and Thomas Ulen, *Law and Economics*, (Harlow, Essex : Pearson, 2014), 305; See also Richard A. Posner, "The Economic Approach to Law," *Texas Law Review* 53, (1975): 761.

[77] Alan Devlin, *Fundamental Principles of Law and Economics,* (London: Routledge, 2015), 178. See for general overvıew of the hıstorical development of law and economics theory, Herbert, Hovenkamp, "Law and Economics in the United States: a brief historical survey," *Cambridge Journal of Economics* 19, no. 2 (April 1995): 331, https://doi.org/10.1093/oxfordjournals.cje.a035316.

[78] Liao, *The Application,* 45-46.

agreement, it might turn out that the contract is no longer going to be advantageous to the parties. In this case, contract law should induce people to act appropriately, including renegotiation and the breach of contract. Concerning opportunism, the law must deter this kind of behaviour in order to increase total welfare.[79] If instead of performing the obligation paying damages would be more efficient to the parties, then they can breach the contract to ensure this.

Efficient breach theory is developed by law and economics scholars to theorise how parties might breach a contract voluntarily for the sake of efficiency. This theory was has been developed by Richard Posner.[80] Holmes stated that a party to the contract could has discretion to either perform the obligations or pay the damages for the loss suffered by the other party due to non-performance.[81] This theory states that contractual parties are allowed to breach a contract and pay expectation damages if the breaching party concludes that breaching the contract would be more efficient than paying the expectation damages.[82] This theory is only feasible if other party's expected gain is lower than the breached party's gain.[83] Contract law would play a decisive role in efficient breach theory by limiting the damages sought by the other party with regard to their expectation from the contract, otherwise contractual parties would be induced to perform the contract even if it were inefficient to do so. Liao

---

79 Timothy J. Muris, "Opportunistic Behavior and the Law of Contracts," *Minnesota Law Review* 65, (1981): 521.

80 Richard A. Posner, *Economic analysis of law* (Boston: Little Brown, 1973).

81 Oliver Wendell Holmes, "The Path of the Law," *Harvard Law Review* 10, (1897): 462.

82 Gregory Klass, "Efficient Breach," in *Philosophical Foundations of Contract Law*, eds. Gregory Klass, George Letsas and Prince Saprai, (Oxford, United Kingdom: Oxford University Press, 2014), 396.

83 Richard A. Posner, *Economic analysis of law* (Austin, USA : Wolters Kluwer for Aspen Publishers, 2007), 47.

emphasises that imposing punitive damages for breach of the contract would deter efficient breach as this damages intentions to cover more than the expected profits.[84] Therefore, expectation damages as the primary remedy under common law are compatible with the idea of efficient breach.[85]

Even though there is no explicit and direct reference to the efficient breach theory in the cases in the English law,[86] Kilvington provides a variety of case law which is related to the efficient breach theory and ıts compatibility within the English contract law.[87] As an example from Supreme Court, in *Morris-Garner v One Step (Support) Ltd*[88] the respondent had purchased a firm from the appellants that provided help to young people who had been in foster care. They agreed to a non-compete and non-solicitation clause in their contract. However, then the non-compete and non-solicitation clause was breached. The Supreme Court held that except in extraordinary circumstances, common law damages for breach of contract could not be given only for the purpose of depriving the defendant of profits earned as a result of the breach. The defendant agreed that he intentionally breached the contract, which is in line with the characteristic with efficient breach theory. Secondly, when the Court quantifying the compensatory damages, the Court did not deprıve the defedant of the profıts made as a result of breach.

---

84 Liao, The Application, 47.

85 For the view that English law does not allow efficient breach, see: Al-Tawil, "English Contract Law," 413; See for the argument that specific performance can be considered as efficient as paying damages, Alan Schwartz, "The case for specific performance," *The Yale Law Journal* 89, (1979): 305-306.

86 Liam David Kilvington, "Justfying the application of the theory of efficient breach specifically within the context of commercial contracting," (PhD Thesis, University of York, September 2018), 152, accessed April 28, 2020, https://etheses.whiterose.ac.uk/23552/1/Liam%20Kilvington%20PhD%20Thesis%20Revised%20for%20Final%20Submission.pdf.

87 Kilvington, *Justfying*, 153.

88 Morris-Garner v One Step (Support) Ltd, [2018] UKSC 20.

This approach also is in line with efficient breach theory since it allows contractual parties to get further benefit from the breach of the contract.

Even though law and economics theory relies on economic theory to justify efficient breach, it is not safe from a variety of criticisms. The first is, understandably, the moral disapproval of this theory. Klass reiterates that promises create a moral obligation to perform a contract, and the law should not incentivise the breach of a contract despite its efficient results.[89] Specific performance, as a primary remedy in civil law, hinges on this moral theory to justify its position. Secondly, this theory considers performance interest to be the same as compensation interest on the basis that the expectation damages are sufficient for the breach of the contract. Tareq rebukes this understanding by noting that performance interest is a primary interest in the conclusion of a contract.[90] Kimel defends the idea that deviation from the specific performance of the obligation to the remedies requires a justification.[91] Thirdly, it is argued that efficient breach theory disregards the transactional costs incurred in the litigation or settlement procedure.[92] The costs incurred in these procedures would ultimately produce inefficient results due to the associated consumption of resources after the breach occurs. Even though these defences against efficient breach theory are fair, the possibility of an efficient breach reflects a potential response by contractual parties if a fortunate contingency comes to light after the agreement is finalised. This theory is merely a good illustration of how people can change their minds after the conclusion of a contract. For this reason, it will be used as an example to show the inflexibilities of smart contracts.

---

89 Klass, "Efficient Breach," 367.

90 Al-Tawil, "English Contract Law," 399-400.

91 Dori Kimel, From promise to contract: towards a liberal theory of contract, (Oxford: Hart Publishing, 2003), 113.

92 Klass, "Efficient Breach," 367-68.

The idea of the smart contract would ignore people's tendencies to pursue more profitable transactions even after the conclusion of another contract. Specific performance is automated and guaranteed without any human intervention. At a glance, it seems to represent an effective solution for parties who want to secure the performance of the contract. This function of the smart contract would make it appealing in most such instances. However, due to circumstances that might occur after the conclusion of the contract, it would be more efficient for parties to avoid specific performance and pay expectation damages instead. Because of the immutability of smart contracts, parties would not be able to benefit from this choice and would be forced to perform their obligations. For instance, in *Vitol SA v Beta Renowable Group SA*[93], the contract is made for the claimant to purchase a certain amount of biofuel from the defendant and have it delivered between June 16 and June 30, 2016. The claimant agreed to designate a vessel by the 27th of June. The claimant hedged the contract against price volatility by selling gasoil futures contracts at a predetermined price, which is usual procedure in the biofuels market. On June 1, 2016, the defendant informed the claimant that it would be unable to fulfill its contractual obligation of providing biofuel. The defendant suggested on June 14 to supply a lesser amount than was contracted for, but stated that it would be unable to do so between June 16 and 30. The claimant responded with a request for more delivery information. It did not name a vessel by the 27th of June, but warned the defendant that if full delivery did not occur in accordance with the contract, it would hold it in breach of contract. The claimant gave notice of contract termination on July 7th. It claimed that by failing to perform its contractual obligations, the defendant was in repudiatory breach, and that it had accepted that breach either by not designating a vessel or by terminating the contract on July 7th.

[93] Vitol SA v Beta Renowable Group SA, [2017] EWHC 1734 (Comm).

At the end, it is clear that the defendant intentionally avoid the performance of the contract and tried to renegotiate the contract[94] and also agreed to pay damages but they did not agree on the amount of the compensation. Assume that the whole process are automated with the use of smart contracts and there is no way of escaping from the performance of the contract. It would mean that the automatic execution of the specific performance would not be always an ideal solution. Dell'Erba considers the efficient breach theory to be a challenge against the automated performance provided by smart contracts.[95] This lack of flexibility would negatively affect how the smart contract is perceived among its potential users. Having the right to change their mind, even after the conclusion of a contract, would have to be provided in smart contracts or the uniform approach towards securing specific performance would be considered a barrier to their widespread use.

B. The Possible Solution within Smart Contracts: Securing the Liquidated Damages

It can be argued that allowing a breach of contract would make the smart contract useless as it is the distinct feature of smart contracts. This article maintains that this distinct feature would not be eroded because this particular characteristic of smart contracts can be manifest in other ways, such as securing compensation for non-performance. Securing compensation as well as specific performance would facilitate the adaptation of smart contracts to the possibility of the efficient breach without losing its advantages. Accordingly, smart contract developers would dilute the inflexible consequences caused by the immutable nature of smart contracts by allowing parties to

94 *Vitol v Beta*, [17]- [18].

95 Dell'Erba, "Demystifying Technology," 20.

incorporate liquidated damages,[96] as a form of compensation, to smart contract code.

This type of structure gives the parties two choices, either paying liquidated damages or specific performance. This basic structure can be achieved by giving limited discretion to the contractual parties the choice of either. In this scenario, the automatic performance feature will not be compromised due to this discretion since the liquidated damages are secured. When the liquidated damages clause triggers can be inserted into the smart contract. Holden and Malani confirm the use of liquidated damages as part of the renegotiation mechanism in smart contracts.[97] Oracles would help parties to feed relevant data to the smart contract to determine whether the condition of liquidated damages has occurred or otherwise one of the parties can make a choice between fulfilling the obligation or paying the liquidated damages. As both the specific performance and liquidated damages are secured, the distinct feature of the smart contract is protected but with the flexibility of paying liquidated damages. For instance, A and B agree to transfer of shares which are digitally registered and transferred on the blockchain on May 31, 2020. If A and B agree to integrate a liquidated damages clause by which the pre-determined sum is secured technically, as well as the transfer of the share by the smart contract. If there is an unexpected increase in the value of the share, A can choose to pay the liquidated damages instead of transferring the shares, believing that this option is more advantageous to him. This illustration shows that inserting the liquidated damages clause

---

[96] Liquidated damages are defined as a fixed money agreed under a contract becomes payable if the breach of the contract is occurred. Under English law, the liquidated damages is valid and enforceable as long as it equals to the estimated loss of the parties. However, If the pre-determined sum by the parties is far more than the estimated loss, this clause is considered penalty clause and invalid, see: Duxbury, *Contract Law: Textbook Series*, 16.052-53.

[97] Holden and Malani, "Can Blockchain Solve," 5-6.

would provide flexibility for parties by enabling them to avoid specific performance and instead pay the pre-determined sum in the context of smart contracts. Having two options within smart contracts does not prejudice the distinct feature of a smart contract because the automatic execution of damages is retained instead of specific performance.

CONCLUSION

Smart contracts have attracted people's interest over the last few years. This essay discusses smart contracts from a legal perspective. The distinct feature of the smart contract is determined as the guaranteed performance of the associated obligations. As the use of blockchain facilitates the automatic execution of the performance, smart contracts are sometimes defined with reference to the features of blockchain. Indeed, blockchain technology, by its extended immutability and distributed nature and integration of oracles, has contributed to the improvement of the smart contracts. However, smart contracts are the code written on top of blockchain technology and can exist without it.

Regarding the legal nature of smart contracts, due to the flexible nature of contract law, smart contracts can fall within the current scope of contract law. If the meeting of minds, intention to create legal relations and consideration occur, a smart contract can be considered enforceable under the current framework. Using algorithms in the conclusion of a smart contract would not change enforceability since these algorithms are delegated by the parties.

Even the technical guarantee of the performance seems desirable for contractual parties; this guarantee would result in inflexibility, which might deter the widespread use of smart contracts. Firstly, the secured performance of the contract might exacerbate the incompleteness of the contract problem as the performance, as a principle, cannot be stopped even should an unfortunate contingency arise, and there is a need to renegotiate

to adjust people's obligations under the new contingencies. However, integrating the renegotiation mechanism into the smart contract is one option by which this problem could be alleviated. Additionally, the use of oracles can bring real-life changes to the smart contract, relieving its inflexibility.

More importantly, even though the secured performance of the contract is one of its distinct features, not allowing for the possibility of breach of the contract could be considered inflexible because of the occurrence of contingencies, be they fortunate or unfortunate. Breach of the contract might well be the more efficient route for contractual parties rather than specific performance in such circumstances. Accordingly, the law and economics approach posits "efficient breach theory". By applying this theory to the smart contract relations, it is maintained that insisting on the specific performance of the obligation under a smart contract would not be desirable for the contractual parties. Therefore, in the design of smart contracts, liquidated damages can be added in addition to specific performance to secure, such as an alternative to specific performance if the breach is efficient for one of the parties. Granting this choice to the parties would not prejudice the advantages of using a smart contract as compensation is secured. Therefore, the possibility of adding liquidated damages must be considered in the design phase of smart contracts.

BIBLIOGRAPHY

Cases

Fibrosa Spolka Ackyjna v Fairbairn Lawson Combe Barbour Ltd, *[1943] A.C. 32.*

Morris-Garner v One Step (Support) Ltd, [2018] UKSC 20.

Vitol SA v Beta Renowable Group SA, [2017] EWHC 1734 (Comm).

Books

Cooter, Robert and Ulen, Thomas. *Law and Economics*. Harlow, Essex: Pearson, 2014.

De Filippi, Primavera and Wright, Aaron. *Blockchain and the law: the rule of code*. Cambridge, Massachusetts: Harvard University Press, 2018.

Devlin, Alan. Fundamental Principles of Law and Economics. London: Routledge, 2015.

Duxbury, Robert. *Contract Law: Textbook Series.* London: Sweet & Maxwell, 2014.

Gatteschi, Valentina, Lamberti, Fabrizio and Demartini, Claudio. "Technology of Smart Contracts." in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, eds. Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò. Cambridge: Cambridge University Press, 2019.

Hart, Oliver Simon D'Arcy. *Firms, Contracts, and Financial Structure*. New York: Oxford University Press, 1995.

Klass, Gregory. "Efficient Breach." in *Philosophical Foundations of Contract Law*, eds. Gregory Klass, George Letsas and Prince Saprai. Oxford, United Kingdom: Oxford University Press, 2014.

Kimel, Dori. From promise to contract: towards a liberal theory of contract. Oxford: Hart Publishing, 2003.

Marino, Bill and Juels, Ari. "Setting Standards for Altering and Undoing Smart Contracts." in *Rule Technologies. Research, Tools, and Applications*, eds. Jose Julio Alferes, Leopoldo

Bertossi, Guido Governatori, Paul Fodor, Dumitru Roman. Cham: Springer International Publishing, 2016.

Möslein, Florian. "Legal Boundaries of Blockchain Technologies: Smart Contracts as Self-Help?." in *Digital Revolution-New challenges for Law (Forthcoming)*. eds. Alberto Franceschi, Reiner Schulze, Michele Graziadei, Oreste Pollicino, Federica Riente, Salvatore Sica, Pietro Sirena. 2019. Accessed April 25, 2020, https://ssrn.com/abstract=3267852.

Murray, Andrew. *Information technology law: the law & society.* Oxford, United Kingdom: Oxford University Press, 2019.

Poncibò, Cristina and Dimatteo, Larry A. "Smart Contracts: Contractual and Noncontractual Remedies." in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. eds. Cristina Poncibò, Larry A. DiMatteo and Michel Cannarsa. Cambridge: Cambridge University Press, 2019.

Posner, Richard A., *Economic analysis of law*. Boston: Little Brown, 1973.

Posner, Richard A. *Economic analysis of law*. Austin, USA: Wolters Kluwer for Aspen Publishers, 2007.

Scholz, Lauren Henry. "Algorithmic Contracts and Consumer Privacy." in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. eds. Cristina Poncibò, Larry A. DiMatteo and Michel Cannarsa. Cambridge: Cambridge University Press, 2019.

Wenqing, Liao. The Application of the Theory of Efficient Breach in Contract Law: A Comparative Law and Economics Perspective. Cambridge: Intersentia, 2015.

Articles

Al-Tawil, Tareq. "English Contract Law and the Efficient Breach Theory: Can They Co-Exist?." *Maastricht Journal of European and Comparative Law* 22, no. 3 (2015): 396-416.

Anderlini, Luca and Felli, Leonardo. "Bounded rationality and incomplete contracts." *Research in Economics* 58, no. 1 (2004): 3-30.

Bacina, Michael. "When Two Worlds Collide: Smart Contracts and the Australian Legal System." *Journal of Internet Law* 21, no. 8 (2018): 1-27.

Cuccuru, Pierluigi. "Beyond bitcoin: an early overview on smart contracts." *International Journal of Law and Information Technology* 25, no. 3 (Autumn 2017): 179–195. https://doi.org/10.1093/ijlit/eax003.

Cutts, Tatiana. "Smart Contracts and Consumers." *LSE Legal Studies Working Paper*, no. 1 (2019): 1-52. Accessed April 28, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354272.

Dell'Erba, Marco. "Demystifying Technology. Do Smart Contracts Require a New Legal Framework? Regulatory Fragmentation, Self-Regulation, Public Regulation." (2018): 1-49. http://dx.doi.org/10.2139/ssrn.3228445.

European Commission. *Study on Blockchains. Legal, governance and interoperability aspects (SMART 2018/0038)*. Luxembourg: Publications Office of the European Union, 2020. https://op.europa.eu/s/pi6i.

