ISSN: 2667-5676 e-ISSN: 2667-6109

BİLİŞİM HUKUKU DERGİSİ

(ASBÜ BHD)

Cilt: 1 Sayı: 2 Aralık-2019
Vol.: 1 no.: 2 December-2019

ADALET YAYINEVİ
Ankara - 2019

BİLİŞİM HUKUKU DERGİSİ
(ASBÜ BHD)

ISSN: 2667-5676 **e-ISSN:** 2667-6109
Cilt: 1 Sayı: 2 **Vol.: 1 no.: 2**
Aralık-2019 **December-2019**

Dergi İletişim Bilgileri / ASBU BHD 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

YAYINA HAZIRLAYAN
Adalet Yayınevi
Strazburg Caddesi No: 10/B Sıhhiye-Ankara
Tel: (0312) 231 17 00 Fax: (0312) 231 17 10
www.adalet.com.tr

Baskı
Ay-bay Kırtasiye İnş. Gıda Paz. ve Tic. Ltd. Şti.
Sertifika No: 33365
Tel: (0 312) 472 58 55 - Ankara

Basım Tarihi:
Ocak, 2020

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 yukarıdaki 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.
4. 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. Eğer 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 FORM

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. Abstract 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.

- **False:** ... given[1]. **True:** ... 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 aptly *writing form rules* of the Journal, please see at http://dergipark.org.tr/download/journal-file/14917

Spelling and Footnotes Rules

1. The works should be prepared aptly the spelling and orthographic rules of Turkish Language Association. See at http://tdk.gov.tr/
2. " The Chicago Manual of Style" is accepted for footnotes and bibliography. For further information please see at

https://librarybestbets.fairfield.edu/citationguides/chicagonotes-bibliography#BookwithTwoorThreeAuthors

https://www.chicagomanualofstyle.org/book/ed17/frontmatter/toc.html

İÇİNDEKİLER / CONTENTS

MAKALE BÖLÜMÜ

ÇEVİRİ BÖLÜMÜ

MAKALE
BÖLÜMÜ

ELEKTRONİK PARAYA İLİŞKİN AVRUPA BİRLİĞİ VE TÜRK DÜZENLEMELERİ*

European Union and Turkish Regulations on Electronic Money

Abdüssamed KAHRAMAN**

Öz

Geçtiğimiz 40 yılda paralar kâğıt hallerinden yavaşça soyutlanarak dijitalleşmeye başlamıştır. Banka hesaplarındaki rakamlardan ibaret paralar elektronik kartlar aracılığıyla kullanılmaya başlanmıştır. Bu akımla beraber ortaya çıkan elektronik para da günümüze kadar işlerliğini artırmıştır. Elektronik para hususunu düzenlemek adına ülkemizde kısa zaman önce yasalaştırma çalışmaları yapılmış ve konuya ilişkin kanun, yönetmelik ve tebliğler çıkarılarak hukukî altyapı oluşturulmuştur. Makalenin amacı ülkemizdeki ve Avrupa'daki düzenlemeler bağlamında henüz yeni sayılabilecek elektronik para kavramını inceleyerek mahiyetini açıklamaktır.

Anahtar Kelimeler: Para, Elektronik Para, Ödeme Sistemleri, Türkiye Cumhuriyet Merkez Bankası, Bankacılık Düzenleme ve Denetleme Kurumu.

Abstract

Couple of decades ago money have begun to digitalize. Money, which is no longer a concrete material but a number of digits on

---

* Bu makale yazarın "Türk Ve Avrupa Birliği Düzenlemeleri Işığında Elektronik Para" adlı yüksek lisans tezinden türetilmiştir.

** Avukat, Bursa Barosu, Bursa, Türkiye. av.kahramanabdussamed@gmail.com, ORCID: 0000-0001-7244-7563.

Makale Gönderim Tarihi: 24.07.2019.

Makale Kabul Tarihi: 16.12.2019.

bank accounts, is used by electronic cards. Electronic money has emerged in this flow and got people's interest in a short time. To regulate electronic money, legislation efforts has been started years ago and law, regulation, communiqués have been made and legal infrastructure of the concept have been constituted. Purpose of this article is to examine the relatively new concept of electronic money through both national legislations and European Union Directives.

Keywords: Money, Electronic Money, Payment Systems, Central Bank of Republic of Turkey, Banking Regulation And Supervison Agency.

I. GİRİŞ

Elektronik paranın ortaya çıkıp çeşitli avantajları[1] nedeniyle yaygınlaşması ve Avrupa'da kullanılmaya başlanmasıyla birlikte hukukî düzenleme hususu tartışılmaya başlanmıştır. Bazı çevrelerce, henüz gelişimini tamamlamamış bir sistemin hukukî açıdan düzenlenmesi ile potansiyelinin zedelenebileceği, bu sebeple gelişiminin önleneceği endişesi ile hukukî düzenleme için erken olduğunu savunulmuştur.[2] Bununla birlikte hukukî düzenlemenin kavrama olumlu biçimde etki edeceği ve kullanımını artıracağını öne sürenler de mevcuttur. Amerikan uygulaması, hukukî düzenlemeyi erteleyerek sistemin gelişimine müdahale etmemek şeklinde olurken, Avrupa uygulaması ise sistemin düzenlenerek hukukî altyapısının ve güvenilirliğinin sağlanması şeklinde olmuştur.

Türkiye uygulaması ise hem pratikte hem de hukukî düzenleme açısından gerek Avrupa gerekse Amerika Birleşik Devletleri(ABD) uygulamalarını çok geriden takip etmektedir. Öncelikle, bankaların sanal kart uygulamalarını bir kenara koyarsak, hukukî düzenleme

---

1 Elektronik paraya ilişkin temiz olması, hızlı olması, uzaktan alışverişe imkân sağlaması gibi diğer tüm avantajları bir yana konulsa dahi elektronik para kullanımıyla yapılacak tasarruf dahi çok büyük düzeydedir. Yapılan bir çalışmaya göre İngiltere, Almanya, Fransa, İtalya ve İspanya'da elektronik para kullanımı sebebiyle yapılan tasarruf yıllık 60 milyar dolara kadar çıkmaktadır. Bu konuda ayrıntılı bilgi için, bkz. Erdoğan Ekşioğlu, "Elektronik Para Kullanımının Ekonomik Etkileri (Türkiye Üzerinde Bir Uygulama)" (Doktora Tezi, Sivas: Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü, 2017), 109.

Nakitten kartlı kullanımlara geçişin senede ortalama %5 artmasıyla kayıt dışı ekonomide düşüş ve maliyetlerin azalması nedeniyle 3 sene içerisinde Türkiye ekonomisinde 40 milyar TL'nin üzerinde kazanç oluşturacağına yönelik çalışmalar mevcuttur. Bu konuda ayrıntılı bilgi için, bkz. Ceyhun Elgin, Refik Erzan ve Umut Kuzubaş, *Türkiye'de Nakit ve Kart Ödemelerinin Karşılaştırmalı Maliyeti* (İstanbul: Boğaziçi Üniversitesi Ekonomi ve Ekonometri Merkezi, 2013), 22, https://newsroom.mastercard.com/eu/files/2015/06/MasterCard-Arastirma-NakitsizYasam-131013.pdf.

2 Malte Krueger, "Innovation and Regulation -The Case of e-Money Regulation in the EU- Background Paper No. 5 Electronic Payment Systems Observatory (ePSO)," *Sevilla: Institute for Prospective Technological Studies*, 12 Ocak 2002, 21, http://www.paysys.de/download/Krueger%20e-money%20regul.pdf.

öncesi herhangi bir elektronik para uygulamasından söz etmek mümkün değildir. Türkiye'de hukukî düzenlemeler, 2000 yılında ilk elektronik para direktifini yürürlüğe koyan Avrupa Birliği(AB) Direktifleri örnek alınarak hazırlandığı halde 2009 yılında yürürlüğe giren ikinci elektronik para direktifinden de sonra, ancak 2013 yılında gerçekleştirilmiştir.

II. HUKUKİ DÜZENLEMELERİN GENEL TANITIMI

A. Avrupa Birliği Düzenlemeleri

90'lı yıllarda Avrupa'da kullanılmaya başlanan elektronik para 2000 yılı itibariyle 2000/46/EC numaralı AB direktifi ile düzenlenmiştir. 2009 yılındaki 2009/110/EC numaralı AB direktifi ile 2000 yılındaki 2000/46/EC numaralı AB direktifi ilga edilmiştir. Bu düzenlemelerde elektronik para gelişimine önayak olmak ve sistemi kontrol altında tutarak zafiyetleri önlemek çabası ön plandadır. Elektronik para uygulamaları Avrupa'da olduğu kadar yaygın olmayan ABD'de, düzenlemelerde bekle ve gör politikası hâkim olup ağır düzenlemelere girilmemiştir.[3] Bununla birlikte elektronik para, ABD'de gerek yerel gerek federal düzeyde bazı düzenlemelere tâbi tutulmuştur.

1994 yılında Elektronik Para Kurumu'nun (Electronic Money Institution-EMI) hazırladığı rapora göre yalnızca kredi kurumları elektronik para çıkarma yetkisine sahipti. 1994'te hazırlanan bu raporda merkez bankalarının elektronik para üzerindeki rolü de tartışılmış ve beş senaryo üzerinde durulmuştur. Bunlardan birincisi: merkez bankalarının elektronik paraya hiçbir şekilde müdahale etmemesi; ikincisi, ihraç eden kurumlar üzerinde herhangi bir kısıtlama olmamakla beraber merkez bankalarının gözetiminde olmaları; üçüncüsü, merkez bankaların ihraç eden kuruluşlar ile rekabet halinde kendi elektronik cüzdanlarını çıkararak mevcut altyapılarını bu sistemleri yaymak için kullanmaları; dördüncüsü, merkez bankalarının münhasıran elektronik para altyapısı

[3] 1998'de yayınlanan Avrupa Merkez Bankası'nın raporunda bekle ve gör politikasının neden olabileceği sonuçlar belirtilerek erken hukukî düzenleme desteklenmiştir. Bu konuda ayrıntılı bilgi için, bkz. Krueger, "Innovation," 19.

sunması gerektiğidir. Nihayet kabul edilen senaryo ise elektronik paranın kredi kuruluşları tarafından çıkarılması gerektiği ve bu kredi kuruluşlarının özellikle likidite bağlamında merkez bankalarınca denetlenmesi gerektiği şeklindedir. Diğer senaryolar gerek merkez bankalarına büyük sorumluluklar yüklemesi gerekse uzun vadede takibinin imkânsız hale gelmesi sebebiyle mantıksız bulunmuştur.[4]

Avrupa Birliği, düzenleme hususundaki politikasını, akıllı kart teknolojisindeki liderliğini elektronik para hususunda da korumak için 'şeffaf düzenlemelerle hukukî çerçeveyi oturtarak gelişime önayak olmak' olarak belirlemiştir.[5] Şu anda AB ülkelerinde elektronik para kullanımının diğer ülkelere nazaran daha yaygın olduğu göz önünde bulundurulduğunda, benimsenen politikanın olumlu sonuç verdiği düşünülebilir.

Elektronik para hususunda tüm AB ülkelerini kapsayan tek bir düzenlemenin varlığı iki açıdan önemlidir. Birincisi, farklı ulusal düzenlemeler elektronik paranın tam potansiyeline ulaşacak şekilde gelişmesini engelleyebilir. İkincisi, elektronik para kuruluşlarını denetleyen kuruluşların, daha üst kurumlarca denetlenmesi sağlanarak pratikte farklı uygulamaların önüne geçilebilir.[6] AB'de ilk olarak 2000/46/EC numaralı AB direktifi ile düzenleme altına alınan elektronik para hususu ardından 2005/60/EC ve 2006/48/EC numaralı AB direktifleri ile birkaç noktada değiştirilmiş akabinde 2009/110/EC numaralı AB direktifi ile yeni baştan düzenlenmiştir. Bu direktiflere sırasıyla baktığımızda;

---

4 Yuksel Gormez ve Forest Capie, *Prospects for Electronic Money: A US-European Comperative Survey* (Ankara: The Central Bank of Turkey, 2003), 9, https://mafiadoc.com/the-central-bank-of-the-republic-of-turkey-tcmb_59f5e4201723ddb3267d72d4.html.

5 Krueger, "Innovation," 15.

6 Phoebus Athanassiou ve Natalia Mas-Guix, "Electronic Money Institutions (Current Trends, Regulatory Issues and Future Prospects)," *European Central Bank Legal Working Paper Series*, Temmuz 2008, 31, https://www.ecb.europa.eu/pub/pdf/scplps/ecblwp7.pdf?21a28d70b208180883a898dad73451c4.

1. 2000/46/EC[7]

Avrupa Para Enstitüsü'nün hazırladığı rapora göre elektronik para ihracı yalnızca kredi kuruluşları tarafından yapılmalıdır.[8] Çünkü bu; perakende ödeme sistemlerinin kontrol altında tutulmasını sağlayacak, kullanıcıları ihraç edenlerin hatalarından koruyacak, bir para politikası üretmeyi kolaylaştıracak ve ihraç edenler arasında adil rekabeti sağlayacaktır.[9] Bu bağlamda bu direktifte elektronik para kuruluşları da kredi kuruluşlarından sayılmışlardır.[10]

Direktifle getirilen düzenlemelerin ulusal kanunlara aktarılması çok hızlı gerçekleşmemiştir. Direktifin bazı konularda yeterince açıklık getirmediği veya sınırlayıcı olduğu düşünüldüğünden direktiflerin iç hukuka aktarılması zaman almıştır.[11] Yine direktif elektronik para kuruluşları açısından da yeterli ilgiyi görmemiştir. Yalnızca birkaç elektronik para kuruluşu lisans almıştır. Birlik genelinde tek pasaport ilkesi denilen tek ülkeden alınan yetki ile tüm üye ülkelerde işlem yapabilme hakkından yararlanabilen elektronik para kuruluşu ise yalnızca üç tanedir.[12]

---

7 "Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions," EUR-Lex, erişim tarihi 9 Nisan 2018, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0046&from=EN.

8 Elektronik para çıkaracak kurumların belirli bir güveni haiz kuruluşlar olması gerektiğinden bahisle bu işin kredi kuruluşları tarafından yapılması gerektiği gibi bir görüş mevcut olmakla birlikte bu durumun rekabeti baltalayacağı ve toplumun yararına olmayacağı dolayısıyla kredi kuruluşları haricindeki kurumlara da elektronik para çıkarma yetkisi verilmesi gerektiği şeklindeki görüş daha çok kabul görmüştür. Bu konuda ayrıntılı bilgi için, bkz. Nurettin Öztürk ve Asuman Koç, "Elektronik Para, Diğer Para Türleriyle Karşılaştırılması ve Olası Etkileri," *Sosyal ve Ekonomik Araştırmalar Dergisi* 6, no. 11 (Haziran 2006): 235.

9 Athanassiou ve Mas-Guix, "Electronic Money," 13.

10 Krueger, "Innovation," 15.

11 Krueger, "Innovation," 17.

12 Mehmet Sıddık Yurtçiçek, "The Legal Nature of Electronic Money and the Effects of the EU Regulations Concerning The Electronic Money Market," *Law & Justice Review* V, no. 1 (Haziran 2013): 292.

Söz konusu direktifin yapılma amacı, başlangıç bölümünün dördüncü ve beşinci fıkralarında belirtildiği üzere, Avrupa Birliği ülkeleri arasında elektronik para düzenlemeleri açısından teknolojik gelişmelerin önünü tıkamamak ve elektronik paranın gelişmesine destek olmaktır. Elektronik para konusunda kullanıcıların korunması için elektronik para kuruluşlarının tanınma, yetkilendirilme ve ihtiyatî denetiminin gerekliliği üzerine bu düzenleme yapılmıştır.

27 Ekim 2000'de oluşturulan direktif elektronik para kurumlarının ihtiyatî denetimi ve takibi üzerinedir. Söz konusu direktif 18 fıkralık bir başlangıç bölümü ile başlar. Bu kısmın başında, direktif için alınan görüşler ve taslakları belirtilir. Başlangıç kısmı direktife neden ihtiyaç duyulduğu ve direktifte yapılan düzenlemelerde dikkate alınan hususlardan oluşmaktadır. Direktif ile elektronik para kuruluşları ve kredi kuruluşları arasındaki rekabet dengesinin korunmasının amaçlandığı belirtilmiştir. Yine tek pasaport denilen tek ülkeden alınan yetki ile tüm üye ülkelerde işlem yapabilme hakkının tanınmasının, direktifin amaçlarından biri olduğu belirtilmiştir.

2. 2005/60/EC[13]

25 Kasım 2005'te oluşturulan bu direktif elektronik para hususunda yapılmış bir düzenleme değildir. Direktifin konusu, finansal sistemlerin kara para aklama ve terörizm finansmanında kullanılmasının önlenmesidir.[14] Söz konusu direktifin 11. maddesinin 5. fıkrasının (d) bendi elektronik para ile ilgilidir. Mezkûr hükme göre, tekrar şarj olamayan cihazlarda saklanabilecek en yüksek elektronik para miktarı 150 avro ile sınırlandırılmıştır. Şarj olabilen cihazlarda

---

13 "Directive 2005/60/Ec of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing," EUR-Lex, erişim tarihi 9 Nisan 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri= CELEX: 32005L0060&from=EN.

14 Elektronik parada anonimliğin kara para aklama hususunda kullanılabileceği ve bu hususta devletin kontrolünü zayıflatabileceği de pek çok yazar tarafından ifade edilmiştir. Bu konuda ayrıntılı bilgi için, bkz. George Farrugia, "Money Laundering in Cyberspace," 6, erişim tarihi 17 Aralık 2017, https://fiumalta.org/library/PDF/ml_cyberspace.pdf.

ise bir takvim yılı içerisinde işleme konu olabilecek toplam miktar en fazla 2500 avrodur. Elektronik para hesabından bu süre zarfında 1000 avro ve daha fazla para çekilmiş olması durumu istisna tutulmuştur. Düzenleme anonimlik imkânı sunan elektronik paranın,[15] kara para aklama ve terörizmi finanse etme yolu olarak kullanılması ihtimalini ortadan kaldırmak yahut bu ihtimali verimsiz ve zor hale getirmek üzere yapılmıştır.[16]

3. 2006/48/EC[17]

30 Haziran 2006'da yapılan bu direktif kredi kuruluşları ile alakalı düzenlemeler yapmak üzere hazırlanmıştır. Söz konusu direktifin kredi kuruluşlarını tanımlayan 4/1(b) maddesinde elektronik para kuruluşları da kredi kuruluşu sayılmıştır. Ancak bu hüküm 2009/110/EC numaralı direktif ile yürürlükten kaldırılarak, elektronik para kuruluşlarına nevi şahsına münhasır/sui generis bir hüviyet atfedilmiştir.

4. 2009/110/EC[18]

2009/110/EC numaralı AB direktifinde hükümler dört ayrı başlık altında düzenlenmiştir. Bu başlıklar; kapsam ve tanımlar adı altında birinci başlık, elektronik para kuruluşlarının ihtiyatî denetim

---

15 Anonimlik oranı yüksek olan elektronik paralar kara para aklama işlemine daha çok imkân tanımaktadır. Bu konuda ayrıntılı bilgi için, bkz. Leyla Keser Berber, *İnternet Üzerinden Yapılan İşlemlerde Elektronik Para ve Dijital İmza* (Ankara: Yetkin, 2002), 109.

16 Elektronik paranın kara para aklamada kullanılması ile alakalı yöntemler ve çözüm önerileri için, bkz. U.S. Congress-Office of Technology Assessment. *Information Technologies For The Control Of Money Laundering* (Washington, DC: U.S. Government Printing Office, Eylül 1995) 1*ff.*

17 "Dırective 2006/48/Ec of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast)," EUR-Lex, erişim tarihi 9 Nisan 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0048&from=EN.

18 "Dırective 2006/48/Ec of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC," EUR-Lex, erişim tarihi 9 Nisan 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0110&from=EN.

ve takibi için gereklilikler adı altında ikinci başlık, elektronik paranın ihracı ve paraya çevrilebilirliği adı altında üçüncü başlık ve son hükümler ve uygulama tedbirleri adı altında dördüncü başlık olacak şekilde düzenlenmiştir.

10.10.2009'da oluşturulan bu direktif elektronik para kurumlarının ihtiyatî denetimi ve takibi üzerine olan ikinci direktiftir. 2000/46/EC numaralı AB direktifi ile beklenen olumlu etki oluşmadığı ve direktifin bazı hususlarda getirdiği ağır yükümlülükler, elektronik para kuruluşlarınca sağlanamadığı ve eleştirildiği için yeni bir direktife ihtiyaç duyulmuştur. Söz konusu direktif 28 fıkralık bir başlangıç bölümü ile başlar. Bu bölümün başında direktif için alınan görüşler ve taslakları belirtilir. Başlangıç bölümünün ilk iki fıkrası da direktifin çıkması için gerekli şartların oluştuğunu belirtmektedir. Buna göre, 2000/46/EC numaralı AB direktifi yeni ortaya çıkan ön ödemeli elektronik ödeme sistemlerine yasal bir çerçeve kazandırmak ve pazarı bir ihtiyatî denetim altına alırken aynı zamanda güçlendirmek için kabul edilmiştir. Ancak getirilen düzenlemeler incelendiğinde, bazı hükümlerin elektronik paralar için gerçek manada tek piyasa oluşumunu ve kullanıcı dostu yeni hizmetler getirilmesini engelleyici unsurlar içerdiği saptanmıştır.

Söz konusu direktifin başlangıç bölümünün 15. fıkrasında, birlik dışında kalan elektronik para kuruluşlarının üye ülkelerde yer alan ortak düzenlemelerden faydalanamayacağı belirtilmiştir. Mezkûr direktifin başlangıç bölümünün son hükümlerinde 2000/46/EC numaralı direktifin ilgası ve uyumun sağlaması için yapılması gerekenler sıralanmıştır. Bu hükümlerden 26. fıkrada söz konusu direktif hükümlerinin 2000/46/EC numaralı direktifin hükümleri yerine geçeceğinden, ilgili direktifin ilga edildiği belirtilmiştir. Bu, direktifin 21. maddesi ile de hüküm altına alınmıştır. 2009/110/EC numaralı AB direktifinin 27. fıkrasında ise düzenlemenin uyum içerisinde yürütülmesi gerektiğinden ve üye ülkelerin yerel düzenlemelerinin birbirinden farklı olması sebebiyle Birlik düzeyinde bunun çözümlenemeyeceğinden ötürü, Birliğin bu konuda gerekli tedbirleri almaya yetkili olduğu ancak orantılılık ilkesi gereğince bu düzenlemenin hedefleneni yerine getirmenin ötesinde bir düzenleme yoluna

gitmeyeceği açıklanmıştır. Başlangıç bölümünün son maddesinde ise üye ülkelerin gerekli uyumu sağlamak adına düzenlemelerini bu direktife uygun şekilde yapmaları gerektiği ifade edilerek uyum konusundaki önem belirtilmiş ve bu husus mezkûr direktifin 16. maddesi ile de hükme bağlanmıştır.

2009/110/EC numaralı AB direktifi ile 2000/46/EC numaralı AB direktifindeki birçok husus değiştirilmiştir. Bunların en başında elektronik para kuruluşlarının kredi kuruluşu olarak tanımlanmamaları gelir. Elektronik para kuruluşlarının kredi kuruluşu olarak tanımlanmaları, elektronik para kuruluşlarına karşılaşacakları risklerden çok daha büyük yükümlülükler yükleyerek, bu kuruluşların verimli bir şekilde çalışmasının önüne geçmekteydi. Paraya çevrilebilirlik hususunda elektronik para kuruluşunun lehine olan minimum paraya çevrilebilecek miktar uygulaması, elektronik para kullanıcıları lehine kaldırılmıştır. Paraya çevrilebilirlik hususunda kullanıcıların güvenini sağlamak adına bu şekilde bir düzenleme yoluna gidilmiştir. Bunlarla birlikte muafiyet, toplanan fonların mevduat teşkil etmemesi ve herhangi faiz yahut fayda temininin söz konusu olmayacağı, minimum sermaye yükümlülükleri, müsavi işleyiş oluşturma amacı ve uyum hususlarına önceki direktifte olduğu gibi yüksek önem atfedilmiştir.

B. Türkiye Düzenlemeleri

Elektronik paraya ilişkin ulusal düzenlemelerimiz Avrupa Birliği düzenlemelerine nazaran daha geç gerçekleşmiştir. AB'de 90'lı yılların ortasından itibaren düzenleme hususu konuşulmaya ve üzerinde çalışılmaya başlanmıştır. Yine AB çapında ilk düzenleme 2000 yılındaki direktif ile gelmiştir. Bununla birlikte AB'de bu tarihten önce de çalışan birçok elektronik para uygulaması mevcut idi.[19] Ancak Türkiye'de düzenlemenin öncesinde bankaların ürettiği sanal

[19] 90'lı yılların başında ortaya çıkan Proton, Danmont ve Mondex Avrupa'daki ilk kuşak elektronik paraları oluşturmaktadır. Bu konuda ayrıntılı bilgi için, bkz. "Electronic Money and E-money Institutions," Association of E-money Institutions in the Netherlands, 5, erişim tarihi 17 Aralık 2017 https://www.simonl.org/docs/empp1511.doc.

kartlar, ulaşım ve iletişimde kullanılan ön ödemeli kartlar haricinde ciddi bir çalışma söz konusu değildi. 6493 sayılı kanun öncesinde Türkiye'de resmi bir elektronik para kuruluşu da mevcut değildi.[20]

Hâlihazırda elektronik paraya ilişkin Türkiye'deki yasal düzenlemeler şunlardır:

- 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun,
- Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik,
- Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ.[21]

1. 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun

Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun Türkiye'de elektronik para hakkında yapılan ilk düzenlemedir. Söz konusu kanun, 20 Haziran 2013'te kabul edilmiş ve 27 Haziran 2013'te Resmi Gazetede yayınlanmıştır. 43 madde ve 2 geçici maddeden müteşekkil olup elektronik para kuruluşları haricinde ödeme ve menkul kıymet mutabakat sistemleri ve ödeme hizmetleri ile alakalı hükümler de içermektedir. Kanunun hazırlanmasında yukarıda mezkûr AB direktiflerinden faydalanılmıştır.

6493 sayılı kanunun 3. maddesinin 1. fıkrasının (v) bendine göre göre ödeme sistemleri; "*üç veya daha fazla katılımcı arasındaki transfer emirlerinden kaynaklanan fon aktarımlarının gerçekleştirilmesini sağlamak*

---

[20] 18.12.2019 tarihi itibariyle Türkiye'de 17 adet yetkilendirilmiş elektronik para kuruluşu mevcuttur. Elektronik para kuruluşları listesi için, bkz. "Elektronik Para Kuruluşları," BDDK, erişim tarihi 18 Aralık 2019, https://www.bddk.org.tr/Kuruluslar-Kategori/Elektronik-Para-Kuruluslari/7.

[21] Ödeme Kuruluşları ve Elektronik Para Kuruluşlarının Bilgi Sistemlerinin Yönetimine ve Denetimine İlişkin Tebliğ'de ödeme kuruluşları ve elektronik para kuruluşlarının bilgi sistemlerinin yönetimi ve denetimine ilişkin düzenlemeler yapılmış olup teknik yanı itibariyle çalışmamızın kapsamı dışında kalmaktadır.

amacıyla yapılan takas ve mutabakat işlemleri için gerekli altyapıyı sunan ve ortak kuralları olan yapıdır". Elektronik para da üç taraftan oluşan bir çalışma prensibine sahiptir. Bu taraflardan birincisi elektronik parayı ödeme aracı olarak kullanan ve aldığı ürüne karşılık bir miktar elektronik para veren kişi; ikincisi elektronik parayı verdiği ürüne karşılık olarak kabul eden kişi; üçüncüsü ise birinci kişiden aldığı fon karşılığı ihraç ettiği[22] elektronik para için tuttuğu bedeli ikinci kişiye vermek yükümünde olan elektronik para kuruluşudur.[23]

Bu kanunun elektronik paraya ilişkin hükümleri, tanımları havi 3. maddesinde başlar. Söz konusu maddede doğrudan elektronik para hususu ile alakalı olarak; elektronik para, elektronik para kuruluşu ve fon tanımlamaları yer almaktadır.

Mezkûr maddenin (ç) bendine göre, Elektronik para, "Elektronik para ihraç eden kuruluş tarafından kabul edilen fon karşılığı ihraç edilen, elektronik olarak saklanan, bu (6493 sayılı) Kanunda tanımlanan ödeme işlemlerini gerçekleştirmek için kullanılan ve elektronik para ihraç eden kuruluş dışındaki gerçek ve tüzel kişiler tarafından da ödeme aracı olarak kabul edilen parasal değeri (ifade eder.)" şeklindedir. Daha önce bahsettiğimiz üzere bu tanım elektronik paranın taşıması gereken beş unsura işaret etmektedir. Elektronik paranın taşıması gereken bu unsurlar; yetkili kuruluş tarafından ihraç, fon karşılığı ihraç, elektronik olarak saklanma, ödeme işlemi gerçekleştirme ve ihraç eden dışındaki kişilerce tanınma şeklinde ifade edilebilir.

6493 sayılı kanunun 3. maddesinin (d) bendinde, elektronik para kuruluşu, yetkilendirilme kıstas alınarak "(Bu) Kanun kapsamında elektronik para ihraç etme yetkisi verilen tüzel kişiyi (ifade eder.)" şeklinde tanımlanmıştır. Bu tanımlama AB düzenlemelerin-

---

22 Bu bağlamda elektronik para ödemenin önden yapıldığı bir ödeme sistemidir. Bu konuda ayrıntılı bilgi için, bkz. Gabriele Kabelac, "Cyber Money as Medium of Exchange," *Deutsche Bundesbank Discussion Paper Series*, no. 1999,05E (Ekim 1999): 5, https://papers.ssrn.com/sol3/Delivery.cfm/107192.pdf?abstractid=2785816&mirid=1.