Finck, Michèle. "Smart contracts as a form of solely automated processing under the GDPR." *International Data Privacy Law* 9, no. 2 (May 2019): 78-94. https://doi.org/10.1093/idpl/ipz004.

Giancaspro, Mark. "Is a 'smart contract' really a smart idea? Insights from a legal perspective." *Computer Law & Security Review* 33, no. 6 (2017): 825-835. https://doi.org/10.1016/j.clsr.2017.05.007.

Grimmelmann, James. "All Smart Contracts Are Ambiguous." *Journal of Law & Innovation* 2, no. 1 (2019): 1-22. Accessed April 21, 2020.

https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1006&context=jli.

Hermalin, Benjamin E. and Katz, Michael L. "Information and the Hold-Up Problem." *The RAND Journal of Economics* 40, no. 3 (2009): 405-423. Accessed April 22, 2021. http://www.jstor.org/stable/25593717.

Holmes, Oliver Wendell. "The Path of the Law." *Harvard Law Review* 10, (1897): 457-478.

Hovenkamp, Herbert. "Law and Economics in the United States: a brief historical survey." *Cambridge Journal of Economics* 19, no. 2 (April 1995): 331–352. https://doi.org/10.1093/oxfordjournals.cje.a035316.

Juels, Ari, Kosba, Ahmed and Shi, Elaine. "The Ring of Gyges: Using Smart Contracts for Crime." Accessed March 29, 2020, http://www.arijuels.com/wp-content/uploads/2013/09/Gyges.pdf.

Lando, Henrik and Rose, Caspar. "On the enforcement of specific performance in Civil Law countries." *International Review of Law & Economics* 24, no. 4 (2004): 473-487. https://doi.org/10.1016/j.irle.2005.01.005.

Lauslahti, Kristian. Mattila, Juri and Seppala, Timo. "Smart Contracts – How Will Blockchain Technology Affect Contractual Practices?." *ETLA Reports*, no. 68 (2017): 1-32. Accessed April 21, 2020. https://ssrn.com/abstract=3154043.

Levy, Karen E. C.. "Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law." *Engaging Science, Technology, and Society* 3, (2017): 1-15.

Macrinici, Daniel, Cartofeanu, Cristian and Gao, Shang. "Smart contract applications within blockchain technology: A systematic mapping study." *Telematics and Informatics* 35, no. 8 (2018): 2337-2354. https://doi.org/10.1016/j.tele.2018.10.004.

Mik, Eliza. "Smart contracts: terminology, technical limitations and real world complexity." *Law, Innovation and Technology* 9,

no. 2 (2017): 229-300. https://doi.org/10.1080/17579961.2017.1378468.

Muris, Timothy J.. "Opportunistic Behavior and the Law of Contracts." *Minnesota Law Review* 65, (1981): 521-590.

Posner, Richard A.. "The Law and Economics of Contract Interpretation." *Texas Law Review* 83, (2005): 1581-1614.

Savelyev, Alexander. "Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law." *Information & Communications Technology Law* 26, no. 2 (2017): 116-134. https://doi.org/10.1080/13600834.2017.1301036.

Scoca, Vincenzo, Uriarte, Rafael Brundo and Nicola, Rocco De. "Smart Contract Negotiation in Cloud Computing." *2017 IEEE 10th International Conference on Cloud Computing*. (Honololu, HI, USA: IEEE, 2017): 592-599. https://doi.org/10.1109/CLOUD.2017.81.

Schwartz, Alan. "The case for specific performance" *The Yale Law Journal* 89, (1979): 271-306.

Singh, Amritraj, M.Parizi, Reza, Zhang, Qi, Raymond Choo, Kim-Kwang and Dehghantanha, Ali. "Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities." *Computers & Security* 88, (2020): 1-16. https://doi.org/10.1016/j.cose.2019.101654.

Sklaroff, Jeremy M.. "Smart Contracts and The Cost of Inflexibility." *University of Pennsylvania Law Review* 166, no. 1 (2017): 263-303. Accessed April 21, 2020. https://scholarship.law.upenn.edu/penn_law_review/vol166/iss1/5.

Tjong Tjin Tai, Eric. "Force Majeure and Excuses in Smart Contracts." *European Review of Private Law* 26, no. 6 (2018): 787-804.

Werbach, Kevin and Cornell, Nicolas. "Contracts ex machina." *Duke Law Journal* 67, no.2 (2017): 313-382. Accessed May 4, 2020. https://scholarship.law.duke.edu/dlj/vol67/iss2/2.

Greenspan, Gideon. "Beware of the Impossible Smart Contract." Accessed April 23, 2020. https://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract.

Holden, Richard T. and Malani, Anup. "Can Blockchain Solve the Hold-up Problem in Contracts?." *The National Bureau of Economic Research Working Papers*, no. 25833 (2019): 1-39.

Kilvington, Liam David. "Justfying the application of the theory of efficient breach specifically within the context of commercial contracting." PhD Thesis, University of York, September 2018. Accessed April 28, 2020. https://etheses.whiterose.ac.uk/23552/1/Liam%20Kilvington%20PhD%20Thesis%20Revised%20for%20Final%20Submission.pdf.

Szabo, Nick. "Smart Contracts: Building Blocks for Digital Markets." Accessed March 20, 2020. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html/.

The Right Honourable Lord Hodge, "The Potential and Perils of Financial Technology: Can the Law Adapt to Cope?" *The First Edinburgh FinTech Law Lecture*, (Edinburgh Law School, South Bridge, Edinburgh, March 14, 2019). Accessed April 24, 2020. https://www.law.ed.ac.uk/sites/default/files/2020-09/speech-190314%20-%20Acc.pdf.

ELEKTRONİK TİCARETTE KİŞİSEL VERİLERİN KORUNMASI

Personal Data Protection in Electronic Trade

Ömer Faruk KUNTOĞLU*

Öz

Bilişim teknolojilerinin hayatın tüm alanlarına yönelik genişlemesi hızla sürmekte, ticari hayat da bu durumdan yoğun olarak etkilenmektedir. Günümüzde en küçük günlük ihtiyaçlar dahi elektronik ticaret kanalıyla karşılanabilirken ticari sözleşmelerin tarafı olan kişi ya da kurumlar büyük miktarda kişisel veri elde etmektedir. Öte yandan, kişilik hakları ve özel hayatın gizliliği bağlamında her türlü kişisel verinin gerek uluslararası düzenlemelerle gerekse iç mevzuatımızla korunması amaçlanmaktadır.

Çalışmamızda kişisel veriler ve elektronik ticaret konularında temel bilgiler sunulduktan sonra elektronik ticarette kişisel verilerin korunması bağlamında mevcut hukuki düzenlemelerle kişilere/şirketlere yüklenen yükümlülükler ortaya konulacaktır. Uygulamada bu yükümlülüklerin kişisel verilerin korunmasına yönelik arzu edilen korumayı ne ölçüde sağladığı konusu irdelenerek sorunlara ilişkin çözüm önerileri sunulmaya çalışılacaktır.

* İstanbul Medeniyet Üniversitesi Özel Hukuk Doktora Programı Öğrencisi, Hâkim, kuntoglu@hotmail.com, ORCID: 0000-0002-6927-9973.

Makale Gönderim Tarihi/Received: 02.06.2020.

Makale Kabul Tarihi/Accepted: 27.05.2021.

Atıf/Citation: Kuntoğlu, Ömer Faruk. "Elektronik Ticarette Kişisel Verilerin Korunması." *Bilişim Hukuku Dergisi* 3, no: 1 (2021): 176-229.

Anahtar Kelimeler: Kişisel Veri, Elektronik Ticaret, Veri Güvenliği, Veri Sorumlusu, İlgili Kişi.

Abstract

Expansion of information technologies in every part of our lives still continues and business life is intensively affected by this, as well. Currently, even the most basic daily needs are satisfied by means of electronic trade and this provides the personal or institutional parties of the contracts with so much personal information. On the other hand, in the context of personal rights and right of privacy, it is aimed to be protected of every kind of personal information by the international regulations and internal law.

In this study, after mentioning basic information in the subject of personal information and electronic trade, the obligation of the companies/persons put by law in force is going to be explained in the context of protection of personal information in electronic trade. Finally, solutions are going to be presented to the problems addressed by the question of how much those applied obligations ensure desired protection in protection of personal information.

Keywords: Personel Data, Electronic Trade, Data Security, Data Controller, Data Subject.

GİRİŞ

Teknolojinin hayatımızın tüm alanlarında hızla yaygınlık kazanması nedeniyle adaletten sağlığa, eğitimden ekonomiye akla gelen tüm alanlarda bilişim teknolojilerinin etkinliği her geçen gün daha fazla hissedilmektedir. Bilişim sistemleri üzerinden toplanan oldukça büyük miktarda verinin işlenme, değerlendirilme ve analiz edilme süreçleri, birçok alanda çok köklü değişiklikler doğurmaktadır. Büyük Veri (*Big Data*), Yapay Zekâ, Makine Öğrenmesi gibi kavramlar hayatı değiştirirken yeni sorunlar da doğurmakta, bu durum hukuk dünyasına da bariz şekilde yansımaktadır.

Bilişim teknolojileri vasıtasıyla toplanan verinin önemli bir kısmı kişisel verilerdir. Daha önce sınırlı düzeyde elde edilen kişisel verilerin teknoloji vasıtasıyla devasa düzeye ulaşması; reklam faaliyetlerinden seçim sonuçlarını etkilemeye varıncaya kadar pek çok alanda veri sahiplerinin rızaları dışında ve güç odaklarınca menfaat temelli kullanılması, kişilik haklarına doğrudan bir müdahale anlamına gelmektedir.

1981 Yılında imzalanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Uluslararası Sözleşmesi" kişisel verilerin korunması anlamında bir dönüm noktasıdır. Ülkemiz bu anlaşmaya taraf olmuş ve sonrasında iç hukukunda da gerekli düzenlemeleri yapmaya başlamış, son olarak Kişisel Verilerin Korunması Kanunu'nu[1] çıkartmıştır. Yine, Türkiye'nin bu konuda attığı önemli adımlardan birisi Kişisel Verileri Koruma Kurumunun kurulmasıdır. Ancak bütün bunlara rağmen bu konuda çok başlarda olduğumuz, özellikle uygulama anlamında emekleme döneminde olduğumuz da bir gerçektir. Kişisel verilerin korunmasına ilişkin gerek toplumun farkındalığının yeterli düzeyde olmaması, gerekse gerekli kamusal denetim mekanizmalarının tam olarak tesis edilememesi nedeniyle uygulamada ciddi sorunlar olduğu ortadadır. Öte yandan, günümüzde artık günlük mutfak ihtiyaçlarımızı karşılamaya varıncaya kadar kullandığımız elektronik ticaretin alanı her geçen gün genişlemektedir. Tecrübe edilmekte olan Covid-19 salgını söz konusu genişlemeyi hızlandırmıştır.

Elektronik ticaret işlemleri yapılırken yoğun olarak kişisel veriler kaydedilmektedir. Kullanıcı profilleri dâhil söz konusu kişisel veriler büyük sermaye şirketleri için üreten-tüketen kitleleri yönlendirmede kullanılmaktadır. Elektronik ticarette, alıcıların kişisel verilerinin korunması konusunda farkındalıklarının artırılması gerekmektedir. Yine hizmet

[1] RG. 07.04.2016, S. 29677.

sağlayıcı/aracı hizmet sağlayıcıların bu konudaki yükümlülüklerinin ortaya konulması, söz konusu yükümlülüklerin icra edilip edilmediğini denetleyecek mekanizmaların oluşturulması ve işlevsel hale getirilmesi şarttır.

Üç bölümden oluşan çalışmamızın temel araştırma sorusu, kanundan kaynaklanan yükümlülüklerin uygulamada kişisel verilerin korunmasına yönelik arzu edilen korumayı ne ölçüde sağladığı noktasında toplanmaktadır. Çalışmanın birinci bölümünde kişisel verilerin korunması kavramı incelenecektir. İkinci bölümde elektronik ticaret ve elektronik sözleşmelere ilişkin temel hususlar açıklanmaya çalışılacaktır. Üçüncü bölümde genel anlamda kişisel verilerin korunmasına ilişkin düzenlemeler çerçevesinde elektronik ticaret yapan veri sorumlularının yükümlülükleri ile bu yükümlülüklerin hayata geçirilmesi amacıyla tesis edilen bazı uygulamalar incelenecek ve düzenlemelere uygun hareket edilmediği takdirde karşılaşılacak yaptırımlara değinilecektir. Sonuç kısmında ise mevzuat ile hedeflenen korumanın uygulamada gerçekleşip gerçekleşmediği ve bu konuda kanaatimizce izlenmesi gerekli yol açıklanmaya çalışılacaktır.

I. KİŞİSEL VERİLERİN KORUNMASI

21. yüzyılda bilişim teknolojilerinin etki alanının hızla genişlediği görülmektedir. Eğitimden sağlığa, ticaretten siyasete neredeyse her alanda bilişim teknolojilerinin varlığı güçlü bir şekilde hissedilmektedir.

Hukuk sistemini devlet otoritesinin gücüyle tesis edilen yaptırımlara bağlanmış kurallar bütünü olarak tanımlamak mümkündür.[2] Hukuk sisteminin, topluma dokunan tüm yeniliklerle değişime uğrayacağı muhakkaktır. Bu çerçevede, bilişim teknolojilerinde meydana gelen değişim ve gelişmeler de

[2] TDK Sözlük, "Hukuk," erişim tarihi: Kasım 18, 2019, https://sozluk.gov.tr/?kelime=.

hukuk dünyasında yeni sorunlara neden olarak yasama organını yeni hukuki düzenlemeler yapmaya zorlamaktadır.

Bilişim teknolojileri vasıtasıyla gerek kamu gerekse özel sektör sürekli kişisel verilerimizi elde etmektedir. Elde edilen veriler başka kişilerin özel bilgilerimize vakıf olması anlamına gelmektedir. Üzerinde biraz düşünüldüğünde, örneğin sosyal medya aracılığıyla ya da alışveriş, spor salonu kullanımı gibi etkinlikler sırasında kolaylıkla elde edilen kişisel verilerin bir istihbarat kurumunun ulaşmak istediği verilerin ötesine geçebildiğini görmek mümkün olur. Burada önemli olan kamunun ya da özel sektörün topladığı bu verileri kimlere aktardığı, başka amaçlarla kullanıp kullanmadığı hususlarıdır.[3]

Post-fordist üretim tarzına geçilmesi ile kişisel verilerin önemi artmıştır. Zira bu üretim tarzı içerisinde iletişim teknolojileri yoğun olarak kullanılmaktadır. Tüketiciler bir taraftan mal ve hizmetleri tüketirken; elde edilen kişisel veriler üzerinden yapılan analizler ile tüketim alışkanlıkları tespit edilerek, sermaye şirketlerinin geliştireceği stratejilere malzeme üretmiş olmaktadırlar. Dolayısıyla, bu anlamda tüketiciler için üreten-tüketiciler ifadesi kullanılabilecektir. Tüketiciler, kişisel verilerinin korunmasını isterken; bu verileri kazançlarını artıracak bir araç olarak gören sermaye şirketleri, kişisel verileri kullanmayı sürdürmek istemektedirler.[4] Kişisel verilere ilişkin bu durum özel yaşamın bittiği endişesine yol açmıştır. Bu noktada, kişisel verilerin korunması hakkının ortaya çıkarılması ve bu kapsamda hukuki düzenlemelerin hayata geçirilmesi, özel hayatın korunması anlamında ciddi bir koruma kalkanının oluşmasına vesile olmuştur.[5]

---

3 Elif Küzeci, "Anayasal Bir Hak: Kişisel Verilerin Korunması," *Türkiye Bilişim Derneği Bilişim Dergisi*, no. 128 (Ocak 2011): 43.

4 Serpil Karlıdağ, "Ekonomi Politik Acıdan Kişisel Verilerin Korunması,", *Amme İdaresi Dergisi* 46, no. 1 (Mart 2013): 128.

5 Küzeci, "Anayasal Bir Hak," 142.

Kişisel verilerin korunmasına ilişkin düzenlemeler, kişisel veri işleme süreçlerinin nesnesi durumunda olan bireyleri, kişisel verinin hak süjesi haline getirmektedir.[6] Konuya ilişkin ilk çalışmalar Almanya başta olmak üzere Batı Avrupa ülkelerinde 1970'lerde başlamıştır. Zira bu tarihler bilgisayarlar aracılığıyla geçmişe nazaran daha büyük miktarda kişisel verinin toplanmaya başladığı yıllardır.[7]

Kişisel verilerin korunması anlamında milletlerarası kriterlerin belirlendiği ilk çalışma Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) tarafından yapılmış ve 1980 yılında "*Gizliliğin Korunması ve Sınır Ötesi Kişisel Veri Akışları Hakkında Rehber İlkeler*" belirlenmiştir.[8] Bu ilkeler tavsiye niteliğinde, bağlayıcı olmayan ilkelerdir. Bu nedenle, yeni bir çalışmaya ihtiyaç duyulmuştur. Bu çerçevede, 1981 yılında "*Kişisel Verilerin Otomatik İşleme Tâbi Tutulma Sürecinde Şahısların Korunması Sözleşmesi*" kabul edilmiştir. Bu belge, Avrupa'da ortaya çıkan kişisel verilerin korunması konusundaki ilk uluslararası hukuk metnidir. Sözleşme 1981 yılında kabul edilse de 1985 yılında yürürlüğe girmiştir. Sözleşme, kişisel verilerin korunmasında etkili bir mekanizma getirmemektedir. Ancak, sözleşmenin bağlayıcı olması ve verilerin işlenmesi, depolanması ve aktarılması konularında hükümler içeriyor olması oldukça

6 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu Tasarısı ve Adalet Komisyonu Raporu*, (Ankara: TBMM, 2016), 64, https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf.

7 Küzeci, "Anayasal Bir Hak," 143-144.

8 Alaattin Bük, *Bilişim Alanında Kişisel Verilerin Korunması*, (Ankara: Seçkin Yayıncılık, 2018), 65.

önemlidir.[9] Türkiye bu sözleşmeyi imzalamış, sonraki süreçte iç hukukuna da aktarmıştır.[10]

Avrupa Birliği 1995 yılında "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi (95/46/EC)"ni kabul etmiştir. Söz konusu yönergeyi tamamlamak üzere 1997 yılında "Telekomünikasyon Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması Yönergesi (97/66/EC)" kabul edilmiştir. 2002 yılında icra edilmeye başlanan "Elektronik İletişimde Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönergesi (2002/58/EC)" de bir diğer önemli düzenlemedir.[11]

1982 tarihli Anayasamızın "Özel Hayatın Gizliliği ve Korunması" başlıklı bölümünün "Özel Hayatın Gizliliği" başlıklı 20. maddesine 7 Mayıs 2010 tarihinde kişisel verilerin korunmasına ilişkin olarak şu fıkra eklenmiştir: *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."*[12]

Anayasada bahsi geçen değişikliğin gerekçesinde, tarafı olduğumuz uluslararası sözleşmelerde "kişisel verilerin korunması" kavramının ısrarla vurgulandığı ifade edilerek, Türkiye'de farklı kanunlarda yer alan dolaylı hükümlerin yeterli

---

9 Habip Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum," *Uyuşmazlık Mahkemesi Dergisi*, no. 3 (2013): 8.

10 Bkz. 6669 Sayılı Kişisel Verilerin Otomatik İşleme Tâbi Tutulma Sürecinde Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, RG. 18.02.2016, S. 29628.

11 Oğuz, "Elektronik Ortamda Kişisel," 9.

12 RG. 13.05.2010, S. 27580.

olmadığı belirtilmiştir.[13] Anayasa değişikliği ile getirilen *"Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"* hükmünün gereği olarak 7 Nisan 2016 tarihinde 6698 sayılı Kişisel Verilerin Koruması Kanunu (KVKK) yürürlüğe girmiştir.

KVKK'nın gerekçesi incelendiğinde; kişisel verilerin kullanılmasında bireyler ile mal ve hizmet sunanlar bakımından bazı kolaylıklar veya avantajların olduğu kabul edilse de söz konusu bilgilerin istismar edilme riskinin de söz konusu olduğu, bu risk ve fayda arasında makul bir dengenin oluşturulması gerektiği ifade edilmektedir. Gerekçede kişisel verilere ilişkin düzenlemelerin ayrı ayrı kanunlarda düzenlenmesinin sakıncalarına da değinilmektedir.

KVKK yürürlüğe girmeden önceki dönemde kişisel verilere ilişkin mevzuatta bir belirsizlik söz konusudur. Örneğin, 5237 sayılı Türk Ceza Kanunu'nun "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlıklı dokuzuncu bölümü içerisinde, "kişisel verilerin kaydedilmesi" (m.135), "verileri hukuka aykırı olarak verme veya ele geçirme" (m.136), "verileri yok etmeme" (m.138) gibi suçlara yer verilmiştir. Ancak, o tarih itibariyle mevzuatta kişisel verinin ne olduğunu tanımlayacak bir kanun bulunmadığından uygulamada ve yargılamada birçok tereddüt hasıl olmuştur.

Yine gerekçede, Avrupa Birliği'nin bu konudaki beklentilerine işaret edilerek; müstakil bir kanunumuzun olmamasının, emniyet birimlerinin uluslararası koordinasyonu için gerekli olan EUROPOL ve yargı birimlerinin uluslararası koordinasyonu için gerekli olan EUROJUST adlı sistemlerle entegrasyon kurmamıza engel oluşturduğu belirtilmektedir. Gerekçede, aynı nedenlerle, yabancı sermayenin ülkemizdeki yatırımlarını fonksiyonel olarak kullanması için zaruri olan veri

[13] Türkiye Büyük Millet Meclisi, 2709 Sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun Teklifi ve Anayasa Komisyonu Raporu, (Ankara: TBMM, 2010), 9, https://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss497.pdf.

aktarım sistemlerinin kurulmasının da mümkün olamadığına vurgu yapılmaktadır.[14] Zira, bu konularda kendi iç hukuklarında düzenleme bulunan ülkeler bizim müstakil bir kanunumuzun bulunmamasını, kişisel verilerin korunması anlamında bir eksiklik olarak ileri sürmüş ve anılan veri aktarım mekanizmalarının kurulmasını kabul etmemiştirler.

Konuyu açıklayabilmek için KVKK'da düzenlenen hususlara ana hatlarıyla değinmemiz gerekmektedir.

A. Kişisel Verilerin Korunması Kanunu'nun Amacı ve Kapsamı

KVKK'nın iki temel amacı vardır: Temel hak ve özgürlüklerin korunması ile veri sorumlularının yükümlülükleri ile uyacakları usul ve esasların belirlenmesi (m.1). Kanunun kapsamında verileri işlenen gerçek kişiler ile veri sorumluları yer almaktadır (m.2). Kanun ilgili kişiyi, "*kişisel verisi işlenen gerçek kişi*" (m.3) olarak tanımlamaktadır. Dolayısıyla bir kişisel veriden bahsedebilmek için ortada muhakkak bir gerçek kişi bulunmalıdır.

KVKK kapsamında tüzel kişinin kişisel verisinden bahsetmek mümkün değildir. Örneğin, bir vakfın, şirketin ya da siyasal partinin kişisel verisi olmaz. Bu tüzel kişilikler şartları varsa ancak veri sorumlusu olabilecektir. Dolayısıyla, KVKK kapsamında tüzel kişilerin kişisel verilerinin korunması söz konusu değildir.[15] Bu durum Alman mevzuatında da benzer şekilde düzenlenmiştir.[16] Tüzel kişilere ait veri ve bilgiler, Türk Medeni Kanunu'nun kişilik hakkının korunmasına ilişkin hükümleri ve ilgili tüzel kişiye ilişkin özel mevzuatlarda hüküm

---

14 TBMM, Kişisel Verilerin Korunması Kanunu Tasarısı, 5.

15 Sefer Oğuz, "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri," *Bilgi Ekonomisi ve Yönetimi Dergisi* 13, no.2 (2018): 125.

16 Harun Demirbaş, 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Kapsamında Hizmet Sağlayıcıları ve Aracı Hizmet Sağlayıcılarının Yükümlülükleri, (Ankara: Seçkin Yayıncılık, 2015), 62.

varsa bu hükümler çerçevesinde korunacaktır.[17] Yine, ölen kişinin kişisel verilerinin de KVKK kapsamında korunması söz konusu olmayacaktır.[18]

B. Kişisel Veri, Veri Sorumlusu ve Veri İşleyen Kavramları

Kişisel verilerin toplanması devlet kurumunun ortaya çıkması sonrasında başlamıştır. Devlet, güvenlik ve kamu hizmeti gibi gerekçelerle kişisel verileri toplamaya başlamıştır. Zamanla tüketim ekonomisine geçilmiş ve bu noktada şirketler de işletmenin unsurları arasında yer alan müşteri çevresi bağlamında kişisel verileri toplamaya başlamışlardır.[19]

KVKK'nın 3. maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir. Doktrinde kişinin ailesine ilişkin veriler de kişisel veri olarak kabul edilmekte ve "*bireyin şahsi, mesleki ve ailesine ilişkin özelliklerini gösteren, o bireyi diğer bireylerden ayırmayı ve niteliklerini ortaya koymayı sağlayan her türlü bilgi*" olarak tanımlanmaktadır.[20] Avrupa Birliği Direktifi m. 2'deki tanım[21] da mevzuatımızdaki tanımla örtüşmektedir.[22]

Kimliği doğrudan tanımlayan verilere "telefon numarası, yaş, IP adresi (*Internet Protocol Address*), cinsiyet" verileri, örnek

---

17 Demirbaş, "6563 Sayılı Elektronik Ticaretin", 62.

18 Yıldırım Keser, "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 28, no.3 (2020): 1184.

19 Oğuz, "Kişisel Verilerin Korunması," 122.

20 Sinan Sami Akkurt, "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış," *Kişisel Verileri Koruma Dergisi* 2, no.1 (2020): 21.

21 "Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

22 Hayrünnisa Özdemir, Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**,** **(**Ankara: Seçkin Yayıncılık, 2009), 124.

olarak verilebilir.[23] Kimliği belirlenebilir gerçek kişiye ilişkin kişisel verilere sigorta sicil numarası, vergi kimlik numarası örnek verilebilir zira bu veriler ek verilerle gerçek kişinin kimliğine ulaşmayı mümkün kılacaktır. Bu durum Kanunun gerekçesinde de ifade edilmiştir.[24]

Avrupa Adalet Divanı *Breyer v. Federal Republic of Germany* davasına ilişkin kararında[25]; kendilerine ait siteleri ziyaret edenlerin IP adreslerini, "siber saldırılara karşı korunma" gerekçesiyle depolamakta olan Alman kurumlarının işlemlerini değerlendirmiştir. Divan kararında, IP adreslerinin her ne kadar kime ait olduğu bilinmese de erişim sağlayıcılardan elde edilecek ek bilgi ile kime ait oldukları anlaşılacağından söz konusu IP adres verilerinin kimliği belirlenebilir kişiye ait kişisel veriler olduğu sonucuna varmıştır. Divana göre, ek verinin veri sorumlusunun elinde olması şart olmayıp mühim olan ek veriye ulaşılabilmesidir. Ancak ek veriye ulaşmak yasaksa ya da masraf, emek ve zaman bakımından güçlük söz konusu ise veriler belirlenebilir kabul edilmeyecektir.[26]

Gerek işlenmesi gerekse aktarımı bakımından normal verilere göre farklı koşullara tabi olan ve en önemlisi, niteliği itibariyle ayrımcılığa neden olabileceği değerlendirilen özel nitelikli kişisel veriler de KVKK kapsamında korunmaktadır.[27]

---

[23] Cengiz Paşaoğlu, "Kişisel Verilerin Korunması Kanunu Kişilerin Temel Hak ve Özgürlüklerini Korumak Amacındadır," Video, 6:02, *1.e-Safe Boğaziçi Kişisel Verileri Korumada Yerli Çözümler Zirvesi*, yükleyen: e-Safe, yükleme tarihi: Ağustos 25, 2019, erişim tarihi: Şubat 21, 2020, https://www.youtube.com/watch?v=e-M392izsks&ab_channel=e-Safe.

[24] Keser, "Tüketicinin Kişisel Verisinin," 1186.

[25] Avrupa Birliği Adalet Divanı, *Judgment of 19 October 2016, Breyer*, C-582/14, EU: C: 2016: 779, (http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2725971).

[26] Keser, "Tüketicinin Kişisel Verisinin," 1187-1188.

[27] Cengiz Paşaoğlu, "Kişisel Verilerin Korunması," 6:27.

Özel nitelikte kişisel veriler, kanunun 6. maddesinde *"kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"* olarak tanımlanmıştır.

Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GDPR) bu verilerden "Hassas Veri" şeklinde bahsedilmektedir. Hassas veriler, esas itibariyle birer kişisel veridirler. Tüzüğün 9. maddesine göre, etnik mensubiyet, sağlığa ilişkin veriler, düşünceye ilişkin veriler bu kapsamdadır. Bu verilerin açıklanması özellikle son dönemde Avrupa ülkelerinde yaşanan ırk temelli saldırılar gibi durumlar da dikkate alındığında ciddi riskler taşıyabilecektir.

İşlenen her türlü kişisel veri KVKK kapsamında değildir. İlgili düzenlemeye göre; *"tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla"* (m.3) işlenen kişisel veriler KVKK kapsamında korunmaktadır. KVKK, veri kayıt sistemini ise 3. maddesinde *"kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi"* olarak tanımlamaktadır.

KVKK kapsamında yer alan ilgili kişi dışındaki muhatap yani "veri sorumlusu" *"kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi"* (m.3) olarak tanımlanmıştır. Veri sorumlusu, aslında kişisel verilere ilişkin süreci yöneten kişidir. Burada vurgulamamız gereken nokta, kişisel veriyi işleyen kişi bir gerçek kişi ise, örneğin karşımızda bir doktor, avukat, arabulucu varsa, veri sorumlusu bu gerçek kişi olacaktır. Ancak verinin işlenmesinde karşımıza muhatap olarak bir tüzel kişi çıktığında veri sorumlusu bu tüzel kişilik olacaktır. Bu durumda, yani veri sorumlusu tüzel kişi olduğunda, veri işlemeden sorumlu gerçek kişiler veri sorumlusu olamazlar. Tüzel kişinin sorumluluğu yetkili organlarınca yerine getirilecek ancak yine bu organlar ya da

organlarda yer alan gerçek kişiler değil, tüzel kişi, veri sorumlusu olarak kabul edilecektir.[28]

Kamu kurumları söz konusu olduğunda, örneğin Adalet Bakanlığının muhatap olduğu varsayılırsa, veri sorumlusu Adalet Bakanlığı tüzel kişiliği olacaktır. Benzer şekilde, muhatap bir şirket ise veri sorumlusu bu şirketin görevlendirdiği kişi veya kişiler değil şirket tüzel kişiliği olacaktır.

KVKK kapsamında veri işleyen, "*Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi"* (KVKK m.3) şeklinde tanımlanmıştır. Veri işleyen sıfatını taşıyanlara, bulut depolama hizmeti sağlayan platformlar örnek gösterilebilir. Bu platformlar kişisel veriyi saklamakta, ancak irade veri sorumlusunda üzerinde kalmaktadır. Bulut hizmeti veren platformlar veri sorumlusunun talimatlarıyla hareket etmektedir.[29]

C. Veri Sorumlusunun Yükümlülükleri

KVKK veri sorumlusuna bazı yükümlülükler yüklemektedir. Aşağıda bu sorumluluklar irdelenecektir.

1. Genel İlkelere Uyum Sağlama

KVKK 4. maddede kişisel verilerin işlenmesinde dikkate alınması gereken genel ilkeler sayılmaktadır. Bu ilkeler: "verileri dürüstlük kurallarına ve hukuka uygun olarak işleme", "verileri güncel ve doğru şekilde tutma", "Verilerin tutulduğu amacın meşru ve aleni olması", "verilerin, işlenmelerine dayanak olan belirli amaçlar kapsamında, ölçülü ve sınırlı olarak işlenmesi", "verileri, mevzuatta öngörüldüğü süre kadar, mevzuatta bir süre öngörülmemişse işlenmelerine dayanak olan amacın

---

[28] "Kişisel Verileri Koruma Kanunu Hakkında Sıkça Sorulan Sorular," KVKK, 32-33, erişim tarihi: Şubat 13, 2020, https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular.

[29] Cengiz Paşaoğlu, "Kişisel Verilerin Korunması," 5:22.

gerçekleşmesine uygun olan süre kadar tutma" şeklinde belirlenmiştir. Bu genel ilkeler "KVKK'nın ruhu" olarak nitelendirilebilecektir.[30]

2. Kişisel Veri İşleme Şartlarına Uyum Sağlama

Kanun'un 5/1. maddesine göre kişisel veriler açık rıza ile işlenebilecektir. Aynı maddenin ikinci fıkrasında açık rıza dışında kişisel verilerin işlenebileceği istisnai durumlar belirtilmiştir. Kişisel verilerin işlenmesinde asıl olan açık rızadır. Açık rıza, KVKK'da "*belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza*" (m.3) olarak tanımlanmıştır.

Açık rızanın şekli konusunda gerek KVKK'da gerekse GDPR'de bir düzenleme bulunmadığından açık rıza yazılı veya sözlü olarak alınabilir. Hatta duruma göre ilgili kişi bir davranışı ile de açık rıza vermiş olabilir. Örneğin, "*bu odaya girdiğinizde kişisel verileriniz işlenecektir*" şeklinde bir uyarıya rağmen odaya giren kişiler, diğer koşullar da sağlanırsa açık rıza vermiş sayılabilecektir. Ancak bu çerçevede salt susmaya bir sonuç yüklenemez. Zira, GDPR çerçevesinde somut olayda ilgilinin açık rızası var diyebilmek için ilgili kişinin beyanı ya da aktif bir davranışı söz konusu olmalıdır. Yukarıdaki örnekte ilgili kişinin beyanı bulanmasa da kişisel verilerinin işleneceğini bilerek odaya girmesi ile ortaya koyduğu aktif bir davranış mevcuttur. Bundan başka, açık rızanın verinin işlenmeye başlanmasından önce alınması gerekmektedir.[31]

Açık rıza, başka bir şeyin ön koşulu olarak istenemez, yani "*bu hizmete ulaşmak istiyorsan açık rıza vereceksin*" denilemez.[32] Doktrinde yaptırımın hafif düzeyde olması halinde dahi özgür

---

30 Cengiz Paşaoğlu, "Kişisel Verilerin Korunması," 8:55.

31 "Aydınlatma Yükümlülüğü", KVKK, erişim tarihi: Kasım 17, 2019, https://www.kvkk.gov.tr/Icerik/4118/Videolar?&page=2.