23 Jerry Gao, "Electronic Cash Payment Protocols and Systems," erişim tarihi 17 Aralık 2017. http://www.dmi.unipg.it/bista/didattica/sicurezza-pg/sistemi-pagamento/ e-cash-payment.v1.10.20.pdf.

de biraz farklı bir işlev taşımaktadır. Çünkü AB düzenlemelerinde elektronik para kuruluşları, elektronik para ihraç eden kuruluşların bir türü olarak tanımlanmış ve elektronik para ihraç eden kuruluşlar adlı daha geniş bir grup düşünülmüştür. Bu gruba kredi kuruluşları, posta havale ofisleri gibi kurumlar da dâhildir. Hâlbuki bu madde bağlamında ileride incelenecek olan ve ihraç eden kuruluşlar kapsamına dâhil olan bankalar ve PTT de elektronik para kuruluşu olarak tanımlanmaktadır. Bu husus da uygulamada ilgili kuruluşların elektronik para kuruluşlarının tabi oldukları yükümlülüklere tabi olması gerektiği gibi gereksiz bir sonuç ortaya çıkarabilir. Aynı kanunun fon kavramını tanımlayan (e) bendinde elektronik paralar da fon kapsamına dâhil edilmiştir.

Kanunda 13. maddenin birinci fıkrasında ödeme hizmeti sağlayıcıları tanımlanmıştır. Ödeme hizmeti sağlayıcıları tanımlanırken (b) bendinde elektronik para kuruluşlarının da ödeme hizmeti sağlayıcılarından olduğu belirtilmiştir.

Söz konusu kanunun beşinci bölümü elektronik para kuruluşları ve elektronik para ihracı başlıklı olup üç maddeden oluşmaktadır. Kanunun 18. maddesi elektronik para ihraç eden kuruluşlar başlıklıdır. Buna göre; bankalar, PTT A.Ş. ve bu kanun bağlamında yetkilendirilen kuruluşlar dışındaki kişilerin elektronik para ihracı faaliyetinde bulunmaları yasaktır. Bu madde de AB düzenlemelerine yakın bir kapsam içerse de, AB düzenlemelerinde merkez bankaları ve devletlerin kendisinin de elektronik para ihracı yapabilecekleri özellikle belirtilmiştir. Bu bakımdan AB düzenlemeleri ile ulusal düzenlemelerimiz arasında farklılık olduğu aşikârdır. Bu maddenin ikinci fıkrasında ise elektronik para kuruluşlarının Bankacılık Düzenleme ve Denetleme Kurulu'ndan izin almak suretiyle hizmette bulunabileceğine yer verilmiştir.

2. Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik[24]

Elektronik para hakkında AB direktifleri, 6493 sayılı Kanun'daki düzenlemelere nazaran daha geniştir. Mezkûr kanunda

[24] RG. 27.06.2014, S. 29043.

direktifler doğrudan hüküm olarak ihdas edilmemiş bazı alanlar yönetmelik ile düzenlenmiştir. Bu bağlamda Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmelik, 6493 sayılı kanunda düzenlenmemiş ilgili alanları kapsayacak niteliktedir.

Söz konusu yönetmelik de kanun gibi tanımlar bölümüyle başlamaktadır. Tanımlar bölümünde elektronik paraya ilişkin tanım 6493 sayılı Kanun'dakinin aynısı iken, elektronik para kuruluşları tanımı bakımından AB direktiflerine uygun olarak elektronik para ihraç eden kuruluşlar ve elektronik para kuruluşları şeklinde bir ayrıma gidilmiştir. Bu hususun düzenlenmesi yerinde olmuştur. Ancak yine de düzenleme direktifte belirlenen şekilde yapılmamıştır. Elektronik para ihraç eden kuruluşlara PTT eklenmemiş ve elektronik para kuruluşları da elektronik para ihracına yetki verilen tüzel kişiler olarak düzenlendiğinden elektronik para ihraç eden kuruluşlar da birer elektronik para kuruluşu imiş gibi bir algı oluşturulmuştur. Bu sebeple 6493 sayılı kanunda elektronik para kuruluşları ile elektronik para ihraç eden kuruluşlar, olması gerektiği gibi farklı iki küme olarak tanımlandıysa da yönetmelikte bu ayrım net bir şekilde ortaya konamamış elektronik para ihraç eden kuruluşlar ile elektronik para kuruluşları aynı şeylermiş gibi algı oluşturabilecek bir düzenlemeye gidilmiştir. Bunun sakıncası ise elektronik para kuruluşlarına uygulanacak yükümlülüklerden muaf olacak PTT ve bankaların bu yükümlülüklere tabi tutulması olabilir.

III. HUKUKİ DÜZENLEMELERDE ÖNE ÇIKAN HUSUSLAR

Gerek Türkiye gerekse AB hukuki düzenlemelerinde öne çıkan elektronik paraya ilişkin ortak unsurlar vardır. Bunlar elektronik para konusunda üzerinde tartışmalar olan hususlar olarak da karşımıza çıkmaktadır. Bu hususlar; paraya çevrilebilirlik, ihtiyatî denetim, muafiyet, mevduat teşkil etmeme. Hukuki düzenlemeler yürürlüğe girdiğinde önceden kurulmuş elektronik para kuruluşlarının bundan nasıl etkilenecekleri de geçici düzenlemelerin önemini artırmaktadır.

A. Paraya Çevrilebilirlik

Paraya çevrilebilirlik ilkesi, elektronik paranın temsili nitelikte olduğunu ortaya koymak ve elektronik para kuruluşlarının bu hususta kullanıcıları zarara uğratabilecek herhangi bir iş yapmalarını önlemek adına konulmuştur.[25] Gerek Türk Hukukunda gerekse AB düzenlemelerinde paraya çevrilebilirliğe ilişkin hükümler bulunmaktadır. Paraya çevrilebilirlik elektronik parayı gerçek paranın temsili haline getirmesi açısından önemlidir.

2000/46/EC numaralı AB direktifi, başlangıç kısmından itibaren paraya çevrilebilirliğe ilişkin değerlendirmeler bulundurmaktadır. Başlangıç kısmının 9. ve 10. maddelerinde belirtildiği üzere kullanıcının güveninin sağlanması paraya çevrilebilirlik ile mümkündür ve bu çevrilebilirlik de nominal değer üzerinden olmalıdır.

Aynı direktifin paraya çevrilebilirlik kenar başlıklı üçüncü maddesi, bu hususu ayrıntılı olarak düzenlemiştir. Bu maddede elektronik para kullanıcılarının, elektronik paraların fon karşılığını talep etmelerine ilişkin konular düzenlenmiştir.

Buna göre söz konusu maddenin ilk fıkrasında elektronik paranın geçerli olduğu süre boyunca paranın nakit karşılığının yahut belirtilen hesaba transferinin istenebileceği ve bunun için yalnızca transfer için gerekli ücretin talep edilebileceği bunun haricinde bir ücret talep edilemeyeceği belirtilmiştir.[26]

İlgili maddenin ikinci fıkrasında ise paraya çevrilebilirliğe ilişkin hususların sözleşmede özellikle belirtilmesi gerektiği düzenlenmiştir. Çekilebilecek minimum tutarın sözleşmede belirlenebileceği ancak bunun 10 avroyu geçemeyeceği üçüncü fıkrada belirtilmiştir. Bu minimum tutar, Danimarka'da 3,35 avro, İtalya'da ise 5 avroya kadar düşürülmüştür.[27]

---

25 Mehmet Sıddık Yurtçiçek, "Hukuki Açıdan Elektronik Para" (Doktora tezi, Marmara Üniversitesi, 2012), 154.

26 Bu madde; birinci maddede yer alan tanımın *"elektronik para kuruluşu tarafından kabul edilen ve karşılığında çıkarılacak elektronik paradan az olmayan fon karşılığı"* ibaresini tamamlayıcı niteliktedir. Bu konuda ayrıntılı bilgi için, bkz. Athanassiou ve Mas-Guix, "Electronic Money," 21.

27 Yurtçiçek, "Hukuki Açıdan Elektronik Para," 164.

2009/110/EC numaralı direktifte ise başlangıç kısmında kullanıcıları koruma ve nominal değer üzerinden çevrilebilirlik zikredildikten sonra minimum değer dayatmanın yanlış olacağı ve yapılan masrafların karşılığı bir ücret talep edilebileceği belirtilmiştir.

2009/110/EC numaralı direktifin 11. maddesi de paraya çevrilebilirliğe ilişkindir. İhraç ve paraya çevrilebilirlik başlıklı bu maddenin birinci fıkrasına göre, üye ülkeler elektronik para ihraç eden kuruluşların topladıkları fonların nominal değeri üzerinden elektronik para ihraç etmelerini sağlamalıdır. Ayrıca üye ülkeler elektronik para kuruluşlarının her an kullanıcıdan gelen talep üzerine elektronik paranın fon karşılığını vermesini sağlamalıdır. Elektronik para kuruluşu ve kullanıcısı arasında elektronik para kullanımına ilişkin yapılan sözleşmede paraya çevrilebilirlik hususu ve paraya çevirme ihtimalinde doğabilecek ücretler hakkında bilgi bulunmalıdır ve bu sözleşme söz konusu bilgi karşı tarafa aktarılmadan kurulmamalıdır.

Paraya çevrilme esnasında ücret talebi ancak 11. maddenin üçüncü fıkrasında belirtildiği üzere bunun sözleşmede geçmesi halinde mümkün olabilir. Kanun koyucu bunun üç farklı durumda nasıl gerçekleşeceğini belirtmiştir. Bu durumlar; *"sözleşme sona ermeden paranın geri istenmesi hali", "eğer sözleşmenin bir sonlanma tarihi var ve kullanıcı bundan önce sözleşmeyi sonlandırmışsa", "paraya çevrilmenin sözleşmenin sona ermesinden bir yıl sonra talep edilmiş olması halinde"* şeklindedir.

Bu durumlarda talep edilen ücret yalnızca yapılan masrafı karşılayacak uygun ve orantılı bir miktar olmalıdır. Sözleşmenin sona ermesinden önce talep edilen paraya çevirme paranın tamamına yahut bir kısmına yönelik olabilir. Eğer sözleşmenin sona ermesinin üzerinden bir yıl veya daha fazla süre geçtikten sonra paraya çevrilme talep ediliyorsa ancak paranın tamamı talep edilebilir kısmî paraya çevirme talep edilemez.

Elektronik para kullanıcısı değil de tüketici olmayıp elektronik para kabul eden kişinin paraya çevirme hususunda hakları elektronik para kuruluşu ile aralarındaki sözleşmeye göre belirlenir.

6493 sayılı Kanunda paraya çevrilebilirlik hususu şu şekildedir. Kanunun 20. maddesinin kenar başlığı elektronik para ihracıdır. Bu maddenin ilk fıkrası ile fon karşılığı ihraç hususu netleştirilerek, alınan fon kadar elektronik para ihracı yapılabileceği belirtilmiştir. 2000/46/EC numaralı AB direktifinin 1/3(b)ii maddesi de benzer hükmü muhtevidir.

Söz konusu maddenin ikinci fıkrasında ise yatırılan fonların gecikmeksizin elektronik paraya çevrileceği hususu ifade edilerek, elektronik para kullanıcıların gecikmeden kaynaklı muhtemel zararı önlenmek istenmiştir. 2000/46/EC numaralı AB direktifinde bu husus, md. 2/3'te *"derhal"* olarak ifade edilirken, 2009/110/EC numaralı AB direktifinde 6493 sayılı kanunumuzda geçtiği şekli olan "*gecikmeksizin"* ibaresiyle değiştirilmiştir. Bu husus, elektronik para karşılığında temin edilen fon için faiz ve herhangi bir fayda sağlanamayacağı hususuyla da yakın ilişki içerisindedir.

İlgili maddenin üçüncü fıkrasında elektronik para karşılığında toplanan fonların 5411 sayılı kanunda belirtilen bankalar nezdinde tutulacak hesapta bloke edileceği belirtilmiştir. Bu husus, elektronik para kuruluşlarının elektronik para ihracı işini yapmaktan elde edeceği faydayı ciddi anlamda ortadan kaldırmaktadır. AB düzenlemelerinde fonların ne şekilde kullanılabileceğine ilişkin ciddi yaptırımlar olmasına rağmen bu şekilde bir düzenleme 6493 sayılı kanunda yer almamaktadır. Bu husus elektronik para ihracı için toplanan fonun mevduat teşkil etmemesi ile de bağlantılıdır.

Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmeliğin yedinci maddesi elektronik paranın paraya çevrilebilirliği başlıklıdır. Bunun birinci fıkrasına göre talep üzerine paraya çevirme gecikmeksizin yerine getirilmelidir. İkinci fıkrada da belirtildiği üzere, paraya çevrilme sahip olunan elektronik paranın tamamına yönelik olabileceği gibi kısmî de olabilir. AB direktiflerinde bu husus sözleşmenin sona ermesinden önce ve sona ermesinden sonra şeklinde iki kısma ayrılarak ayrıca incelenmiştir. Ulusal düzenlemelerimizde bu şekilde geçmesi kullanıcı açısından daha olumlu olmuştur. Üçüncü fıkrada AB direktifleri ile uygun şekilde, fona çevirme ile

alakalı yükümlülük ve ücretlerin sözleşmede açıkça belirtilmesi gerektiği ifade edilmiştir. Fona çevirme ihtimalinde talep edilebilecek ücretler de AB düzenlemeleriyle ortak olarak sözleşmenin sona ermesinden önce, sözleşmede belirlenmiş son kullanma tarihinden önce yahut son kullanma tarihinin geçmesinin üzerinde bir sene ve daha sonra talep edilmesi halleri ile sınırlandırılmıştır. Yine AB düzenlemelerinde olduğu gibi ücret yapılan masrafla orantılı olmalıdır. Kullanıcının tüketici olmaması ihtimali de istisna tutulmuştur.

B. İhtiyatî Denetim

Elektronik para kuruluşlarının yedinde kullanıcılarına ait büyük miktarda para bulundurmalarından ötürü bir denetime tabi tutulmaları gerekliliği açıktır. Ancak yapılan düzenlemelerle getirilen denetimin, olması gerekenden çok daha ağır bir denetim öngördüğü doktrinde dile getirilmiştir.[28] Bizzat düzenlemelerde dahi bu husus yerini bulmuş ve 2009/110/EC numaralı AB direktifinde 2000/46/EC düzenlemesinde getirilen düzenlemelerin yerinde olmadığı, elektronik para kuruluşlarını olması gerekenden fazla kısıtladığı belirtilmiştir. İhtiyatî denetim elektronik para kuruluşlarını denetleyerek kullanıcıları korumak açısından önemli olmakla birlikte bunun için alınan önlemlerin elektronik para kuruluşları kârlılığını düşürdüğü açısından eleştirilmiştir.

Elektronik para kuruluşlarına ilişkin iki AB direktifi de elektronik para kuruluşlarının ihtiyatî denetimi ve takibi başlığını taşımaktadır. Elektronik para direktiflerinin amacı bu kuruluşlarının denetimini sağlamaktır.

2000/46/EC numaralı AB direktifin başlangıç kısmının 11. ve 13. fıkraları konuya ilişkin olarak iki maddede de elektronik para kuruluşları, kredi kuruluşları ile karşılaştırılmış ve bu bakımdan bir denetime ihtiyaç duyulduğu belirtilmiştir. 11. fıkrada denetimin hantal bir yapıda olmaması gerektiği belirtilmiştir.

---

[28] Krueger, yalnızca lisans zorunluluğun bile piyasaya girişi yeterince zorlayacağı bir piyasada sermaye ve özkaynak yükümlülüklerinin en iyi ihtimalde büyük firmaları zorlamasa bile küçük firmaların piyasaya girişini ciddi manada engelleyeceğini zikretmektedir. Bu konuda ayrıntılı bilgi için, bkz. Krueger, "Innovation," 20.

2000/46/EC numaralı AB direktifinin birinci maddesinin beşinci fıkrasına göre, elektronik para kuruluşlarının yapabileceği işlemlere birtakım sınırlar getirilmiştir. Fıkranın (a) bendinde elektronik para kuruluşları elektronik paranın ihracı ve yönetimi ile alakalı ve diğer ödeme sistemleri ihracı işleri ile uğraşabilirler ancak kredi sağlamak bu işlerden biri olamaz.[29] (b) bendine göre ise elektronik para kuruluşu diğer kuruluşlar adına veri saklama işi yapabilir. Ayrıca elektronik para kuruluşlarının diğer kuruluşlarda ortaklıklarının bulunması da mümkün değildir. İstisnası ise elektronik para ihracına ilişkin işleriyle alakalı kurumlardır. Bu sınırlandırmalar elektronik para kurumlarının banka hüviyeti kazanmaması için getirilmiş düzenlemelerdir. Düzenlemelerin aşırı olduğu ve elektronik para kuruluşlarının çalışma alanını çok daralttığı iddia edilmiştir.[30] Ancak düzenlemeler elektronik para kuruluşlarının istikrarını korumak amaçlıdır.[31]

2000/46/EC numaralı AB direktifinin altıncı maddesinde direktifin 4. ve 5. maddelerinde sıralanan başlangıç sermayesi, özkaynak yükümlülükleri ve yatırım sınırlamalarının kontrol süresi belirtilmiştir. Buna göre yılda en az iki kere kontrol yapılmalıdır. Bu kontrol elektronik para kuruluşlarının kendileri tarafından yapılabileceği gibi ilgili bilgilerin yetkili otoritelere gönderilmesi suretiyle yetkili otoritelerce de yapılabilir. Üye ülkelerden Polonya hariç tüm ülkeler yılda en az 2 kontrol hükmünü kabul etmişlerdir. Polonya'da yılda bir kontrolün yeterli olacağı şeklinde düzenleme yapılmıştır.[32] Bunun haricinde kontrolleri aylık seviyeye kadar çıkaran ülkeler söz konusudur.

Yine 2000/46/EC numaralı AB direktifinin yedinci maddesinin kenar başlığı sağlam ve ihtiyatlı işleyiştir. Bu maddeye göre elektronik para kuruluşlarının yönetim, idare ve muhasebesinin sağlam ve

---

29 Elektronik para kuruluşlarına mevduat toplama ve kredi verme imkânı olmadığından ötürü bankalara uygulanandan daha hafif yükümlülükler belirlenmiştir. Bu konuda ayrıntılı bilgi için, bkz. Athanassiou ve Mas-Guix, "Electronic Money," 15.

30 Krueger, "Innovation," 16.

31 Yurtçiçek, "Hukuki Açıdan Elektronik Para," 161.

32 Yurtçiçek, "Hukuki Açıdan Elektronik Para," 169.

ihtiyatlı prosedürlere tâbi olması ve yeterli iç kontrol mekanizmasına sahip olması gerekir. Bu kontrol mekanizmaları gerek finansal gerek finansal olmayan risklere cevap verebilecek nitelikte olmalıdır. Kendi faaliyet alanı ile bağlantı olarak operasyonel veya yardımcı işler yapan herhangi bir kuruluş ile yapılan işbirliğine ilişkinin teknik ve prosedürel riskler de buna dâhildir. Maddede elektronik para kuruluşunun işleyişinin sağlam olması, dolayısıyla elektronik para kullanıcılarına olan yükümlülüklerin yerine getirilmesi hususunda herhangi bir sorun çıkmaması adına bu şekilde düzenleme yapılmıştır.

2009/110/EC numaralı AB direktifinde ise 2000/46/EC numaralı AB direktifinde öngörülen denetimin ağırlığı başlangıç kısmının dokuzuncu fıkrasında zikredilmiştir. Buna göre, elektronik para kuruluşlarına yönelik ihtiyatî denetim hususu kurumların muhatap oldukları riskler göz önünde bulundurularak gözden geçirilip düzenlenmelidir. Bu düzenleme ödeme kuruluşlarına yönelik olarak düzenlenen 2007/64/EC numaralı AB direktifi ile uyumlu olmalıdır. Dolayısıyla belirtilen direktifin ilgili maddeleri mutatis mutandis(gereken değişiklikler göz önünde bulundurularak) elektronik para kuruluşlarına da herhangi bir önyargı olmadan uygulanmalıdır. Fıkranın devamında, belirtilen direktifteki bazı atıfların bu durumda nasıl anlaşılması gerektiği belirtilmiştir.

2009/110/EC numaralı AB direktifinin üçüncü ve yedinci maddeleri de ihtiyatî denetim için bazı yollar belirlemiştir. Genel ihtiyatî kurallar başlıklı üçüncü maddenin birinci fıkrasına göre, 2007/64/EC numaralı AB direktifinin 5, 10 ila 15, 17/7 ve 18 ilâ 25 maddeleri gereken değişiklikler göz önünde bulundurularak elektronik para kuruluşlarına da uygulanır. Belirtilen maddeler ödeme kuruluşlarının yetkilendirilme ve yetkisinin sürdürülmesine ilişkin düzenlemelerdir.

2009/110/EC numaralı AB direktifinin üçüncü maddesinin ikinci fıkrasına göre elektronik para kuruluşları elektronik para karşılığında topladıkları fonları değerlendirme biçimini değiştirdiği takdirde yetkili otoriteleri buna ilişkin bilgilendirmeleri gerekir. Önceki direktifte buna ilişkin bir düzenleme olmadığından elektronik para kuruluşlarının fon değerlendirmeleri açısından daha sıkı bir kontrole alındığı söylenebilir.

2009/110/EC numaralı AB direktifinin üçüncü maddesinin üçüncü fıkrasına göre elektronik para kuruluşlarının ortaklığına katılmak, ortaklığından ayrılmak, ortaklık payını artırmak veya düşürmek isteyen gerçek veya tüzel kişiler yetkili kurumları bu işlem ve bu işlemdeki amaçları ile alakalı bilgilendirmeleri gerekir. Teklif olunan alıcı gerekli bilgileri yetkili otoriteye sağlar. Yetkili otoriteler teklif olunan kişiyi uygun bulurlarsa görüşlerini bu şekilde açıklarlar. Teklif olunan kişi yetkililerce uygun bulunmazsa gerekli tedbirler alınarak işlem sonlandırılır. Bu tedbirler ilgili müdür ve yetkililere yönelik tedbir kararları veya yaptırımlar şeklinde olabileceği gibi söz konusu hisse sahibinin oy hakkının askıya alınması şeklinde de olabilir. Belirtilen bilgileri sağlamayan tüzel kişiler de aynı şekilde tedbirlere konu olabilirler. Eğer yetkili otoritenin itirazına rağmen işlem gerçekleşirse -alınacak diğer tedbirlerden bağımsız olarak- söz konusu hisse sahibinin oy hakkı askıya alınır ve hâlihazırda vermiş olduğu oylar geçersiz sayılır. Elektronik para kuruluşları tarafından elektronik para ihracı dışında yapılan işlerle alakalı olarak üye devletler yetkili otoriteleri bu fıkrada geçen önlemleri almaktan muaf tutabilirler. Önceki direktifte yer almayan ve elektronik para kuruluşlarının işleyişlerini sürdürmelerinde sorun oluşturabilecek ve dolayısıyla elektronik para kullanıcılarını zarara uğratabilecek bu husus düzenleme kapsamında denetim altına alınmıştır. Belirtilen önlemler ciddi yaptırımlar içermektedir.

Üye ülkeler elektronik para kuruluşlarına kendi adlarına elektronik para ihracı yapmaları için yetki verebilirler. Ancak bu durumda 2007/64/EC numaralı AB direktifinin 25. maddesinde öngörülen prosedüre uymaları gerekir.

2009/110/EC numaralı AB direktifinin üçüncü maddesinin son fıkrasına göre elektronik para kuruluşları acenteler üzerinden elektronik para ihracı yapamazlar. Ancak 2007/64/EC numaralı AB direktifinin 17. maddesinde tanımlanan şartlar sağlandığı takdirde 2009/110/EC numaralı AB direktifinin 6/1(a) maddesinde tanımlanan ödeme hizmetlerini acenteler üzerinden sunabilirler.

2009/110/EC numaralı AB direktifinin yedinci maddesine göre ise üye ülkeler elektronik para kuruluşlarının elektronik para ihracı

neticesinde topladıkları fonları 2007/64/EC numaralı AB direktifinin md. 9/1 ve 9/2 hükümlerine göre korumalarını sağlamalıdır. Ödeme aracı olarak kullanılacak fonların elektronik para kuruluşunun ödeme hesabına geçmedikçe korunması gerekmez. Aksi takdirde 2007/64/EC numaralı AB direktifinde belirtilen süre neticelenene kadar korunur. 2007/64/EC numaralı AB direktifinin 4/27 maddesi gereği bu süre beş iş günüdür.

Maddenin ikinci fıkrasında da yatırımların değerlendirilmesi hususu incelenmiştir. Buna göre ilgili direktifte belirtildiği üzere sermaye bedeli özgün riski % 1,6'nın üzerinde olmamalıdır. Yatırımlar yüksek oranda likit, paraya çevrilebilir ve düşük riskli yatırım alanlarında muhafaza edilmelidir. İstisnai durumlarda yetkili kurumlar elektronik para kuruluşlarına gerekli değerlendirmeler üzerine yatırımlarını belirtilen tipte olmayan şekilde değerlendirmesine izin verebilir.

Elektronik para kuruluşlarının elektronik para ihracı haricindeki -2009/110/EC numaralı AB direktifinin 6/1(a) maddesinde tanımlanan- işlerine 2007/64/EC numaralı AB direktifinin 9. maddesi uygulanır.

Aynı direktifin 14. maddesinde ise enflasyon veya değişen teknolojik şartlara uygun olarak önlemler alınabileceği belirtilmiştir.

6493 sayılı kanunun 18. maddesinin üçüncü fıkrasında ise elektronik para kuruluşlarının başlangıç sermayesi ve yükümlü olduğu diğer hususlar belirtilmiştir. Buna göre elektronik para kuruluşlarının; "*Anonim şirket*[33] *şeklinde kurulması; sermayesinde yüzde on ve üzerinde paya sahip olanların ve kontrolü elinde bulunduranların 5411 sayılı Kanunda banka kurucuları için aranan nitelikleri haiz olması; pay senetlerinin nakit karşılığı çıkarılması ve tamamının nama yazılı olması; nakden ve her türlü muvazaadan ari ödenmiş sermayesinin en az beş milyon Türk*

[33] Anonim şirketlerde daha belirgin bir şekilde gerçekleşen büyük sermayelerin toplanabilmesi, sorumluluğun sınırlandırılması ve işletmede devamlılık ve kurumsallaşma hususu anonim şirketlere olan güveni artırır. Bu konuda ayrıntılı bilgi için, bkz. Hasan Pulaşlı, *Şirketler Hukuku Genel Esaslar* (Ankara: Adalet Yayınevi, 2015), 260.

Lirası olması; bu Kanun kapsamındaki işlemleri gerçekleştirebilecek yönetim, yeterli personel ve teknik donanıma sahip olması, şikâyet ve itirazlarla ilgili birimleri oluşturması; bu Kanun kapsamında yürütecekleri faaliyetlerin sürekliliğine ve elektronik para kullanıcılarına ilişkin fon ve bilgilerin güvenliğine ve gizliliğine dair gerekli tedbirleri alması; kurumun denetimini engellemeyecek şeffaf ve açık bir ortaklık yapısı ve organizasyon şemasına sahip olması," gerekmektedir. Başlangıç sermayesi ve yönetimdeki kişilerle alakalı hükümlerin benzerleri AB düzenlemelerinde de bulunmakla birlikte diğer hükümler AB düzenlemeleri ile tam manada aynı değildir.

6493 sayılı kanunun 21. maddesinde ödeme kuruluşları ve PTT A.Ş. ile birlikte elektronik para kuruluşlarının denetimine esas oluşturacak hükümler belirlenmiştir. Bu hükümlere göre, elektronik para kuruluşlarının denetimi Bankacılık Düzenleme ve Denetleme Kurumu tarafından yapılacaktır. Elektronik para kuruluşları gizli statüde yahut ticari sır, meslek sırrı gibi nitelikte olsalar dahi Kurum tarafından talep edilen her tür belgeyi sunmak zorundadırlar.

6493 sayılı Kanunun 22. maddesinde fonların korunması ve teminat hususu düzenlenmiştir. Buna göre, elektronik para kuruluşunun topladığı fonları değerlendirme biçimi yönetmelikle belirlenir. Bankacılık Düzenleme ve Denetleme Kurulu tarafından elektronik paraların Merkez Bankası nezdinde bir miktar para bulundurmaları yükümlülüğü getirilebilir. Üçüncü fıkrada da fon sahiplerinin haklarının tazmini için bu teminatların kullanılacağı ve elektronik para kuruluşlarının bu tazminden sorumlu oldukları belirtilmiştir. Elektronik para kullanıcılarının haklarını korumak adına getirilmiş bu teminat yükümlülüğü AB düzenlemelerinde mevcut değildir.

Madde 25'te elektronik para kuruluşları ile alakalı önemli pay devirlerinin Bankacılık Düzenleme ve Denetleme Kurulu iznine tâbi olacağı belirtilmiştir. 2009/110/EC numaralı AB direktifi md. 3/3 de benzer bir düzenleme içermektedir.

6493 sayılı Kanunun 28. maddesinde izinsiz faaliyette bulunma ile ilgili cezai sorumluluk hükümleri ihdas edilmiştir.[34] Buna göre, izinsiz faaliyette bulunma yahut elektronik para kuruluşu olmadığı halde kendisini bu şekilde gösterme gibi bir durum söz konusu olursa ilgili kişiler bir ilâ üç yıl hapis cezası ve beş bin güne kadar adli para ile cezalandırılırlar. Bunu gerçekleştiren işyerinin iki aydan altı aya kadar geçici olarak tekrarı halinde ise sürekli olarak kapatılmasına karar verilir.

AB direktifleriyle benzer şekilde Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmeliğin 25. maddesinde belirtilen asgari öz kaynak yükümlülüklerini tedavüldeki ortalama elektronik para tutarının %2'si olarak belirlemiştir. Ödeme hizmeti de sunan elektronik para kuruluşunun buna ilişkin asgari öz kaynak yükümlülüğü ayrıca hesaplanır. Öz kaynağın belirlenen miktarların altına düşmesi ihtimalinde kurum bilgilendirilir.

Elektronik para kuruluşları, elektronik para ihracı karşılığında topladığı fonları bankalar nezdinde açtıkları hesaplarda tutarlar ve başka amaçlarla kullanamazlar.

C. Muafiyet

Birçok müellif elektronik para kuruluşlarını denetim için getirilen düzenlemelerin gerekenden daha ağır olduğu hususunu ifade etmiştir. Elektronik para kuruluşlarına yönelik ağır düzenlemelerin bunların istisnalarını oluşturmayı da gerektirdiği görülmüştür. Bu bağlamda gerek Türk gerekse AB düzenlemelerinde elektronik para kuruluşlarına yönelik bazı istisnalar getirilmiştir. AB düzenlemelerinde bu istisnalar yerel çalışan ve kıyasla daha küçük olan elektronik para kuruluşlarına yöneliktir.[35] Türk düzenlemelerinde ise belirli bir hizmet alanına yönelik olan veya belli sınırlar dâhilinde kullanı-

---

[34] Ayrıntılı bilgi için, bkz. Çiğdem Güven, "6493 sayılı Kanunda İdari ve Cezai Sorumluluk," *Ankara Barosu Dergisi* 72, no. 3 (2014).