32 "Açık rıza nedir," KVKK, erişim tarihi: Kasım 17, 2019, https://www.kvkk.gov.tr/Icerik/4118/Videolar?&page=2.

rızanın söz konusu olmayacağı ifade edilmiştir.[33] Bu çerçevede, çerezleri kabul etmeden sitede işlem yapılamaması nedeniyle kullanıcı çerezi kabul ediyorsa, kişisel verilerin kaydedilmesine dair açık rızasından bahsedilemeyecektir.[34] Avrupa Birliği Adalet Divanı'na göre kişinin aydınlatma metnini açtığında kişisel verilerin işlenmesine dair seçenek kutucukları hazır işaretlenmiş geliyorsa burada açık rızadan bahsedilemeyecektir.[35]

Açık rıza üç unsuru bünyesinde barındırmalıdır. Bunlar, açık rızanın; bilgilendirmeye dayanması, belirli bir konuya ilişkin olması, özgür irade ile açıklanması unsurlarıdır.[36]

Açıklanan rıza "her türlü veri işleme faaliyetine" ya da "her türlü ticari işleme ilişkin" veya bu ifadelere benzer şekilde konu sınırlandırması yapılmadan verilmişse battaniye rıza söz konusu olacaktır. Battaniye rıza açık rıza olarak kabul edilmeyecektir.[37] Avrupa Birliği'nde de bu tür rıza metinleri geçerli görülmemektedir.[38]

---

33 Keser, "Tüketicinin Kişisel Verisinin," 1201.

34 Merih Taşkaya ve Ömür Talay, "Dijital Gözetimin Pazarlama Amaçlı Aracıları: 'Çerezler' ve Çerez Kullanımında 'Açık Rıza'," *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, no. 31 (2019): 370.

35 Keser, "Tüketicinin Kişisel Verisinin," 1210.

36 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 370.

37 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 370. Belirli bir konu ile sınırlandırılmayan ve ilgili işlemle sınırlı olmayan genel nitelikteki açık rızalar "battaniye rızalar" olarak kabul edilmekte ve hukuken geçersiz sayılmaktadır. Örneğin; "her türlü ticari işlem, her türlü bankacılık işlemi ve her türlü veri işleme faaliyeti" gibi belirli bir konu ve faaliyeti işaret etmeyen rıza beyanları battaniye rıza kapsamında değerlendirilebilecek durumlardır. Bkz. "Açık Rıza Alırken Dikkat Edilecek Hususlar," KVKK, erişim tarihi: Kasım 20, 2019, https://www.kvkk.gov.tr/Icerik/2037/Acik-Riza-Alirken-Dikkat-Edilecek-Hususlar.

38 Leyla Keser, "Kişisel Veriler Kanunu'nun Getirdikleri," Video, 07:11, yükleyen: E-Ticaret ve İnternet Hukuku Derneği, yükleme tarihi: Kasım 22, 2016, erişim tarihi: Kasım 16, 2019, https://www.youtube.com/watch?v=yyMUPZSXtoY.

Şunu da vurgulayalım ki açık rıza konusunda baskı yapılmış ve şeklen açık rıza alınmış görünse de burada kesin hükümsüzlük hali söz konusu olacaktır. Benzer durum sözleşme için olduğunda, örneğin tehdit sonucu sözleşme yapılmışsa, sözleşme ancak tehdit eylemine maruz kalan tehdit ortadan kalktığında sözleşmeye onay verirse geçerli hale gelecektir. Ancak, açık rıza için sonradan verilen onama açık rızanın geçerli olmasını sağlamaz. Zira, kesin hükümsüzlükle sakat bir hukuki işlem söz konusudur.[39]

Kişisel veriler normalde veri sahibinin açık rızası olmaksızın işlenemez. Ancak bazı durumlarda kanun rıza aramamaktadır (m.5). Bunları şu şekilde özetleyebiliriz:

-kanunlarda açık hüküm bulunması hali,

-fiili imkânsızlık,

-bir akdin kurulabilmesi için gerekli olma,

-veri sorumlusunun hukuken yükümlü olduğu bir husus için gerekli olma,

-alenileştirme,

-bir hakkın kurulması, kullanılması veya muhafazası,

-veri sorumlusunun hukuka uygun, geçerli menfaatleri.

Bu durumlar söz konusu olduğunda kişinin açık rızası aranmaksızın kişisel veriler işlenebilecektir.

KVKK, açık rızanın bulunmadığı durumlarda özel nitelikte kişisel verilerin ancak "kanunlarda öngörülme" şartı ile işlenebileceğini kabul etmektedir. Buna göre, genel nitelikteki kişisel verilerin işlenme şartları arasında yer alan yukarıda sayılan haller özel nitelikli kişisel verilerin işlenmesi bakımından geçerli olmayacaktır. Özel nitelikli kişisel veriler ancak kanunlarda öngörülmüşse açık rıza olmaksızın işlenebilecektir (KVKK m.6).

---

39 Keser, "Tüketicinin Kişisel Verisinin," 1201.

Kanun özel nitelikli kişisel veriler içerisinde sağlık ve cinsel hayat ile ilgili verileri bir derece daha önemli saymıştır. Söz konusu veriler, ilgilinin açık rızası aranmaksızın *"ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar"* tarafından işlenebilecektir (KVKK m.6).

3. Silme, Yok Etme, Anonim Hale Getirme

Veri sorumlusu, işlenmiş olan kişisel verilerin, işlenmelerini gerektiren sebeplerin ortadan kalkması hâlinde söz konusu verileri silmeli, yok etmeli veya anonim hâle getirmelidir. Bu konudaki işlemler "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik[40]" çerçevesinde yapılacaktır (KVKK m.7).

4. Aktarım Usul ve Esaslarına Uyum Sağlama

Kişisel veriler bazı durumlarda veri sorumlusu dışında başka gerçek veya tüzel kişilere aktarılabilmektedir. Bazen bir şirket içinde yürütülmekte olan ya da ilk defa yapılacak bir iş, dışarıdan bir firmadan alınabilir. Buna dış kaynak alımı denir ve genellikle muhasebe, insan kaynakları, çağrı merkezi hizmetleri gibi konularda dış kaynak alımına gidilmektedir.[41] Örneğin, bir şirketin muhasebe işlemleri hizmet alımı yoluyla dışarıdan bir muhasebe firması tarafından yapılıyorsa maaşların hesaplanması, vergilerin ödenmesi gibi nedenlerle şirket tarafından tutulan kişisel verilerin muhasebe işlerini yapmak üzere anlaşılan firmaya aktarılması gerekebilecektir. Aktarım söz konusu olduğunda kanun genel prensip olarak yine açık rızayı aramakta, açık rızanın aranmayacağı halleri ise

---

40 RG. 28.10.2017, S. 30224.

41 Nilgün Başalp, "Bilgi Teknolojileri Dış Kaynak Alımında (Outsourcing) Kişisel Verilerin Korunması ve Gizlilik Sözleşmeleri," (Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2013), 3-4.

saymaktadır. Buna göre, normal nitelikteki kişisel veriler için işleme şartları neyse aktarım şartları da aynıdır. Özel nitelikte kişisel veriler için de benzer şekilde işleme şartları aktarım için de gerekli olmakla beraber Kanun bu durumda ilaveten yeterli tedbirlerin alınmasını da şart koşmaktadır (KVKK m.8).

Eğer aktarım yapılacak birim yurtdışında ise aktarım yapılacak ülkede yeterli korumanın bulunması gerekmektedir. Yeterli korumanın bulunduğunu belirleme yetkisi Kişisel Verileri Koruma Kurulu'ndadır. Kurul, şu an için yeterli korumanın bulunduğu ülkelere ilişkin bir liste yayımlamamıştır. Dolayısıyla şu anda hiçbir ülke için yeterli korumanın bulunduğunu söylemek mümkün değildir. Ancak Kanun ikinci bir alternatif yol sunmaktadır. Buna göre, veri sorumluları yeterli korumayı sağlayacaklarını yazılı şekilde taahhüt ederler ve Kurul da aktarıma izin verirse, yurt dışına veri aktarımı mümkün olabilecektir (KVKK m.9/2-b). Dolayısıyla yurtdışına veri aktarımı söz konusu olduğunda Kurul, yeterli korumanın bulunduğu ülkelere ilişkin bir liste yayınlayıncaya kadar zikredilen alternatif yol kullanılabilecektir.

5. Aydınlatma

Veri sorumlusunun bir diğer yükümlülüğü, verisi işlenen ilgili kişiyi aydınlatmaktır. Bu yükümlülük kapsamında ilgili kişiye aşağıdaki konularda bilgi verilmesi gerekmektedir (KVKK m.10):

-veri sorumlusunun kimliği (varsa temsilcisinin de kimliği),

-kişisel verinin işlenme amacı,

-verinin hangi amaçlarla kimlere aktarılabileceği,

-kişisel verinin toplanmasına dayanak oluşturan hukuki sebep ya da sebepler,

-kişisel veri toplanmasında uygulanacak yöntem,

-ilgili kişinin KVKK m. 11'de sayılan diğer hakları.

Aydınlatma yükümlülüğünün yerine getirildiğini ispat etme yükümlülüğü veri sorumlusuna ait olacaktır. Ayrıca işleme şartlarında bir değişiklik meydana gelirse değişiklik hakkında da aydınlatma yükümlülüğünün yerine getirilmesi gerekecektir. Aydınlatma yükümlülüğü, Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ'in[42] 5. maddesine göre yazılı ya da sözlü olarak yapılabilecektir.[43]

6. Veri Güvenliğini Sağlama

Veri güvenliği sağlanamadığı takdirde bazen bireysel mahremiyet ihlalleri ortaya çıkabileceği gibi bazen de kitleleri, toplumları tehdit edebilecek boyutlarda sorunlar ortaya çıkabilecektir. Bu kapsamda veri güvenliğinin sağlanması konumuz bağlamında en önemli hususlardan biridir.

Bu çerçevede veri sorumlusunun öncelikle çalışanlarının kötü niyetle hareket etme ihtimalini göz önüne alması ve çalışanlarını seçerken titiz davranması, gerekli denetimleri yapması gereklidir.[44] Veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesi ve bu verilere hukuka aykırı olarak erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamakla yükümlüdür. Ayrıca, muhafaza yükümlülüğü kapsamında uygun güvenlik tedbirleri bağlamında gerek idari yönden gerekse teknik yönden her türlü önlemi almak zorundadır. Eğer kişisel veriler veri sorumlusu adına başka bir kişi tarafından işleniyorsa veri sorumlusu bahsi geçen kişi ile birlikte ortak sorumluluk altında olacaktır (KVKK m.12).

7. Sicile Kayıt

KVKK veri sorumlularına ilişkin bir sicil sisteminin kurulmasını öngörmüştür. Kişisel Verileri Koruma Kurumu tarafından bu sistem dijital ortamda oluşturulmuş

---

42 RG. 10.03.2018, S. 30356.

43 Keser, "Tüketicinin Kişisel Verisinin," 1194.

44 Oğuz, "Kişisel Verilerin Korunması," 125.

bulunmaktadır. Bu sistem, kişisel verileri işleyen gerçek ve tüzel kişilerin, kişisel veri işlemeye başlamadan önce kaydolmaları gereken ve işlemekte oldukları kişisel verilerle ilgili kategorik bazda bilgi girişi yapmaları talep edilen bir kayıt sistemidir. Kısa adı "VERBİS" olan bu sisteme kayıtlar başlamıştır. Bu sistem şeffaflık ve hesap verebilirlik prensipleri gereğince kamuya açık olarak tutulmaktadır. Sistemde isteyen kişiler sorgulama yapabilmektedir.

VERBİS kapsamında, söz konusu şirkete ilişkin; işlenen kişisel veri kategorilerinin, kişisel verilerin işlenme amaçlarının, veri sorumlusunun kişisel verileri aktaracağı alıcıların, kişisel verilerin saklama sürelerinin, kişisel verileri işlenen kişi gruplarının, kişisel verilerin yabancı ülkelere aktarım durumlarının, kişisel verilerin korunması için alınan güvenlik tedbirlerinin, ilgili veri sorumluları tarafından kategorik temelde sisteme işlendiği görülmektedir.[45]

Kanunun 16. maddesinin 2. fıkrası Kurul'a bazı veri sorumlularını VERBİS'e kayıt sorumluluğu yönünden istisna tutma yetkisi tanımıştır. Kurul da bu yetki çerçevesinde şimdiye

[45] VERBİS'e kayıt için zorunlu tarihler daha önce ertelenmiş ve son olarak Kişisel Verileri Koruma Kurulunun 11/03/2021 tarihli ve 2021/238 sayılı Kararı ile; yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den çok olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine, yıllık çalışan sayısı 50'den az ve yıllık mali bilançosu 25 milyon TL' den az olup ana faaliyet konusu özel nitelikli kişisel veri işleme olan gerçek ve tüzel kişi veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine, Kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşu veri sorumlularının Sicile kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2021 tarihine kadar uzatılmasına karar verilmiştir. Bkz. RG. 16.03.2021, S. 31425.

kadar çeşitli istisnalar belirlemiştir.[46] Bu istisnalar, herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler, noterler, dernekler, vakıflar ve sendikalar (yalnızca ilgili mevzuat ve amaçlarına uygun, faaliyet alanlarıyla sınırlı ve sadece kendi çalışanlarına, üyelerine, mensuplarına ve bağışçılarına yönelik olarak tuttukları kişisel veriler yönünden), siyasi partiler, avukatlar, gümrük müşavirleri, arabulucular, serbest muhasebeci mali müşavirler ve yeminli mali müşavirler, yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25 milyon TL'den az olan gerçek veya tüzel kişi veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar şeklinde sıralanabilecektir. Burada belirlenen istisnaların kanundan değil sadece VERBİS'e kayıt zorunluluğundan istisna olduğunu vurgulamak gerekmektedir.

D. İlgili Kişinin Hakları

KVKK'nın 11. Maddesine göre ilgili kişinin hakları şunlardır:

-kişisel verilerinin işlenme durumunu (işlenip işlenmediğini) öğrenme,

-işlenen kişisel verileri hakkında bilgi isteme,

-kişisel verilerinin hangi amaçla işlendiğini öğrenme,

-kişisel verilerinin işlendiği amaca uygun olarak kullanılıp kullanılmadığını öğrenme,

-kişisel verilerinin aktarıldığı kişileri öğrenme,

-eksik veya yanlış işlenen kişisel verilerinin düzeltilmesini isteme,

---

[46] Kişisel Verileri Koruma Kurulunun 2018/32 Sayılı Kararı için bkz. RG. 15.05.2018, S. 30422; Kişisel Verileri Koruma Kurulunun 2018/68, 2018/75 ve 2018/87 Sayılı Kararları için bkz. RG. 18.08.2018, S. 30513.

-şartları oluşmuşsa (KVKK m. 7) kişisel verilerinin yok edilmesini veya silinmesini isteme,

-düzeltilen, silinen veya yok edilen kişisel verilerinin, daha önce kendilerine aktarım yapılanlara bildirilmesini isteme,

-işlenen kişisel verilerinin sistematik olarak (münhasıran otomatik sistemler aracılığıyla) analiz edilerek kendisi aleyhine bir durumun ortaya çıkartılmasına itiraz etme,

-kanuna aykırı olarak işlenen kişisel verileri nedeniyle zarar görmüşse bu zararın tazminini isteme.

İlgili kişi zikredilen haklarını veri sorumlusuna başvurarak kullanabilir. Bu müracaat Kurum'un yayımladığı "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"[47] çerçevesinde yapılmalıdır.

E. Kişisel Verileri Korumu Kurumu ve Kurulu

KVKK ile "Kişisel Verileri Koruma Kurumu" kurulmuş ve bu Kurumun karar organı olarak "Kişisel Verileri Koruma Kurulu" belirlenmiştir. Bu adım kişisel verilerin korunması anlamında çok önemlidir. Temel haklar anlamında önemli bir hak olarak gelişmekte olan kişisel verilerin korunması hakkı sadece yasa ile belirtilip, yasanın uygulanmasını sağlayacak bir kurum bulunmasaydı, yasada belirtilen hususların tatbikinin takip edilmesi mümkün olmayabilirdi. Bu konudaki endişemizin temel nedeni bugün için söz konusu hak konusunda bireylerin ve kurumların farkındalığının yeterli düzeyde olmamasıdır.