[35] Birlik üyesi 6 ülke muafiyet tanıma işlemi yapmamış, 19 ülke ise bazı kurumlara muafiyet tanımıştır. Bu konuda ayrıntılı bilgi için, bkz. Yurtçiçek, "Hukuki Açıdan Elektronik Para," 171.

lan elektronik paralar için istisna getirilmiştir. Böylece elektronik para kuruluşlarına ilişkin ağır düzenlemelerden bazı küçük ya da yerel kuruluşları ayrı tutarak orantılılık sağlanır.

AB düzenlemelerinde amacın elektronik para kuruluşlarına ilişkin ulusal düzenlemelerin uyumlu hale getirilerek AB içerisinde tek pasaport ilkesinin uygulanacağı[36] ve Birlik içerisinde her yerde geçerli elektronik para kuruluşları kurulmasına imkân sağlamak olmasına rağmen ulusal elektronik para kuruluşlarına yönelik muafiyet düzenlemelerinin bulunması doktrinde çokça eleştirilmiştir.

2000/46/EC numaralı AB direktifinin başlangıç bölümünün 15. fıkrasında muafiyet hususu ele alınarak çok fazla kapsam daraltılmadan yalnızca *"ülkelerin -kendi sınırları içerisinde faaliyet gösterdikleri takdirde- elektronik para kuruluşları için direktifte öngörülen bazı yükümlülükler açısından muafiyet tanımaları mümkündür"* şeklinde bir düzenleme yaparak ayrıntılı sınırlandırmayı hükümler kısmına bırakmıştır. Direktifin muafiyet kenar başlıklı sekizinci maddesine göre belirli şartlar altında üye ülkeler yetkili otoritelerine 2000/46/EC numaralı AB direktifinin ve 2000/12/EC numaralı AB direktifinin bazı maddelerini veya maddelerinin tamamının uygulanmamasına, ilgili elektronik para kuruluşları sıralanan aşağıdaki şartları sağlıyorsa araçlarının 150 avrodan yüksek miktar taşımaması şartıyla izin verebilir;

- Elektronik para kuruluşunun direktifin 1/3(a) maddesine göre yükümlü olduğu ödenmemiş elektronik para miktarı genelde 5 milyon avroyu ve asla 6 milyon avroyu aşmıyorsa ya da,
- İhraç edilen elektronik para yalnızca elektronik para ihraç eden kuruluşların yan şirketleri tarafından kabul ediliyorsa ya da,
- İhraç edilen para sınırlı sayıda girişim tarafından kabul ediliyor ve bunlar da belli bir sınırlı alan veya aynı binada hizmet vermeleri yahut ihraç eden kuruluş ile ortak pazarlama veya dağıtım planı gibi yakınlıkları sebebiyle ayırt edilebiliyor ise.

---

[36] Birlik genelinde tek pasaport ilkesi denilen tek ülkeden alınan yetki ile tüm üye ülkelerde işlem yapabilme hakkından yararlanabilen elektronik para kuruluşu ise yalnızca üç tanedir. Bu konuda ayrıntılı bilgi için, bkz. Yurtçiçek, "The Legal Nature," 292.

Mezkûr maddenin ikinci fıkrası birinci fıkraya göre muafiyet tanınmış elektronik para kuruluşlarının karşılıklı tanıma anlaşmalarından faydalanamayacağını belirtmiştir.[37] Üçüncü fıkra ise üye devletlerin muafiyet tanınan elektronik para kuruluşlarının yükümlülükleri sağlayıp sağlamadıklarına bildirim yükümlülüğü getirmeleri gerektiğini düzenlenmiştir.

Elektronik para kuruluşları için direktifte bazı ağır yükümlülükler belirlenmiştir. Bundan dolayı nispeten küçük yahut sınırlı işlev gören bazı durumlar için muafiyet tanınması gerekliliği hâsıl olmuştur.[38] Ağır yükümlülüklerden kurtulmak isteyen küçük elektronik para kuruluşlarının tek pasaport imkânından men edilmesi doktrinde eleştirilmiştir. Bu husus hem elektronik para kuruluşları için geçerli olması planlanan tek pasaport ilkesine ters düşeceği hem de bundan da öte ülkeler içindeki rekabeti olumsuz yönde etkileyeceği yönünde eleştirilmiştir.[39] Almanya gibi bazı ülkeler muafiyetlerden yararlanmayarak direktifi doğrudan uygulama yönünde politika benimseseler de İngiltere gibi bazı ülkeler ise muafiyetlerden sonuna kadar faydalanmayı düşünmektedir.[40]

2009/110/EC numaralı AB direktifinde hem başlangıç hem de hükümler kısmında daha ayrıntılı düzenlemeye gidilmiştir. İlk olarak başlangıç kısmının 5. fıkrasına göre, bu direktifin elektronik para ihracı yapan ödeme hizmeti sağlayıcılarına yönelik olması uygun olacaktır. Direktif sınırlı alanda veya belirli ürün yahut hizmetlerin temininde kullanılan elektronik paralara uygulanmamalıdır. Bu sınırlı alanda kullanımın tespiti için de şu kıstaslar kullanılmalıdır; belirli bir market veya marketler zincirinde kullanılma veya coğrafi alandan bağımsız olarak belirli tip mal veya hizmetleri alımında kullanılma. Bu araçlar petrol istasyonları için özel tasarlanmış kart-

---

37 Standartların düşürülmesinin karşılığı olarak tek pasaport imkânından yararlanılmaması belirlenmiştir. Bu konuda ayrıntılı bilgi için, bkz. Krueger, "Innovation," 15.

38 Athanassiou ve Mas-Guix, "Electronic Money," 24-25.

39 Athanassiou ve Mas-Guix, "Electronic Money," 25.

40 Krueger, "Innovation," 17.

lar, ulaşım kartları, üyelik kartları vs. olabilir. Sınırlı alanda hizmet veren bu tarz uygulamalar genel seviyede hizmet verme yoluna giderlerse muafiyetin dışında tutulacaklardır. Yalnızca belli bir liste dâhilindeki yerlerde hizmet sunan uygulamalar da bu listeler genelde gittikçe büyüyen bir ağ şeklinde çalıştığından ötürü muafiyet kapsamında olmayacaklardır.

Yine başlangıç bölümünün 16. fıkrasına göre, üye ülkelerin sınırlı miktarda para ihracı yapan elektronik para kuruluşlarını direktifin bazı maddelerinden muaf tutabileceğini kabul etmek gerekir. Bu muafiyetten yararlanan kuruluşlar birlik içerisinde kurulum ve servis sağlama özgürlüğünden yararlanamazlar. Bir ödeme sisteminin parçası olarak da bu hizmeti sağlamaları mümkün değildir. Direktiflerde belirtilen muafiyetten faydalansa dahi tüm elektronik para kuruluşlarının kayıtlı olmaları gerekir. Bu bağlamda bu kuruluşların da kayıt altında tutulmaları gerekir. 17. fıkrada da diğer elektronik para ihraç eden kuruluşlar ile birlikte muaf tutulmuş elektronik para kuruluşları da belirtilerek üye devletlerin bunlar haricindeki kurum ve kuruluşlara elektronik para ihracı yetkisi tanımaması gerektiği zikredilmiştir. Bu husus direktifin üçüncü maddesinin ikinci fıkrasında da benzer şekilde geçmektedir.

2009/110/EC numaralı AB direktifinin muafiyete ilişkin 9. maddesine göre, üye ülkeler yetkili kuruluşlarını, direktifin 3, 4, 5 ve 7. maddelerinde belirtilen şartları sağlıyorsa bazı tüzel kişilere yükümlülükleri uygulayıp uygulamamak hususunda serbest bırakabilir. Bu şartlar;

- Muaf tutulacak tüzel kişiliğin ödenmemiş ortalama elektronik para miktarı üye ülke tarafından belirlenecek ve 5 milyon avroyu geçmeyecek bir sınırın altında olması ve,
- Tüzel kişiliğin yönetim ve idaresinde olan hiçbir gerçek kişinin daha önce terörizm finansmanı ve kara para aklama suçlarından suçlu bulunmamış olmasıdır.

Elektronik para kuruluşunun elektronik para ihracı haricindeki işler için ödenmemiş ortalama elektronik para hesabı yapmaya yeter bilgisi yok ise yetkili otorite temsili bilgiler ve geçmiş veriler üzerin-

den hesap yapılmasına izin verir. Eğer bu veriyi hesaplayacak yeterli süre geçmemişse iş planı üzerinden yetkili otoritenin düzeltmesine tâbi bir hesap yapılır. Üye ülkeler aynı zamanda bu muafiyeti sağlamak için elektronik para cihazında taşınabilecek bir maksimum miktar belirleyebilir. Bu şekilde yetkilendirilen elektronik para kuruluşları 2007/64/EC numaralı AB direktifinin 26. maddesinde belirtilen şartlar yerine getirildiği takdirde ödeme hizmetleri sunabilir. İkinci fıkraya göre, bu şartlar altında yetkilendirilebilecek tüzel kişinin merkezi üye ülkenin içerisinde olmalıdır. Bu şartlar altında yetkilendirilmiş kuruluş elektronik para kuruluşu gibi muamele görür. Ancak 2007/64/EC numaralı AB direktifinin 10/9 ve 25. maddesi bu kuruluşlara uygulanmaz.

Yine 2009/110/EC numaralı AB direktifinin 9. maddesinin beşinci fıkraya göre, bu şekilde yetkilendirilen kuruluşlar durumlarında oluşan herhangi bir değişikliği yetkili birimlere iletmek durumundadır. Bununla birlikte en az yıllık olarak ödenmemiş ortalama elektronik para miktarını yetkili otoriteye belirtmek durumundadır. Üye devletler şartları sağlamadığı anlaşılan bu kuruluşlar için gerekli önlemleri alırlar. Bu durumda elektronik para kuruluşu 30 gün içerisinde yetkilendirme almalıdır. Bu süre içerisinde yetkilendirme almayan kuruluşun elektronik para ihraç etmesi yasaklanır. 2009/110/EC numaralı AB direktifinin 9. maddesi kara para aklama söz konusu olduğunda ise uygulanmaz.

6493 sayılı kanunun 18. maddesinin beşinci fıkrasında ise önemli bir istisna mevcuttur. Buna göre elektronik para ihraç eden kuruluşun *"sadece kendi mağaza ağında, sadece belirli bir mal veya hizmet grubunun satın alınmasında veya yapılan bir anlaşma sonucunda sadece belirli bir hizmet ağında kullanılabilen ön ödemeli araçlar"* 6493 sayılı kanun kapsamı dışında tutulmuştur. AB düzenlemelerinde daha fazla muafiyet yer almasına rağmen ulusal düzenlemelerimizde muafiyetler daha az tutulmuştur. Özellikle bu hususta muafiyetin tanınması kanaatimizce gereksiz yoğunluğun önüne geçmek adına faydalı olmuştur.

D. Mevduat Teşkil Etmeme

Mevduat teşkil etmeme konusu elektronik para kuruluşlarının kredi kuruluşlarından ayrı tutulması için öngörülen önlemlerden biridir. Elektronik para kuruluşlarını kendi iş alanında sınırlı tutmak için kredi kuruluşlarının yaptıkları bazı işleri yapmasına özellikle izin verilmemiştir.[41] Mevduat toplama yasağı ve toplanan elektronik paranın mevduat teşkil etmemesi hususu da bu bağlamda değerlendirilebilir. Elektronik para kuruluşları 2000/46/EC numaralı AB direktifinde özel bir kredi kuruluşu sayıldığı halde bu hususlarda yapabileceği işler yine de sınırlanmıştı. 2009/110/EC numaralı AB direktifiyle kredi kuruluşu da sayılmayan elektronik para kuruluşlarının kredi kuruluşlarının yapabileceği işler açısından sınırlandırılması daha sağlam bir temele oturmuş oldu. Bununla birlikte elektronik paranın ödeme hizmetleri sağlamak açısından yetkileri 2009/110/EC numaralı AB direktifi ile artırılmıştır. Belirli şartlar sağlandığı takdirde elektronik para kuruluşlarının kredi verebileceğine ilişkin bir düzenleme istisna olarak 2009/110/EC numaralı AB direktifinde düzenlenmiştir.

2000/46/EC numaralı AB direktifinin ikinci maddesinin üçüncü fıkrasına göre, toplanan fonlar geciktirilmeksizin elektronik paraya çevrilir ve mevduat veya geri ödenebilir fon teşkil etmezler.[42]

2009/110/EC numaralı AB direktifinin başlangıç bölümünün 13. fıkrasına göre, elektronik para ihracı 2006/48/EC numaralı direktif bağlamında bir mevduat toplama işlemi olarak değerlendirilemez çünkü elektronik para yatırım için değil ödeme yapmak için kullanılır. Elektronik para kuruluşları ihraç ettikleri elektronik para karşılığında topladıkları fonlar ile kredi veremezler. Elektronik para ihraç eden kuruluşlar ihraç edilen elektronik paranın elde tutulduğu

---

41 Elektronik paranın mevduat teşkil etmemesi gerektiği yönündeki görüş genel kabul görse de bu durum bazılarınca eleştirilmiştir. Bu konuda ayrıntılı bilgi için, bkz. Yurtçiçek, "Hukuki Açıdan Elektronik Para," 162, 169.

42 2006/48/EC numaralı AB direktifine göre elektronik para ihracı mevduat toplama olarak düşünülemez. Bu konuda ayrıntılı bilgi için, bkz. Yurtçiçek, "Hukuki Açıdan Elektronik Para," 169, 185.

müddet için bir faiz veya benzeri bir fayda sağlaması da söz konusu olamaz. Söz konusu direktifin 12. maddesi de benzer şekilde, elde tutulan elektronik para için faiz veya herhangi bir menfaat sağlamanın yasaklanması gerektiğini belirtmiştir.

6493 sayılı kanunun 20. maddesinin dördüncü ve devamı fıkralarında elektronik para kuruluşlarının yapamayacakları işlemler belirtilmiştir. Buna göre, elektronik para kuruluşu kredi verme faaliyeti yapamaz. 2000/46/EC numaralı AB direktifi benzer düzenleme içerse de 2009/110/EC numaralı AB direktifinin 6/1(b) hükmü kapsamında küçük bir alan ve belirli şartlar çerçevesinde elektronik para kuruluşunun kredi verebileceği hükmü getirilmiştir. Beşinci fıkraya göre ise elektronik para kuruluşları kullanıcının elektronik parayı elinde tuttuğu müddetle ilişkili olarak faiz yahut herhangi bir menfaat sağlayamaz. Bu husus da aynı şekilde 2009/110/EC numaralı AB direktifinin 12. maddesinde geçmektedir. Toplanan fonların mevduat olarak değerlendirilemeyeceği ise söz konusu maddenin yedinci fıkrasında hüküm altına alınmıştır. Bu husus da AB direktiflerinde aynı şekliyle yer almaktadır.

Ödeme Hizmetleri ve Elektronik Para İhracı ile Ödeme Kuruluşları ve Elektronik Para Kuruluşları Hakkında Yönetmeliğin elektronik para başlıklı bölümü iki maddeden oluşur. Elektronik para ihracı başlıklı altıncı maddesinin ilk fıkrası, yine fon karşılığı ve gecikmeksizin ihraç hususlarını özellikle belirtmiştir. İkinci fıkrada ihracın, karşılığı fonun ödemesinin yapıldığı anda gerçekleştiği varsayımı ifade edilmiştir. Üçüncü fıkrada da elektronik para kuruluşlarınca elektronik para karşılığında kabul edilen fonun miktarına ilişkin dekontun kâğıt veya elektronik kaynak üzerinde kullanıcıya vermek zorunda olduğu hususu düzenlenmiştir. Dördüncü fıkrada ise elektronik para karşılığı temin edilen fon ile alakalı elektronik paranın elde tutulduğu müddete ilişkin herhangi bir menfaat verilemeyeceği hususu kanunda belirtildiği gibi tekrar edilmiştir.

Yönetmeliğin kuruluşların yapamayacağı işler başlıklı bölümünde elektronik para kuruluşlarının yapamayacağı işlerden de bahsedilmiştir. Buna göre yönetmeliğin onuncu maddesine göre elektronik para kuruluşları; elektronik para ihraç edilmesi, ödeme

hizmetlerinin sunulması, ödeme hizmetinin sunulmasıyla ilgili olmak kaydıyla döviz alım satım işlemleri ve belli şartlar altında ödeme sistemlerinin işletilmesi haricinde hiçbir ticari faaliyette bulunamaz. AB düzenlemelerine paralel olarak elektronik para kuruluşunun herhangi bir şekilde mevduat veya katılım fonu kabul etmesi de yasaklanmıştır. Ayrıca elektronik para kuruluşları bankaymış gibi de tanıtılamaz. Yine kredi verme faaliyetleri de kuruluş tarafından yerine getirilemez. Ayrıca kuruluşun sunduğu ödeme işlemleri kuruluş tarafından taksitlendirilemez. Bu da kredi verme işlevini bu yöntemle yapılmasını önlemek adına gerekli bir düzenlemedir.

E. Geçici Düzenlemeler

Her elektronik paraya ve elektronik para kuruluşlarına ilişkin düzenlemede muhakkak bu düzenlemeden önce kurulmuş olan elektronik para kuruluşlarına ilişkin olarak geçici bazı hükümler bulunur. Hukuki güvenlik ilkesinin[43] de gereği olarak mevcut elektronik para kuruluşlarına yeni düzenlemelere uyum sağlamak için genelde bir müddet süre ve muafiyet tanınır.

2000/46/EC numaralı AB direktifinin 9. maddesine göre, direktiften önce kurulmuş bulunan elektronik para kuruluşları için düzenlenmiş olan direktif yahut yerel düzenlemelerden önce olan hangisi ise bundan önce kurulmuş olan elektronik para kuruluşları yetkili elektronik para kuruluşu sayılırlar. Bu kuruluşlar altı ay içerisinde direktife uygunluk açısından yükümlülüklerini tamamlarlar. Aksi halde karşılıklı tanımadan yararlanamazlar.

2009/110/EC numaralı AB direktifinin başlangıç bölümünün 23. fıkrasına göre, hukukî kesinlik açısından 2000/46/EC numaralı AB

---

[43] Hukuki Güvenlik İlkesi: Hukuk devletinde kişilerin kendilerine uygulanacak hukuk kurallarını önceden bilmeye hakları vardır. Mevcut durumda geçerli hukuk kuralı uygun davranış, gelecekte değişen hukuk kuralı dolayısıyla hukuka aykırı hale gelirse kişiler hukuka olan güvenlerini yitirirler. Bundan ötürü kural olarak geçmişe etki yasağı söz konusudur. Bu konuda ayrıntılı bilgi için, bkz. Kemal Gözler, *Türk Anayasa Hukuku Dersleri* (Bursa: Ekin Basım Yayın Dağıtım, 2016), 87.

direktifi zamanında kurulmuş elektronik para kuruluşları için yeni direktif ile ihdas edilmiş yükümlülükleri yerine getirmeleri için belirli bir süre verilmelidir. Önceki direktifte muafiyet kapsamında kalan kuruluşlar için bu sürenin biraz daha uzun tutulması gerekir.

2009/110/EC numaralı AB direktifinin geçici hükümler başlıklı 18. maddesine göre, üye ülkeler belirli bir tarihten önce yetki için başvuran elektronik para kuruluşlarına önceki düzenlemelere göre yetkilendirme yapmalıdır. Bu kuruluşlara yeni direktif ile getirilen düzenlemelere uymaları için süre verilir. Uymadıkları takdirde yetkilerinin düşürülmesi için gerekli işlemler yapılır. Uyumu sağlayan elektronik para kuruluşlarının ise yetkilendirilmesi yapılır.

6493 sayılı kanunun geçici md. 2/3 ve 2/5'te ise kanun yürürlüğe girdiğinde hâlihazırda elektronik para ihracı yapmakta olan kurumların bir sene içerisinde gerekli izinleri alması gerektiği almadıkları takdirde kanun kapsamında faaliyette bulunamayacakları belirtilmiştir.

IV. SONUÇ

Makalemiz elektronik paraya ilişkin ulusal düzenlemelerimiz ve AB düzenlemelerini tanıtmak ve karşılaştırmak üzere bu düzenlemelerin genel değerlendirilmesi, benzer hususları ve ayırt edici kısımları üzerinden hazırlanmıştır. Bu bağlamda ulusal düzenlemelerimiz büyük oranda çeviri hüviyeti taşımakta olup temelden farklılıklar içermemektedir. Yalnız AB düzenlemelerinin en önemli amaçlarından biri olan AB içerisinde tek yetkilendirme çabası ülkemiz için geçerli olmadığından buna ilişkin kısımları da ulusal düzenlemelerimiz içermemektedir. Bununla birlikte ulusal düzenlemelerimizde bazı kavramların birbirine geçtiği ve olması gereken farkların ortaya konamadığı ileri sürülebilir.

Elektronik para her ne kadar ülkemiz adına yeni bir kavram olsa da, dünyada kullanımı uzun yıllardır mevcuttur. Ülkemizde yeni olması hasebiyle söylediğimiz henüz bir iddia niteliğinde olup herhangi bir delillendirme yapamayacak olsak da şunu belirtmek gerekir ki elektronik para potansiyeli hukuki düzenlemeler ile ortadan kaldırılmış bir kavram olarak varlığını kullanımı sınırlı düzeyde

kalmak üzere sürdürebilecektir. Bunun nedeninin elektronik para kavramının hem tüketici hem de elektronik para kuruluşu açısından gerekli yeniliği sunamaması ve gerekli faydaları sağlamasının önünün alınması olduğu söylenebilir. Mevcut durumda elektronik para; özellikle bankamatik ve kredi kartlarına alternatif oluşturabilecek bir potansiyele sahip değildir.[44]

Anlattığımız üzere elektronik paranın belirtilen şartlar altında bir yenilik ortaya koyma ihtimali erken düzenlemeler ve bankalarla rekabet sonucunda ortadan kalkmış gibi görünmektedir. Ancak yine de belirtmek gerekir ki elektronik paranın fitilini yaktığı dağıtık para yapısı elektronik para başarılı olsun ya da olmasın para sisteminde yerini bulmuş ve uygun zamanda büyük yenilikler getirmek üzere sırasını beklemektedir.

---

[44] Elektronik paranın bir başarısızlık olması ile alakalı bir çalışma için, bkz. Hugo Godschalk ve Malte Krueger. "Why e-Money Still Fails," erişim tarihi 17 Aralık 2017 https://www.researchgate.net/publication/244136842_Why_e-money_still_fails_ -_chances_of_e-money_within_a_ competitive_payment_instrument_market.

KAYNAKÇA

Association of E-money Institutions in the Netherlands. "Electronic Money and E-money Institutions." Erişim tarihi 17 Aralık 2017. https://www.simonl.org/docs/empp1511.doc.

Athanassiou, Phoebus ve Natalia Mas-Guix. "Electronic Money Institutions (Current Trends, Regulatory Issues and Future Prospects)." *European Central Bank Legal Working Paper Series*. Temmuz 2008. https://www.ecb.europa.eu/pub/pdf/scplps/ecblwp7.pdf?21a28d70b208180883a898dad73451c4.

BDDK. "Elektronik Para Kuruluşları." Erişim tarihi 18 Aralık 2019. https://www.bddk.org.tr/Kuruluslar-Kategori/Elektronik-Para-Kuruluslari/7.

Ekşioğlu, Erdoğan. "Elektronik Para Kullanımının Ekonomik Etkileri (Türkiye Üzerinde Bir Uygulama)." Doktora Tezi, Sivas: Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü, 2017.

Elgin, Ceyhun, Refik Erzan ve Umut Kuzubaş. *Türkiye'de Nakit ve Kart Ödemelerinin Karşılaştırmalı Maliyeti*. İstanbul: Boğaziçi Üniversitesi Ekonomi ve Ekonometri Merkezi, 2013. https://newsroom.mastercard.com/eu/files/2015/06/MasterCard-Arastirma-NakitsizYasam-131013.pdf.

EUR-Lex. "Dırective 2006/48/Ec of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing." Erişim tarihi 9 Nisan 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri= CELEX:32005L0060&from=EN.

EUR-Lex. "Dırective 2006/48/Ec of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast)." Erişim tarihi 9 Nisan 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri= CELEX:32006L0048 &from=EN.

EUR-Lex. "Dırective 2006/48/Ec of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC." Erişim tarihi 9 Nisan 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0110&from=EN.

EUR-Lex. "Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions." Erişim tarihi 9 Nisan 2018. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0046&from=EN.

Farrugia, George. "Money Laundering in Cyberspace." Erişim tarihi 17 Aralık 2017. https://fiumalta.org/library/PDF/ml_cyberspace.pdf.

Gao, Jerry. "Electronic Cash Payment Protocols and Systems." Erişim tarihi 17 Aralık 2017. http://www.dmi.unipg.it/bista/didattica/sicurezza-pg/sistemi-pagamento/e-cash-payment.v1.10.20.pdf.

Godschalk, Hugo ve Malte Krueger. "Why e-Money Still Fails." Erişim tarihi 17 Aralık 2017. https://www.researchgate.net/publication/244136842_Why_e-money_still_fails_-_chances_of_e-money_within_a_ competitive_payment_instrument_market.

Gormez, Yuksel ve Forest Capie. *Prospects for Electronic Money: A US-European Comperative Survey*. Ankara: The Central Bank of Turkey, 2003. https://mafiadoc.com/the-central-bank-of-the-republic-of-turkey-tcmb_59f5e4201723ddb3267d72d4.html.

Gözler, Kemal. *Türk Anayasa Hukuku Dersleri*. Bursa: Ekin Basım Yayın Dağıtım, 2016.

Güven, Çiğdem. "6493 sayılı Kanunda İdari ve Cezai Sorumluluk." *Ankara Barosu Dergisi* 72, no. 3 (2014): 451-462.

Kabelac, Gabriele. "Cyber Money as Medium of Exchange." *Deutsche Bundesbank Discussion Paper Series*, no. 1999,05E (Ekim 1999). https://papers.ssrn.com/sol3/Delivery.cfm/107192.pdf?abstractid=2785816&mirid=1.

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

Krueger, Malte. "Innovation and Regulation -The Case of e-Money Regulation in the EU- Background Paper No. 5 Electronic Payment Systems Observatory (ePSO)." *Sevilla: Institute for Prospective Technological Studies*, 12 Ocak 2002. http://www.paysys.de/download/Krueger%20e-money%20regul.pdf.

Öztürk, Nurettin ve Asuman Koç. "Elektronik Para, Diğer Para Türleriyle Karşılaştırılması ve Olası Etkileri." *Sosyal ve Ekonomik Araştırmalar Dergisi* 6, no. 11 (Haziran 2006): 207-243.

Pulaşlı, Hasan. *Şirketler Hukuku Genel Esaslar*. Ankara: Adalet Yayınevi, 2015.

U.S. Congress-Office of Technology Assessment. *Information Technologies For The Control Of Money Laundering*. Washington, DC: U.S. Government Printing Office, Eylül 1995.

Yurtçiçek, Mehmet Sıddık. "Hukuki Açıdan Elektronik Para." Doktora tezi, Marmara Üniversitesi, 2012.

Yurtçiçek, Mehmet Sıddık. "The Legal Nature of Electronic Money and the Effects of the EU Regulations Concerning The Electronic Money Market." *Law & Justice Review* V, no. 1 (Haziran 2013).

6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNU VE AVRUPA BİRLİĞİ HUKUKUNDA KİŞİSEL VERİLERİN SİLİNMESİ VE DÜZELTİLMESİ

Erasure and Rectification of Personal Data under Code on The Protection of Personal Data No. 6698 and European Union Law

Hilal Tuğba ÖKSÜZOĞLU*

Öz

Anayasa'nın 20. maddesinin 3. fıkrasıyla kişisel verilerin korunması bir temel hak olarak tanınmıştır. 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi ve düzeltilmesine ilişkin ana esaslar düzenlenmiş; fakat kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesine ilişkin diğer usul ve esaslar yönetmelikle düzenlenmek üzere bırakılmıştır. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ile kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi kavramları tanımlanmıştır. Bununla birlikte kişisel verilerin silinmesini talep hakkı bağlamında Avrupa Birliği hukuku ile Türk hukuku arasında bir terminoloji farklılığı söz konusudur. Bu çalışmada kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi ve düzeltilmesini talep hakları 6698 sayılı Kişisel Verilerin Korunması Kanunu, ilgili

* Avukat, İstanbul Barosu, İstanbul, Türkiye. E-posta: av.hilaloksuzoglu@hotmail. com. org.tr, ORCID: 0000-0002-4498-860X.

Makale Gönderim Tarihi: 09.08.2019.

Makale Kabul Tarihi: 30.12.2019.

diğer mevzuat ve Avrupa Birliği hukuku bakımından incelenmiştir. Çalışmada son olarak kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi veya düzeltilmesi talebinin yerine getirilmemesinin neticeleri ele alınmıştır.

Anahtar Kelimeler: 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Kişisel Verilerin İmhası, Anonimleştirme, Genel Veri Koruma Tüzüğü.

Abstract

The protection of personal data is regulated as a fundamental right under Article 20, paragraph 3 of the Constitution. Guidelines regarding erasure, destruction, anonymization, and rectification of personal data have been regulated by Code on The Protection of Personal Data No. 6698. However, other procedures and principles for the erasure, destruction, and anonymization of personal data are laid down through a by-law. Concepts of erasure, destruction, and anonymization of personal data are defined by the Regulation on Erasure, Destruction or Anonymization of Personal Data. Nevertheless, there is a terminological difference between European Union law and Turkish law regarding the erasure of personal data. In this study, the rights to erasure, destruction, anonymization, and rectification of personal data are examined under Code on The Protection of Personal Data No. 6698, other the related legislation and European Union law. Lastly, the consequences of not carrying out erasure, destruction, anonymization or rectification of personal data are analyzed.

Keywords: Code on The Protection of Personal Data No. 6698, Regulation on Erasure, Destruction or Anonymization of Personal Data, Extermination of Personal Data, Anonymization, General Data Protection Regulation.

I. GİRİŞ

Özellikle 1960'lı yıllardan itibaren verilerin otomatik olarak işlenmesini mümkün kılan teknolojilerin geliştirilmesiyle birlikte, devlet kurumları bireylerin kişisel verilerine dair kapsamlı bilgi bankaları oluşturmaya başlamışlardır.[1] Bunun sonucunda bireylerin mahremiyetinin korunması ve devletin bireylerin kişisel verilerine dair bilgi hâkimiyetinin sınırlandırılması yönündeki talepler artış göstermiştir.[2] Bilgi ve iletişim teknolojilerinde yaşanmakta olan gelişmeler sonucunda bilgiye elektronik ortamda erişimin kolaylaşmış olması da kişisel verilerin korunmasının önemini artırmıştır.[3] Günümüzde teknolojik olanakların gelişmesiyle birlikte bireyler üzerindeki gözetim öncesine göre çok daha fazladır.[4]

Kişisel verilerin günümüzde ticarî meta hâline getirilmiş olduğunu söylemek mümkündür.[5] Öyle ki veri, dijital toplumun petrolü olarak nitelendirilmektedir.[6]

---

1 Mesut Serdar Çekin, *Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu* (İstanbul: On İki Levha, 2018), 5.

2 Çekin, *Kişisel Verilerin Korunması Kanunu*, 5. Bu bağlamda bireyin kişisel verilerinin korunması hakkını insan onuru bağlantısıyla genel kişilik hakkının korunması ile gerekçelendirmiş olan Alman Anayasa Mahkemesi'nin Almanya'daki 1983 Nisan ayı nüfus sayımına ilişkin kararı (*Volkszählung*, BVerfG, 15.12.1983 - 1 BvR 209/83) büyük önem taşımaktadır. Bkz. Oğuz Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması* (İstanbul: Beta, 2008), 114-115. Karar hakkında detaylı açıklamalar için, bkz. Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 114-119; Can Yavuz, *İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı* (Ankara: Seçkin, 2016), 60-62. Kararda kişisel verilerin korunması hakkı, kişilik hakkının bir alt kategorisi olarak değerlendirilmiştir. Bu konuda bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 13.

3 Doğan Kılınç, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması," *AÜHFD* 61, no. 3 (2012): 1089.

4 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York and London: New York University Press, 2004), 2; İbrahim Korkmaz, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme," *TBB Dergisi*, no. 124, (2016): 82.

5 Habip Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum," *Uyuşmazlık Mahkemesi Dergisi*, no. 3 (2013): 2.

Türk hukuku bakımından kişisel verilerin korunmasına dair hukuki düzenlemelerin uzun bir geçmişe sahip olmadığı belirtilmektedir.[7] Anayasa'nın *"Özel Hayatın Gizliliği"* kenar başlıklı 20. maddesine 2010 yılında 5892 sayılı Kanun'un[8] 2. maddesi uyarınca eklenen üçüncü fıkra ile kişisel verilerin korunması bir temel hak olarak tanınmıştır.[9] Anayasa m. 20/3 uyarınca; "*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.*". Anayasa'nın bu hükmü, ikincil mevzuattaki düzenlemelerin tamamının temelini oluşturmaktadır.[10]

Türk hukukunda kişisel verilerin korunmasına dair esaslar 6698 sayılı Kişisel Verilerin Korunması Kanunu[11] ("KVKK" veya "Kanun") ile düzenlenmiştir. KVKK'nın Resmî Gazete'de 07.04.2016 tarihinde yayımlanmasından yalnızca 7 gün sonra 14.04.2016 tarihinde, Avrupa Birliği Parlamentosu tarafından Genel Veri Koruma Tüzüğü[12] ("Tüzük") kabul etmiştir.[13] Bununla birlikte KVKK Tü-

---

6 Çekin, *Kişisel Verilerin Korunması Kanunu*, 2. *"Data is the new oil."* sloganının öncelikle kim tarafından ifade edilmiş olduğunun tartışmalı olduğu hakkında bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 2, dn. 6.

7 Çekin, *Kişisel Verilerin Korunması Kanunu*, 8.

8 5982 sayılı Türkiye Cumhuriyeti Anayasasının Bazı Maddelerinde Değişiklik Yapılması Hakkında Kanun. Kabul Tarihi: 07.05.2010. Bu kanunla yapılan Anayasa değişiklikleri 12.9.2010 tarihinde halk oylamasına sunularak kabul edilmiş, buna ilişkin 22.09.2010 tarihli ve 846 sayılı Yüksek Seçim Kurulu Kararı 23.09.2010 tarihli ve 27708 sayılı Resmî Gazete'de yayımlanmıştır.

9 Çekin, *Kişisel Verilerin Korunması Kanunu*, 8.

10 Mustafa Tevfik Kartal, "Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme," *Uluslararası Ekonomi ve Yenilik Dergisi* 4, no. 1 (2018): 10.

11 Kabul tarihi: 24.03.2016; RG. 07.04.2016, S. 29677.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

zük'e değil, 1995 tarihli Avrupa Birliği Veri Koruma Yönergesi'ne[14] ("Yönerge") dayanmaktadır.[15]

KVKK'nın ardından yürürlüğe girmiş olan ilgili yönetmelikler ise Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik[16], Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik[17], Veri Sorumluları Sicili

---

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Tüzük metni için bkz. "Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," EUR-Lex, erişim tarihi 8 Ağustos 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

13 Tüzük; kişisel verilerin korunmasına ilişkin olarak önceki düzenlemeye göre daha yüksek standartlar belirlemek, Avrupa Birliği üyesi ülkeler bakımından daha uyumlu bir koruma rejimi kurmak ve Avrupalı olmayan şirketlerin hukuki düzenlemelere uyum sağlamasını kolaylaştırmak hedefleriyle oluşturulmuştur. Bkz. Furkan Güven Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması* (İstanbul: On İki Levha Yayıncılık, 2017), 15.

14 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. Yönerge metni için, bkz. "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, erişim tarihi 8 Ağustos 2019, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046. Yönerge ile veri işlemede gerçek kişilerin temel hak ve özgürlüklerini korumaya yönelik normların uyumlaştırılması ve kişisel verilerin Avrupa Birliği'ne üye olan ülkeler arasında serbest akışının sağlanması hedeflenmiştir. Bkz. Metin Turan, *Karşılaştırmalı Hukukta Kişisel Verilerin Korunması* (Ankara: Adalet Yayınevi, 2017), 41; Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 13.

15 Çekin, *Kişisel Verilerin Korunması Kanunu*, 3. KVKK hazırlanırken kanun koyucunun ilk aşamada Tüzük'e değil Yönerge'ye dayalı bir düzenlemeye gitme tercihinin isabetli olduğu yönünde bkz. Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 24-25. Bu tercihin isabetli olarak nitelendirilemeyeceği, bununla birlikte ilgili normların uygulanması esnasında 20 yıldan fazla bir tecrübeye sahip olan Avrupa Birliği uygulamasını dikkate almanın yerinde olacağı yönünde bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 3-4.

16 RG. 28.10.2017, S. 30224.

17 RG. 16.11.2017, S. 30242.

Hakkında Yönetmelik[18], Kişisel Verileri Koruma Uzmanlığı Yönetmeliği[19], Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği[20], Kişisel Sağlık Verileri Hakkında Yönetmelik[21], Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği[22] ve Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği'dir.[23] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik[24] ise KVKK öncesinde yürürlüğe girmiştir.

Bunun dışında Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uygulanacak Usul ve Esaslar Hakkında Tebliğ[25] ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ[26] yürürlüktedir.[27]

KVKK ile ilgili kişiye[28] birtakım haklar tanınmış, veri sorumlularına[29] ise bazı yükümlülükler yüklenmiştir. KVKK m. 10 hükmüy-

---

18 RG. 30.12.2017, S. 30286.

19 RG. 09.02.2018, S. 30327.

20 RG. 26.04.2018, S. 30403.

21 RG. 21.06.2019, S. 30808.

22 RG. 05.05.2018, S. 30412.

23 RG. 17.05.2019, S. 30777.

24 RG. 24.07.2012, S. 28363.

25 RG. 10.03.2018, S. 30356.

26 RG. 10.03.2018, S. 30356.

27 Kişisel veri koruma hukukunda geçerli olan Türk hukuku düzenlemeleri ile Avrupa Birliği hukuku düzenlemeleri için bkz. Mehmet Bedii Kaya ve Furkan Güven Taştan, *Kişisel Veri Koruma Hukuku Mevzuat & İçtihat* (İstanbul: On İki Levha, 2018), v-x.

28 KVKK m. 3/1-ç uyarınca "ilgili kişi"; kişisel verisi işlenen gerçek kişidir.

29 KVKK m. 3/1-ı uyarınca "veri sorumlusu"; kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. "Veri işleyen" ise başka bir kavramdır ve KVKK m. 3/1-ğ uyarınca veri sorumlusunun verdiği yetkiye dayanarak ve onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder. Yönerge m. 2/d ve Tüzük m. 4/7 uyarınca yalnız başına veya başkalarıyla birlikte kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen gerçek veya tüzel kişi *"controller"* olarak tanımlanmıştır. Çalışmada terminoloji birliği olması açısından *"controller"* kelimesinin tercümesinde *"veri kontrolörü"* değil, *"veri sorumlusu"* teriminin kullanımı tercih edilmiştir.

le veri sorumlusunun aydınlatma yükümlülüğü, m. 12 hükmüyle de veri sorumlusunun sahip olduğu veri güvenliğine dair yükümlülükler düzenlenmiştir.

İlgili kişinin hakları ise KVKK m. 11 hükmünde sayılmıştır. İlgili kişinin hakları, ilgili kişi tarafından veriler üzerinde denetim sağlanabilmesi ve kişisel verilerin niteliğine ilişkin ilkelerin gerçekleşebilmesi bakımından son derece önemlidir.[30] Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme hakkı ve kişisel verilerin silinmesini veya yok edilmesini isteme hakkı, KVKK m. 11/1 fıkrasının "d" ve "e" bentleri uyarınca ilgili kişinin veri sorumlusuna karşı ileri sürebileceği haklardandır. Keza ilgili kişi; KVKK m. 11/1 fıkrasının "d" ve "e" bentleri gereği yapılmış olan işlemlerin, ayrıca kişisel verilerin aktarılmış olduğu üçüncü kişilere bildirilmesini isteme hakkını da haizdir (KVKK m. 11/1-f).

KVKK m. 28 hükmünde Kanun'un uygulama alanı dışında tutulan hususlar düzenlenmiştir. KVKK m. 28/1 tamamen, KVKK m. 28/2 ise kısmen Kanun'un uygulama alanı dışında tutulan hallere ilişkindir.[31] Dolayısıyla ilgili kişinin kişisel verilerin silinmesi, yok edilmesi ve düzeltilmesine ilişkin haklarının da düzenlenmiş olduğu KVKK m. 11 hükmü, KVKK m. 28'de belirtilmiş hallerde uygulama alanı bulmayacaktır.[32]

Bu çalışmada kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi ve düzeltilmesini talep haklarının KVKK ve Avrupa Birliği hukuku bakımından incelenmesi konu edilmiştir. Bu bağlamda KVKK hükümleri, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, Avrupa Birliği hukuku bakımından ise Yönerge ve Tüzük hü-

---

30 Elif Küzeci, *Kişisel Verilerin Korunması* (Ankara: Turhan Kitabevi Yayınları, 2018), 223.

31 Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku* (İstanbul: Hukuk Akademisi, 2019), 201.

32 Yönerge ve Tüzük uyarınca da bazı hususlar uygulama alanı dışında bırakılmıştır. Yönerge'nin "istisnalar ve sınırlamalar" kenar başlıklı 13. maddesi ve Tüzük'ün "sınırlamalar" kenar başlıklı 23. maddesi ile uygulama alanına ilişkin istisna ve sınırlamalar düzenlenmiştir.

kümleri değerlendirilmiştir. Çalışmanın son bölümünde ise kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi veya düzeltilmesi talebinin yerine getirilmemesinin sonuçları ele alınmıştır.

II. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİNİ TALEP ETME HAKKI

KVKK m. 3/1-d gereği kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir. Kişisel verilerin korunmasına dair temel hak kapsamında kişisel verilerin silinmesi hakkı temel olarak Anayasa m. 20/3 hükmüyle düzenlenmiştir. Buna göre herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkını haizdir ve bu hak kişinin kendisiyle ilgili kişisel verilerin silinmesini talep etmesini de kapsamaktadır.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi hususları KVKK m. 7 hükmüyle düzenlenmiştir. KVKK m. 11/1-e bendi uyarınca ise herkes veri sorumlusuna başvurmak suretiyle KVKK m. 7'de öngörülmüş olan koşullar kapsamında kişisel verilerin silinmesini veya yok edilmesini isteme hakkına sahiptir. KVKK m. 7/3 ve m. 22/1-e hükümlerine dayanılarak hazırlanmış ve 01.01.2018 tarihinde yürürlüğe girmiş olan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ("Yönetmelik") kapsamında bu hususa dair detaylı düzenlemelere yer verilmiştir.[33] Bahsedilen Yönetmelik; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esas-

[33] KVKK m. 19/4 uyarınca Kişisel Verilerin Korunması Kurulu ("Kurul"); KVKK hükümleriyle kurulmuş olan Kişisel Verileri Koruma Kurumu'nun karar organı olarak görev yapar. Yönetmelik uyarınca kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerinin ne şekilde yapılacağı hakkında uygulamada açıklık sağlanması amacıyla Kurul tarafından "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi" hazırlanmıştır. Bahsedilen rehber için bkz. "KVKK Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi," KVKK, erişim tarihi 8 Ağustos 2019, <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/bc1cb353-ef85-4e58-bb99-3bba31258508.pdf>.

ları belirlemek amacıyla düzenlenmiştir (Yönetmelik m. 1). Yönetmelik veri sorumluları hakkında uygulama alanı bulmaktadır (Yönetmelik m. 2).

Bu bağlamda öncelikle kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesini talep haklarının Türk hukuku bakımından KVKK ile Yönetmelik, Avrupa Birliği hukuku bakımından Yönerge ve Tüzük hükümlerine göre incelenmesi gereklidir.

A. Hakların Düzenlemelere Göre İncelenmesi

1. KVKK ve Yönetmelik Bakımından

KVKK m. 7 ile kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin temel esaslar düzenlenmiş, fakat maddenin üçüncü fıkrası gereği bunlara ilişkin diğer usul ve esaslar yönetmelikle düzenlenmek üzere bırakılmıştır.

Yönetmelik kapsamında imha; kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi anlamına gelen genel bir kavram olarak tanımlanmaktadır (Yönetmelik m. 4/1-c).

Kişisel verilerin silinmesi; kişisel verilerin ilgili kullanıcılar[34] için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade eder (Yönetmelik m. 8/1). Bu bağlamda veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlü kılınmıştır (Yönetmelik m. 8/2).[35]

Kişisel verilerin yok edilmesi ise kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve yeniden kullanı-

---

[34] Yönetmelik kapsamında ilgili kullanıcı; *"verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler"* şeklinde tanımlanmıştır (Yönetmelik m. 4/1-b).

[35] Blockchain mantığına dayanan sistemlerde ilgili kişinin verisinin silinmesi veya düzeltilmesi talebinin gerçekleştirilmesinin an itibariyle mümkün olmadığı belirtilmektedir; zira talepte bulunan ilgili kişiye dair kişisel verinin silinmesi veya düzeltilmesi, diğer bütün işlemleri de etkileyecektir. Bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 96.

lamaz duruma getirilmesi işlemi olarak tanımlanmaktadır (Yönetmelik m. 9/1). Kişisel verinin yok edilmesi için, verilerin bulunduğu donanım ve evrakın fiziken yok edilmesinin gerektiği belirtilmektedir.[36] Yönetmelik uyarınca veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlü kılınmıştır (Yönetmelik m. 9/2).

Son olarak kişisel verilerin anonim hale getirilmesi ise kişisel verilerin başka verilerle eşleştirilse bile hiçbir şekilde kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi şeklinde tanımlanmaktadır (Yönetmelik m. 10/1).[37] Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla da yükümlü kılınmıştır (Yönetmelik m. 10/3). Kişisel verilerin; veri sorumlusu, alıcı veya alıcı grupları[38] tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı bakımından uygun tekniklerin kullanılması yoluyla bile kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi durumunda, artık kişisel verilerin anonim hale getirildiğini söylemek mümkündür (Yönetmelik m. 10/2). Nitekim kişisel verilerin anonim hale getirilmiş olduğunu ifade edebilmek için, verilerin başka verilerle eşleştirilse bile hiçbir şekilde gerçek bir kişiyle ilişkilendirilemeyecek hale dönüştürülmüş olması gerektiği belirtilmektedir.[39] [40]

---

[36] Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 70.

[37] Veri anonimleştirme yöntemleri için bkz. Merve Gözüküçük, "Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi" (Yayımlanmamış yüksek lisans tezi, İstanbul Bilgi Üniversitesi, 2014), 48*ff*.

[38] Yönetmelik uyarınca alıcı grubu; veri sorumlusunun kişisel verileri aktardığı gerçek veya tüzel kişi kategorisini ifade eder (Yönetmelik m. 4/1-a).

[39] Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 70; Dülger, *Kişisel Verilerin Korunması Hukuku*, 257. Türkiye İstatistik Kurumu tarafından her yıl yayımlanan istatistik bilgilerinin anonim verilere örnek gösterilmesi mümkündür. Örnek için bkz. Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 70.

[40] KVKK m. 7 gerekçesinde kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesi arasındaki farklar şöyle açıklanmıştır:

"Kişisel verilerin silinmesiyle, bu verilerin tekrar hiçbir şekilde kullanılamayacak ve geri getirilemeyecek şekilde imhası amaçlanmaktadır. Buna göre veriler, kayıtlı oldukları ev-

Teknolojik gelişmeler sonucunda günümüzde *"anonim"* verilerle dahi kişilerin kimlik tespitinin mümkün olduğu ifade edilmektedir; nitekim AOL[41] ve Netflix[42] firmaları tarafından yayımlanmış olan müşteri verileri bu hususta örnek gösterilmektedir.[43]

2. Yönerge Bakımından

Yönerge m. 12-b gereği ilgili kişiler, özellikle verinin eksik veya yanlış olmasından dolayı Yönerge hükümlerine uygun olmayan bir şekilde işlenmiş olan verilerin, uygunluğa göre düzeltilmesi, silinmesi veya bloke edilmesini veri sorumlusundan talep etme hakkına sahiptir. Görüldüğü üzere ilgili kişinin KVKK ve Yönetmelik uyarınca kişisel verilerin imhasına dair bahsedilen hakları, bu hususta Yönerge kapsamında yer verilmiş olan haklar ile birebir olarak örtüşmemektedir. Zira Yönerge kapsamında ilgili kişinin kişisel verilerin düzeltilmesi, silinmesi veya bloke edilmesine[44] dair hakları söz konusudur.

---

rak, dosya, CD, disket, hard disk gibi araçlardan geri dönüştürülemeyecek şekilde silinecektir. Verilerin yok edilmesi ise, bilgilerin tekrar geri getirilemeyecek ve kullanılamayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi veri saklamaya elverişli materyallerin imha edilmesini ifade etmektedir. Verilerin anonim hale getirilmesiyle, kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi kastedilmektedir." Kaynak: Corpus Web Hukuk Mevzuat ve İçtihat Programı, www.corpus.com.tr.

41 Haberciler, AOL tarafından anonim hale getirilmelerinin ardından açıklanmış olan arama motoru kayıtlarını kullanılarak gerçek kişileri tespit edilebilmişlerdir. Bkz. Ryan Singel, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims," *Wired*, Aralık 17, 2009, erişim tarihi 8 Ağustos 2019, https://www.wired.com/2009/12/netflix-privacy-lawsuit/.

42 Texas Üniversitesi'nde araştırmacı olan Arvind Narayanan ve Vitaly Shmatikov; Netflix'in anonim hale getirip açıklamış olduğu veriler ile Internet Movie Database internet sitesinde yer alan verileri karşılaştırarak birçok Netflix kullanıcısının kimliğini tespit edebilmişlerdir. Bkz. Singel, "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims."

43 Çekin, *Kişisel Verilerin Korunması Kanunu*, 95. Anonimleştirmenin güvenilirliğine ilişkin tartışmalar için bkz. Gözüküçük, "Veri Anonimleştirmesi," 84*ff*.

44 Yönerge m. 12-b bendinde yer alan *"blocking of data"* ifadesinin "verilerin bloke edilmesi" (bkz. Nilgün Başalp, *Kişisel Verilerin Korunması ve Saklanması* (Ankara: Yetkin Yayınları, 2004), 50) veya "verilere erişimin engellenmesi" (bkz. Sedat Erdem Aydın, *AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu* (İstanbul: On İki Levha Yayıncılık, 2015), 119) şeklinde ifade edilmesi mümkündür.

Yönerge kapsamında verilerin silinmesi, silme işlemi sonucunda verilerin veri sorumlusunun hâkimiyet alanından çıkmasını gerektirir.[45] Bu bağlamda silmenin verinin yazılı olduğu evrakın yok edilmesi ya da verinin kayıtlı olduğu dijital ortamdan silinmesi şeklinde gerçekleşebileceği ifade edilmektedir.[46]

Silmenin kişisel veri taşıyıcısının yok edilmesi yoluyla gerçekleşebileceği belirtildiğinden[47], Yönerge kapsamındaki *"silme"* kavramının, KVKK ve Yönetmelik uyarınca *"silme"* ve *"yok etme"* kavramlarını[48] kapsadığı görülmektedir.

Her ne kadar Yönerge m. 12-b hükmünde verilerin anonimleştirilmesinden bahsedilmemiş olsa da bu husus Yönerge kapsamında fakat farklı bir şekilde düzenlenmiştir. Yönerge'nin 26. paragrafı uyarınca anonimleştirilmiş veriler, tüm veri koruma süreçlerinin bir istisnası olarak belirlenmiştir.[49] Bu düzenleme gereği, kişisel verilerin korunmasına dair esaslar, veri öznesinin artık belirlenebilir olmadığı bir şekilde anonim hale getirilmiş olan verilere uygulanmayacaktır.[50] [51]

---

[45] Başalp, *Kişisel Verilerin Korunması ve Saklanması*, 50; Aydın, *Kişisel Verilerin Kaydedilmesi Suçu*, 120.

[46] Aydın, *Kişisel Verilerin Kaydedilmesi Suçu*, 120; Selen Uncular, *İş İlişkisinde İşçinin Kişisel Verilerinin Korunması* (Ankara: Seçkin, 2014), 68. Doğrudan ilgili ile ilişkilendirmeyi sağlayacak kişisel bilgilerin ayrıştırılarak yok edilmesinin bir silme yöntemi olarak ifade edilmesine de rastlanmaktadır. Bkz. Başalp, *Kişisel Verilerin Korunması ve Saklanması*, 50. Bununla birlikte bahsedilen yöntem anonimleştirme kavramına daha yakın görünmektedir.

[47] Ulrich Dammann, *Bundesdatenschutzgesetz*, ed. Spiros Simitis (München: Nomos, 2014), Art. 12 Rn. 16*ff*. (Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 93'ten naklen).

[48] Yönerge'de "düzeltme, silme veya bloke etme" terimlerinin kullanılmış olmasına karşın KVKK'da "silme veya yok etme" kelimeleriyle farklı bir terminolojinin tercih edilmiş olması eleştiri konusu olmuştur. Bkz. Nurullah Tekin, "Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi," *Uyuşmazlık Mahkemesi Dergisi*, no. 4 (2014): 252.

[49] Gözüküçük, "Veri Anonimleştirmesi," 71.

[50] Anonim hale getirilmiş olan veriler kişisel verilerin korunmasına dair mevzuatın uygulama alanı dışında bulunsa da veri öznesinin iletişimin gizliliğini koruyan

Yönerge uyarınca verilerin bloke edilmesi kavramı ise, veri sorumlusunun verileri hâkimiyet alanında tutmaya devam etmesi, fakat verilerle ilgili herhangi bir işlem yapılmasını engellemesi halini açıklar.[52] KVKK ve Yönetmelik kapsamında kişisel verilerin silinmesini talep hakkı bağlamında böyle bir düzenlemeye rastlanmamaktadır.

Yönerge kapsamında kişisel verilerin bloke edilmesi; ilgili verilerin doğruluğunun tartışmalı olması ve verilerin doğru olup olmadığının belirlenemiyor olması durumunda söz konusudur.[53] Kişisel verilerin bloke edilmesi durumunda veri sorumlusunun veriler üzerindeki tasarruf yetkisi tamamen sona ermez; fakat tamamen ya da kısmen durdurulur.[54]

Yönerge hükümlerinde kişisel verilerin bloke edilmesinin ne anlama geldiği açık bir şekilde tanımlanmamış olmakla birlikte[55], doktrinde bu uygulamanın kişisel verilerin doğru olup olmadığı konu-

hükümler gibi diğer bazı hükümler uyarınca korunma hakkı olabileceği belirtilmektedir. Bkz. "Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques," European Commission, erişim tarihi 8 Ağustos 2019, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, 3.

51 Madde 29 Veri Koruma Çalışma Grubu *(Article 29 Data Protection Working Party)* tarafından hazırlanmış olan 10.04.2014 tarihli Anonimleştirme Teknikleri Hakkında Görüş için bkz. European Commission, "Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques."

Görüşte anonimleştirme tekniklerinin sağlamlığı, kıstas olarak üç soru temelinde ele alınmıştır:

1. Bireyin belirlenmesi hala mümkün mü?

2. Bireye ilişkin kayıtlarla bağlantı kurmak hala mümkün mü?

3. Birey hakkında bilgi çıkarımında bulunmak mümkün mü?

Bkz. European Commission, "Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques." 3.

52 Başalp, *Kişisel Verilerin Korunması ve Saklanması*, 50.

53 Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 93.

54 Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 93.

55 Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 93; Küzeci, *Kişisel Verilerin Korunması*, 229.

sunda tereddüt oluşması halinde, bu tereddüdün giderilmesine kadar söz konusu verilerin işlenmemesi amacına yönelik bir önlem niteliğinde olduğu belirtilmektedir.[56] Dolayısıyla kişisel verilerin bloke edilmesinde önleyici bir koruma söz konusudur.[57] Bu önlemle amaçlanan, doğru olup olmadığı kesin olarak belli olmayan kişisel verilerin kullanılmasının engellenmesi yoluyla ilgili kişilerin korunmasıdır.[58]

3. Tüzük Bakımından

Yönerge'de ilgili kişiye sağlanmış olan kişisel verilerin silinmesini talep hakkının karşılığı, Tüzük m. 17 hükmünde bulunmaktadır.[59]

Tüzük m. 17/1 hükmünde ilgili kişiye kişisel verilerin gereksiz gecikmeye mahal vermeksizin silinmesini talep hakkı tanınmış ve veri sorumlusunun kişisel verileri gereksiz gecikmeye mahal vermeksizin silmekle yükümlü olduğu haller sayılmıştır.

Tüzük kapsamında kişisel verilerin silinmesi *(erasure)*, elektronik olarak saklanmış olan kişisel verilerin ayırt edilemez hale getirilmesi olarak tanımlanırken, yok etme *(destruction)* kavramı kişisel verilerin saklanmış olduğu fiziksel eşyalara ilişkindir.[60] Verinin bulunduğu araçların fiziksel olarak yok edilmiş olması veya özel bir yazılım kullanılarak verinin kalıcı olarak üzerine yazılmış olması yeterli görülmektedir.[61] Dolayısıyla Yönerge ter-

---

56 Ulrich Dammann, *Bundesdatenschutzgesetz*, ed. Spiros Simitis (München: Nomos, 2014), Art. 12 Rn. 16*ff*. (Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 93'ten naklen).

57 Küzeci, *Kişisel Verilerin Korunması*, 229.

58 Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 94.

59 Nilgün Başalp, "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri," *MÜHFD* 21, no. 1 (2015): 93.

60 Robert Kazemi, *General Data Protection Regulation (GDPR)* (Hamburg: Tredition, 2018), § 2, Recital 61.

61 "Key Issues, GDPR Right to be Forgotten," Intersoft Consulting, erişim tarihi 8 Ağustos 2019, https://gdpr-info.eu/issues/right-to-be-forgotten/.

minolojisinde olduğu gibi, Tüzük uyarınca kişisel verilerin silinmesini talep hakkının KVKK ve Yönetmelik anlamında kişisel verilerin silinmesi ve yok edilmesi kavramlarını kapsadığını söylemek mümkündür.

Maddenin kenar başlığı incelendiğinde, silme hakkı *(right to erasure)* ve unutulma hakkı *(right to be forgotten)* ifadelerinin kullanılmış olduğu görülmektedir.[62] Unutulma hakkına ilişkin birçok tartışma mevcuttur; nitekim silme hakkı *(right to erasure)*, unutma hakkı *(right to oblivion)*, dizinden çıkarma hakkı *(right to delisting)* kavramlarının da birbirleri yerine kullanıldığına rastlanılmaktadır.[63]

Tüzük'ün yürürlüğe girmesinden önce unutulma hakkı Avrupa Birliği mevzuatında henüz bir hak olarak tanınmamış, fakat bu hakkın temelleri Avrupa yargı organları tarafından atılmıştı.[64] Keza Avrupa Komisyonu; unutulma hakkının yeni bir konsept olmadığı ve bu hakkın temelini oluşturan prensiplerin, artık gerekli olmayan kişisel verilerin silinmesinin talep edilebileceğine dair Yönerge m. 12 hükmüyle zaten düzenlenmiş olduğu görüşündedir.[65]

---

62 Unutulma hakkı Avrupa Komisyonu tarafından öngörülmüş olmakla birlikte, hak Avrupa Birliği Parlamentosu nezdindeki görüşmelerde önemli kısıtlamalara maruz kalmış, öyle ki "unutulma hakkı" ismi dahi uygun bulunmamış ve hakkın mevcut sınırlamalar kapsamında "kişisel verilerin silinmesi hakkı" şeklinde tanımlanması tercih edilmiştir. Başalp, "Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri," 98. Bkz. "European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," European Parliament, erişim tarihi 8 Ağustos 2019, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//EN.

63 Bu hususta bkz. Küzeci, *Kişisel Verilerin Korunması*, 231-232.

64 Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 17-18.

65 W. Gregory Voss, "The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation," *Journal of Internet Law*, (July 2014): 3.