Kişisel Verileri Koruma Kurumu önce Başbakanlığa bağlı olarak kurulmuş daha sonra 2018/1 sayılı Cumhurbaşkanlığı Genelgesi[48] ile Adalet Bakanlığına bağlı hale gelmiştir. Ancak, bu durum Avrupa Veri Koruma Tüzüğü'ne aykırılık

47 RG. 10.03.2018, S. 30356.

48 RG. 02.08.2018, S. 30497.

oluşturmaktadır. Zira, bu tüzüğe göre bir denetim kurumu olan Kişisel Verileri Koruma Kurumu bağımsız olmalıdır.[49]

Kurul, 9 üyeden oluşmaktadır ve üyelerin dördünü Cumhurbaşkanı, beşini Türkiye Büyük Millet Meclisi seçmektedir. Kurulun bağımsız ve tarafsız hareket edebilmesi için bazı hükümler tesis edilmiştir. Anayasada mahkemelerin bağımsızlığını düzenleyen 138. maddede yer alan hükümlerin kurul için de tekrar edilmiş olması; kurul üyelerinin görevleri dışında başka görev almamaları ve kazanç getirici faaliyette bulunamamaları; görevden alınamamaları, kurula tüzel kişilik verilerek mali ve idari yönden rahat hareket edeceği bir teşkilatlanmanın öngörülmesi bu kapsamdaki düzenlemelerdir. Kurula üye olabilmek için; siyasi parti üyesi olmamak, devlet memurluğuna ilişkin bazı nitelikleri taşımak, dört yıllık lisans düzeyinde yükseköğrenim almış olmak gibi şartlar aranmaktadır (KVKK m.21).

F. Suçlar ve Kabahatler

KVKK'nın 17. maddesinde suçlar düzenlenmiş ve 5237 sayılı Türk Ceza Kanunu'na atıfta bulunulmuştur. KVKK'nın 18. maddesinde ise kabahatler düzenlenmiştir. Kabahatler bağlamında yaptırım olarak özel kişiler yönünden (gerçek kişi ya da tüzel kişi) para cezaları, kamu görevlileri yönünden ise disiplin hükümleri öngörülmüştür.[50] Bu konuya ilişkin detaylı açıklamalar üçüncü bölümde ilgili başlık altında yapılacaktır.

G. Kişisel Verilerin Korunmasının Hukuki Niteliği

Anglo-Amerikan Hukukunda (*common law*) kişisel verilerin "fikri hak" ve/veya "mülkiyet hakkı" bağlamında değerlendirmesi söz konusudur. Kıta Avrupası hukukunda ise

---

49 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 373.

50 "Kişisel Verileri Koruma Kanununa İlişkin Uygulama Rehberi," KVKK, 118, erişim tarihi: Şubat 19, 2020, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF.

kişisel verilerin korunmasının "temel insan hakları" ve/veya "kişilik hakkı" çerçevesinde değerlendirilmesi gerektiği görüşü hâkimdir.[51] Kişisel verilerin korunması konusunda ABD ve AB arasındaki görüş farklılığının ABD'deki siyasi kültür nazara alındığında kamu otoritelerinin AB ülkelerine oranla sermaye şirketlerinin oluşturduğu lobilere daha fazla bağımlı olmalarından kaynaklandığı söylenebilir.[52]

"Mülkiyet hakkı" ve "fikri hak" ve görüşleri, "ekonomik hak yaklaşımı" çatısı altında birleştirilebilir.[53] Mülkiyet hakkı, sahibine; kullanma, yararlanma ve tasarruf yetkileri vermektedir. Kişisel veriler mülkiyet hakkı kapsamında değerlendirildiğinde veri sahibinin tüm bu hakları devredebilmesi gerekir. Bununla birlikte, kişinin dini inancına veya biyometrik özelliklerine ilişkin verileri gibi birçok kişisel verisi bakımından mülkiyet hakkını devredebilme imkânı yoktur. Öte yandan, fikri mülkiyet hukukunun temel amacı fikri üretimi korumaktır. Veri koruma hukukunda ise böyle bir amaç bulunmamaktadır. Kişisel verilerin ekonomik hak yaklaşımı kapsamında değerlendirilmesi açıklanan bu nedenlerle eleştirilmektedir.[54]

AİHS'de kişisel verilerin korunmasına ilişkin müstakil bir düzenleme bulunmamakta olup AİHM, kişisel verilerin korunmasını Sözleşme'nin 8. maddesinde düzenlenen "Özel Hayata ve Aile Hayatına Saygı Hakkı" bağlamında değerlendirmektedir.[55] Yargıtay Hukuk Genel Kurulu da kişisel verilerin korunmasını AİHM ile benzer şekilde

51 Akkurt, "Kişisel Veri Kavramının," 22.

52 Karlıdağ, "Ekonomi Politik Açıdan," 139.

53 Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, (İstanbul: On İki Levha Yayınları, 2017), 54.

54 Akkurt, "Kişisel Veri Kavramının," 23-24.

55 Küzeci, "Anayasal Bir Hak," 148.

değerlendirmektedir.[56] Kişisel verilerin temel haklar arasında değerlendirilmesini savunanlar için bu değerlendirme tarzı önemlidir.

Kişisel verilerin kişilik hakkı bağlamında değerlendirilmesi gerektiğini savunanlar bakımından ise kişisel verilerin korunması bir temel insan hakkı olarak nitelendirildiğinde dahi dayanak prensip "özel hayatın gizliliği ilkesi" olup bu ilke de kişilik hakkı kapsamında yer alan değerlerdendir.[57]

II. ELEKTRONİK TİCARET VE ELEKTRONİK SÖZLEŞMELER

Dünya Ticaret Örgütü elektronik ticareti, "mal ve hizmetlerin üretim, reklam, satış ve dağıtımlarının telekomünikasyon ağları üzerinden yapılması"; OECD ise "sayısallaştırılmış yazılı metin, ses ve görüntünün işlenmesi ve iletilmesine dayanan kişileri ve kurumları ilgilendiren tüm ticari işlemler" olarak tanımlamaktadır.[58] Elektronik ticaret geniş anlamıyla "sipariş alıp vermek için tasarlanmış elektronik ortamlarda, bilgisayar ağları üzerinden yürütülen mal/hizmet alışverişi" şeklinde de tanımlanabilir.[59]

6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un[60] (ETDHK) 2-a maddesinde elektronik ticaret "fiziki olarak karşı karşıya gelmeksizin, elektronik ortamda gerçekleştirilen çevrim içi iktisadi ve ticari her türlü faaliyet" şeklinde tanımlanmaktadır. Kanun'da elektronik ortam ibaresi

---

56 Murat Ketizmen ve Aslıhan Kart, "Kişisel Veri ve Rekabet Hukuku Kapsamında 'Big Data'", *Kişisel Verileri Koruma Dergisi* 1, no.1 (2019): 65; Yar. HGK, E.2014/56, K.2015/1679, 17.06.2015, (Yargıtay Karar Arama).

57 Akkurt, "Kişisel Veri Kavramının," 26.

58 Halil Elibol ve Burcu Kesici, "Çağdaş İşletmecilik Açısından Elektronik Ticaret," *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, no. 11 (2014): 306.

59 Engin Yılmaz ve İbrahim Sarper Karakadılar, "Türkiye'deki Elektronik Ticaret Uygulamalarına Müşteri Gözenden Bakış ve İyileştirme Önerileri," *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi* 6, no. 1 (2019): 54.

60 RG. 23.10.2014, S. 29166.

tanımlanmamıştır. Ancak, Kanun'un 2-c maddesinde ticari elektronik iletinin "*telefon, çağrı merkezleri, faks, otomatik arama makineleri, akıllı ses kaydedici sistemler, elektronik posta, kısa mesaj hizmeti gibi vasıtalar kullanılarak elektronik ortamda gerçekleştirilen ve ticari amaçlarla gönderilen veri, ses ve görüntü içerikli iletileri*" şeklinde tanımlanması ve bu tanımda yer alan "*…gibi*" ifadesi dikkate alındığında elektronik ortamın oldukça geniş olarak değerlendirileceği anlaşılmaktadır.[61]

Elektronik ticaret, internet aracılığıyla şirketlere küçük bütçelerle küresel ölçekte iş yapabilme ve dünyaya açılma imkânları sunmaktadır.[62] Böylece, küçük ve orta ölçekli işletmeler rekabet ortamına girebilme imkânı elde ettiğinden fırsat eşitliğine zemin hazırlanmaktadır.[63] Yine elektronik ticaret vasıtasıyla müşteriler daha az para ve emek harcayarak profesyonel satış görevlilerinin baskısı altında kalmadan ihtiyaçlarına uygun alışveriş yapma fırsatı elde etmekte[64] ve bulundukları yerden, gerektiğinde coğrafi sınırları aşarak ihtiyaçlarını karşılayabilmektedirler.[65] Elektronik ticaret son yıllarda ciddi bir potansiyele ulaşmış durumdadır. Özellikle Covid-19 salgını sürecinde yüz yüze temasın minimum düzeye inmesi elektronik ticarette de ciddi bir artışa neden olmuştur.[66]

---

61 Esra Hamamcıoğlu, "Elektronik Ticaretin Hukuksal Boyutu," *Kocaeli Üniversitesi Sosyal Bilimler Dergisi*, no. 35 (2018): 48.

62 Elibol ve Kesici, "Çağdaş İşletmecilik Açısından," 304.

63 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 44.

64 Yılmaz ve Karakadılar, "Türkiye'deki Elektronik Ticaret," 57.

65 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 44.

66 İsmet Kahraman Arslan ve Neslihan Öz, "Elektronik Ticaret Sözleşmelerine Uygulanacak Hukuk," *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi* 19, no. 38 (2020): 14; Ticaret Bakanlığının verilerine göre Türkiye'nin elektronik ticaret hacmi 2019'da 136 Milyar TL olarak gerçekleşmişken 2020'de elektronik ticaret hacmi 226,2 Milyar TL'ye ulaşmıştır. Bkz. "İstatistikler," Ticaret Bakanlığı, erişim tarihi: Nisan 30, 2021, https://www.eticaret.gov.tr/istatistikler.

Elektronik ticaret; işletmeler arasında, işletme-tüketici arasında, tüketici-tüketici arasında olabileceği gibi idare-işletme arasında ve idare-tüketici arasında da gerçekleşebilir.[67] Elektronik ticaret ile elektronik sözleşmeler zaman zaman birbirinin yerine geçecek şekilde kullanılsa da elektronik ticaret, elektronik sözleşmeleri de içine alan ve elektronik ortamda gerçekleştirilen ticari faaliyetleri ve hukuki işlemleri kapsayan daha geniş bir anlama sahiptir.[68]

Elektronik ticaret kapsamında elektronik sözleşmelere değinilecek olursa yeni bir sözleşme türünden bahsedilmiş olmayacaktır. Zira, yazılı sözleşmeler ile elektronik sözleşmeler arasındaki temel fark elektronik sözleşmelerin elektronik ortamda kurulmasıdır.[69] Elektronik sözleşmeler, internet araçlarının kullanılması suretiyle internet üzerinden gerçekleşen iletişim esnasında kurulmuş olmaktadır.[70] Elektronik sözleşmelerde taraflar iradelerini sayısallaştırılmış biçimde karşı tarafa bildirmektedir. Bu aşamada sayısallaştırılan unsurlar ses, yazı veya görüntü olabilir.[71]

Elektronik sözleşmeden bahsedebilmek için karşılıklı iradelerin elektronik ortamda aktarılması şarttır. Taraflardan biri elektronik ortamda iradesini bildirirken diğeri fiziki ortamda cevap verirse elektronik sözleşme söz konusu olmayacaktır.[72] Elektronik sözleşmelerin kuruluş ve ifasında elektronik araçlarla kurulmaları dışında normal sözleşmelerden

---

67 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 45.

68 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 49.

69 Semiha Önder Balaban, " Milletlerarası Özel Hukukta Elektronik Sözleşmeler", (Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2016,) 49.

70 İpek Sağlam Atabarut, "Elektronik Sözleşmeler," (Doktora Tezi, Marmara Üniversitesi, 2003), 49.

71 Sinan Sami Akkurt, "Elektronik Ortamda Hizmet Sunumu ve Buna İlişkin Sözleşmelerin Hukuki Niteliği," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 60, no. 1 (2011): 26.

72 Balaban, "Milletlerarası Özel Hukukta," 28.

ayrılan bir yönleri bulunmadığından Borçlar Hukukundaki genel düzenlemeler elektronik sözleşmeler için de geçerli olacaktır.[73] Bu nedenle, yeni borçlar kanunu 2012 yılında yürürlüğe girmesine rağmen; bu Kanun'da elektronik sözleşmelerle ilgili özel hükümlere yer verilmemiş ve elektronik sözleşmelere ilişkin hükümler ETDHK'da yer almıştır.[74]

Elektronik sözleşmeleri taraflarına göre, tüketici-kamu, tüketici-özel sektör, kamu-özel sektör, özel sektör-özel sektör şeklinde dört türe ayırmak mümkündür.[75] Yine, ticarete konu ürünlerin niteliği bakamından da elektronik sözleşmeler ikiye ayırılabilecektir. Sözleşme elektronik araçlarla kurulup teslimat fiziki olarak yapılırsa dolaylı (*offline*) elektronik sözleşme söz konusu olacaktır. Hem sözleşme hem de teslimat elektronik araçlarla gerçekleştiriliyorsa doğrudan (*online*) elektronik sözleşme kurulmuş olacaktır.[76] Örneğin, internetten alınan müzik CD'sinin kargoyla gönderilmesinde akdedilen sözleşme dolaylı elektronik sözleşme olarak nitelendirilecekken internetten satın alınan yazılımın yine internet üzerinden bilgisayara yüklenmesi durumunda akdedilen sözleşme doğrudan elektronik sözleşme olacaktır. Ayrıca, uçak biletinin internet üzerinden alınmasında olduğu gibi hizmet sunumuna ilişkin elektronik sözleşmeler de bulunmaktadır.[77]

Elektronik ticarete ilişkin en önemli uluslararası düzenlemeler, Avrupa Birliği'nin 8 Haziran 2000 tarihli, 2000/31/EG Bilgi Toplumu Hizmetlerinin, Özellikle Elektronik

---

[73] Gamze Turan, "Elektronik Sözleşmeler ve Elektronik Sözleşmelere Uygulanacak Hukukun Tespiti," *Türkiye Barolar Birliği Dergisi* 21, no. 77 (2008): 92.

[74] Balaban, "Milletlerarası Özel Hukukta," 27.

[75] Elibol ve Kesici, "Çağdaş İşletmecilik Açısından," 316.

[76] Ümit Gezder, "Elektronik Ticaret Hukuki İşlemlerinin Ayrımı-Dijital İçerik ve Hukuki Niteliği," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 22, no. 3 (2016): 1124.

[77] Arslan ve Öz, "Elektronik Ticaret Sözleşmelerine," 18.

Ticaretin Ortak Pazardaki Bazı Yönleri Hakkında Direktifi[78] ile 2002/58/EC sayılı Elektronik İletişimde Kişisel Verilerin İzlenmesi ve Gizliliğinin Korunması Direktifi[79] olarak söylenebilecektir.

Ulusal düzenlemelerin başında 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun[80] ve bu kanuna dayanarak çıkartılan "Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcıları Hakkında Yönetmelik[81]" ile Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik[82] gösterilebilecektir. Ayrıca, 6502 sayılı Tüketicinin Korunması Hakkında Kanun[83] (TKHK) ve bu kanunun 48 ve 84. maddelerine dayanarak çıkartılan "Mesafeli Sözleşmeler Yönetmeliği[84]" elektronik ticaret alanında uygulama bulmaktadır. Bunlardan başka, 5070 sayılı Elektronik İmza Kanunu, 6340 Sayılı Ödeme ve Menkul Kıymet Mutabakat

78 "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market," EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=DE.

79 "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," EUR-Lex, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

80 Kanunun gerekçesinde kanunun amaçlarından birisinin mevzuatımızla yukarıda zikredilen 2000/31/EG sayılı Direktif arasındaki uyumun sağlanması olduğu belirtilmektedir. Bkz. Türkiye Büyük Millet Meclisi, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı ile Avrupa Birliği Uyum Komisyonu, Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonu ile Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu Raporları, (Ankara: TBMM, 2011,) 6, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss240.pdf.

81 RG. 26.08.2015, S. 29457.

82 RG. 15.07.2015, S. 29417.

83 RG. 07.11.2013, S. 28835.

84 RG. 27.11.2014, S. 29188.

Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun[85] ve 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu[86] elektronik ticaret alanında tatbik edilmektedir. Elektronik ticaretin birçok hukuk dalıyla ilgili olması sebebiyle anılan düzenlemelerin yanı sıra fikri mülkiyet hukuku, bankacılık hukuku, ticaret hukuku, vergi hukuku, ceza hukuku ve tüketici hukuku gibi birçok hukuk dalındaki düzenlemelerin devreye girmesi söz konusu olabilecektir.[87]

III. ELEKTRONİK TİCARETTE KİŞİSEL VERİLERİN KORUNMASI

Türkiye'nin mevcut iş miktarına nazaran elektronik ticaret işlemlerinin Türkiye'deki yoğunluğu benzer ülkelere göre istenilen seviyede olmayıp bu durum müşterilerin elektronik ticarete ilişkin algılarından kaynaklanmaktadır. Elektronik ticarette müşterilerin en büyük korkusu güvenliğe ilişkindir. Bu noktada bireysel çözümlerden ziyade makro düzeyde kamu otoritelerince atılacak adımlarla sektörün bir bütün olarak alacağı tedbirler son derece önemlidir.[88] Güven sorunu müşteriler için olduğu gibi kimi zaman işletmeler bakımından da gündeme gelebilmektedir.[89] Güven sorunu kapsamında en önemli konu kişisel verilerin korunması konusudur.