Avrupa Birliği Adalet Divanı'nın 13.05.2014 tarihli *Google-Spain* Kararı[66], unutulma hakkı bakımından Tüzük çalışmalarında etkili olmuştur.[67] Karar *"unutulma hakkı kararı"* olarak anılmaktadır.[68]

Google-Spain Kararı'nda, belirlenmiş olan bazı koşulların gerçekleşmesi halinde bireylerin kişisel verilerinin yer aldığı bağlantıların arama motorlarından kaldırılmasını isteme hakkının mevcut olduğu sonucuna varılmıştır.[69] Buna göre sonuç listesinde sunulmuş olan verinin uygunsuz veya alakasız olması ya da artık güncel olmaması veya verinin işlenme amaçlarıyla kıyaslandığında orantısız olması durumlarında, söz konusu bilgi ve bağlantıların silinmesi gerekecektir.[70] Zira arama motoru şirketinin ekonomik çıkarları, bireyin özel yaşamının gizliliği hakkından üstün değildir.[71] Bununla birlikte kararda unutulma hakkının mutlak bir hak olmadığı da ifade edilerek, somut olayın özellikleri dikkate alınarak basın özgürlüğü ve düşünceyi açıklama özgürlüğü gibi diğer bazı temel haklar ile unutulma hakkı arasında denge kurulması gerektiği belirtilmiştir.[72]

---

66 Karar; İspanyol M. C. G. tarafından İspanyol Veri Koruma Otoritesi, bir İspanyol Gazete, Google İspanya ve Google Inc.'e karşı 2010 yılında yapılan bir başvuruya ilişkindir. M. C. G.; borçları sebebiyle evinin açık artırmaya çıkarılmış olmasına ilişkin yıllar öncesinde verilen ilanın Google arama sonuçlarında hala mevcut olmasının özel yaşamın gizliliği hakkını ihlal ettiğini, açık artırma gerekçelerinin yıllar öncesinde ortadan kalkmış olduğunu, hatta bu evi geri almış olduğunu ve bu bilgilerin artık gereksiz olduğunu ileri sürerek, gazetenin ilgili sayfalarının kaldırılması veya değiştirilmesini ve bu kişisel verilerin arama sonuçlarından da çıkarılmasını talep etmiştir. Davayı görmekte olan İspanya'daki yetkili mahkeme, konu hakkında Avrupa Birliği Adalet Divanı'na başvurmuştur. Bkz. Küzeci, *Kişisel Verilerin Korunması*, 232. Kararın unutulma hakkı haricinde ele aldığı sair hususlar için bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 143; Küzeci, *Kişisel Verilerin Korunması*, 232.

67 Küzeci, *Kişisel Verilerin Korunması*, 230; Voss, "The Right to Be Forgotten," 5.

68 Hasan Elmalıca, "Bilim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı," *AÜHFD* 65, no. 4 (2016): 1613.

69 Küzeci, *Kişisel Verilerin Korunması*, 232.

70 Çekin, *Kişisel Verilerin Korunması Kanunu*, 143.

71 Küzeci, *Kişisel Verilerin Korunması*, 232-233.

72 Küzeci, *Kişisel Verilerin Korunması*, 233.

Unutulma hakkı; Avrupa Birliği tarafından 2010 yılında yapılan bir basın açıklamasıyla ismen anılarak tanımlanmıştır.[73] Buna göre unutulma hakkı; bireyin toplandıkları amaçlar doğrultusunda artık ihtiyaç duyulmayan kişisel verilerinin tamamen silinmesini isteme hakkıdır.[74]

Türk hukukunda unutulma hakkı Yargıtay Hukuk Genel Kurulu'nun 17.06.2015 tarihli, 2014/56 E., 2015/1679 K. sayılı kararıyla[75]

---

[73] Steven C. Bennett, "The 'Right to Be Forgotten': Reconciling EU and US Perspectives," *Berkeley Journal of International Law* 30, no. 1 (2012): 162; Başalp, "Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri," 97.

[74] Bennett, "The Right to Be Forgotten," 162; Başalp, "Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri," 97. Unutulma hakkının, veri sahibine kişisel verisinin silinmesini, kişisel verisinin yayımlanmasının ve potansiyel üçüncü kişilere aktarılmasının önlenmesini talep etme hakkı tanıdığı belirtilmektedir. Bkz. Murat Volkan Dülger, "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması," *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* 5, no. 1 (2018): 101.

[75] Karara konu uyuşmazlık haksız fiil nedeniyle manevi tazminat istemine ilişkindir. Davacının cinsel taciz suçundan şikâyetçi olduğu ceza davasında yapılan yargılama sonucunda temyiz üzerine Yargıtay tarafından verilen karar, Yargıtay 4. Ceza Dairesi Başkanı ve tetkik hâkimleri olan davalıların, Nisan 2010'da "Yorumlu-Uygulamalı Türk Ceza Kanunu" isimli ve altı ciltten oluşan eserinde yayımlanmıştır. Bu eserin örnek Yargıtay kararlarının başlamış olduğu 3262 ve devamındaki sayfalarında davacının başına gelen olaylar, tüm aktörlerin isimlerinin açıkça yazılması suretiyle açık bir şekilde anlatılmıştır. Bunun üzerine davacı kişilik haklarına saldırı olduğu gerekçesiyle isminin geçtiği söz konusu ciltlerin toplatılmasını ve davalıların manevi tazminatla sorumlu tutulmalarını talep etmiştir. Karar uyarınca davacının rızası olmaksızın bir kitapta geçen ismi kişisel veri niteliğindedir. Kararda, kişinin adının açık bir şekilde yazılarak kitapta yer alması halinde unutulma hakkının bunun sonucunda da davacının özel hayatının gizliliğinin ihlal edildiğinin kabul edilmesi gerektiği belirtilmiştir. Ayrıca Avrupa Birliği Adalet Divanı'nın Google-Spain Kararı'na da atıf yapılarak, verinin kamu hayatında oynadığı önemli rol ve halkın ilgili veriye yönelik yoğun ilgisi şeklinde üstün bir kamu yararını ortaya koyan özel sebepler bulunmadığından, bilimsel esere alınan kararda kişisel verilerin açık bir şekilde yer almaması gerektiği belirtilmiştir. Yargıtay Hukuk Genel Kurulu tarafından sonuç olarak, davacının ismine rumuzlanmadan kitapta yer verilmesinin unutulma hakkını ve bunun sonucunda özel hayatın gizliliğini ihlal ettiği dikkate alındığında, davacı lehine manevi tazminat koşullarının gerçekleştiğine karar verilmiştir. Kaynak: Corpus Web Hukuk Mevzuat ve İçtihat Programı, www.corpus.com.tr.

tanımlanmıştır.[76] Buna göre *unutulma hakkı; üstün bir kamu yararı olmadığı sürece, dijital hafızada yer alan geçmişte yaşanılan olumsuz olayların bir süre sonra unutulmasını, başkalarının bilmesini istemediği kişisel verilerin silinmesini ve yayılmasının önlemesini isteme hakkı olarak ifade edilebilir*.

Anayasa Mahkemesi'nin N.B.B. Kararı'nda da Avrupa Birliği Adalet Divanı'nın *Google-Spain* Kararı'na[77] ve Yargıtay Hukuk Genel Kurulu'nun belirtilen 17.06.2015 tarihli kararına atıf yapılmıştır.[78] Kararda unutulma hakkının Anayasa'da açıkça düzenlenmemiş olmasına rağmen Anayasa'nın 5. maddesinde *"insanın maddi ve manevi varlığının gelişmesi için gerekli şartları hazırlamaya çalışmak"* ifadesi ile devlete pozitif bir yükümlülük yüklenmiş olduğu, bu yükümlülük kapsamında Anayasa'nın 17. maddesinde düzenlenen kişinin mane-

---

[76] Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 18, dn. 51.

[77] Küzeci, *Kişisel Verilerin Korunması*, 230, dn. 107.

[78] AYM E.2013/5653, K.2013/5653, 03.03.2016 N.B.B. Başvurusu Kararı 24.08.2016 tarihinde 29811 sayılı Resmî Gazete'de; AYM E.2014/17143, K.2014/17143, 01.03.2017 N.B.B. Başvurusu (2) Kararı ise 22.03.2018 tarihinde 30015 sayılı Resmî Gazete'de yayımlanmıştır. Kaynak: Corpus Web Hukuk Mevzuat ve İçtihat Programı, www.corpus.com.tr. Bu iki başvuru arasındaki tek fark, aynı haberin farklı gazetelerin internet arşivlerinde yayımlanmasıdır. Başvurular; gerçeğe aykırı ya da uydurma haber olduğu iddia edilmeyen 1999 yılında yapılmış bir yargılamaya ilişkin haberin, halen arşivde yer alması ve internet üzerinden habere erişimin kolayca mümkün olması sebepleriyle kişinin özel ve iş hayatının olumsuz etkilendiği, itibarının zedelendiği iddialarına ilişkindir. Anayasa Mahkemesi tarafından 03.03.2016 tarihinde karara bağlanan ilk başvuru, bir gazetenin internet haber arşivinde erişilebilir durumda olan haber ve yayınlar ile ilgili içeriğin yayından kaldırılması yönündeki talebin reddedilmesinin şeref ve itibarın korunması hakkını ihlal ettiği iddiasına ilişkindir. Mahkeme, başvuru hakkında şeref ve itibarın korunması hakkının ihlal edildiğine ilişkin iddianın kabul edilebilir olduğuna ve Anayasa'nın 17. maddesinin birinci fıkrasında güvence altına alınan şeref ve itibarın korunması hakkının ihlal edildiğine karar vermiştir. Anayasa Mahkemesi tarafından 01.03.2017 tarihinde karara bağlanmış olan ikinci başvuru sonucunda ise incelemenin sürdürülmesini haklı kılan bir nedenin kalmamış olması sebebiyle başvurunun düşmesine karar verilmiştir. Zira Anayasa Mahkemesi'nin 03.03.2016 tarihli ilk kararı referans alınarak yetkili yargı mercilerinden tekrar içeriğe erişimin engellenmesinin talep edilmesi mümkündür.

vi bütünlüğü bağlamında şeref ve itibarının korunması hakkı ve Anayasa'nın m. 20/3 hükmünde güvence altına alınan kişisel verilerin korunmasını isteme hakkı birlikte düşünüldüğünde, devletin bireyin geçmişte yaşadıklarının başkaları tarafından öğrenilmesini engelleyerek bireye *"yeni bir sayfa açma"* olanağı verme hususunda bir sorumluluğu olduğunun açık olduğu ifade edilmiştir.

Yönerge m. 12 aksine, Tüzük hükümlerinde *"kişisel verilerin bloke edilmesi"* kavramı yer almamaktadır. Yönerge'de yer alan *"kişisel verilerin bloke edilmesi" (blocking of data)* kavramı yerine Tüzük hükümlerinde *"kişisel verilerin işlenmesinin kısıtlanması" (restriction of processing)* kavramı kullanılmıştır.[79] Tüzük m. 4/3 uyarınca kişisel verilerin işlenmesinin kısıtlanması; kaydedilmiş olan verilerin gelecekte işlenmesini sınırlandırmak amacıyla işaretlenmesi anlamına gelmektedir.[80] Tüzük m. 18 hükmüyle kişisel verilerin işlenmesinin kısıtlanmasını talep hakkı, kişisel verilerin silinmesini talep hakkından ayrı bir şekilde düzenlenmiştir.

Anonimleştirilmiş veriler bakımından Yönerge ve Tüzük paralel bir anlayışa sahiptir. Bununla birlikte Tüzük maddelerinde anonimleştirme kavramı tanımlanmış değildir.[81] Tüzük'ün 26 numaralı şerh paragrafı uyarınca veri koruma ilkeleri, belirli veya belirlenebilir gerçek kişilere ilişkin her türlü bilgi hakkında uygulama alanı bulur. Fakat veri koruma ilkelerinin, belirli veya belirlenebilir bir gerçek kişiye ilişkin olmayan anonim veriler hakkında ve veri öznesinin artık belirlenemeyeceği şekilde anonim hale getirilmiş olan kişisel veriler hakkında uygulama alanı bulmayacağı aynı paragrafta açık bir şekilde belirtilmiştir. Dolayısıyla Tüzük hükümleri anonim bilgilerin işlenmesi hakkında uygulama alanı bulmamaktadır. Verinin

---

79 Kazemi, *GDPR*, § 2 Recital 59.

80 Tüzük'ün 67 numaralı şerh paragrafında kişisel verilerin işlenmesinin kısıtlanması yöntemlerine örnekler verilmiştir. Buna göre seçilmiş olan verinin geçici olarak başka bir işleme sistemine taşınması, seçilmiş olan verinin başkaları için erişilmez kılınması veya yayımlanmış olan bir verinin geçici olarak internet sitesinden silinmesi kişisel verilerin işlenmesinin kısıtlanması yöntemlerine örnektir.

81 Kazemi, *GDPR*, § 2, Recital 65.

yeteri kadar anonim hale getirilmiş olduğuna dair ispat yükü veri sorumlusu üzerindedir.[82]

Tüzük m. 4/5 ile *"takma ad verme" (pseudonymization)* kavramı ilk kez açıklanmıştır. Buna göre takma ad verme; kişisel verilerin ek bilgi kullanılmadan belirli bir veri sahibine atfedilemeyeceği bir şekilde işlenmesi olarak tanımlanır.[83] Takma ad verme yöntemi kişisel verilerin anonimleştirilmesinden farklı bir kavramdır ve bu yöntemle bir kişinin kimliğinin tespit edilmesi ihtimalinin kalıcı olarak engellenmesi amaçlanmaz.[84] [85]

B. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesini Gerektiren Haller

KVKK m. 5 ve 6 hükümlerinde sırasıyla kişisel verilerin işlenme şartları ve özel nitelikli kişisel verilerin işlenme şartları düzenlenmiştir. KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, KVKK m. 5 ve 6 hükümlerinde düzenlenmiş olan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından re'sen

---

[82] Kazemi, *GDPR*, § 2, Recital 65.

[83] Cennet Alas Şekerbay, "GDPR ile gelen "Pseudonymization" (Takma Ad Verme) Kavramı," *Academia*, erişim tarihi 8 Ağustos 2019, https://www.academia.edu/36711924/GDPR_ile_gelen_Pseudonymization_Takma_Ad_Verme_Kavram%C4%B1?auto=download.

[84] Kazemi, *GDPR*, § 2, Recital 63.

[85] Kişisel Sağlık Verileri Hakkında Yönetmelik ile "kimliksizleştirme" kavramı Türk hukukunda kişisel verilerin korunmasına dair mevzuatta ilk kez kullanılmış olup, kavramın kaynağını Tüzük m. 4/5'te tanımlanmış olan "takma ad verme" *(pseudonymization)* oluşturmaktadır. Kişisel Sağlık Verileri Hakkında Yönetmelik ile "kimliksizleştirme" ifadesi tercih edilmiş olmakla birlikte, tanımlama Tüzük m. 4/5 ile aynı doğrultuda yapılmıştır. Bkz. Murat Volkan Dülger, "Kişisel Sağlık Verileri Hakkında Yönetmelik'e İlişkin Değerlendirme," *Hukuki Haber*, Temmuz 14, 2019, erişim tarihi 8 Ağustos 2019, https://www.hukukihaber.net/kisisel-saglik-verileri-hakkinda-yonetmelike-iliskin-degerlendirme-makale,6847.html. Kişisel Sağlık Verileri Hakkında Yönetmelik m. 4/1-ı uyarınca kimliksizleştirme; kişisel verilerin kimliği belirli veya belirlenebilir gerçek kişiyle ilişkilendirilememesi için teknik ve idari tedbirlerin alınması şartıyla ve farklı bir ortamda muhafaza edilen diğer verilerle bir araya getirilmeksizin ilgili kişiyle ilişkilendirilemeyecek şekilde işlenmesini ifade eder.

veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekmektedir (KVKK m. 7/1, Yönetmelik m. 7/1).[86] Bununla birlikte kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklı tutulmuştur (KVKK m. 7/2).[87]

Yönerge uyarınca ise ilgili kişiler; özellikle eksik veya yanlış olmasından dolayı bu Yönerge hükümlerine uygun olmayan bir şekilde işlenmiş olan verilerin, uygunluğa göre düzeltilmesi, silinmesi veya bloke edilmesini veri sorumlusundan talep etme hakkına sahiptir (Yönerge m. 12-b).

Tüzük'ün *"silme hakkı"* ve *"unutulma hakkı"* kenar başlıklı 17. maddesinin ilk fıkrası uyarınca veri sahibi olan ilgili kişi, veri sorumlusundan kendisi ile ilgili kişisel verilerin gereksiz gecikmeye mahal vermeksizin silinmesini talep etme hakkına sahiptir. Tüzük m. 17/1 gereği veri sorumlusu, altı bent halinde açıklanmış olan hallerden birinin söz konusu olması halinde, kişisel verileri gereksiz gecikmeye mahal vermeksizin silmekle yükümlüdür. Dolayısıyla m. 17/1 gereği;

- Kişisel verilerin toplanma veya işlenme amaçları bakımından artık gerekli olmaması,
- Veri sahibinin rızasını geri alması ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması,

---

[86] Yönetmelik m. 7/4 gereği veri sorumlusunun, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemiyle ilgili olarak uyguladığı yöntemleri ilgili politika ve prosedürlerinde açıklama yükümlülüğü söz konusudur.

[87] Kişisel verilerin silinmesi, yok edilmesi veya anonim hâle getirilmesine ilişkin diğer kanunlarda yer alan hükümlerin saklı tutulduğu KVKK m. 7/2 hükmünün; kuralın çok geniş kapsamlı olduğu, bireylerin hangi kişisel verilerinin hangi kanunda hangi düzenleme ile silineceği veya ne kadar sürede silineceğini bilemeyeceği, kişisel verilerin yok edilme ve anonim hale getirilmesi şartlarının belirsiz olduğu, kamu yararı ve ölçülülük ilkesinin gözetilmediği belirtilerek kuralın Anayasa'nın 2. maddesine aykırı olduğu ileri sürülmüştür. Anayasa Mahkemesi tarafından KVKK m. 7/2 hükmü Anayasa'ya aykırı bulunmamış ve iptal talebi oy birliğiyle reddedilmiştir. 23.01.2018 tarihli, 30310 sayılı Resmî Gazete'de yayımlanmış olan AYM E.2016/125, K.2017/143, 28.09.2017 kararı için bkz. Corpus Web Hukuk Mevzuat ve İçtihat Programı, www.corpus.com.tr.

- Veri sahibinin itirazda bulunması,
- Kişisel verilerin hukuka aykırı bir şekilde işlenmiş olması,
- Veri sorumlusunun tabi olduğu Avrupa Birliği veya üye devlet hukukundaki bir hukuki yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması,
- Kişisel verilerin m. 8/1'de belirtilmiş olan bilgi toplumu hizmetlerinin sağlanması ile ilgili olarak toplanmış olması

hallerinden birinin mevcut olması durumunda veri sorumlusunun kişisel verileri silme yükümlülüğü doğacaktır.

Veri sorumlusunun kişisel verilerin silinmesine dair yükümlülüğünün doğması için bu hallerden birinin gerçekleşmesi gerekli ve yeterlidir. Bahsedilen hallerden hiçbirinin mevcut olmaması durumunda kişisel verilerin silinmesini talep hakkı doğmayacağı gibi, unutulma hakkı da söz konusu olmayacaktır.

Tüzük m. 17/2 düzenlemesi ise kamuya açıklanmış olan kişisel verilerin silinmesi hususunda atılması gereken makul adımlara ilişkindir.[88]

Bununla birlikte Tüzük m. 17/3 fıkrasıyla ilk ve ikinci fıkraya ilişkin istisnalar öngörülmüştür. Buna göre Tüzük m. 17/3 fıkrasında sayılmış olan amaçlar doğrultusunda kişisel verilerin işlenmesinin gerekli olduğu hallerde maddenin ilk ve ikinci fıkrası uygulama alanı bulmaz; dolayısıyla ilgili kişi kişisel verilerin silinmesi talebinde bulunma hakkını haiz olmaz.

---

[88] Tüzük'ün 66 numaralı şerh paragrafı uyarınca çevrimiçi ortamda unutulma hakkını kuvvetlendirmek amacıyla silme hakkı genişletilmeli ve kişisel verileri kamuya açıklamış olan bir veri sorumlusu, bu kişisel verileri işleyen veri sorumlularını kişisel verilere ilişkin linklerin, kopyaların veya tekrarların silinmesi yönünde bilgilendirmekle yükümlü olmalıdır. Veri sorumlusu bu yükümlülüğünü yerine getirirken, kişisel verileri işleyen veri sorumlularını veri sahibinin talebi hakkında bilgilendirmek amacıyla, mevcut teknoloji ve teknik önlemler de dâhil olmak üzere kullanabileceği araçları hesaba katarak makul adımları atmalıdır.

Ayrıca Tüzük m. 19 gereği veri sorumlusu; m. 17/1 uyarınca yapılan kişisel verilerin silinmesi işlemini, bu durum imkânsız veya aşırı bir çabayı gerektirir olmadıkça kişisel verilerin açıklanmış olduğu tüm alıcılara bildirmelidir. Yine aynı madde uyarınca ilgili kişinin talebi üzerine veri sorumlusu ilgili kişiyi bu alıcılar hakkında bilgilendirmelidir.

KVKK uyarınca veri sorumlusunun kişisel verileri silmesi, yok etmesi veya anonim hale getirmesi gereken hallerin belirlenmesi için öncelikle kişisel verilerin ve özel nitelikli kişisel verilerin işlenme şartlarının incelenmesi gerekmektedir. Zira ancak bu şartların ortadan kalkması durumunda veri sorumlusunun kişisel verileri silmesi, yok etmesi veya anonim hale getirmesi zorunludur.

1. Kişisel Verilerin İşlenme Şartlarının Ortadan Kalkması

Kişisel verilerin işlenme şartları KVKK m. 5 hükmünde açıklanmıştır. Buna göre kural olarak kişisel verilerin ilgili kişinin açık rızası alınmadan işlenmesi yasaktır (KVKK m. 5/1).[89] Bununla birlikte devam eden fıkra ile ilgili kişinin rızası olmaksızın kişisel verilerin işlenmesinin mümkün olduğu haller açıklanmıştır.[90]

---

[89] KVKK m. 3/1-a hükmüyle açık rıza; *"belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza"* olarak tanımlanmıştır. Tüzük m. 4/11 uyarınca ise *"ilgili kişinin rızası, ilgili kişinin isteklerinin özgür, somut, bilgilendirmeye dayalı ve kesin olan her türlü göstergesini ifade eder ki kişi, bir ifade ya da olumlu eylem sayesinde kendisiyle ilgili kişisel verinin işlenmesini kabul ettiğini bu sayede belirtsin."*. Açık rızanın Tüzük'te daha geniş ve somut bir şekilde tanımlanmış olduğu görülmektedir. Çekin, *Kişisel Verilerin Korunması Kanunu*, 55. Açık rızanın hukuki niteliğine dair mukayeseli hukuktaki tartışmalar için bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 56-58. Açık rızanın kişisel verilerin işlenmesinden önce açıklanmış olması gerekmektedir. Bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 58; Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 159. KVKK kapsamında açık, belirli bir konuyla bağlantılı ve bilgilendirmeye dayanan özgür bir rızanın verilmiş olması arandığından (KVKK m. 3/1-a), genel ve geniş çaplı bir rıza yeterli görülmemektedir. Bkz. Mesut Serdar Çekin, "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi," *İÜHFM* 74, no. 2 (2016): 636-637.

[90] KVKK kapsamında kişisel verilerin açık rıza olmaksızın işlenebildiği hukuka uygunluk sebepleri hakkında detaylı bilgi için bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 63*ff*.; Dülger, *Kişisel Verilerin Korunması Hukuku*, 216-220.

Buna göre;

1. "Kanunlarda açıkça öngörülmesi,
2. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,
4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
5. İlgili kişinin kendisi tarafından alenileştirilmiş olması,
6. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması"

durumlarından herhangi birinin mevut olması halinde, ilgili kişinin açık rızası olmaksızın kişisel verilerin işlenmesi hukuka uygundur (KVKK m. 5/2).[91]

Dolayısıyla ilgili kişinin KVKK m. 5/1 uyarınca vermiş olduğu açık rızasını geri alması[92] veya KVKK m. 5/2 hükmünde düzenlen-

[91] KVKK m. 5/2 hükmünde belirtilmiş olan hukuka uygunluk sebeplerinden birinin mevcut olması ihtimalinde, buna rağmen ilgili kişiden açık rıza talep edilmesi sonucunda ilgili kişi rızasını dilediğinde geri alabileceğini düşünebilecek; fakat hâlihazırda hukuka uygunluk sebebi mevcut olduğundan kişinin rızasını geri almasının bir anlamı olmayacaktır. Bu nedenle hukuka uygunluk sebebinin bulunmasına rağmen ilgili kişiden açık rıza vermesinin talep edilmesi yanıltıcı bir uygulama olarak nitelendirilmekte ve genel işlem şartları kapsamında böyle bir maddeye yer verilmesi halinde bunun geçersiz olacağı savunulmaktadır. Bkz. Astrid Auer-Reinsdorff ve Isabell Conrad, *Handbuch IT- und Datenschutzrecht* (München: C. H. Beck, 2015), 1658, 1662*ff*. (Çekin, *Kişisel Verilerin Korunması Kanunu*, 64'ten naklen).

miş olan açık rıza olmaksızın kişisel verilerin işlenebileceği durumların ortadan kalkması halinde, KVKK m. 7/1 ve Yönetmelik m. 7/1 gereği kişisel verilerin veri sorumlusu tarafından re'sen ya da ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekmektedir.

2. Özel Nitelikli Kişisel Verilerin İşlenme Şartlarının Ortadan Kalkması

Özel nitelikli kişisel veri; "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 tanımlanmaktadır (KVKK m. 6/1).

Özel nitelikli kişisel verilerin, bu niteliği haiz olmayan kişisel verilerde olduğu gibi, ilgilinin açık rızası olmaksızın işlenmesi kural olarak yasaktır (KVKK m. 6/2).[93] Fakat bu kurala ilişkin de birtakım istisnalar düzenlenmiştir.[94]

Buna göre sağlık ve cinsel hayat dışındaki özel nitelikli kişisel verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası gerekmeksizin işlenmesi mümkündür (KVKK m. 6/3).

---

92 KVKK ve Yönetmelik kapsamında açık rızanın nasıl geri alınabileceği düzenlenmemiştir. Bununla birlikte Tüzük m. 7/3 hükmüyle verisi işlenen kişinin her an rızasını iptal edebileceği ve iptal işleminin rızanın verilmesi kadar basit olması gerektiği düzenlenmiştir. Bu düzenlemenin Türk hukukunda da kabul edilmesi gerektiği belirtilmektedir. Bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 62.

93 Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şart koşulmuştur (KVKK m. 6/4). Kurul'un 07.03.2018 tarihli, 30353 sayılı Resmî Gazete'de yayımlanmış olan 31.01.2018 tarihli, 2018/10 numaralı kararıyla, özel nitelikli kişisel veri işleyen veri sorumluları tarafından alınması gereken yeterli önlemler belirlenmiştir.

94 Yönerge m. 8/1 uyarınca da özel nitelikli kişisel veriler bakımından işlem yasağı söz konusudur. Bkz. Başalp, *Kişisel Verilerin Korunması ve Saklanması*, 111. Bununla birlikte Yönerge'nin 8. maddesinin devam eden fıkralarında bu kurala ilişkin istisnalara yer verilmiştir. Keza Tüzük m. 9/1 uyarınca da özel nitelikli kişisel verilerin işlenmesi kural olarak yasaktır; fakat bu kuralın istisnaları Tüzük m. 9/2 hükmünde sıralanmıştır.

Sağlık ve cinsel hayata ilişkin özel nitelikli kişisel verilerin ancak sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi mümkündür (KVKK m. 6/3). Bu tür özel nitelikli kişisel veriler ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla ilgili kişinin açık rızası gerekmeksizin işlenebilmektedir (KVKK m. 6/3).

Sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesi için belirlenmiş olan bu koşulların ortadan kalkması durumunda, kişisel verilerin veri sorumlusu tarafından re'sen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi KVKK m. 7/1 ve Yönetmelik m. 7/1 gereği zorunludur. İlgilinin açık rızasına dayanılarak işlenmiş olan özel nitelikli kişisel verilerin ise bu açık rızanın geri alınması durumunda yine KVKK m. 7/1 ve Yönetmelik m. 7/1 gereği silinmesi, yok edilmesi veya anonim hâle getirilmesi zorunlu olacaktır.

C. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Yöntemlerinden Birinin Seçimi

Veri sorumlusu; Kurul tarafından aksi yönde bir karar alınmış olmadıkça, kişisel verileri re'sen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını kendisi seçecektir (Yönetmelik m. 7/5). Bununla birlikte ilgili kişinin kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yöntemlerinden hangisinin uygulanmasını istediği yönündeki talebini veri sorumlusuna iletmesi halinde, veri sorumlusu uygun yöntemi gerekçesini de açıklamak suretiyle seçer (Yönetmelik m. 7/5).

Dolayısıyla ilgili kişinin kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi yöntemlerinden tercihinin veri sorumlusu tarafından direkt yerine getirilmesi gerekmemekte; bu bakımdan veri sorumlusu uygun yöntemi gerekçesini bildirmek suretiyle tercih edebilmektedir. Örneğin ilgili kişi kişisel verilerinin yok edilmesini talep etmiş olsa da veri sorumlusunun uygun yöntemin kişisel verilerin anonim hale getirilmesi olduğunu gerekçesiyle birlikte

bildirerek, ilgili kişinin verilerini yok etmek yerine anonim hale getirmesi mümkündür. Bununla birlikte veri sorumlularının kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde KVKK m. 4 hükmünde düzenlenmiş olan genel ilkelere[95] ve KVKK m. 12 hükmü kapsamında alınması gereken teknik ve idari tedbirlere, ayrıca ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket etmeleri zorunludur (Yönetmelik m. 7/2).

D. Veri Sorumluları Sicili ve Veri Sorumlularının Kişisel Veri Saklama ve İmha Politikası Hazırlama Yükümlülüğü

Veri Sorumluları Sicili'ne kayıt olmakla yükümlü olan veri sorumluları, kişisel veri saklama ve imha politikası hazırlamakla yükümlüdürler (Yönetmelik m. 5/1).

Kişisel veri saklama ve imha politikalarının asgari kapsamının ne olduğu Yönetmelik m. 6 hükmünde detaylı bir şekilde belirtilmiştir. Kurul tarafından, Veri Sorumluları Sicili'ne kayıtla yükümlü olan veri sorumlularına kişisel veri saklama ve imha politikası hazırlama konusunda örnek ve yardımcı olması amacıyla "*Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası"* hazırlanmıştır.[96]

---

[95] Bu ilkeler KVKK m. 4/2 hükmünde; "*a) Hukuka ve dürüstlük kurallarına uygun olma, b) Doğru ve gerektiğinde güncel olma, c) Belirli, açık ve meşru amaçlar için işlenme, ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme*" şeklinde sayılmıştır. İlkelerin bu sıra ve isimlerle açıklaması için bkz. Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 44-50. Bununla birlikte kişisel veri işlenmesinin kural olarak yasak olması da KVKK'da esas alınan temel ilkelerden biri olarak değerlendirilmektedir. Bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 42-44.