İnternetin ilk ortaya çıktığı zamanlarda kişiler, sadece internet üzerinden kendilerine sunulan bilgiye ulaşırken zamanla dijital gözetim kavramı ortaya çıkmış ve aynı kişiler içerik üretir hale gelmişlerdir. Ekonomik ve politik iktidarlar dijital gözetim ile elde ettikleri verileri kendi iktidarları için kullanmakta ve bu kapsamda kişilerin mahremiyetinin ihlali söz konusu olmaktadır.[90] Dijital gözetim kavramı "*belirli grupların*

85 RG. 20.06.2013, S. 28690.

86 RG. 23.02.2006, S. 26095.

87 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 46.

88 Yılmaz ve Karakadılar, "Türkiye'deki Elektronik Ticaret," 53-54.

89 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 44.

90 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 372.

diğer gruplar üzerinde davranış kontrolü sağlamak amacıyla veri toplama, depolama, analiz etme, değerlendirme ve amaca uygun biçimde kullanma, bunu yaparken de potansiyel olarak fiziksel, ideolojik ve/veya yapısal şiddetten kaçınmaksızın, insanları belirli davranışlara yöneltme süreci" olarak tanımlanmaktadır. [91]

OECD Genel Sekreteri Angel Gurria internet ekonomisinin geleceği üzerine adlı bir toplantıda kişisel verileri para birimi olarak lanse etmiştir.[92] Türkçe karşılığı büyük veri olan, *Big Data* ile toplanan devasa boyutta kişisel veriler çeşitli algoritmalar ile analiz edilmekte ve şirketler için piyasayı yönetmeye dair çok önemli araçlara dönüşmektedir.[93] Öte yandan, kredi kartı veya internet bankacılığı bilgileri gibi kişisel verilerin ele geçirilmesi sonrasında da birçok suç işlenmektedir.[94]

Bu bölümde elektronik ticaret özelinde kişisel verilerin korunmasına ilişkin düzenlemelere, geliştirilen sistemlere ve kişisel veriler korunmadığı takdirde karşılaşılacak yaptırımlara değinilecektir.

A. Genel Düzenlemeler

2014 yılında yürürlüğe giren 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'da kişisel verilen korunması hususu açıkça düzenlenmiştir. ETDHK m. 10 hükmü çerçevesinde hizmet sağlayıcı veya aracı hizmet sağlayıcılar, kişisel verileri korumak için gerekli önlemleri alacaktır. İlgili kişinin rızası olmaksızın kişisel verilerin aktarılması ya da başka bir gaye ile kullanılması da söz konusu olamaz.[95]

---

91 Mukadder Çakır, *İnternette Gösteri ve Gözetim Eleştirel Bir Okuma*, (Ankara: Ütopya Yayınevi, 2015,) Aktaran: Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 359.

92 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 362.

93 Ketizmen ve Kart, "Kişisel Veri ve Rekabet," 66.

94 Oğuz, "Kişisel Verilerin Korunması," 124.

95 Ferman Kaya, *E-Ticaret Hukuku ve Tüketici Hukukundaki Yansımaları*, (Ankara: Seçkin Yayıncılık, 2018), 127.

ETHDK'nın 2. maddesinde; hizmet sağlayıcı, *"elektronik ticaret faaliyetinde bulunan gerçek ya da tüzel kişiler"* aracı hizmet sağlayıcı ise *"başkalarına ait iktisadi ve ticari faaliyetlerin yapılmasına elektronik ticaret ortamını sağlayan gerçek ve tüzel kişiler"* olarak tanımlanmıştır. Örneğin, n11 isimli sanal pazar sitesi aracı hizmet sağlayıcıyken bu site üzerinden satış yapan bir firma da hizmet sağlayıcı konumunda olacaktır.

ETHDK m. 10 ile getirilen sorumluluğun ana hedefinin elektronik ticarete olan güvenin tesis edilmesi olduğu belirtilmektedir.[96] ETHDK m. 10 kapsamında kişisel verileri korunacak kişinin, hizmet sağlayıcı ve aracı hizmet sağlayıcılar ile arasında bir sözleşme ilişkisinin bulunması şart değildir. Alıcıların ya da herhangi bir şekilde elektronik ortama kişisel verisi girilmiş olan herkesin kişisel verilerinin korunması söz konusu olacaktır.[97] Genel olarak ETHDK'daki hükümlere aykırı hareket edilmesi halinde uygulanacak yaptırımlar da kanunda düzenlenmiştir. Ancak, 10. maddeye aykırı hareket edilmesi herhangi bir yaptırıma bağlanmamıştır. 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu'nda öngörülen yaptırımların uygun olduğu ölçüde 10. madde bağlamında da uygulanması söz konusu olacaktır.

Kişisel verilerin korunması alanında önemli bir düzenleme de Ticaret Bakanlığınca hazırlanan Elektronik Ticarette Hizmet Sağlayıcı ve Aracı Hizmet Sağlayıcılar Hakkında Yönetmelik'tir[98]. Yönetmeliğin Kişisel "Verilerin Korunması" başlıklı 10. Maddesi aşağıdaki şekildedir:

"(1) Hizmet sağlayıcı ve aracı hizmet sağlayıcı, bu Yönetmelik çerçevesinde yaptığı işlemler ve sunduğu hizmetler nedeniyle elde ettiği kişisel verilerin, 23.2.2006 tarihli ve 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu ve diğer ilgili mevzuat hükümleri saklı kalmak

96 TBMM, Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı, 11.

97 Demirbaş, "6563 Sayılı Elektronik Ticaretin," 64.

98 RG. 26.08.2015, S. 29457.

kaydıyla muhafazasından ve hukuka aykırı olarak bunlara erişilmesini ve işlenmesini önlemek amacıyla gerekli tedbirlerin alınmasından sorumludur.

(2) Kişisel veriler, ilgili kişinin açık irade beyanını içerecek şekilde önceden alınan onayı olmaksızın üçüncü kişilerle paylaşılamaz, işlenemez ve başka amaçlarla kullanılamaz."

"Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik[99]" de erişim sağlayıcılara kişisel verilerin korunması ile ilgili yükümlülükler vermiştir(m. 15/2). Dolayısıyla, hizmet sağlayıcı ve aracı hizmet sağlayıcılarla benzer şekilde erişim sağlayıcıların da kişisel verilerin korunması konusunda sorumluluğu söz konusu olacaktır.[100]

ETDHK'da hizmet sağlayıcı ve aracı hizmet sağlayıcıların elektronik ticaret kapsamında alıcılardan hangi bilgileri isteyebilecekleri belirtilmemiştir. Bu hususa ilişkin düzenlemeler KVKK'da yer almaktadır. Açık rıza, kişisel verinin işlenmesi için en temel şarttır. Ayrıca istisnalar arasında sayılan "bir sözleşmenin kurulması veya ifası için gerekli olma" durumu da elektronik ticaret için önemli bir kişisel veri işleme gerekçesi oluşturacaktır.

Elektronik işlemlerde kişisel verileri üçe ayırmak mümkündür. Birinci sırada yer alan "sözleşmenin kurulması için gerekli temel veriler"e telefon numarası, e posta adresi, ilgilinin adı-soyadı gibi bilgiler örnek oluşturacaktır. İkincisi, malın niteliklerini ya da hizmetin özellikleri gösteren, "içerik verileri"dir. Üçüncüsü ise kullanıcıların internette yaptığı gezintilere ilişkin *log* kaydı, şifre gibi unsurlardan oluşan "bağlantı verileri"dir.[101]

---

99 RG. 24.10.2007, S. 26680.

100 Demirbaş, "6563 Sayılı Elektronik Ticaretin," 63.

101 Demirbaş, "6563 Sayılı Elektronik Ticaretin," 66-68.

B. Ödeme Verilerine İlişkin Özel Düzenleme

Elektronik ticarette, bir taraftan mal ve hizmetin internet ortamında satılması söz konusu olurken, diğer taraftan mal ve hizmetin bedelinin de internet üzerinden ödenmesi söz konu olmaktadır. Kredi kartı, banka kartı ve hesap bilgileri ödeme bilgileridir. Ödeme bilgileri de kişisel verilerin korunması kapsamına giren verilerdendir. Bu verilere ilişkin genel korumanın yanı sıra 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nda da özel düzenleme bulunmaktadır.[102]

5464 sayılı Kanun'un "Bilgilerin Saklanması" başlıklı 23. maddesinde ödeme bilgilerinin, üye işyerlerince, bilgi sahiplerinin yazılı rızası dışında paylaşılma yasağından bahsedildikten sonra söz konusu bilgilerin korunması konusunda üye iş yerleri ile anlaşma yapan bankalar ile sair kuruluşlara gözetim yükümlülüğü getirilmektedir.[103] Ayrıca, banka kartı ve kredi kartı üreten başta bankalar olmak üzere tüm kuruluşlara elde ettikleri kişisel verileri başka amaçlarla kullanmama ve bu verilere başkalarının ulaşmasına engel olacak tedbirleri alma yükümlülüğü yüklenmektedir.

C. Kullanıcı Profili

Kullanıcı profilleri; kullanıcıların, internette gerçekleştirdikleri işlemlerin ayrıntılı tespiti ve analizi ile alışveriş tercihleri, kişisel ve psikolojik alışkanlıkları çerçevesinde ortaya konulan kişisel profilleridir.[104]

Kullanıcıların, internette gerçekleştirdikleri işlemlerin takibi bazen kullanıcı ilgili sayfayı kapatsa bile çerezler ile sürdürülebilmektedir.[105] Çerezler, kişilerin internette izledikleri

---

[102] Demirbaş, "6563 Sayılı Elektronik Ticaretin," 68.

[103] Demirbaş, "6563 Sayılı Elektronik Ticaretin," 69-70.

[104] Demirbaş, ""6563 Sayılı Elektronik Ticaretin," 70-71.

[105] Vefa Reşat Moral ve İpek Aşıkoğlu, "E-Ticarette Kişisel Verilerin Korunması," erişim tarihi: Aralık 29, 2019, http://moral.av.tr/e-ticarette-kisisel-verilerin-korunmasi?l=null.

yolu takip ederek elde ettikleri verileri analiz eder ve daha sonra başka amaçlarla kullanılır. Örneğin, kişiye en uygun reklamın gönderilmesi amacıyla çerezler kullanılabilecektir. Çerezlerin kullanılabilmesi ancak kişisel verileri elde edilecek kişinin açık rızası ile mümkün olması gerekirken; kişinin çerez kullanımını kabul etmediği takdirde ilgili sayfayı kullanamaması ya da çerez kullanımını kabul ettiği takdirde ne tür kişisel verilerinin elde edileceği konusunda yeterince aydınlatılamaması ilgili kişinin iradesine bir müdahale olup bir insan hakları sorunudur.[106]

Çerezlerin sağladığı bazı kolaylıklar vardır. Örneğin, fotoğraf gibi görsel materyaller bir kez yüklendikten sonra çerezler sayesinde kullanıcı tarafından aynı siteye yeniden erişim sağlandığında söz konusu materyallerin yüklenmesi için ayrıca bir zaman harcanmamaktadır. Ancak, günümüzde internetin oldukça hızlı hale gelmiş olması nedeniyle bu özelliğe ihtiyaç duyulmamaktadır. Öte yandan çerezler sayesinde bir siteye erişirken kullanıcı adı ya da şifrelerin yeniden girilmesine gerek duyulmamaktadır. Ancak bu kolaylık kişisel verilerin teslim edilmesine ve pazarlama hedefleri doğrultusunda sömürülmesine değecek bir kolaylık değildir. Veri, 21. yüzyılın petrolü; çerezler ise bu petrolün çıkarıldığı sondaj cihazları konumundadır. Amerika'nın çerez diliminin %50'si Google'ın elinde; geri kalan önemli bir kısmı ise Amazon, Facebook ve Twitter gibi kuruluşların elindedir.[107]

Her ne kadar çerez üretenler elde ettikleri veriler ile ilgili kişiyi belirleyemediklerini iddia ediyorlarsa da teknolojinin geldiği aşama nazara alındığında ilgili kişilerin ek bilgilerle belirlenebileceği açıktır.[108] Bu itibarla, ETDHK 10. madde kapsamında hizmet sağlayıcılar ve aracı hizmet sağlayıcıların kişisel verilerin korunması kapsamındaki sorumlulukları

---

106 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 357-358.

107 Taşkaya ve Talay, "Dijital Gözetimin Pazarlama," 365.

108 Keser, "Tüketicinin Kişisel Verisinin", 1211.

şüphesiz kullanıcı profillerini (çerezleri) de kapsayacaktır.[109] Avrupa Birliği Adalet Divanına göre de çerezler kişisel veri mahiyetindedir.[110]

D. Elektronik Ticarette Kişisel Verilerin Korunmasına Hizmet Eden Uygulamalar ve Kuruluşlar

Doğrudan kişisel verilerin korunmasına yönelik olmasa da genel olarak elektronik ticarete ilişkin geliştirilen bazı uygulamalar dolayı olarak kişisel verilerin korunmasına hizmet etmektedir. Aşağıda kısaca bu uygulamalara ve bu hususta çalışma yürüten kuruluşlara değinilecektir.

1. Ticari Elektronik İleti Yönetim Sistemi

Elektronik ticarette bir diğer önemli sorun rıza dışı gönderilen elektronik iletilerdir. Ticari elektronik iletinin tanımı yukarıda da belirttiğimiz üzere ETDHK'nın 2/1-c maddesinde yapılmıştır.

Ticari elektronik iletiler, Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik[111] ile düzenlenmiştir. Söz konusu iletilerin gönderilmesi için alıcılardan onay almak gerekmektedir. Bu durumun bazı istisnaları vardır. Örneğin, esnaf ve tacirlere gönderilecek elektronik iletiler ile alıcının iletişim için bildirdiği numaraya, temin edilen mal ve hizmetlerin bakım, kullanım ve değişimleri konusunda yapılacak bilgilendirmeler, bu istisnalar arasındadır.[112]

Anılan yönetmelikte 04 Ocak 2020 tarihinde önemli değişiklikler yapılmıştır. Bu değişikliklerden birisi de "Ticari Elektronik İleti Yönetim Sistemi"nin kurulmasıdır. Zira, 6365 sayılı Kanun'un 11/4. maddesinde Ticaret Bakanlığının *"ticari elektronik ileti onaylarının alınmasına ve reddetme hakkının*

---

109 Demirbaş, "6563 Sayılı Elektronik Ticaretin," 70-71.

110 Keser, "Tüketicinin Kişisel Verisinin," 1210.

111 RG. 15.07.2015, S. 29417.

112 Keser, "Tüketicinin Kişisel Verisinin," 1192.

kullanılmasına imkân tanıyan bir elektronik sistem kurmaya veya kurdurmaya yetkili…" olduğu belirtilmektedir.[113] İşte bu hükme istinaden Ticari Elektronik İleti Yönetim Sistemi kurulmuştur.

Ticari Elektronik İleti Yönetim Sistemi kapsamında ileti göndermek isteyen gerçek ve tüzel kişiler ileti göndermek üzere izin aldıkları müşterilerini Bakanlığın kontrolündeki sisteme işleyecek ve bu yönetim sistemine sundukları kayıtlar doğrultusunda elektronik ileti gönderebileceklerdir. İleti gönderilecek kişiler de bu sisteme girmek suretiyle hangi firmalara/kişilere izin verdiklerini görebilecek ve istedikleri takdirde bu onayları sona erdirebileceklerdir. Yine bu sistem aracılığıyla ilgili kişiler ayrıca kendilerine ileti gönderen firmalara ret bildiriminde bulunmak suretiyle de ileti gönderilmesini engelleyebileceklerdir.

Kanun'da, Bakanlığın sadece Ticari Elektronik İleti Yönetim Sistemini "kurma" yetkisini devredebileceği belirtildiği halde uygulamada Bakanlığın, sistemi hem "kurma" hem de "yönetme" yetkisini Türkiye Odalar ve Borsalar Birliğine (TOBB) devrettiği, anılan kuruluşun da aynı yetkileri "İleti Yönetim Sistemi Anonim Şirketi"ne devrettiği anlaşılmaktadır. İleti Yönetim Sistemi A.Ş.'nin yasal değişiklik öncesinde -2019 yılında- kurulmuş olması, yine şirketin özel hukuk tüzel kişisi olması, Bakanlık tarafından özellikle "yönetme" konusundaki yetkinin devredilmesinin yasal dayanaktan yoksun olması gibi nedenlerle mevcut uygulama eleştirilmektedir. Bu eleştirilerle bağlantılı olarak Kişisel Verilerin Korunması Kanunu bağlamında bir dayanağı bulunmayan İleti Yönetim Sistemi A.Ş.'nin ilgili kişilerin verilerini "açık rıza" dışında işleyemeyeceği de belirtilmektedir.[114]

---

[113] Mahmut Furkan Balaban, "İleti Yönetim Sisteminin Kurulması ve Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik'in Değerlendirilmesi", *Bilişim Hukuku Dergisi* 2, no. 2 (2020): 192.

[114] Balaban, "İleti Yönetim Sisteminin," 193-196, 209.

Elektronik ileti yönetim sistemi, kişinin daha önce elde edilen kişisel verilerinin reklam göndermek suretiyle kullanılmasının ilgili tarafından engellenmesi bakımından önemli bir düzenlemedir. Bu sisteme e-devlet üzerinden erişmek mümkündür. Ayrıca, Kurul, bir kararında[115] ticari elektronik ileti göndermek üzere kişisel verilerin işlenebilmesi için 6698 sayılı Kanun'un 5. maddesinde yer alan şartların gerçekleşmesinin gerektiğini belirtmektedir. Anılan karara göre aksi durumda veri sorumluları hakkında Kanun'un 18. maddesinde yazılı kabahatler nedeniyle işlem tesis edilmesi gerekmektedir.

2. Güven Damgası

Kişisel veriler ile ilgili olan bir diğer uygulama "Güven Damgası"dır. Güven Damgası, elektronik ticarette asgari hizmet kalitesinin ve güvenlik standartlarının tesis edilmesi amacıyla geliştirilmiştir. Elektronik Ticarette Güven Damgası Hakkında Tebliğ[116] ile Güven Damgası'na ilişkin temel hususlar düzenlenmiştir. Bu Tebliğe göre belirli şartları taşıyan elektronik ticaret sitelerine Güven Damgası kullanma yetkisi verilecektir. Alıcılar güven damgası olan sitelerin asgari güven ve kalite standartlarına sahip olduğunu bilecek ve alışverişlerini buna göre yapacaklardır. Güven Damgası Sağlayıcı (GDS) kuruluş olarak 1 Şubat 2018 tarihinde imzalanan protokolle TOBB yetkilendirilmiştir

Güven Damgası almanın şartları söz konusu Tebliğin 5. maddesinde düzenlenmiştir. Bu hükme göre, Güven Damgası alabilmek için kişisel verilerin korunması anlamında bazı özel sertifikalara sahip olmak gerekmektedir. Ayrıca, TSE onaylı firmalara sızma testi yaptırılması; gerçek kişiler müracaat etmişse bu kişilerin 1 yıldan fazla hapis cezası almamış olmaları; iflas etmiş bir firma söz konusu ise itibarın iadesi kararının

---

115 Kişisel Verileri Koruma Kurulu Kararı, 2018/119, 16.10.2018, RG. 01.11.2018, S. 30582.

116 R.G. 06/06/2017, S. 30088.

alınmış olması gibi şartların taşınması da gerekmektedir. Bu hükümler de dolaylı olarak kişisel verilerin korunmasına hizmet edebilecek hükümlerdir.

Güven Damgası almak zorunlu değil tercihe bağlı bir uygulamadır. Güven Damgası'na sahip olan elektronik ticaret siteleri, Ticaret Bakanlığı tarafından ilan edilmektedir.[117] Alınması, aracı hizmet sağlayıcıların ve hizmet sağlayıcıların takdirine bırakılan güven damgasının alınma süreci zor ve maliyetlidir. Ancak müşteriler nezdinde güven sağlayabilmek için elektronik ticaret sitelerinin zamanla güven damgası elde etmek üzere daha fazla talepte bulunacakları değerlendirilmektedir.[118]

3. Elektronik Ticaret Bilgi Sistemi

Yukarıda açıkladığımız Güven Damgasının alınması ihtiyaridir. Ancak, 11 Ağustos 2017 tarih ve 30151 sayılı resmî gazetede yayımlanarak yürürlüğe giren 'Elektronik Ticaret Bilgi Sistemi ve Bildirim Yükümlülükleri Hakkında Tebliğ'e[119] göre Elektronik Ticaret Bilgi Sistemi'ne (ETBİS) üyelik, elektronik ticaret yapanlar için zorunludur.

ETBİS, elektronik ticareti genel anlamda kayıt altına almaya yönelik önemli bir adımdır. Bu yönüyle sistemin, kişisel verilerin korunması anlamında dolaylı da olsa uzun vadede ciddi faydası olacağını değerlendiriyoruz. Ayrıca, söz konusu tebliğin "bildirim yükümlülüğü" başlıklı 6. maddesinde ETBİS'e kaydedilen hizmet sağlayıcı ve aracı hizmet sağlayıcıların bildirmekle yükümlü oldukları bilgiler arasında "kişisel verilerin ve müşteri bilgilerinin tutulduğu veri tabanlarının bulunduğu ülke ve adres bilgileri" de yer almaktadır.

---

117 "Güven Damgası Olan E-Ticaret Siteleri," TOBB, erişim tarihi: Ocak 12, 2020, https://www.guvendamgasi.org.tr/guvendamgasialan.php.

118 Hamamcıoğlu, "Elektronik Ticaretin Hukuksal," 61.

119 RG. 11.08.2017, S. 30151.

4. Sektörel Kuruluşlar

Türkiye Odalar ve Borsalar Birliği, gerek güven damgası sağlayan kuruluş olması gerekse oluşturduğu Türkiye E-Ticaret Meclisi ile konumuz bağlamında önemli fonksiyonlar üstenmesi gereken bir kuruluştur. Yine Elektronik Ticaret İşletmecileri Derneği (ETİD) gibi kuruluşların da elektronik ticarette kişisel verilerin korunması konusuna ilişkin bazı çalışmaları bulunmaktadır. Doktrinde bu tür kuruluşların elektronik ticarette güveni zedeleyen firmaları ifşa etmek gibi çalışmalar yaparak sürece katkı sağlayabileceği görüşü ileri sürülmektedir.[120]

E. Elektronik Ticarette Kişisel Verilerin Korunmamasının Sonuçları

Öncelikle belirtelim ki elektronik ticarette alışverişin yüz yüze yapılmaması, coğrafi sınırların kalkması, bu hususta dolandırıcıların her geçen gün farklı yöntemler geliştiriyor olması gibi hususlar nazara alındığında kişisel verilerin korunması hususunda gösterilecek zafiyetler elektronik ticaret yapan şirketlere olan güveni ortadan kaldıracaktır. Güvenilmeyen site iş yapamaz hale gelecektir. Bu sonuç işin ticari boyutuyla ilgili bir sonuçtur.

Yine kamu kurumu olan veri sorumluları, kişisel verilerin korunmasına ilişkin yükümlülüklere aykırı hareket ettiklerinde ilgililer hakkında disiplin hükümlerinin devreye gireceği belirtilmişti. Özel hukuk kapsamındaki kişiler/tüzel kişiler kişisel verilerin korunmasına ilişkin yükümlülüklere uygun hareket etmediklerinde ise süreç aşağıdaki şekilde işleyecektir.

Öncelikle 1. bölümde "Suçlar ve Kabahatler" başlığı altında belirttiğimiz idari para cezaları devreye girecektir. Kanunun 18. maddesinde sonucu idari para cezasına bağlanan eylemler aşağıdaki şekilde belirtilmiştir:

---

120 Yılmaz ve Karakadılar, "Türkiye'deki Elektronik Ticaret," 70.

-Aydınlatma yükümlülüğüne aykırı hareket edenlere 5.000-100.000 TL (2021 yılı için: 9.834-196.686 TL)

-Veri güvenliğine ilişkin sorumluluklarını yerine getirmeyenlere 15.000-100.000 TL (2021 yılı için: 29.503-1.966.862 TL),

-Kurulun kararlarını icra etmeyenlere (m.15) 25.000-100.000 (2021 yılı için: 49.172-1.966.862 TL),

-VERBİS'e kayıt ve bildirim hususundaki kurallara uymayanlara 20.000-1.000.000 TL (2021 yılı için 39.337 TL – 1.966.862) tutarında idari para cezası verilebilecektir.[121] Ayrıca, yine Ceza Hukuku anlamında maddi ve manevi unsurları bulunduğu takdirde Türk Ceza Kanunu'nda yazılı olduğu şekilde sorumluların; *Kişisel Verilerin Kaydedilmesi* (m. 135); *Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme* (m. 136); *Verileri Yok Etmeme* (m. 138) suçları kapsamında cezalandırılmaları söz konusu olacaktır.

Bir ihlal nedeniyle hem suç hem de kabahat söz konusu olduğunda yani aynı eylem nedeniyle hem yukarıda yazılı idari para cezalarından birini vermek gerekiyor hem de söz konusu eylem TCK'nın m.135 ilâ 138. maddeleri arasındaki suçların oluşmasına neden oluyorsa Kabahatler Kanunu'nun 15/3. maddesi devreye girecektir. İlgili hüküm: "*Bir fiil hem kabahat hem de suç olarak tanımlanmış ise, sadece suçtan dolayı yaptırım uygulanabilir. Ancak, suçtan dolayı yaptırım uygulanamayan hallerde kabahat dolayısıyla yaptırım uygulanır*" şeklindedir.

Genel kural bu ise de istisnai olarak hem ceza hükümlerinin hem de kabahat hükümlerinin uygulanacağı kanunda açıkça öngörülebilecektir. Örneğin Vergi Usul Kanunu'nun 359. maddesi kapsamındaki suçtan bir kişi mahkûm olduğu halde hakkında vergi zıyaı cezası da uygulanabilecektir. Ancak kişisel

[121] 2021 yılında uygulanacak cezalar için miktarlar 20 Kasım 2020 tarihli ve 31318 sayılı resmi gazetede yayımlanan yeniden değerlendirme oranına (%9,11) göre belirtilmiştir.

verilerin korunması bağlamında böyle bir istisna geçerli olmayıp genel düzenleme caridir.[122]

Kabahatler Kanunu'nun 15/3. maddesinde belirtilen "*suçtan dolayı yaptırım uygulanamayan haller*"e şu örnekler verilebilir: Kabahatler Kanunun 9. Maddesine göre kabahat fiilleri hem kast hem taksir ile işlenebilirken; TCK 22/1.maddesine göre taksirli fail, ancak fiilin taksirle işlenmesi suç olarak düzenlenmişse ilgili hükme istinaden cezalandırılabilir.[123] TCK'da yer alan kişisel verilerin ihlaline ilişkin suçlar (m.135-138) kasten işlenebilecek suçlardır. Dolayısıyla kişisel verilerin korunmasına ilişkin hükümleri taksirle ihlal eden kişi hakkında ceza mahkûmiyeti verilemeyecek ancak bu kişinin idari para ceza ile cezalandırılması söz konusu olabilecektir.

Yine, şikâyete bağlı bir suç mevcut olmasına rağmen şikâyet gerçekleşmemiş ise ya da olayda bir hukuka uygunluk nedeni varsa suçtan dolayı yaptırım uygulanamayan bir hal söz konusu olacaktır.[124] Bu tür durumlarda da ceza kovuşturması yapılamasa da idari para cezası verilebilecektir.

Yukarıda yazılı olduğu şekilde Kurul'a, Kurul'un her türlü kararını yerine getirmeyenlere yönelik idari para cezası verebilme yetkisinin tanınması, kurulun güçlü yetkilerinin icrasına ilişkin önemli bir düzenlemedir.[125] Yine, Kanun veri ihlali olduğunda veri sorumlusuna veri ihlali bildiriminde bulunma yükümlülüğü getirmektedir. Buna göre, "*işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde*

---

122 Murat Kart ve Aslıhan Ketizmen, "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme", *Kişisel Verileri Koruma Dergisi* 1, no.2 (2019): 19-27.

123 Kart ve Ketizmen, "Kabahatler Kanunu'nun İçtima," 20.

124 Kart ve Ketizmen, "Kabahatler Kanunu'nun İçtima," 20.

125 Kart ve Ketizmen, "Kabahatler Kanunu'nun İçtima," 26.

ya da uygun göreceği başka bir yöntemle ilan edebilir (m. 12/5)". Örneğin "Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ" isimli elektronik ticaret yapan şirketin veri ihlali bildirimi üzerine Kişisel Verileri Koruma Kurulu, 29.03.2021 tarih ve 2021/321 sayılı kararı ile veri ihlalinin bazı detaylarını internet sitesinden paylaşmış ve incelemenin devam ettiğini kamuoyuna duyurmuştur. Kurul, inceleme neticesinde gerekli göreceği yaptırımların uygulanmasına karar verebilecektir.

Kurul, kişisel verilerin korunması hususunda ilgili kişinin şikâyeti üzerine veya resen devreye girebilir. İlgili kişinin şikâyet hakkını kullanabilmesi için öncelikle veri sorumlusuna müracaat etmesi gerekmektedir. Veri sorumlusu en geç otuz gün içinde ilgili kişiye cevap vermelidir. Verilen cevabı yetersiz bulan ya da müracaatı cevapsız bırakılan ilgili kişi 30 gün içinde Kural'a şikâyet hakkını kullanabilecektir. Aşağıda konumuz bağlamında Kurul'un şikâyet üzerine ve resen yaptığı incelemelere ilişkin örnek kararlara değinmek istiyoruz.

Kurul'un önüne gelen bir olayda[126] ilgili kişi, veri sorumlusundan, abonelik sözleşmesi yapmak üzere yaptığı telefon görüşme kayıtlarını istemiştir. Veri sorumlusu şirket, telefon görüşmesinde müşteri temsilcisinin ses kayıtlarının da yer aldığını ve bu kayıtların da kişisel veri olduğunu, bu nedenle söz konusu verilerin ilgili kişiye verilemeyeceğini ancak yetkili adli ve idari mercilere verilebileceğini belirtmiştir. Kurul konuyu değerlendirmiş ve kararında şu hususlara değinmiştir:

-6365 Sayılı Kanun'unda elektronik iletişim araçlarıyla yapılan sözleşmelerin Kanun kapsamında olduğu belirtilmekle beraber elektronik sözleşmelerin tanımı yapılmamıştır. Ancak Kanunun 2. maddesinde yer alan "elektronik ileti" tanımının içeriği nazara alındığında telefon ile yapılan sözleşmeler 6365 Sayılı Kanun kapsamında elektronik sözleşme kabul edilmelidir.

---

126 Kişisel Verileri Koruma Kurulu Kararı, 2020/746, 29.09.2020.

-İlgili kişinin, KVKK 11/b. maddesinde belirtilen "*Kişisel verileri işlenmişse buna ilişkin bilgi talep etme*" hakkı kapsamında talep ettiği veriye erişim hakkı bulunmaktadır. Ancak erişim hakkı kullanılırken veri sorumlusunun veri güvenliğine ilişkin yükümlülükleri nazara alınarak, veri içeriğine makul şekilde ulaşılabilecektir. Bu çerçevede erişim hakkının, söz konusu ses kayıtlarının doğrudan verilmesi yerine başkasına ait kişisel veriler maskelenmek suretiyle ses kayıtlarının dökümlerinin verilerek kullandırılması gerekmektedir.

Kurul'un "Amazon Turkey" hakkında yapılan bir ihbar üzerine resen yaptığı inceleme sonucunda verdiği bir kararda[127] da konumuz bağlamında önemli hususlar yer almaktadır:

İhbarda özetle; 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun uyarınca hizmet sağlayıcı ve aracı hizmet sağlayıcı niteliğinde olan www.amazon.com.tr sitesinin ilgililerden elektronik ticari ileti gönderebilmek için açık rıza almadığı, site tarafından açık rıza dışında bir işleme nedeninin varlığına ilişkin açıklamanın da yapılmadığı; sitede yer alan açıklamalardan, siteyi sadece ziyaret eden bir kişinin kişisel verilerinin işlenmesine ve kendisine ticari elektronik ileti gönderilmesine (bu ziyaret nedeniyle) onay verdiğinin varsayıldığı; alışveriş için üye hesabı açmanın zorunlu olduğu, üye hesabı açılırken kullanım ve satış şartlarının da kabul edildiği ve bu kapsamda ticari elektronik iletiye de onay vermenin zorunlu olduğu, bu durumun Kurul'un önceki kararlarında belirtildiği üzere açık rızanın hizmet şartına bağlanamayacağı ilkesine aykırı olduğu; yine sitede yer alan açıklamalardan kişisel verilerin yurtdışına aktarıldığının anlaşıldığı ancak üyelik hesabı oluşturma ve alışveriş yapma sırasında bu hususta ilgili kişiden açık rıza alınmadığı, bu durumun Kanun'un 9. maddesine aykırılık oluşturacağı hususları belirtilmiştir.

---

127 Kişisel Verileri Koruma Kurulu Kararı, 2020/173, 27.02.2020.

Veri Sorumlusu savunmasında: ticari elektronik iletilere ilişkin şikâyetlerin Ticaret Bakanlığına iletilmesi gerektiğini; ticari elektronik iletiler bakımından müşterilere tercih hakkı tanındığı; müşteri hesabı oluşturulduğunda "Gizlilik Bildirimi"nin de kabul edildiğini, böylece ilgililerin kişisel verilerinin işlenmesine ve yurtdışına aktarımına onay vermiş olduklarını, belirtmiştir.

Kurul'un yaptığı değerlendirmede şu hususlara yer verilmiştir:

Öncelikle, Veri Sorumlusunun ihbara bakmaya yetkili merciin Ticaret Bakanlığı olduğu yönündeki savunması bakımından; ticari elektronik ileti gönderilmesi için telefon, e posta gibi verilerin işlenmesi gerekmekte olup ihbarcının şikâyeti bu hususa ilişkin olduğundan mezkûr savunma reddedilmiştir. Ayrıca, ihbarcının aynı konuya ilişkin Ticaret Bakanlığı'na yaptığı başvurusu da anılan Bakanlık tarafından Kurul'un yetkili olduğu belirtilmek suretiyle başvuru Kurul'a gönderilmiştir.

Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğin 5/1; 7/1 ve 12/2 maddeleri gereğince ticari elektronik ileti gönderilebilmesi için onay alınması şart olduğu gibi bu kapsamda kişisel verilerin işlenebilmesi için de ilgili kişiden onay alınması gerekmektedir.