[96] "Kişisel Verileri Koruma Kurumu Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası, Veri Sorumlularına Örnek Olması İçin Kurum İnternet Sayfasında Yayınlanmıştır," KVKK, erişim tarihi 8 Ağustos 2019, https://www.kvkk.gov.tr/Icerik/5387/KVKK-Kisisel-Veri-Saklama-ve-Imha-Politikasi. Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası örneği için bkz. "KVKK Kişisel Veri Saklama ve İmha Politikası," KVKK, erişim tarihi 8 Ağustos 2019, https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e95a5392-23bf-4b30-8114-0526284c5837.pdf.

KVKK m. 16/2 gereği kural olarak kişisel verileri işleyen gerçek ve tüzel kişiler için veri işlemeye başlamadan önce Veri Sorumluları Sicili'ne kaydolmak zorunludur.[97] Fakat KVKK m. 28/2 gereği belirli hallerde Veri Sorumluları Sicili'ne kayıt yükümlülüğü bulunmamaktadır. KVKK m. 28/2 uyarınca; *"kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması veya ilgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi veya kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması ya da kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması"* hallerinde Veri Sorumluları Sicili'ne kayıt yükümlülüğü yoktur.

Ayrıca KVKK m. 16/2 gereği Kurul tarafından Veri Sorumluları Sicili'ne kaydolma zorunluluğuna istisna getirilmesi mümkündür.[98] Nitekim Kurul bugüne kadar Veri Sorumluları Sicili'ne kayıt yükümlülüğüne istisna getirilmesine dair dört ayrı karar almıştır. Kurul'un bu hususta ki ilk kararı 02.04.2018 tarihli ve 2018/32 numaralı olup, 15.05.2018 tarihli ve 30422 sayılı Resmî Gazete'de yayımlan-

---

[97] Veri Sorumluları Sicili Hakkında Yönetmelik m. 5/1-ç gereği, Veri Sorumluları Sicili'ne kayıtla yükümlü olan veri sorumlularının, kişisel veri işleme envanteri hazırlama yükümlülükleri de bulunmaktadır ve Veri Sorumluları Sicili'ne başvuru yapılırken açıklanan bilgiler kişisel veri işleme envanterine dayalı olarak hazırlanmalıdır. Kişisel veri işleme envanterinde yer verilmesi gereken hususlardan biri de kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresidir (Veri Sorumluları Sicili Hakkında Yönetmelik m. 4/1-h).

[98] KVKK m. 16/2 fıkrası hakkında; Veri Sorumluları Sicili'ne kayıt zorunluluğuna getirilecek istisnanın kişisel verileri işlenen kişiyi korumasız hale getireceği, bu durumun kişinin maddi ve manevi varlığına doğrudan, ölçüsüz bir müdahale olduğu, hukuk devleti ilkesi ile bağdaşmadığı ve istisnanın uluslararası sözleşmelere aykırı olduğu belirtilerek kuralın Anayasa'nın 2. ve 90. maddelerine aykırılık iddiasında bulunulmuştur. Anayasa Mahkemesi tarafından KVKK m. 16/2 hükmü Anayasa'ya aykırı bulunmamış ve iptal talebi oy çokluğuyla reddedilmiştir. 23.01.2018 tarihli, 30310 sayılı Resmî Gazete'de yayımlanmış olan AYM E.2016/125, K.2017/143, 28.09.2017 kararı için bkz. Corpus Web Hukuk Mevzuat ve İçtihat Programı, www.corpus.com.tr.

mıştır. Bu karar uyarınca; herhangi bir veri kayıt sisteminin parçası olmak kaydıyla yalnızca otomatik olmayan yollarla kişisel veri işleyenler, noterler, avukatlar, siyasi partiler, mali müşavirler, dernekler, vakıflar ve sendikalar Veri Sorumluları Sicili'ne kayıt olmak zorunda değildir.

Kurul'un tamamı 18.08.2018 tarihli, 30513 sayılı Resmî Gazete'de yayımlanmış olan 28.06.2018 tarihli, 2018/68 numaralı kararı ile gümrük müşavirleri ve yetkilendirilmiş gümrük müşavirleri bakımından; 05.07.2018 tarihli, 2018/75 numaralı kararı ile arabulucular bakımından, 19.07.2018 tarihli, 2018/87 numaralı kararı ile yıllık çalışan sayısı 50'den az ve yıllık mali bilanço toplamı 25.000.000 TL'den az olan veri sorumlularından ana faaliyet konusu özel nitelikli kişisel veri işleme olmayanlar bakımından Veri Sorumluları Sicili'ne kayıt yükümlülüğüne istisna getirilmiştir. Veri Sorumluları Sicili'ne kayıt yükümlülüğünün başlama tarihleri ise yine aynı gün Resmî Gazete'de yayımlanmış olan Kurul'un 19.07.2018 tarihli, 2018/88 numaralı kararı ile belirlenmiştir.[99]

Sonuç olarak Veri Sorumluları Sicili'ne kaydolmak zorunda olmayan veri sorumluları, kişisel veri saklama ve imha politikası hazırlamakla yükümlü değildir (Yönetmelik m. 5/1). Bununla birlikte Veri Sorumluları Sicili'ne kaydolmak zorunda olmayan veri sorumlularının KVKK'dan doğan yükümlülüklerden muaf tutulması söz konusu değildir.[100] Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan veri sorumlularının da KVKK ve bahsedilen Yönetmelik uyarınca kişisel verileri saklama, silme, yok etme veya anonim hale getirme yükümlülükleri bakidir (Yönetmelik m. 5/3).

Veri sorumlularının kişisel veri saklama ve imha politikası hazırlamakla yükümlü olup olmadıkları, kişisel verilerin re'sen imhası

---

[99] Sonradan Kurul'un 07.09.2019 tarihinde 30881 sayılı Resmî Gazete'de yayımlanmış olan 03.09.2019 tarihli ve 2019/265 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 Veri Sorumluları Siciline kayıt yükümlülüğünü yerine getirmeleri için belirlenen sürenin 31.12.2019 tarihine kadar uzatılmasına"* karar verilmiştir.

[100] Çekin, *Kişisel Verilerin Korunması Kanunu*, 131.

hususunda Yönetmelik m. 11 hükmüyle getirilmiş olan süreler bakımından önem arz etmektedir.

E. Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi İçin Belirlenmiş Olan Süreler

Veri sorumlularının kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemlerini belirli sürelerde yerine getirmeleri aranmıştır. Bu bakımdan kişisel verilerin re'sen veya ilgili kişinin talebi üzerine imhası Yönetmelik'in 11 ve 12. maddelerinde farklı sürelere tabi olarak düzenlenmiştir.

Kişisel verilerin veri sorumluları tarafından imhasına ilişkin belirlenmiş olan süreler dışında, kişisel verilerin imhasıyla ilgili olarak yapılan bütün işlemlerin kayıt altına alınması ve ayrıca bu kayıtların diğer hukuki yükümlülükler hariç olmak üzere minimum üç yıl boyunca saklanması da gerekmektedir (Yönetmelik m. 7/3).

1. Re'sen Silme, Yok Etme veya Anonim Hale Getirme Süreleri

Kişisel verilerin re'sen imhasına dair yükümlülük kapsamında, kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olan ve olmayan veri sorumluları bakımından bir ayrıma gidilmiştir.

Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumluları, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde kişisel verileri silmek, yok etmek veya anonim hale getirmekle yükümlüdür (Yönetmelik m. 11/1).

Periyodik imhanın gerçekleştirileceği zaman aralığının veri sorumluları tarafından kişisel veri saklama ve imha politikasında belirlenmesi mümkündür; fakat bu süre her halde en fazla altı ay olabilir (Yönetmelik m. 11/2).

Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan, diğer bir deyişle Veri Sorumluları Sicili'ne kayıt yükümlülüğü bulunmayan veri sorumluları ise kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içerisinde kişisel verileri silmek, yok etmek veya anonim hale getirmekle yükümlüdür (Yönetmelik m. 11/3).

Bununla birlikte telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde, bahsedilen sürelerin kısaltılabilmesi bakımından Kurul yetkili kılınmıştır (Yönetmelik m. 11/4).

2. Talep Üzerine Silme, Yok Etme veya Anonim Hale Getirme Süreleri

İlgili kişi tarafından veri sorumlusuna başvurularak kendisine ait kişisel verilerin silinmesi veya yok edilmesi talep edildiğinde, kişisel verileri işleme şartlarının tamamının ortadan kalkmış olması koşuluyla, veri sorumlusu talebe konu kişisel verileri silmek, yok etmek veya anonim hale getirmekle yükümlüdür. Veri sorumlusunun, ilgili kişinin talebini en geç otuz gün içerisinde sonuçlandırması ve ilgili kişiye bilgi vermesi gerekmektedir (Yönetmelik m. 12/1-a).

Kişisel verileri işleme şartlarının tamamı ortadan kalkmış olmakla birlikte talebe konu olan kişisel verilerin üçüncü kişilere aktarılmış olması durumunda, veri sorumlusu bu durumu üçüncü kişiye bildirmek ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin etmekle yükümlüdür (Yönetmelik m. 12/1-b).

Bununla birlikte şayet kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu durumda ilgili kişinin talebi veri sorumlusunca KVKK m. 13/3 uyarınca gerekçesi de açıklanarak reddedilebilir (Yönetmelik m. 12/1-c). Nitekim Yönetmelik m. 7/1 uyarınca veri sorumluları ancak kişisel verilerin işlenme şartlarının tamamının ortadan kalkmış olması halinde kişisel verilerin imhasıyla yükümlüdür. Kişisel verileri işleme şartlarının tamamen ortadan kalkmamış olması ve veri sorumlusunun ilgili kişinin talebini reddetmesi durumunda, ret cevabı ilgili kişiye en geç otuz gün içinde olmak üzere yazılı olarak veya elektronik ortamda bildirilmelidir (Yönetmelik m. 12/1-c).

III. KİŞİSEL VERİLERİN DÜZELTİLMESİNİ TALEP ETME HAKKI

Kişisel verilerin düzeltilmesini talep etme hakkı, Anayasa m. 20/3 hükmüyle bir temel hak olarak koruma bulmaktadır. İlgili kişinin haklarının belirtilmiş olduğu KVKK m. 11 hükmünde de kişisel verilerin düzeltilmesini talep etme hakkı sayılmıştır.

Buna göre herkes, kendisiyle ilgili kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde veri sorumlusuna başvurarak bunların düzeltilmesini[101] talep etme hakkına sahiptir (KVKK m. 11/1-d). Hak emredici niteliktedir ve taraf iradelerinin tasarruflarında değildir; dolayısıyla bu hakkın kullanılması durumunda ilgili kişiye bir yaptırım uygulanamaz.[102]

Düzeltme hakkı, KVKK m. 4/2-b düzenlemesinde kişisel verilerin işlenmesine dair genel ilkeler arasında sayılmış olan kişisel verilerin doğru ve gerektiğinde güncel olması ilkesine de hizmet eder.[103] Veri sorumlusu bu ilke kapsamında bilgilerin hatasız ve eksiksiz olması için kendisinden beklenebilecek olan gerekli önlemleri al-

---

[101] KVKK m. 11/1-d düzenlemesinde yer verilmiş olan "eksik veya yanlış" ifadeleri ile "düzeltme" ifadesinin örtüşmediği; zira eksiğin tamamlanıp, yanlışın düzeltilebileceği ve bu nedenle "düzeltme" kavramını "düzeltme ve tamamlama" olarak yorumlamanın daha isabetli olacağı yönünde bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 91. Düzeltme hakkı Tüzük'ün 16. maddesinde düzenleme bulmaktadır. "Düzeltme" başlığını taşıyan bu madde kapsamında, düzeltme talepleri ile tamamlama talepleri ayrı ayrı düzenlenmiştir. Çekin, *Kişisel Verilerin Korunması Kanunu*, 91, dn. 200.

[102] Çekin, *Kişisel Verilerin Korunması Kanunu*, 91-92.

[103] Çekin, *Kişisel Verilerin Korunması Kanunu*, 92; Dülger, *Kişisel Verilerin Korunması Hukuku*, 163; Küzeci, *Kişisel Verilerin Korunması*, 229. İlke Yönerge'nin 6/1-d hükmünde zikredilmiştir. Yönerge'nin belirtilen hükmünde, kişisel verilerin *"doğru ve gereken durumlarda güncel olması"* gerektiği düzenlenmiştir. Bununla birlikte kişisel verilerin korunmasına dair her metinde ilkenin bahsedilen şekilde ifade edilmediği belirtilmektedir. Bkz. Küzeci, *Kişisel Verilerin Korunması*, 220. İlke Tüzük kapsamında ise m. 5/1-d hükmünde düzenleme bulmaktadır. Buna göre; *kişisel veriler doğru ve gerektiğinde güncel olmalıdır. Doğru olmayan kişisel verilerin, işlenme amaçları göz önüne alınarak silinmesine veya düzeltilmesine yönelik olarak makul tüm önlemlerin gecikmeksizin alındığından emin olunmalıdır.*

makla yükümlüdür.[104] Veri sorumlusunun kişisel verilerin doğru ve güncel tutulmasına dair sorumluluğunun devri mümkün değildir.[105]

KVKK m. 4/2-b düzenlemesinde yer alan *"gerektiğinde güncel olma"* ifadesi ile ilkenin uygulanmasında somut olay koşullarının değerlendirilmesi gerektiğine dikkat çekilmiştir.[106] Örneğin delillerin muhafaza edilmesi maksadıyla, verilerin haklı bir şekilde güncellenmemesi veya eski verilerin de korunması söz konusu olabilir.[107]

Kişisel verilerin düzeltilmesinin söz konusu olabilmesi için, öncelikle eksik veya yanlış işlenmiş kişisel verinin mevcut olması gerekecektir. Pekâlâ, işlenmiş olan verinin doğru veya yanlış olduğu hangi kriterlere göre değerlendirilmelidir? Kişisel verinin yanlış olup olmadığının tespitinde, verinin objektif içeriğinin dikkate alınması gerektiği savunulmaktadır.[108] Dolayısıyla şayet ilgili kişinin verilere verdiği subjektif anlamdan bağımsız bir şekilde, veriler objektif bir şekilde değerlendirildiğinde bunların yanlış ya da eksik olduğu sonucuna varılırsa, o vakit düzeltme hakkından bahsetmek mümkündür.[109] [110]

---

104 Çekin, *Kişisel Verilerin Korunması Kanunu*, 52.

105 Küzeci, *Kişisel Verilerin Korunması*, 220.

106 Çekin, *Kişisel Verilerin Korunması Kanunu*, 53.

107 Ulrich Dammann, *Bundesdatenschutzgesetz*, ed. Spiros Simitis (München: Nomos, 2014), Art. 6 Rn. 14 (Çekin, *Kişisel Verilerin Korunması Kanunu*, 53'ten naklen).

108 Hans-Georg Kamann ve Martin Braun, *Datenschutzgrundverordnung,* ed. Eugen Ehmann ve Martin Selmayr (München: C.H. Beck, 2018), Art. 16 Rn. 14; Çekin, *Kişisel Verilerin Korunması Kanunu*, 92.

109 Çekin, *Kişisel Verilerin Korunması Kanunu*, 92.

110 Verilerin doğruluğu objektif kriterler doğrultusunda belirlenirken, değer yargılarının nasıl değerlendirilmesi gerektiğine dair bir sorunun doğduğu, bu bakımdan hukuki netice açısından inceleme yapmanın isabetli olacağı belirtilmektedir. Bu görüş uyarınca, değer yargısının ilgili kişinin kişilik hakkına ve mahremiyetine müdahale niteliği taşıması durumunda, bu değer yargısının kişisel veri olarak değerlendirilmesi mümkündür. Bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 92. Konu hakkında, sığınma talebine dair hukuki değerlendirmeler içeren bir cevap yazısı taslağının kişisel veri niteliği taşıyabileceği yönündeki 13.05.2014 tarihli Avrupa Adalet Divanı kararı için, bkz. Çekin, *Kişisel Verilerin Korunması Kanunu*, 92-93.

Konu hakkındaki işlevsel yorum uyarınca ise, verinin işleniş amacına göre kişi hakkında yanlış bir tablonun ortaya çıkması durumunda verinin yanlış olduğu sonucuna varılmalıdır.[111] Bu durumda veri yanlış olmasa bile yanıltıcı, muğlâk ya da yanlış anlaşılmaya müsait olduğu takdirde de düzeltme hakkının gündeme gelmesi mümkün olacaktır.[112]

Kişinin düzeltilmesini talep ettiği verinin kendisi dışında başka birtakım kişileri de kapsaması durumunda, verinin bu niteliğine bakılmaksızın ilgili kişinin düzeltme talebinde bulunmasının mümkün olması gerektiği belirtilmektedir.[113]

İlgili kişinin kişisel verisinin düzeltilmesi hakkını ileri sürerken uyması gereken herhangi bir şekil şartı mevcut değildir.[114] Ayrıca kişinin talebini *"düzeltme talebi"* olarak nitelendirmesi gerekli değildir; fakat ilgili kişinin talebinin içeriğinden, ileri sürülen talebin kişisel verinin düzeltilmesi yönünde olduğu anlaşılabilir olmalıdır.[115]

Yönerge'nin 12/b hükmü uyarınca da ilgili kişi Yönerge hükümlerine uygun olmayan, özellikle eksik veya yanlış olan verilerin düzeltilmesini talep etme hakkına sahiptir. İlgili kişinin verilerinin düzeltilmesi veya silinmesini talep etme hakkının, bilgilere erişim hakkının bir uzantısı olduğu belirtilmektedir.[116]

Kişisel verilerin düzeltilmesini talep hakkı, Tüzük kapsamında m. 16 hükmünde düzenlenmiştir. Buna göre; "*ilgili kişi veri sorumlusundan kendisine dair yanlış olan kişisel verinin gereksiz gecikmeye mahal*

---

111 Çekin, *Kişisel Verilerin Korunması Kanunu*, 92.

112 Otto Mallmann, *Bundesdatenschutzgesetz*, ed. Spiros Simitis (München: Nomos, 2014), § 20 Kn. 12 (Çekin, *Kişisel Verilerin Korunması Kanunu*, 92'den naklen).

113 Çekin, *Kişisel Verilerin Korunması Kanunu*, 93.

114 Çekin, *Kişisel Verilerin Korunması Kanunu*, 93. Düzeltme talebinin nasıl ileri sürülmesi gerektiği hususunda Yönerge kapsamında da bir hüküm bulunmamaktadır. Bkz. Şimşek, *Anayasa Hukukunda Kişisel Verilerin Korunması*, 93. Keza Tüzük m. 16 hükmünde de bu hususta bir kural getirilmemiş; fakat kişisel verilerin düzeltilmesini talep hakkının, ilgili kişi tarafından ek bir beyanda bulunulması yoluyla gerçekleşmesinin de mümkün olduğu belirtilmiştir.

115 Çekin, *Kişisel Verilerin Korunması Kanunu*, 93.

116 Küzeci, *Kişisel Verilerin Korunması*, 229.

vermeksizin düzeltilmesini talep etme hakkına sahiptir. İlgili kişi, kişisel verilerin işlenmesi amacı da göz önüne alınarak, eksik kişisel verilerinin tamamlanmasını talep etme hakkına sahiptir. Bunun ilgili kişi tarafından ek bir beyanda bulunulması yoluyla gerçekleşmesi de mümkündür.".

Tüzük uyarınca, düzeltme veya tamamlama talebine konu kişisel verilerin açıklanmış olduğu alıcılar söz konusu ise, bu durumda veri sorumlusu kişisel verilerin bu alıcılar nezdinde de düzeltilmesi veya tamamlanması için bildirimde bulunmakla yükümlüdür.[117] Tüzük m. 19 gereği veri sorumlusu; m. 16 uyarınca yapılan kişisel verilerin düzeltilmesi işlemini, bu durum imkânsız veya aşırı bir çabayı gerektirir olmadıkça kişisel verilerin açıklanmış olduğu tüm alıcılara bildirmelidir. Yine aynı madde uyarınca ilgili kişinin talebi üzerine veri sorumlusu ilgili kişiyi bu alıcılar hakkında bilgilendirmelidir.

Sonuç olarak kişisel verilerin düzeltilmesini talep hakkı gerek KVKK m. 11/1-d gerekse Yönerge m. 12/b ve Tüzük m. 16 hükümleriyle korunmuştur ve bu hükümlerin temel olarak paralel olduğu görülmektedir. Buna göre eksik veya yanlış işlenmiş olan kişisel verilerin ilgili kişinin talebi üzerine veri sorumlusu tarafından tamamlanması veya düzeltilmesi gerekecektir.

IV. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ, ANONİM HALE GETİRİLMESİ VEYA DÜZELTİLMESİ TALEBİNİN YERİNE GETİRİLMEMESİNİN SONUÇLARI

İlgili kişi tarafından haklı bir şekilde ileri sürülmüş olan kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi veya düzeltilmesi talebinin yerine getirilmemesi durumunda, bunun veri sorumlusu bakımından hukuki ve cezai sonuçları gündeme gelebilecektir.

Çalışmanın bu bölümünde öncelikle ilgili kişinin veri sorumlusuna başvuru hakkı ve bu başvurunun başarılı bir şekilde sonuçlanmaması ihtimalinde gündeme gelen Kurul nezdinde şikâyette bulunma hakkı incelenmiştir. Ardından, bahsedilen taleplerin yeri-

---

[117] Dülger, *Kişisel Verilerin Korunması Hukuku*, 163.

ne getirilmemesi sonucunda zarara uğrayan ilgili kişinin bu zararının giderilmesi bakımından tazminat hakkı inceleme konusu yapılmıştır. Çalışmada son olarak veri sorumlusunun ilgili kişinin kişisel verilerin imhası veya düzeltilmesine yönelik talebini yerine getirmemesinin 5237 sayılı Türk Ceza Kanunu ("TCK")[118] uyarınca neticeleri ve idari para cezasından sorumluluk hususları ele alınmıştır.

A. Veri Sorumlusuna Başvuru Hakkı

İlgili kişinin, KVKK hükümlerine aykırılık halinde veri sorumlusuna karşı Kurul nezdinde şikâyet yoluna başvurması mümkündür. Bununla birlikte Kurul nezdindeki şikâyet öncesinde, şikâyet konusu husus hakkında veri sorumlusuna KVKK m. 13 uyarınca yazılı bir şekilde veya Kurul'un belirleyeceği diğer yöntemlerle başvuruda bulunarak talepleri iletmek gereklidir. Bu başvuru yolu tüketilmeden Kurul nezdinde şikâyet yoluna başvurulması halinde şikâyet reddedilecektir (KVKK m. 14/3).

Veri sorumlusuna yapılacak olan başvuruya ilişkin usul ve esaslar, Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ ("Tebliğ")[119] hükümleriyle belirlenmiştir. Bu tebliğin 5. maddesinde, ilgili kişi tarafından veri sorumlusuna yapılacak olan başvuruların usulü düzenlenmiştir. Buna göre ilgili kişi, KVKK m. 11 hükmünde düzenlenmiş olan hakları kapsamında taleplerini, *"yazılı olarak veya kayıtlı elektronik posta (KEP) adresi, güvenli elektronik imza, mobil imza ya da ilgili kişi tarafından veri sorumlusuna daha önce bildirilen ve veri sorumlusunun sisteminde kayıtlı bulunan elektronik posta adresini kullanmak suretiyle veya başvuru amacına yönelik geliştirilmiş bir yazılım ya da uygulama vasıtasıyla veri sorumlusuna iletir"*.[120] Başvurunun Türkçe yapılması zorunludur (Tebliğ m. 4/2).

---

118 Kabul tarihi: 26.09.2004; RG. 12.10.2004, S. 25611.

119 RG. 10.03.2018, S. 30356.

120 Tebliğ m. 5/2 gereği başvuruda zorunlu olarak bulunması gereken bilgiler; *"ad, soyad ve başvuru yazılı ise imza, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası ve talep konusu"* şeklindedir. Konuya ilişkin bilgi ve belgeler de başvuruya eklenmelidir (Tebliğ m. 5/3).

İlgili kişinin yazılı başvurularında, veri sorumlusuna veya temsilcisine evrakın tebliğ edildiği tarih, başvuru tarihi olarak dikkate alınır (Tebliğ m. 5/4). Diğer yöntemlerle yapılan başvurularda ise, başvurunun veri sorumlusuna ulaştığı tarih başvuru tarihi sayılır (Tebliğ m. 5/5).

İlgili kişi tarafından KVKK m. 13 uyarınca veri sorumlusuna yapılan yazılı başvuru ardından veri sorumlusu, başvuruda yer alan bu talepleri, talebin niteliğine göre en kısa sürede ve en geç otuz gün içerisinde olmak üzere sonuçlandırmalıdır (KVKK m. 13/2). Başvuru kural olarak veri sorumlusu tarafından ücretsiz olarak sonuçlandırılır; fakat işlemin ayrıca bir maliyeti gerektirmesi hâlinde, Kurul tarafından belirlenen tarifedeki ücretin[121] ilgili kişiden alınması mümkündür (KVKK m. 13/2).

Veri sorumlusuna yapılan başvurunun dört şekilde sonuçlanması mümkündür: kabul, ret, yetersiz cevap verme[122] veya cevap vermeme. Veri sorumlusunun ilgili kişinin talebini kabul etmesi ve kişisel veriyi silmesi, yok etmesi, anonim hale getirmesi veya düzeltme talep edildiyse kişisel verinin düzeltilmesi durumunda, ilgili kişi tarafından Kurul nezdinde şikâyet yoluna başvurmaya gerek kalmayacaktır. Veri sorumlusunun talebi kabul etmesi durumda gereğini en kısa sürede yerine getirmesi gerekir (Tebliğ m. 6/6). Ayrıca talebin kabul edildiği ihtimalde bunun ilgili kişiye yazılı olarak veya elektronik ortamda bildirmesi aranmıştır (KVKK m. 13/3). İlgili kişi tarafından veri sorumlusuna yapılmış olan başvurunun veri sorumlusunun hatasından kaynaklanması hâlinde, başvuru için bir ücret alınmış ise bu tutar ilgiliye iade edilecektir (KVKK m. 13/3).

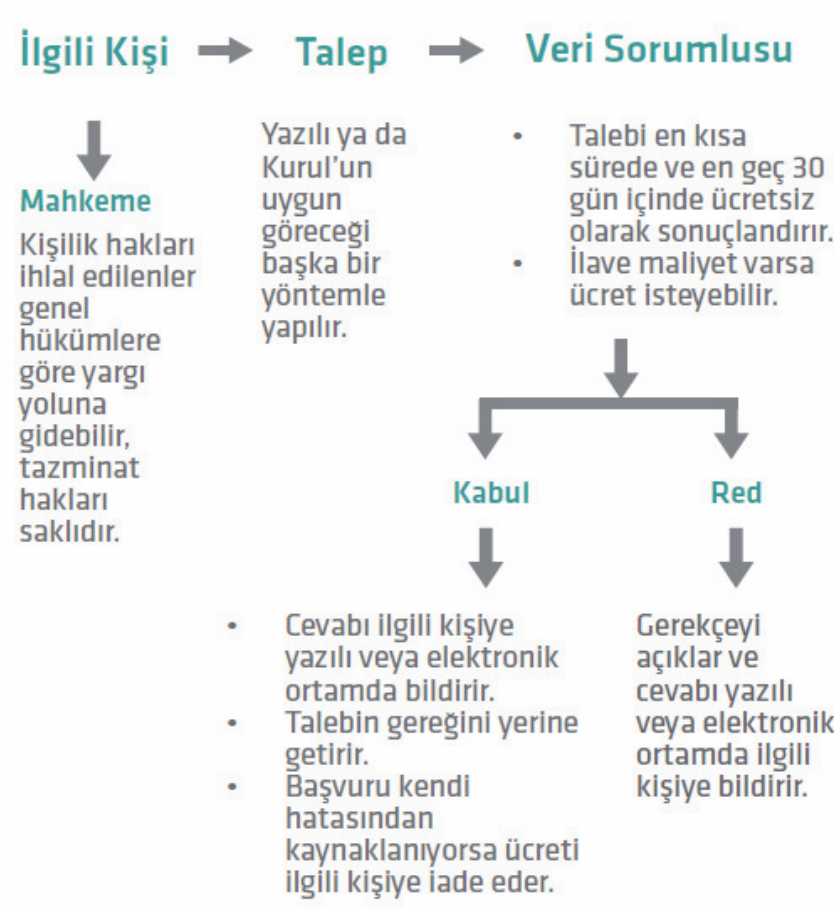
---

[121] Veri sorumlusuna başvuruda veri sorumlusu tarafından ilgili kişiden talep edilebilecek ücret, Tebliğ'in 7. maddesinde belirlenmiştir. Buna göre ilgili kişinin başvurusuna yazılı olarak cevap verilen durumlarda on sayfaya kadar ücret alınmamalıdır; on sayfanın üzerindeki her sayfa içinse 1 TL işlem ücreti alınması mümkündür (Tebliğ m. 7/1). Başvuruya cevabın bir kayıt ortamında (örneğin CD veya flash bellek) verilmesi durumundaysa veri sorumlusu tarafından talep edilebilecek ücret, kayıt ortamının maliyeti ile sınırlıdır (Tebliğ m. 7/2).

[122] Tebliğ m. 6/4 gereği veri sorumlusunun başvuruya cevabında zorunlu olarak bulunması gereken bilgiler; *"veri sorumlusu veya temsilcisine ait bilgiler, başvuru sahibinin; adı ve soyadı, Türkiye Cumhuriyeti vatandaşları için T.C. kimlik numarası, yabancılar için uyruğu, pasaport numarası veya varsa kimlik numarası, tebligata esas yerleşim yeri veya iş yeri adresi, varsa bildirime esas elektronik posta adresi, telefon ve faks numarası, talep konusu ve veri sorumlusunun başvuruya ilişkin açıklamaları"* şeklindedir.

Veri sorumlusunun ilgili kişinin talebini reddetmesi durumunda, ret cevabı da gerekçesiyle birlikte ilgili kişiye yazılı olarak veya elektronik ortamda bildirmelidir (KVKK m. 13/3).

İlgili kişi tarafından veri sorumlusuna yapılan başvuru sürecini aşağıdaki gibi bir şema ile göstermek mümkündür:



Tablo 1: Veri Sorumlusuna Başvuru Süreci[123]

[123] "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," KVKK, erişim tarihi 8 Ağustos 2019, https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASINA%20%C4%B0L%C4%B0%C5%9EK%C4%B0N%20BA%C5%9EVURU%20VE%20%C5%9E%C4%B0K%C3%82YET%20HAKKI.pdf, 6.

B. Kurul Nezdinde Şikâyette Bulunma Hakkı

Başvurunun reddedilmiş olması, başvuruya verilmiş olan cevabın yetersiz bulunması veya başvuruya süresinde cevap verilmemiş olması durumlarında ilgili kişinin Kurul nezdinde şikâyette bulunması mümkündür (KVKK m. 14/1).[124] Bununla birlikte belirtmek gerekir ki her ne kadar veri sorumlusuna başvuru KVKK m. 13 gereği zorunlu olsa da Kurum nezdinde şikâyet yoluna gitmek ihtiyaridir. Dolayısıyla veri sorumlusu tarafından başvurunun zımnen veya açıkça reddedilmesi durumunda ilgili kişi Kurul nezdinde şikâyette bulunması gerekmeksizin doğrudan yargı yoluna da başvurabilir.[125]

İlgili kişi tarafından Kurul nezdinde yapılacak ihbar ve şikâyetler, 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun'un[126] 6. maddesinde belirtilen şartları taşımalıdır; aksi takdirde ihbar ve şikâyetler incelemeye alınmaz (KVKK m. 15/2). Dolayısıyla ihbar ve şikâyet dilekçelerinin belli bir konuyu içermeleri, yargı mercilerinin görevine giren konularla ilgili olmamaları ve dilekçe sahibinin adı soyadı ve imzası ile iş veya ikametgâh adresi bilgilerini içermeleri gerekir (Dilekçe Hakkının Kullanılmasına Dair Kanun m. 6 ve 4).

Şikâyet süresi, veri sorumlusunun cevabını öğrenme tarihinden itibaren otuz ve her hâlde başvuru tarihinden itibaren altmış gündür (KVKK m. 14/1).[127] Bununla birlikte Kurul'un şikâyet ol-

---

[124] Yönerge m. 28/4 ve Tüzük m. 77/1 gereği denetleyici otorite nezdinde şikâyet yoluna başvurmak mümkündür.

[125] KVKK m. 14 gerekçesi (Kaynak: Corpus Web Hukuk Mevzuat ve İçtihat Programı, www.corpus.com.tr); KVKK, "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," 3.

[126] Kabul tarihi: 01.11.1984; RG. 10.11.1984, S. 18571.

[127] Kişisel Verileri Koruma Kurumu'na intikal eden şikâyet başvurularının incelenmesi neticesinde, veri sorumlusuna başvuru yolunu tüketen ilgili kişiler tarafından Kurul'a şikâyette bulunulması sürecinde KVKK hükümlerinde yer alan sürelerin yorumlanmasında farklılıklar olduğu tespit edilmiş, bunun üzerine

maksızın ihlal iddiasını öğrenmesi durumunda da re'sen görev alanına giren konularda gerekli incelemeler yapılacaktır (KVKK m. 15/1).

Veri sorumlusu, şikâyet üzerine Kurul tarafından inceleme konusuyla ilgili olarak istenmiş olan bilgi ve belgeleri on beş gün içinde göndermeli ve ayrıca gerektiğinde yerinde inceleme yapılmasına imkân sağlamalıdır (KVKK m. 15/3). Madde gereği Devlet sırrı niteliğindeki bilgi ve belgeler bu kuralın dışındadır.

Telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması durumunda, Kurul tarafından veri işlenmesinin ya da verinin yurt dışına aktarılmasının durdurulmasına karar verilmesi de mümkündür (KVKK m. 15/7).

Kurul tarafından şikâyet üzerine yapılan incelemeler için altmış günlük bir süre belirlenmiştir.[128] Şikâyet tarihinden itibaren altmış gün içinde cevap verilmemiş olması durumunda talep Ku-

konu hakkında bir karar alınmıştır. Kişisel Verileri Koruma Kurumu'nun 13.02.2019 tarihinde yayımlamış olduğu 24.01.2019 tarih ve 2019/9 sayılı kararla; *"İlgili kişi tarafından yapılan başvuruya veri sorumlusunca 30 gün içinde bir cevap verilmesi halinde ilgili kişinin veri sorumlusunun cevabını müteakip 30 gün içerisinde şikâyette bulunabileceği, bu itibarla söz konusu hallerde ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 günlük süresinin bulunmadığı,*

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca bir cevap verilmediği durumda ise ilgili kişinin veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurul'a şikâyette bulunabileceği,

İlgili kişi tarafından yapılan başvuruya veri sorumlusunca KVKK'da tanınan 30 günlük süre sonrasında bir cevap verilmesi halinde ilgili kişinin, KVKK'da veri sorumlusuna tanınan 30 günlük süre sonrasında verilecek cevabı beklemekle yükümlü olmadığı ve veri sorumlusuna tanınan sürenin dolması ile birlikte Kurul'a şikâyette bulunabileceği göz önüne alınarak, ilgili kişinin veri sorumlusunun kendisine cevap verdiği tarihten itibaren 30 gün değil, veri sorumlusuna başvurduğu tarihten itibaren 60 gün içinde Kurul'a şikâyette bulunabileceği" kamuoyuna duyurulmuştur.

Karar için bkz. "Veri Sorumlusuna Başvuru ve Kurula Şikayet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı," KVKK, erişim tarihi 8 Ağustos 2019, https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu.

128 KVKK, "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," 5.

rul tarafından reddedilmiş sayılır (KVKK m. 15/4).[129] Dolayısıyla şikâyet tarihinden itibaren altmış günlük sürenin geçmesiyle birlikte idari yargıda dava açma süresi başlayacaktır.[130]

Şikâyet üzerine veya Kurul tarafından re'sen yapılan inceleme sonucunda ihlalin mevcut olduğu anlaşılırsa, Kurul tespit etmiş olduğu hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar verecek ve bu karar ilgililere tebliğ edilecektir (KVKK m. 15/5). Kurul'un bu kararının tebliğden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirilmesi gerekmektedir (KVKK m. 15/5).[131]

Kurul kararlarına karşı yargı yolu açık olduğundan, ilgili kişilerin şikâyet üzerine Kurul tarafından verilmiş olan kararlara karşı yetkili idare mahkemelerinde dava açması mümkündür.[132]

Kurul nezdindeki şikâyet sürecini aşağıdaki gibi bir şema ile göstermek mümkündür:

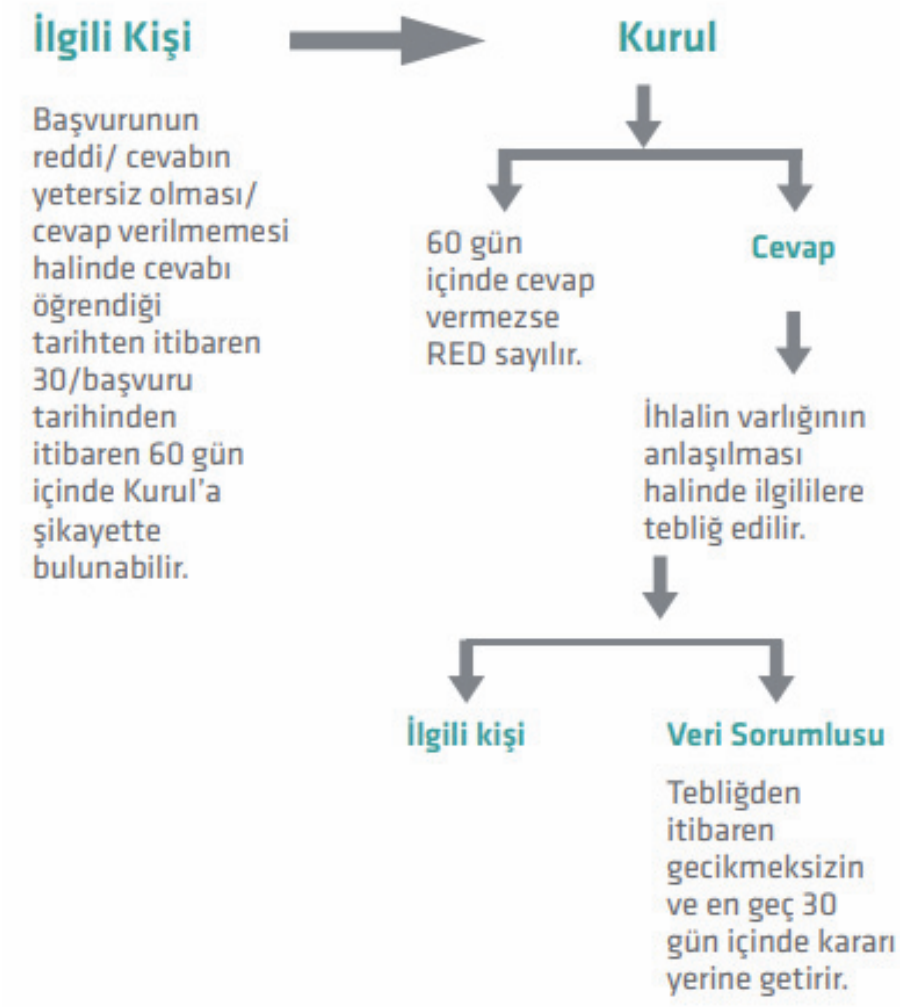
---

[129] Bununla birlikte KVKK hükümlerinde Kurul tarafından re'sen yapılacak incelemeler yönünden herhangi bir süre öngörülmemiştir. Bkz. KVKK, "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," 5.

[130] KVKK, "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," 4.

[131] Şikâyet üzerine veya re'sen yapılan inceleme neticesinde, ihlalin yaygın olduğunun tespit edilmesi durumunda, Kurul tarafından bu hususta ilke kararı alınmakta ve bu karar yayımlanmaktadır (KVKK m. 15/6).

[132] KVKK, "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," 5.



Tablo 2: Kurul Nezdinde Şikâyet Süreci[133]

Kurul kararına konu olmuş olan bir uyuşmazlıkta, bir hazır giyim firmasının internet sitesi üzerinden üyelik bilgileri ile alışveriş yapan kişinin teslimat adresi, adı, soyadı, adres ve telefon numarası gibi kişisel bilgileri, şirkete ait bu internet sitesi üzerinden alışveriş yapan üçüncü kişilerce erişilebilir hale gelmiştir. İlgili kişi bu sebeple veri sorumlusu şirkete başvuruda bulunarak, kişisel verilerinin

[133] KVKK, "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı," 7.

sistemlerinden silinmesini, yok edilmesini, ulaşılamaz hale getirilmesini, yurt içi ve yurt dışında başka bir kurumla paylaşıldı ise o kurumlar nezdinde de silinmesini ve yok edilmesini talep etmiştir. Veri sorumlusu şirketten alınan cevabın yetersiz bulunması üzerine Kurul nezdinde şikâyet yoluna başvurulmuştur. Veri sorumlusu şirket; şikâyette bulunmuş olan ilgili kişinin kişisel verilerinin aynı zamanda başka müşterilerin alışverişe ilişkin işlemleri sırasında görülebilir hale gelmiş olduğundan şikâyete konu olayla birlikte haberdar olduğunu ve olayın sistemsel bir hatadan kaynaklandığını savunmuştur. Kurul 26.07.2018 tarihli, 2018/91 numaralı kararıyla şikâyeti yerinde bularak, ilgili kişinin kişisel verilerinin şirket sistemlerinden silinmesi, yok edilmesi, ulaşılamaz hale getirilmesine, eğer bu veriler başka bir kurumla paylaşılmışsa o kurumlar nezdinde de silinmesi ve yok edilmesi talebinde bulunulmasına ve şirket hakkında idari para cezası uygulanmasına karar vermiştir.[134]

Kurul nezdinde şikâyet konusu olmuş olan başka bir uyuşmazlıkta, bir devlet memuru olan ilgili kişinin, memuriyet döneminde hakkında açılmış inceleme-soruşturma dosyalarına ilişkin evrakın imha edilmesi talebi veri sorumlusu kamu kurumunca yerine getirilmemiştir. Bunun üzerine ilgili kişi Kurul nezdinde şikâyet yoluna başvurmuştur. Kurul 28.06.2018 tarihli, 2018/69 sayılı kararıyla, KVKK m. 7 hükmünde belirtilmiş olan kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması koşulu gerçekleşmediğinden, talebin veri sorumlusu tarafından yerine getirilmemesinin uygun olduğu yönünde karar vermiştir. Zira 657 sayılı Devlet Memurları Kanunu[135] m. 109 ve Kamu Personeli Genel Tebliği[136]'nin (Seri No: 2) "D" bölümü gereğince ilgili kişinin devlet memuru olduğu dönemde hakkında açılmış inceleme-soruşturma dosyalarına ilişkin belgelerin özlük dosyalarında saklanması gerekmektedir ve Devlet

---

134 Karar için bkz. "Kişisel verilere hukuka aykırı erişilmesini önleme yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 26/07/2018 Tarihli ve 2018/91 Sayılı Karar Özeti," KVKK, erişim tarihi 8 Ağustos 2019, https://kvkk.gov.tr/Icerik/5365/2018-91.

135 Kabul tarihi: 14.07.1965; RG. 23.07.1965, S. 12056.

136 RG. 15.04.2011, S. 27906.

Arşiv Hizmetleri Hakkında Yönetmelik[137] m. 3 gereği belgelerin arşiv niteliğini kaybedebilmesi için son işlem tarihi üzerinden geçmesi gereken yüz bir yıllık süre dolmamıştır.[138]

C. İlgili Kişinin Tazminat Hakkı

Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde, re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hâle getirilmesinin gerekmesine rağmen veri sorumlusu tarafından KVKK m. 7/1 hükmünde düzenlenmiş olan bu kurala uyulmaması durumunda kişisel veri KVKK hükümlerine aykırı bir şekilde işlenmiş olacaktır.

Keza veri sorumlusunun ilgili kişi tarafından kendisine yönetilmiş olan haklı düzeltme talebini yerine getirmemesi durumunda, veri sorumlusunun bundan sonraki veri işleme faaliyeti artık hukuka aykırı olur. Zira bu durumda veri sorumlusu, KVKK m. 4/2-b fıkrasında kişisel verilerin işlenmesine dair genel ilkeler arasında sayılmış olan kişisel verilerin doğru ve güncel olması ilkesine aykırı bir şekilde veri işlemiş olacaktır.[139]

Yönerge m. 23/1 uyarınca üye devletler; hukuka aykırı işleme sonucunda veya Yönerge hükümleri gereği ulusal hukukta kabul edilmiş olan herhangi bir kurala aykırı davranış sonucunda zarara uğrayan herkesin veri sorumlusundan uğranan zarar karşılığında tazminat talep etme hakkı olduğuna dair düzenleme getirmelidir. Keza Tüzük m. 82/1 gereği Tüzük hükümlerinin ihlal edilmesi sonucunda maddi veya manevi zarara uğramış olan herkesin uğranan zarara karşılık tazminat talebinde bulunma hakkı vardır.

KVKK m. 11 hükmünde ilgili kişinin hakları arasında kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğranması

---

137 RG. 16.05.1988, S. 19816.

138 Karar için bkz. "Sicil dosyalarındaki kişisel verilerin, işlenmelerini gerektiren sebeplerin ortadan kalkmaması sebebiyle, imha edilmemesi gerektiği hakkında Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Karar Özeti," KVKK, erişim tarihi 8 Ağustos 2019, https://kvkk.gov.tr/Icerik/5366/2018-69.

139 Çekin, *Kişisel Verilerin Korunması Kanunu*, 93.

hâlinde zararın giderilmesini talep etme hakkı da sayılmıştır (KVKK m. 11/1-ğ). Kişisel verilerin KVKK hükümlerine aykırı olarak işlenmesinin, haksız fiilin özel bir görünüm şekli olduğu belirtilmektedir.[140] [141]

Bununla birlikte kişisel verilerin hukuka aykırı bir şekilde işlenmesi sonucunda maddi zarara uğramanın çok ender rastlanacak bir durum olduğu belirtilmekte, bu hususta ilgili kişiye kredi verilmemesi, kişinin işe alınmaması durumları veya kişisel verilerin hukuka aykırı işlenip işlenmediğini tespiti amacıyla yapılan masraflar örnek gösterilmektedir.[142]

---

[140] Çekin, *Kişisel Verilerin Korunması Kanunu*, 101. Aksi yönde, verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğranması durumunda zararın giderilmesini talep etme hakkının 6098 sayılı Türk Borçlar Kanunu ("TBK", Kabul tarihi: 11.01.2011; RG. 04.02.2011, S. 27836) hükümleri karşısında bir tekrardan ibaret olduğu yönünde bkz. Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması," 29. İkinci görüşe paralel bir şekilde, KVKK hükümlerinde sorumluluk hususunda özel hüküm öngörülmemiş olduğu yönünde bkz. Damla Gürpınar, "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Şeref Ertaş'a Armağan* 19, no. özel (2017): 690.

[141] Doktrindeki bir görüşe göre, KVKK'da sorumluluk için kusur şartı aranmamıştır. Bkz. Çekin, "Big Data ve İrade Serbestisi," 638. KVKK ile öngörülen mekanizmanın bir kusur sorumluluğu hali olduğunu kabul etmenin zor olacağı ve veri sorumlusunun KVKK m. 11 hükmünde düzenlenmiş olan tazminat yükümlülüğümün bir sebep sorumluluğu niteliği taşıdığını kabul etmenin daha isabetli olacağı yönünde bkz. Çekin, "Big Data ve İrade Serbestisi," 638. Bu görüş uyarınca, veri sorumlusu KVKK m. 12 hükmünde öngörülen şartları yerine getirdiği takdirde sorumluluk gündeme gelmemelidir.

Dijital ortamda çalışarak çok sayıda veriyi kolaylıkla toplama, saklama ve analiz etme olanaklarına kavuşan veri sorumlularının, verileri bu ortamda uygun şekilde koruyamama riskini de üstlenmiş sayılmalarının hakkaniyet ilkesinin bir gereği olduğu, dolayısıyla burada bir tehlike sorumluluğunun söz konusu olduğunu kabul ederek zarardan sorumlu tutulacak kişilerin kusurunu aramamanın daha isabetli olabileceği fakat KVKK hükümlerinde bu yönde bir açıklık bulunmadığı belirtilmekte, bununla birlikte TBK'nın "tehlike sorumluluğu ve denkleştirme" kenar başlıklı 71. maddesinin bu konuda uygulanıp uygulanamayacağının düşünülmesi de önerilmektedir. Bkz. Gürpınar, "Hukuki Sorumluluk," 694.

[142] Çekin, *Kişisel Verilerin Korunması Kanunu*, 102-103.

Bunun dışında KVKK m. 14/3 gereği kişilik hakları ihlal edilenlerin, genel hükümlere göre tazminat hakkı saklıdır. Kişilik hakkının ihlal edilmesi sonucunda maddi veya manevi zarara uğrayan ilgili kişilerin zararlarının tazmini için veri sorumlusuna karşı tazminat davası açmaları mümkündür.[143]

D. Veri Sorumlusunun Türk Ceza Kanunu Uyarınca Cezai Sorumluluğu

KVKK m. 17/2 gereği, KVKK m. 7 hükmüne aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenler TCK'nın 138. maddesine göre cezalandırılır.[144] [145]

"Verileri yok etmeme" kenar başlıklı TCK m. 138/1 uyarınca, kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde[146] yok etmekle yükümlü olanlara, görevlerini yerine getirmedikleri durumda bir yıldan iki yıla kadar hapis cezası verilir.[147]

---

[143] Gürpınar, "Hukuki Sorumluluk," 690.

[144] Kişisel verilerin korunmasına ilişkin suçlara TCK m. 135 ve devamı maddelerinde yer verilerek, Fransız Ceza Kanunu'nda takip edilen yöntem tercih edilmiştir. Nitekim kişisel verilerin korunmasına ilişkin usul ve esasların yer aldığı kanunlarda aynı zamanda kişisel verilerin korunmasına ilişkin suçlara da yer verilmiş olan Almanya ve İtalya'daki sistemin aksine, Fransa'da kişisel verilerin korunmasına ilişkin suçların Fransız Ceza Kanunu'nda düzenlenmiş olduğu belirtilmektedir. Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları* (Ankara: Adalet Yayınevi, 2008), 217.

[145] KVKK m. 17/2 hükmünde düzenlenmiş olan kişisel verilerin silinmemesi veya anonim hale getirilmemesi suçunun, TCK m. 138 hükmünde düzenlenmiş olan verileri yok etmeme suçundan farklı bir suç olduğu yönünde bkz. Murat Volkan Dülger, "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması," *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* 3, no. 2 (2016): 135; Dülger, *Kişisel Verilerin Korunması Hukuku*, 369-370.

[146] TCK m. 135 ve 136 hükümlerinde suçun konusu olan kişisel veriler açısından otomatik işleme ve otomatik olmayan işleme arasında bir ayrım yapılmamıştır. Oysa TCK m. 138 hükmünde düzenleme bulan verileri yok etmeme suçu bakımından durum böyle değildir. TCK m. 138 hükmünde geçen "sistem" kelimesinin bilişim sistemini ifade ettiği kabul edildiğinde bir çelişki oluşmaktadır. Bu hususta bkz. Ketizmen, *Bilişim Suçları*, 242; Melike Köse Aysun, *Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135)* (Ankara: Seçkin, 2018), 112. Bu nedenle TCK m.

Kişisel veriler süresinden sonra fakat yetkili makamlar tarafından bu sürenin aşılmış olduğu fark edilmeden önce yok edilse dahi, suçtan sorumluluk yine de gündeme gelecektir.[148] Ayrıca ilgili kişinin rızası bulunsa bile, bu rıza suç açısından geçerli bir hukuka uygunluk sebebi olmayacaktır.[149]

Suçun konusunun 5271 sayılı Ceza Muhakemesi Kanunu[150] hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde, verilecek cezanın bir kat artırılması öngörülmüştür (TCK m. 138/2).[151]

TCK m. 139 gereği, kişisel verileri yok etmeme suçunun soruşturulması ve kovuşturulması şikâyete tabi değildir.[152]

İlgili kişinin KVKK m. 11/1-d uyarınca veri sorumlusuna karşı ileri sürdüğü haklı düzeltme talebinin yerine getirilmemesi durumunda, veri sorumlusunun bu tutumu bir suç oluşturacak mıdır? TCK m. 135 ile kişisel verilerin hukuka aykırı olarak kaydedilmesi, TCK m. 136 ile kişisel verilerin hukuka aykırı olarak bir başkasına

---

138 metninden sistemde bulunma şartının çıkartılması tavsiye edilmektedir. Bkz. Ketizmen, *Bilişim Suçları*, 242.

147 Kişisel verileri yok etmeme suçu, ihmali bir suçtur. Ketizmen, *Bilişim Suçları*, 240; Hale Akdağ, *Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması* (Ankara: Adalet Yayınevi, 2013), 145; Köse Aysun, *Kişisel Verilerin Kaydedilmesi Suçu*, 113; Dülger, "Kişisel Verilerin Ceza Normlarıyla Korunması," 134; Dülger, *Kişisel Verilerin Korunması Hukuku*, 365. Suçun taksirle işlenmesi mümkün değildir. Akdağ, *Kişisel Verilerin Korunması*, 148; Dülger, *Kişisel Verilerin Korunması Hukuku*, 367. Kişinin kasıtlı kabul edilebilmesi için bilinmesi ve istenmesi gereken unsurların neler olduğuna dair tartışmalar hakkında bkz. Akdağ, *Kişisel Verilerin Korunması*, 149*ff*.

148 Akdağ, *Kişisel Verilerin Korunması*, 147.

149 Akdağ, *Kişisel Verilerin Korunması*, 154; Dülger, *Kişisel Verilerin Korunması Hukuku*, 368.

150 Kabul tarihi: 04.12.2004; RG. 17.12.2004, S. 25673.

151 Kan veya saç örneği alınmış olan şüphelinin yargılama ardından beraat etmesi halinde bu delillerin yok edilmesi zorunluluğu bu hale örnektir. Bahsedilen ve diğer örnekler için bkz. Köse Aysun, *Kişisel Verilerin Kaydedilmesi Suçu*, 114-115.

152 Bu yaklaşımın yerinde olduğu yönünde bkz. Akdağ, *Kişisel Verilerin Korunması*, 156-157.

verilmesi, yayılması veya ele geçirilmesi, TCK m. 138 ile ise kanunların belirlediği sürelerin geçmiş olmasına karşın verilerin sistem içinde yok edilmemesi suç olarak düzenlenmiştir.[153] KVKK m. 17/2 gereği de kişisel verileri silmeyen veya anonim hâle getirmeyenler TCK m. 138 hükmü uyarınca cezalandırılır. Dolayısıyla kişisel verilerin hâlihazırda hukuka uygun bir şekilde elde edilip kaydedilmiş olması ihtimalinde, ilgili kişi tarafından KVKK m. 11/1-d uyarınca haklı bir şekilde ileri sürülen düzeltme talebinin yerine getirilmemesi bir suç oluşturmayacaktır.

E. Veri Sorumlusunun İdari Para Cezasından Sorumluluğu

KVKK m. 18 hükmünde veri sorumlularının kabahatleri sonucunda gündeme gelecek olan idari para cezaları düzenlenmiştir. KVKK m. 18/2 gereği maddede öngörülmüş olan idari para cezaları veri sorumlusu olan gerçek kişiler ve özel hukuk tüzel kişileri hakkında uygulanmaktadır.[154]

KVKK m. 18/1-c gereği; KVKK m. 15 uyarınca Kurul tarafından verilen kararları yerine getirmeyenler hakkında, 25.000 TL'den 1.000.000 TL tutarına kadar idari para cezası verilir. Kurul kararlarına karşı idari yargı yolu açıktır.[155]

Dolayısıyla kişisel verilerin imhası veya düzeltilmesi talebinin veri sorumlusu tarafından yerine getirilmemesi üzerine Kurul nezdinde şikâyet yoluna başvurulması ve Kurul'un şikâyeti yerinde bulması halinde, Kurul kararını yerine getirmeyen veri sorumlusunun idari para cezasından sorumluluğu gündeme gelecektir.

---

153 Tipiklik açısından bu suçlara ilişkin eylemlerin neler olduğu hakkında bkz. Dülger, "Kişisel Verilerin Ceza Normlarıyla Korunması," 127-137.

154 Bununla birlikte aydınlatma yükümlülüğünü yerine getirmeme, veri güvenliğine ilişkin yükümlülükleri yerine getirmeme, Kurul tarafından verilen kararları yerine getirmeme veya Veri Sorumluları Sicili'ne kayıt ve bildirim yükümlülüğünü yerine getirmeme eylemlerinin kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi durumunda, Kurul'un yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapan kişiler hakkında disiplin hükümlerine göre işlem yapılarak sonucu Kurul'a bildirmektedir (KVKK m. 18/3).

155 Korkmaz, "Değerlendirme," 142.

Veri sorumlusunun bu yöndeki Kurul kararına rağmen kişisel verileri imha etmemesi ihtimalinde, TCK m. 138 uyarınca söz konusu olan ceza dışında KVKK m. 18/1-c uyarınca idari para cezasından sorumluluk ayrıca gündeme gelmiş olacaktır.[156]

Konu Avrupa hukuku bakımından incelendiğinde, Yönerge'de veri ihlalinde bulunulması halinde ihlalde bulunanlara para cezası kesilmesi imkânı bulunmadığı görülmektedir.[157] Tüzük uyarınca ise böyle bir imkân söz konusudur. İlgili kişinin kişisel verilerin silinmesi (Tüzük m. 17) ve düzeltilmesi (Tüzük m. 16) haklarına ilişkin kuralların ihlali, Tüzük m. 83/5-b gereği Tüzük m. 83/5 yaptırımına tabidir. Tüzük m. 83/5 uyarınca veri ihlalinde bulunan şirketlere 20.000.000 Euro tutarına kadar veya ihlalde bulunan kuruluşun dünya çapındaki yıllık cirosunun %4'ü oranına kadar idari para cezası kesilmesi mümkündür.[158]

V. SONUÇ

Anayasa m. 20 hükmüyle kişisel verilerin korunması bir temel hak olarak tanınmış, bu bağlamda herkesin kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu ve bu hakkın kişinin kendisiyle ilgili kişisel verilerin silinmesi veya düzeltilmesini talep etmesini de kapsadığı belirtilmiştir. Kişisel verilerin silinmesi veya düzeltilmesini talep etme hakkı ikincil mevzuatta düzenlenmiş olmakla birlikte bir terminoloji farklılığı söz konusudur.

İlgili kişinin haklarının düzenlenmiş olduğu KVKK m. 11/1-e uyarınca herkes KVKK m. 7 hükmünde öngörülen şartlar çerçevesinde kişisel verilerinin silinmesini veya yok edilmesini isteme hakkına sahiptir. KVKK m. 7 hükmünde, işlenmesini gerektiren sebep-

---

156 5326 sayılı Kabahatler Kanunu (Kabul tarihi: 30.03.2005; RG. 31.03.2005, S. 25772 Mükerrer) m. 15/3 uyarınca, bir fiil hem kabahat hem de suç olarak tanımlanmış ise, sadece suçtan dolayı yaptırım uygulanabilir. Bununla birlikte bahsedilen ihtimalde suç ve kabahati oluşturan durumlar farklıdır. Kişisel verilerin silinmemesi, yok edilmemesi ya da anonim hale getirilmemesi suçu, buna ilişkin Kurul kararına uyulmaması ise kabahati oluşturur.

157 Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 21.

158 Taştan, *Türk Sözleşme Hukukunda Kişisel Verilerin Korunması*, 21.

lerin ortadan kalkması hâlinde kişisel verilerin re'sen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinmesi, yok edilmesi veya anonim hâle getirilmesi gerektiği düzenlenmiştir.

Kişisel verilerin imhası; *"kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi"* anlamlarında kullanılan genel bir kavramdır (Yönetmelik m. 4/1-c). Kişisel verilerin silinmesi; *"kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi"* olarak tanımlanır (Yönetmelik m. 8/1). Kişisel verilerin yok edilmesi ise *"kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir"* (Yönetmelik m. 9/1). Kişisel verinin yok edilmesi için, verilerin bulunduğu donanım ve evrakın fiziken yok edilmesi gerekir. Son olarak kişisel verilerin anonim hale getirilmesi ise *"kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi"* şeklinde tanımlanır (Yönetmelik m. 10/1).