Sitede hesap oluşturulduğunda elektronik ileti gönderilmesine dair seçenekler otomatik tıklanmış olarak gelmektedir ve bu durum açık rızanın *opt-in* yani bireyin bilinçli eylemi ile alınması prensibine aykırıdır.

Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğin[128] 5/1-f maddesinde aydınlatma ve açık rızanın alınmasının aynı anda yapılamayacağı, ayrı ayrı işlemler olarak gerçekleştirilmesi

[128] RG. 10.03.2018, S. 30356.

gerektiği belirtilmesine rağmen, şirketin, müşterinin gizlilik bildirimini onaylayarak açık rızanın alındığı yönündeki savunması da kabul edilebilir bulunmamıştır. Neticede, Şirket'in 6698 sayılı Kanun'un 12. Maddesine aykırı hareket ettiği sonucuna varılmıştır.

Kişisel veriler aynı zamanda kişiye sıkı sıkıya bağlı kişilik hakkı mahiyetinde olduğu için[129] kişisel verileri korunmayan kişi TMK'nın 24-25 maddelerine göre kişilik haklarının saldırıya uğramasından kaynaklı davaları açabilir. Buna göre, ilgili kişi mahkemeden saldırıya ilişkin tespit, önleme ve durdurma taleplerinde bulunabilir. Yine, haksız fiil teşkil eden eylemler nedeniyle Türk Borçlar Kanunu'nun 58. maddesi bağlamında manevi tazminat davası da açılabilir.[130]

Nitekim KVKK 11/ğ maddesinde de kanuna aykırı olarak kişisel verisi işlenen kişinin zararının tazminini isteme hakkından bahsedilmektedir. Bu kapsamda veri sorumlusu özel kişi/kurum olduğunda maddi ve manevi tazminat davaları söz konusu olacaktır. Veri sorumlusu kamu tüzel kişisi olduğunda ise tam yargı davaları söz konusu olacaktır.[131]

Son olarak uluslararası elektronik ticaret sitelerine değinmek isteriz. Uluslararası şirketlerce toplanan verilerin kötü niyetli kullanımı da söz konusu olabilmektedir. Nitekim Londra merkezli bir şirket hakkında milyonlarca Facebook kullanıcısının kişisel verilerini kullanarak 2016 yılındaki ABD başkanlık seçimleri ve İngiltere'deki Brexit Referandumu sonuçlarını etkilemek amaçlı eylemlerde bulunduğu iddiasıyla soruşturma başlatıldığı bilinmektedir. Big Data boyutuna varacak kişisel veriler genel olarak Google, Alibaba, Amazon gibi uluslararası şirketler tarafından toplanmakta olup, söz

---

129 Oğuz, "Kişisel Verilerin Korunması," 121.

130 Kemal Atasoy, "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası," *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 22, no. 3 (2016): 274.

131 Oğuz, "Kişisel Verilerin Korunması," 137.

konusu verilerin bireylerin algılarının yönetilmesinde kullanılma ihtimali oldukça yüksektir.[132]

Bu noktada, söz konusu şirket merkezlerinin Türkiye'de bulunmadığı nazara alındığında KVKK kapsamındaki ihlaller bakımından Türk Hukuku çerçevesinde yaptırım uygulamanın oldukça zor olduğunu belirtmek isteriz. Devletimiz gerek kişisel verilerin korunması alanında gerekse benzer başka alanlarda ortaya çıkan sorunlar nedeniyle söz konusu uluslararası şirketleri Türkiye'de temsilcilik açmaya zorlamaktadır. Bu çerçevede yakın zamanda özellikle sosyal medya siteleri bakımından 7253 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun[133]" yürürlüğe girmiştir. Ancak, bu kanun elektronik ticaret sitelerini kapsamamaktadır. Her ne kadar "Amazon" gibi bazı şirketler Türkiye'de temsilcilik açmış ise de bu hususta zorlayıcı bir düzenleme bulunmamaktadır. Sosyal medya siteleri için getirilen düzenleme benzeri bir düzenlemeye elektronik ticaret siteleri bakımından da ihtiyaç bulunmaktadır.

SONUÇ

Kişisel veri kavramı, teknolojinin baş döndürücü gelişiminin bir yansıması olarak hukuk dünyamızda artık çok daha geniş bir alan bulmaktadır. Kişisel veriler, yeterli düzeyde korunmadığında ve bu alandaki hukuki sınırlar net bir şekilde belirlenmediğinde, hukuk dışı yöntemlerle kişisel veriler toplanıp algıları uluslararası sermaye şirketlerince yönetilen modern köle toplumlarının ortaya çıkması kaçınılmaz olacaktır.

Ülkemizde, Kişisel Verileri Koruma Kanunu'nun kabul edilerek Kişisel Verileri Koruma Kurumu ile Kişisel Verileri Koruma Kurulu'nun tesis edilmesi önemlidir. Yine, Kanun çerçevesinde gerek kamuya gerekse özel sektöre yasal

---

132 Oğuz, "Kişisel Verilerin Korunması," 136.

133 R.G. 31.07.2020, S. 31202.

standartlarla uyumlu hale gelme zorunluluklarının yüklenmiş olması olumlu gelişmelerdir.

Kurum tarafından oluşturulan VERBİS'in konumuz bağlamında bir farkındalığın oluşmasına ciddi katkı sağlayacağı değerlendirilmektedir. VERBİS'e kayıt tarihleri çeşitli gerekçelerle birkaç kez ertelenmiştir. Bu tarihlerin yeniden ertelenmemesi gerektiği kanaatindeyiz. Ayrıca şunu da önemle vurgulamak isteriz ki VERBİS'e kayıt olma süresi ertelenmiş olsa da 6698 sayılı Kişisel Verilerin Koruması Kanunu hükümlerine uymak zorunluluğu devam etmektedir. Kanun hükümlerine uymak bakımından bir erteleme söz konusu değildir.

Öte yandan VERBİS kapsamında, sorumlulardan topladıkları kişisel verilere ilişkin sadece kategorik bazda verilerin istenilmesi; devasa veri tabanlarının yasal standartlara uyumu konusunda etkin bir denetim mekanizmasının kurulamamış olması da ciddi bir eksiklik olarak karşımıza çıkmaktadır. Bu noktada, VERBİS'i etkin ve Kanun'un amaçladığı korumayı sağlayacak hale getirmek için şirketlerin kategorik bazda verilerini girmesi ile yetinilmeyerek güçlü bilişim sistemleriyle detaylı olarak girilen kayıtların kontrol edilip denetlenebilmesi sağlanmalıdır. Bu denetimi yapabilmek üzere Kurum bünyesinde denetim standartları belirlenerek istihdam edilecek uzman denetçilerle Kanun'un etkin olarak uygulamasını sağlamak gerekmektedir. Zira, kurulun resen harekete geçme yetkisi olmasına rağmen harekete geçtiğinde gerekli hukuki-teknik incelemeleri yapabilecek uzman kadrosu bulunmamaktadır.

Ticaret Bakanlığınca geliştirilen ETBİS (Elektronik Ticaret Bilgi Sistemi), İYS (Ticari Elektronik İleti Yönetim Sistemi) ve Güven Damgası uygulamaları kişisel verilerin korunması bağlamında konuya ciddi katkısı olacağı değerlendirilen sistemlerdir. Bu sistemlerin geliştirilmesindeki baskın düşünce elektronik ticarete olan güvenin artırılması düşüncesidir. Söz konusu güven duygusunun gelişiminde kullanıcı profil

bilgisinden, ödeme bilgisine varıncaya kadar kişisel verilerin korunması çok önemlidir.

Konumuz bağlamında Ticaret Bakanlığı ile Kişisel Verileri Koruma Kurumu arasında güçlü bir iletişimin ve iş birliğinin sürekli hale getirilmesi şarttır. Bu iletişim ve iş birliği hem yasal düzenlemelerin yapım sürecinde hem de ayrı ayrı geliştirilen bilgi yönetim sistemleri arasında uyum sağlanması bakımından oldukça önemlidir.

Devasa boyutta kişisel veri elde ettiği halde Türkiye'de temsilciliği bulunmayan uluslararası elektronik ticaret şirketleri hakkında da gerektiğinde denetim yapılabilmesi ve yaptırım uygulanabilmesi için gerekli yasal değişikliklerin yapılması şarttır. Zira söz konusu şirketlerin bugün için denetimi yapılamamaktadır.

Kişisel Verileri Koruma Kanunu'nun getirdiği yükümlülükleri yerine getirmek, elektronik ticaret yapan kişiler ve şirketler için başlangıçta zorluklar içerse de veri güvenliğinin sağlanması, uzun vadede elektronik ticarete güvenin artmasını ve dolayısıyla elektronik ticaretin büyümesini sağlayacaktır. Öte yandan, Kanun'un etkin bir şekilde uygulanmasıyla bireylerin kişisel hakları korunarak özel hayatın gizliliği hakkı teminat altına alınmış olacaktır.

KAYNAKÇA

Akkurt, Sinan Sami. "Elektronik Ortamda Hizmet Sunumu ve Buna İlişkin Sözleşmelerin Hukuki Niteliği." *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 60, no. 1 (2011): 19-49.

Akkurt, Sinan Sami. "Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış." *Kişisel Verileri Koruma Dergisi* 2, no. 1 (2020): 20-32.

Arslan, İsmet Kahraman ve Öz, Neslihan "Elektronik Ticaret Sözleşmelerine Uygulanacak Hukuk." *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi* 19, no. 38, (2020): 13-31.

Atasoy, Kemal. "Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması Ve Veri Sahibinin Rızası." *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 22, no. 3 (2016): 269-301.

Avrupa Birliği Adalet Divanı. *Judgment of 19 October 2016, Breyer*. C-582/14, EU: C: 2016: 779. http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2725971.

Balaban, Mahmut Furkan. "İleti Yönetim Sisteminin Kurulması Ve Ticari İletişim Ve Ticari Elektronik İletiler Hakkında Yönetmelik'in Değerlendirilmesi." *Bilişim Hukuku Dergisi* 2, no. 2 (2020): 181-219.

Balaban, Semiha Önder. "Milletlerarası Özel Hukukta Elektronik Sözleşmeler." Yayımlanmamış Yüksek Lisans Tezi, Isparta: Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, 2016.

Başalp, Nilgün. "Bilgi Teknolojileri Dış Kaynak Alımında (Outsourcing) Kişisel Verilerin Korunması ve Gizlilik Sözleşmeleri." Yayımlanmamış Yüksek Lisans Tezi, İstanbul: İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2013.

Bük, Alaattin. *Bilişim Alanında Kişisel Verilerin Korunması*. Ankara: Seçkin Yayıncılık, 2018.

Demirbaş, Harun. 6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Kapsamında Hizmet Sağlayıcıları ve Aracı Hizmet Sağlayıcılarının Yükümlülükleri. Ankara: Seçkin Yayıncılık, 2015.

Elibol, Halil ve Kesici, Burcu. "Çağdaş İşletmecilik Açısından Elektronik Ticaret." *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, no. 11 (2004): 303-329.

EUR-Lex. "Directive 95/46/EC of The European Parliament and of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN.

EUR-Lex. "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=DE.

EUR-Lex. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN.

Gezder, Ümit. "Elektronik Ticaret Hukuki İşlemlerinin Ayrımı-Dijital İçerik ve Hukuki Niteliği." *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* 22, no. 3 (2016): 1119-1132.

Hamamcıoğlu, Esra. "Elektronik Ticaretin Hukuksal Boyutu." *Kocaeli Üniversitesi Sosyal Bilimler* Dergisi, no. 35 (2018): 43-72.

Kaya, Ferman. E-Ticaret Hukuku ve Tüketici Hukukundaki Yansımaları. Ankara: Seçkin Yayıncılık, 2018.

Karlıdağ, Serpil. "Ekonomi Politik Acıdan Kişisel Verilerin Korunması." *Amme İdaresi Dergisi* 46, no. 1 (2013): 127-152.

Kart, Aslıhan ve Ketizmen, Murat. "Kabahatler Kanunu'nun İçtima Hükümleri Açısından Kişisel Verilerin Korunmasına İlişkin Suç ve Kabahatler ile Kurul'un İdari Ceza Kararlarına İlişkin Bir Değerlendirme." *Kişisel Verileri Koruma Dergisi* 1, no.2 (2019): 17-29.

Ketizmen, Murat ve Kart, Aslıhan. "Kişisel veri ve rekabet hukuku kapsamında 'Big data'." *Kişisel Verileri Koruma Dergisi* 1, no. 1 (2019): 64-76.

Keser, Leyla. "Kişisel Veriler Kanunu'nun Getirdikleri." Video, 1:27:50. Yükleyen: E-Ticaret ve İnternet Hukuku Derneği. Yükleme Tarihi: Kasım 22, 2016. Erişim Tarihi: Kasım 16, 2019. https://www.youtube.com/watch?v=yyMUPZSXtoY.

Keser, Yıldırım. "Tüketicinin Kişisel Verisinin İşlenmesinde Açık Rıza." *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 28, no. 3 (2020): 1181-1215.

Küzeci, Elif. "Anayasal Bir Hak: Kişisel Verilerin Korunması." *Türkiye Bilişim Derneği Bilişim Dergisi*, no. 128 (2011): 142-149.

KVKK. "Açık rıza nedir." Erişim Tarihi: Kasım 17, 2019. https://www.kvkk.gov.tr/Icerik/4118/Videolar?&page=2.

KVKK. "Aydınlatma Yükümlülüğü." Erişim Tarihi: Kasım 17, 2019. https://www.kvkk.gov.tr/Icerik/4118/Videolar?&page=2.

KVKK. "Kişisel Verileri Koruma Kanunu Hakkında Sıkça Sorulan Sorular." Erişim Tarihi: Şubat 13, 2020. https://www.kvkk.gov.tr/Icerik/4196/Kisisel-Verilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular.

KVKK. "Kişisel Verileri Koruma Kanununa İlişkin Uygulama Rehberi." Erişim Tarihi: Şubat 19, 2020.

https://kvkk.gov.tr/SharedFolderServer/CMSFiles/41784a70-2bac-4e4a-830f-35c628468646.PDF.

Moral, Vefa Reşat ve Aşıkoğlu, İpek. "E-ticarette Kişisel Verilerin Korunması," Erişim Tarihi: Aralık 29, 2019. http://moral.av.tr/e-ticarette-kisisel-verilerin-korunmasi?l=null.

Oğuz, Habip. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum." *Uyuşmazlık Mahkemesi Dergisi*, no. 3 (2013): 1-38.

Oğuz, Sefer. "Kişisel Verilerin Korunması Hukukunun Genel İlkeleri." *Bilgi Ekonomisi ve Yönetimi Dergisi* 13, no. 2 (2018): 121-138

Özdemir, Hayrünnisa. Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması**.** Ankara: Seçkin Yayıncılık, 2009.

Paşaoğlu, Cengiz. "Kişisel Verilerin Korunması Kanunu Kişilerin Temel Hak ve Özgürlüklerini Korumak Amacındadır." Video, 32:13. *1.e-Safe Boğaziçi Kişisel Verileri Korumada Yerli Çözümler Zirvesi*. Yükleyen: e-Safe. Yükleme tarihi: Ağustos 25, 2019. Erişim Tarihi: Şubat 21, 2020. https://www.youtube.com/watch?v=e-M392izsks&ab_channel=e-Safe.

Sağlam Atabarut, İpek. "Elektronik Sözleşmeler." Doktora Tezi, İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2003.

Taşkaya, Merih ve Talay, Ömür. "Dijital Gözetimin Pazarlama Amaçlı Aracıları: 'Çerezler' ve Çerez Kullanımında 'Açık Rıza'". *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, no. 31 (2019): 356-376.

Yılmaz, Engin ve Karakadılar, İbrahim Sarper. "Türkiye'deki Elektronik Ticaret Uygulamalarına Müşteri Gözünden Bakış ve İyileştirme Önerileri." *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi* 6, no. 1 (2019): 53-75.

Taştan, Furkan Güven. *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*. İstanbul: On İki Levha, 2017.

Ticaret Bakanlığı. "İstatistikler." Erişim Tarihi: Nisan 30, 2021. https://www.eticaret.gov.tr/istatistikler.

TDK Sözlük, Erişim Tarihi: 18 Kasım 2019. https://sozluk.gov.tr/?kelime=.

Turan, Gamze. "Elektronik Sözleşmeler ve Elektronik Sözleşmelere Uygulanacak Hukukun Tespiti." *Türkiye Barolar Birliği Dergisi* 21, no. 77 (2008): 87-119.

Türkiye Büyük Millet Meclisi. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun Tasarısı ile Avrupa Birliği Uyum Komisyonu, Bayındırlık, İmar, Ulaştırma ve Turizm Komisyonu ile Sanayi, Ticaret, Enerji, Tabii Kaynaklar, Bilgi ve Teknoloji Komisyonu Raporları. Ankara: TBMM, 2011. https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss240.pdf.

Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu Tasarısı ve Adalet Komisyonu Raporu*. Ankara: TBMM, 2016. https://www.tbmm.gov.tr/sirasayi/donem26/yil01/ss117.pdf.

Türkiye Büyük Millet Meclisi. 2709 Sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun Teklifi ve Anayasa Komisyonu Raporu. Ankara: TBMM, 2010. https://www.tbmm.gov.tr/sirasayi/donem23/yil01/ss497.pdf