Kişisel verilerin silinmesini talep hakkı Yönerge kapsamında KVKK ve Yönetmelik hükümlerinden farklı bir terminolojiyle ele alınmıştır. Yönerge m. 12-b gereği ilgili kişiler, özellikle verinin eksik veya yanlış olmasından dolayı Yönerge hükümlerine uygun olmayan bir şekilde işlenmiş olan verilerin, uygunluğa göre silinmesi veya bloke edilmesini veri sorumlusundan talep etme hakkına sahiptir. Yönerge'de *"silme veya bloke etme"* terimlerinin kullanılmış olmasına karşın KVKK'da *"silme veya yok etme"* kelimeleriyle farklı bir terminolojinin tercih edilmiş olması eleştiri konusu olmuştur. Yönerge kapsamındaki *"silme"* kavramının, KVKK ve Yönetmelik uyarınca *"silme"* ve *"yok etme"* kavramlarını kapsadığını söylemek mümkündür. Yönerge hükümlerinde yer alan kişisel verinin bloke edilmesini talep hakkına ise KVKK hükümlerinde rastlanmamaktadır. Diğer bir farklılık ise kişisel verilerin anonimleştirilmesi yönündendir. Her ne kadar Yönerge m. 12-b hükmünde verilerin anonimleştirilmesinden bahsedilmemiş olsa da bu husus Yönerge kapsamında fakat farklı bir şekilde düzenlenmiştir. Yönerge'nin 26. paragrafı uyarınca anonimleştirilmiş veriler, tüm veri koruma süreçlerinin bir istisnası olarak belirlenmiştir. Dolayısıyla Yönerge uyarınca

kişisel verilerin anonimleştirilmiş olması sonucunda kişisel verilerin korunmasına dair esaslar uygulama alanı bulmayacaktır.

Kişisel verilerin silinmesini talep hakkı Tüzük m. 17 hükmünde düzenleme bulur. Bu hükümle ilgili kişiye kişisel verilerin gereksiz gecikmeye mahal vermeksizin silinmesini talep hakkı tanınmış ve veri sorumlusunun kişisel verileri gereksiz gecikmeye mahal vermeksizin silmekle yükümlü olduğu haller sayılmıştır. Tüzük kapsamında kişisel verilerin silinmesini talep hakkı dışında ayrıca verilerin yok edilmesini talep hakkından bahsedilmemektedir. Bununla birlikte Yönerge terminolojisinde olduğu gibi, Tüzük uyarınca kişisel verilerin silinmesi hakkının KVKK ve Yönetmelik anlamında kişisel verilerin silinmesi ve yok edilmesi kavramlarını kapsadığını söylemek mümkündür. Anonimleştirilmiş veriler bakımından ise Yönerge ve Tüzük paralel bir anlayışa sahiptir ve Tüzük hükümleri anonim bilgilerin işlenmesi hakkında uygulama alanı bulmamaktadır.

Tüzük m. 17 hükmünün kenar başlığında silme hakkı *(right to erasure)* ve unutulma hakkı *(right to be forgotten)* ifadelerinin kullanılmış olduğu göze çarpmaktadır. Unutulma hakkının Avrupa Komisyonu tarafından öngörülmesinin ardından, Avrupa Birliği Parlamentosu nezdindeki görüşmelerde hakkın önemli kısıtlamalara maruz kaldığı, öyle ki *"unutulma hakkı"* isminin dahi uygun bulunmadığı ve hakkın mevcut sınırlamalar kapsamında *"kişisel verilerin silinmesi hakkı"* şeklinde tanımlanmasının tercih edildiği bilinmektedir. Sonuç olarak Tüzük'ün nihai halinde madde kenar başlığı ve içeriği bahsedildiği şekilde düzenlenmiştir. Bununla birlikte unutulma hakkına ilişkin birçok tartışma mevcuttur. Nitekim silme hakkı *(right to erasure)*, unutma hakkı *(right to oblivion)*, dizinden çıkarma hakkı *(right to delisting)* kavramlarının da birbirleri yerine kullanıldığı görülmektedir. Tüzük'ün hazırlanma çalışmalarında Avrupa Birliği Adalet Divanı'nın 13.05.2014 tarihli *Google-Spain* Kararı etkili olmuştur. Bu karar *"unutulma hakkı kararı"* olarak bilinmektedir ve bu hakka ilişkin önemli tespitler içermektedir.

Kişisel verilerin düzeltilmesini talep hakkı bakımından terminolojik bir karışıklık söz konusu değildir. KVKK m. 11/1-d gereği her-

kes kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkına sahiptir. Yönerge'nin 12/b hükmü uyarınca da ilgili kişi Yönerge hükümlerine uygun olmayan, özellikle eksik veya yanlış olan verilerin düzeltilmesini talep etme hakkına sahiptir. Kişisel verilerin düzeltilmesini talep hakkı Tüzük m. 16 hükmünde ayrı bir madde şekilde düzenlenmiştir. Buna göre ilgili kişi veri sorumlusundan kendisine dair yanlış olan kişisel verinin gereksiz gecikmeye mahal vermeksizin düzeltilmesini talep etme hakkına sahiptir. Keza ilgili kişinin kişisel verilerin işlenmesi amacı da göz önüne alınarak, eksik kişisel verilerinin tamamlanmasını talep etme hakkına sahip olduğu da belirtilmiştir. Kişisel verilerin düzeltilmesini talep hakkına ilişkin KVKK, Yönerge ve Tüzük hükümlerinin temel olarak paralel olduğunu söylemek mümkündür.

Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi veya düzeltilmesi yönündeki haklı talebin yerine getirilmemesi durumunda, bunun veri sorumlusu bakımından hukuki ve cezai sonuçları söz konusu olabilecektir. İlgili kişinin veri sorumlusuna başvuru yolunun tüketilmesinin ardından Kurul nezdinde şikâyette bulunması mümkündür. Şikâyetin yerinde bulunması ihtimalinde Kurul tespit etmiş olduğu hukuka aykırılıkların veri sorumlusu tarafından giderilmesine karar verecektir (KVKK m. 15/5). KVKK m. 13 gereği zorunlu olan başvurunun yapılmasının ardından Kurul nezdinde şikâyet yoluna gidilmeksizin yargı yoluna başvurulması da mümkündür. Keza Kurul kararlarına karşı da yargı yolu açıktır.

Bunun dışında kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğranılması ihtimalinde KVKK m. 11/1-ğ hükmüne dayanılarak bu zararın giderilmesinin talep edilmesi mümkündür. Ayrıca KVKK m. 14/3 hükmüyle kişilik hakları ihlal edilenlerin genel hükümlere göre tazminat hakkı saklı tutulmuştur.

KVKK m. 17/2 gereği, KVKK m. 7 hükmüne aykırı olarak kişisel verileri silmeyen veya anonim hâle getirmeyenler TCK'nın *"verileri yok etmeme"* kenar başlıklı 138. maddesine göre cezalandırılır. Dolayısıyla kişisel verilerin silinmemesi, yok edilmemesi veya anonim hale getirilmemesi sonucunda TCK m. 138 gereği bir yıldan iki yıla kadar hapis cezası yaptırımı da gündeme gelebilmektedir. Bununla

birlikte kişisel verilerin hâlihazırda hukuka uygun bir şekilde elde edilip kaydedilmiş olması ihtimalinde, ilgili kişi tarafından KVKK m. 11/1-d uyarınca haklı bir şekilde ileri sürülen düzeltme talebinin yerine getirilmemesi bir suç oluşturmayacaktır. Zira kişisel verilerin düzeltilmemesi bir suç olarak düzenlenmemiştir.

Son olarak kişisel verilerin imhası veya düzeltilmesi talebinin veri sorumlusu tarafından yerine getirilmemesi üzerine Kurul nezdinde şikâyet yoluna başvurulması ve Kurul'un şikâyeti yerinde bulması ihtimalinde, Kurul kararını yerine getirmeyen veri sorumlusunun idari para cezasından sorumluluğu gündeme gelecektir.

KAYNAKÇA

Akdağ, Hale. Türk Ceza Kanunu Kapsamında Kişisel Verilerin Korunması. Ankara: Adalet Yayınevi, 2013.

Aydın, Sedat Erdem. AİHM İçtihatları Bağlamında Kişisel Verilerin Kaydedilmesi Suçu. İstanbul: On İki Levha Yayıncılık, 2015.

Başalp, Nilgün. "Avrupa Birliği Veri Koruması Genel Regülasyonu'nun Temel Yenilikleri." MÜHFD 21, no. 1 (2015): 77-105.

Başalp, Nilgün. Kişisel Verilerin Korunması ve Saklanması. Ankara: Yetkin Yayınları, 2004.

Bennett, Steven C.. "The 'Right to Be Forgotten': Reconciling EU and US Perspectives." Berkeley Jorunal of International Law 30, no. 1 (2012): 161-195.

Çekin, Mesut Serdar. "6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun'un Big Data (Büyük Veri) ve İrade Serbestisi Açısından Değerlendirilmesi." İÜHFM 74, no. 2 (2016): 629-644.

Çekin, Mesut Serdar. Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kişisel Verilerin Korunması Kanunu. İstanbul: On İki Levha, 2018.

Dülger, Murat Volkan. "İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması." İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 5, no. 1 (2018): 71-143.

Dülger, Murat Volkan. "Kişisel Sağlık Verileri Hakkında Yönetmelik'e İlişkin Değerlendirme." Hukuki Haber, Temmuz 14, 2019. Erişim tarihi 8 Ağustos 2019. https://www.hukukihaber.net/kisisel-saglik-verileri-hakkinda-yonetmelike-iliskin-degerlendirme-makale,6847.html.

Dülger, Murat Volkan. "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması." İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi 3, no. 2 (2016): 101-167.

Dülger, Murat Volkan. Kişisel Verilerin Korunması Hukuku. İstanbul: Hukuk Akademisi, 2019.

Ehmann, Eugen ve Martin Selmayr. Datenschutzgrundverordnung. München: C.H. Beck, 2018.

Elmalıca, Hasan. "Bilim Çağının Ortaya Çıkardığı Temel Bir İnsan Hakkı Olarak Unutulma Hakkı." AÜHFD 65, no. 4 (2016): 1603-1636.

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." Erişim tarihi 8 Ağustos 2019. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

EUR-Lex. "Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." Erişim tarihi 8 Ağustos 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

European Commission. "Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques." Erişim tarihi 8 Ağustos 2019. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

European Parliament. "European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)." Erişim tarihi 8 Ağustos 2019. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//EN.

Gözüküçük, Merve. "Veri İşleme Süreçlerinde Tartışmalı Bir Çözüm: Veri Anonimleştirmesi." Yayımlanmamış yüksek lisans tezi, İstanbul Bilgi Üniversitesi, 2014.

Gürpınar, Damla. "Kişisel Verilerin Korunamamasından Doğan Hukuki Sorumluluk." Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi Prof. Dr. Şeref Ertaş'a Armağan 19, no. özel (2017): 679-694.

Intersoft Consulting. "Key Issues, GDPR Right to be Forgotten." Erişim tarihi 8 Ağustos 2019. https://gdpr-info.eu/issues/right-to-be-forgotten/.

Kartal, Mustafa Tevfik. "Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme." Uluslararası Ekonomi ve Yenilik Dergisi 4, no. 1 (2018): 1-18.

Kaya, Mehmet Bedii ve Furkan Güven Taştan. Kişisel Veri Koruma Hukuku Mevzuat & İçtihat. İstanbul: On İki Levha, 2018.

Kazemi, Robert. General Data Protection Regulation (GDPR). Hamburg: Tredition, 2018.

Ketizmen, Muammer. Türk Ceza Hukukunda Bilişim Suçları. Ankara: Adalet Yayınevi, 2008.

Kılınç, Doğan. "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması." AÜHFD 61, no. 3 (2012): 1089-1169.

Korkmaz, İbrahim. "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme." TBB Dergisi 124, (2016): 81-152.

Köse Aysun, Melike. Kişisel Verilerin Kaydedilmesi Suçu (TCK m. 135). Ankara: Seçkin, 2018.

Küzeci, Elif. Kişisel Verilerin Korunması. Ankara: Turhan Kitabevi Yayınları, 2018.

KVKK. "Kişisel verilere hukuka aykırı erişilmesini önleme yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 26/07/2018 Tarihli ve 2018/91 Sayılı Karar Özeti." Erişim tarihi 8 Ağustos 2019. https://kvkk.gov.tr/Icerik/5365/2018-91.

KVKK. "Kişisel Verileri Koruma Kurumu Kişisel Verileri Koruma Kurumu Kişisel Veri Saklama ve İmha Politikası, Veri Sorumlularına Örnek Olması İçin Kurum İnternet Sayfasında Yayınlanmıştır." Erişim tarihi 8 Ağustos 2019. https://www.kvkk.gov.tr/Icerik/5387/KVKK-Kisisel-Veri-Saklama-ve-Imha-Politikasi.

KVKK. "Kişisel Verilerin Korunmasına İlişkin Başvuru ve Şikâyet Hakkı." Erişim tarihi 8 Ağustos 2019. https://kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASINA%20%C4%B0L%C4%B0%C5%9EK%C4%B0N%20BA%C5%9EVURU%20VE%20%C5%9E%C4%B0K%C3%82YET%20HAKKI.pdf.

KVKK. "KVKK Kişisel Veri Saklama ve İmha Politikası." Erişim tarihi 8 Ağustos 2019. https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e95a5392-23bf-4b30-8114-0526284c5837.pdf.

KVKK. "KVKK Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi." Erişim tarihi 8 Ağustos 2019. https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20S%C4%B0L%C4%B0NMES%C4%B0,%20YOK%20ED%C4%B0LMES%C4%B0%20VEYA%20ANON%C4%B0M%20HALE%20GET%C4%B0R%C4%B0LMES%C4%B0%20REHBER%C4%B0.pdf.

KVKK. "Sicil dosyalarındaki kişisel verilerin, işlenmelerini gerektiren sebeplerin ortadan kalkmaması sebebiyle, imha edilmemesi gerektiği hakkında Kişisel Verileri Koruma Kurulunun 28/06/2018 Tarihli ve 2018/69 Sayılı Karar Özeti." Erişim tarihi 8 Ağustos 2019. https://kvkk.gov.tr/Icerik/5366/2018-69.

KVKK. "Veri Sorumlusuna Başvuru ve Kurula Şikâyet Sürelerinin Hesaplanmasına İlişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarih ve 2019/9 sayılı Kararı." Erişim tarihi 8 Ağustos 2019. https://www.kvkk.gov.tr/Icerik/5358/Kamuoyu-Duyurusu.

Oğuz, Habip. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum." Uyuşmazlık Mahkemesi Dergisi, no. 3 (2013): 1-38.

Singel, Ryan. "Netflix Spilled Your Brokeback Mountain Secret, Lawsuit Claims." Wired, Aralık 17, 2009. Erişim tarihi 8 Ağustos 2019. https://www.wired.com/2009/12/netflix-privacy-lawsuit/.

Solove, Daniel J.. The Digital Person: Technology and Privacy in the Information Age. New York and London: New York University Press, 2004.

Şekerbay, Cennet Alas. "GDPR ile gelen "Pseudonymization" (Takma Ad Verme) Kavramı." Academia. Erişim tarihi 8 Ağustos 2019. https://www.academia.edu/36711924/GDPR_ile_gelen_Pseudonymization_Takma_Ad_Verme_Kavram%C4%B1?auto=download.

Şimşek, Oğuz. Anayasa Hukukunda Kişisel Verilerin Korunması. İstanbul: Beta, 2008.

Taştan, Furkan Güven. Türk Sözleşme Hukukunda Kişisel Verilerin Korunması. İstanbul: On İki Levha Yayıncılık, 2017.

Tekin, Nurullah. "Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi." Uyuşmazlık Mahkemesi Dergisi, no. 4 (2014): 222-262.

Turan, Metin. Karşılaştırmalı Hukukta Kişisel Verilerin Korunması. Ankara: Adalet Yayınevi, 2017.

Uncular, Selen. İş İlişkisinde İşçinin Kişisel Verilerinin Korunması. Ankara: Seçkin, 2014.

Voss, W. Gregory. "The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation." Journal of Internet Law, (July 2014): 3-7.

Yavuz, Can. İnternet'teki Arama Sonuçlarından Kişisel Verilerin Kaldırılması Unutulma Hakkı. Ankara: Seçkin, 2016.

TERRORIST USE OF THE INTERNET

Terör Örgütlerinin İnternet Kullanımı

Ergül ÇELİKSOY[*]
Smith OUMA[**]

Abstract

This paper offers a brief overview of how and for what purposes the Internet is utilised by terrorists, and discusses whether it plays a vital role for today's terrorist organisations. For this aim, the paper examines how terrorists use the Internet for the purposes of disseminating their propaganda, of achieving the radicalisation of people and the recruitment of new supporters, and of providing online training for their supporters to carry out terrorist attacks as well as terrorist financing. It argues that the Internet is very important for today's terrorist groups for a variety of reasons.

Keywords: terrorism, internet, terrorist use of internet

Özet

Terör örgütleri interneti birçok amaç için kullanmaktadır. Bunların başında, terör propagandası yapmak, insanları radikalleştirmek, internet aracılığı ile uzaklardaki insanlara ulaşarak yeni üyeler devşirmek, terör saldırılarında kullanılmak üzere çeşitli patlayıcıların evde yapımını kolaylaştırıcı nitelikte bilgi içeren materyalleri

[*] PhD Researcher, School of Law, The University of Nottingham, Nottingham, NG7 2RD, UK. E-mail: ergul.celiksoy@nottingham.ac.uk, ORCID: 0000-0003-2980-710X.

[**] PhD Researcher, School of Law and Politics, Cardiff University, Cardiff, CF10 3AS, UK. E-mail: OumaSO@cardiff.ac.uk, ORCID: 0000-0002-0469-333X.

Makale Gönderim Tarihi: 01.04.2019.

Makale Kabul Tarihi: 16.12.2019.

internet üzerinden üyelerine ulaştırmak ve terör örgütlerinin internet aracılığı ile finanse edilmesi gelmektedir. Bu makale, terör örgütlerinin interneti hangi amaçlarla ve nasıl kullandığını inceleyerek internetin teröristlerin amacını gerçekleştirmede ne ölçüde etkili bir araç olduğunu tartışmayı amaçlamaktadır.

Anahtar Kelimeler: terörizm, internet, teröristlerin internet kullanımı

I. Introduction

The Internet is an important part of the daily life of many individuals and has brought with it many opportunities and challenges. Nowadays, over 3.3 billion people use the Internet.[1] This number not only include ordinary users, but also ill-wishers such as hackers, online fraudsters and terrorists. Researchers claim that terrorist organisations utilise the Internet for many reasons.[2] Benson states that terrorist groups exploit the Internet since it offers many opportunities such as anonymity, cheap and easy communication and an abundance of information.[3] The Internet is also utilised by terrorists for a number of other purposes such as dissemination of propaganda, psychological warfare, gathering information, radicalisation and recruitment of individuals, online training and planning and preparing for attacks and terrorist financing.[4] In this respect, terrorist use of the Internet is a broader term than

---

1 "Individuals using the Internet (% of population)," The World Bank, accessed September 20, 2019, https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&start=1960&view=chart.

2 Maura Conway, "Terrorism and the Internet: New Media - New Threat?," Parliamentary Affairs 59, no. 2 (2006): 283–298; Gabriel Weimann, "www.terror.net - How Modern Terrorism Uses the Internet," USIP Special Report, no. 116 (2004): 1–12.

3 David C Benson, "Why the Internet Is Not Increasing Terrorism," Security Studies 23, no. 2 (2014): 298.

4 Stuart Macdonald and David Mair, "Terrorism Online: A New Strategic Environment," in Terrorism Online: Politics, Law and Technology, ed. Lee Jarvis, Stuart MacDonald, and Thomas M. Chen (Abingdon: Routledge, 2015), 10–34.

'cyberterrorism' because the former refers to a wider range of online activities associated with terrorism, whereas the latter is linked to terrorist attacks against information infrastructures, computer systems and programmes and data.[5] The purpose of this paper is to provide an overview of why and how the Internet is used by terrorist organisations for a variety of purposes. It contains four discussion sections: disseminating propaganda, radicalisation and recruitment, online training and attack and terrorist financing. Following the explanation of terrorist usage of the Internet under these four spheres, the conclusion arrived at will be evident: The use of the Internet is becoming vital for today's terrorist groups.

II. Propaganda Dissemination & Communication

Terrorist organisations use propaganda to legitimise their operations and to gain support or show the weakness of their enemies.[6] To understand the importance of propaganda

---

5 Dorothy E. Denning provides best-known and widely used definition of cyberterrorism. According to her, 'Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt non-essential services or that are mainly a costly nuisance would not.' See Dorothy E. Denning, "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives," May 23, 2000, https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm. See also Lee Jarvis and Stuart Macdonald, "What Is Cyberterrorism? Findings from a Survey of Researchers," Terrorism and Political Violence 27, no. 4, (2015): 659, https://doi.org/10.1080/09546553.2013.847827; Lee Jarvis, Stuart Macdonald, and Andrew Whiting, "Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat," European Journal of International Security 2, no. 1 (2017): 65, https://doi.org/10.1017/eis.2016.14.

6 Weimann, "How Modern Terrorism Uses the Internet," 6-8.

dissemination for terrorist organizations, it is worth noting that Osama bin Laden wrote, '[i]t is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90 percent of the total preparation for the battles'.[7] Similarly, in a letter that was sent by Ayman al-Zawahiri to Abu Musab al-Zarqawi, who was the leader of Al-Qaeda in Iraq at that time, al-Zawahiri wrote that '[w]e are in a battle, and more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle in a race for the hearts and minds of our Ummah'.[8] From these statements, it follows that propaganda dissemination is one of the priorities of terrorist organisations. Thus, terrorist groups utilise technology, especially the Internet, whose effectives rivals all the other methods of information dissemination. For example, Mohamed Jarmoune, who promoted jihadist ideology in his Facebook group, spent almost 15 hours a day disseminating terrorist propaganda online before eventually being arrested and sentenced to five years and four months in prison.[9]

Using the Internet for terrorist propaganda has many advantages. For example, prior to the advent of the Internet, terrorist groups depended on mainstream media such as television, radio and newspapers to express their policies and disseminate their propaganda.[10] However, the Internet has freed terrorist groups from the dependency of mainstream media and allowed them to access their audience with little obstacles.[11] In addition to this, the Internet has increased the size of the potential audience of terrorist groups. For instance, the World Bank revealed that more than 45 per cent of the world population (more than 3.3 billion people) used the

---

7 Akil N. Awan, "The Virtual Jihad: An Increasingly Legitimate Form of Warfare," CTC Sentinel 3, no. 5 (2010): 10.

8 Jytte Klausen, "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq," Studies in Conflict & Terrorism 38, no. 1 (2015): 3.

9 Lorenzo Vidino, "The Evolution of Jihadism in Italy: Rise in Homegrown Radicals," CTC Sentinel 6, no. 11 (2013): 19.

10 Weimann, "How Modern Terrorism Uses the Internet," 6.

11 Klausen, "Tweeting the Jihad," 3.

Internet in 2016 (See Figure 1). In addition, the number of social media users as of 2019 was over 2.7 billion, and it is estimated that this figure will increase to 3 billion by 2021 (See Figure 2). This means that terrorist organisations have billions of potential audiences which are impossible to access via mainstream media.

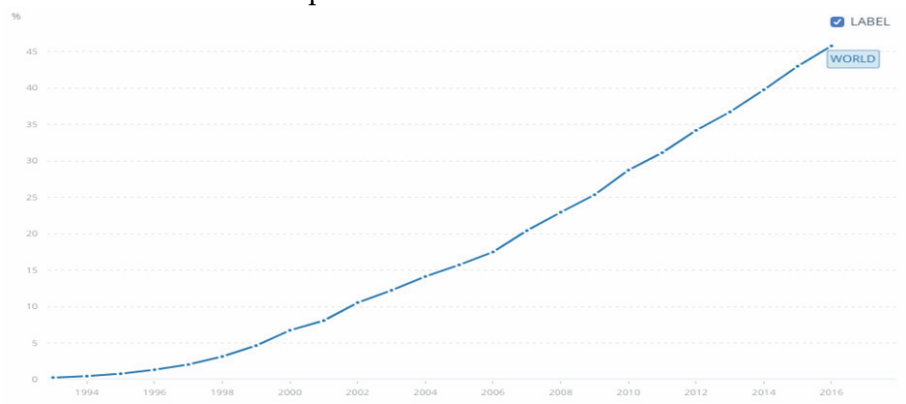


Figure 1: Individuals using the Internet (% of population) in the world.

This figure is reproduced form The World Bank's website. See "Individuals using the Internet (% of population).".

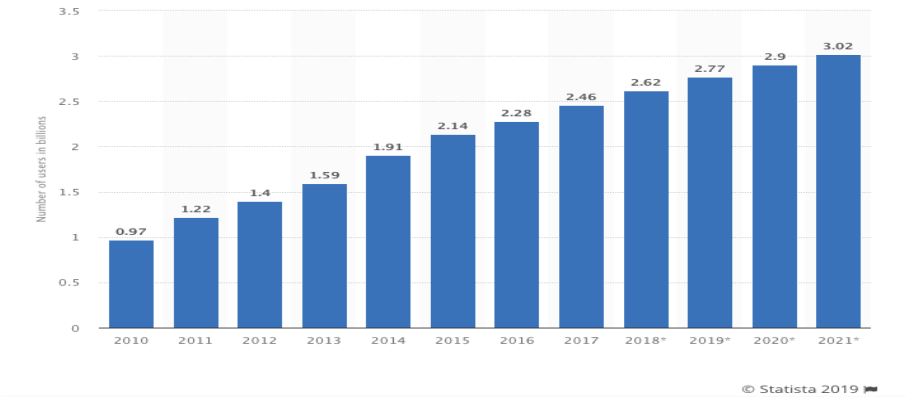


Figure 2: Number of social media users worldwide from 2010 to 2021 (in billions).

This figure is reproduced from Statista's website. See "Number of social Media users worldwide from 2010 to 2021 (in billions)," Statista, accessed March 20, 2019, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

It is known that almost all terrorist organisations have at least one website, and these are written in different languages.[12] For instance, PKK (*Partiya Karkerên Kurdistanê*), a terrorist organisation, mainly active in Turkey, has a website, called *Hêzên Parastina Gel*, written in Kurdish, Turkish, English, German and Arabic languages. This website includes a press release section, a list of terrorist leaders, a list of central commands, information about the terrorist group's legitimisation of activities, a link to the terrorist's group's online TV, book and article recommendations, interviews with individual terrorists and a contact form. Similarly, important messages of, so called terrorist group, Islamic State of Iraq and Al-Sham (ISIS), were published in English, French and German and translated into other languages to access a broader public.[13] Al-Qaeda also has a web-based magazine in English called *Inspire*. This shows that terrorist groups try to access as wide an audience as possible to disseminate their propaganda. For this purpose, the Internet avails them many facilities that are easy to use and inexpensive in comparison with traditional methods.[14] Today's terrorist organisations do not have to distribute hard copies of their publications to their supporters, which can be blocked and removed, because they can easily create a website to do so.[15] Even if their website is banned or rendered inaccessible, creating another one is very easy and inexpensive.[16] Although the content of publications

---

12 Weimann, "How Modern Terrorism Uses the Internet," 3.

13 Anne Aly et al., "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization," Studies in Conflict & Terrorism 40, no. 1 (2017): 5, https://doi.org/10.1080/1057610X.2016.1157402.

14 Benson, "Why the Internet Is Not Increasing Terrorism," 297.

15 Benjamin R. Davis, "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance," Commlaw Conspectus 15, no. 1 (2006): 131.

16 Benson, "Why the Internet Is Not Increasing Terrorism," 297-298.

from today's terrorist organisations is like that of the past, the role of the Internet is in the content's distribution; the Internet allows for the 'digitalisation of information'.[17]

III. Radicalisation & Recruitment

Edwards and Gribbon have stated that, '[f]or reasons of security and safety, accessibility and anonymity, terrorists and extremists have shifted many of their activities from public spaces (such as mosques, in the case of Islamist extremist groups) to private residences, personal computers and tablets'.[18] Similarly, Janbek and Williams stated that the Internet is an excellent tool for terrorist groups to contact and communicate with those who are vulnerable towards indoctrination attempts or who are already interested in terrorism.[19] They also stated that the Internet is not only a good tool for indoctrination, but also consolidates 'existing radical ideology'.[20]

It is claimed that terrorist groups use many facilities such as chat rooms, forums and websites to radicalise people.[21] Keene suggests that 'Internet chat rooms are virtual meeting points for individuals to come together not only to enrol in the cause, and be further radicalised and recruited to the terrorist organisation'.[22] With regards to the role played by online forums in radicalisation and recruitment, Marc Sageman wrote that '[i]t is the forums, not the images of the passive websites, which are crucial in the process of radicalization. People change their minds through discussion with

---

17 Martin Rudner, "'Electronic Jihad': The Internet as Al-Qaeda's Catalyst for Global Terror," Studies in Conflict & Terrorism 40, no. 1 (2017): 12.

18 Charlie Edwards and Luke Gribbon, "Pathways to Violent Extremism in the Digital Era," The RUSI Journal 158, no. 5 (2013): 40.

19 Dana Janbek and Valerie Williams, "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism," Brown Journal of World Affair 20, no. 2 (2014): 299-300.

20 Janbek and Williams, "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism," 300.

21 Weimann, "How Modern Terrorism Uses the Internet," 8.

22 Shima D. Keene, "Terrorism and the Internet: A Double-edged Sword," Journal of Money Laundering Control 14, no. 4 (2011): 365.

friends, not by simply reading impersonal stories'.[23] Thus, it could be said that being active in chat rooms and forums, which involves joining a discussion rather than acting as a passive member who reads just personal stories or looks at pictures, has an important effect on the radicalisation process.

Websites also play an important role in online radicalisation. When an individual who wants to learn more about an ideology visits a website, he or she is led to 'the group's enlistment pages', which feature 'articles about religious beliefs and core ideologies'.[24] This is considered as the first step for the process of radicalisation online; the next step is indoctrination. The individuals who are radicalised try to find ways to act on 'their religious beliefs and core ideologies'.[25] These actions can involve joining terrorist groups to carry out their own attacks.[26] For example, a law student in London, Mohammed Gul, was radicalised after spending some time on cyberspace with people who already had radical views. Later, he made a decision to make some extremist videos and uploaded them onto YouTube and an Anti-Imperialist forum website.[27]

More recently, it was discovered that a web-site called *8chan* was frequently used by the attackers of three terrorist attacks occurred in Christchurch, New Zealand on 15 March 2019; Poway, California on 27 April 2019 and El Paso, Texas on 02 August 2019.[28] *8chan* was a website, which contained a wide range of different

---

23 Marc Sageman, Leaderless Jihad: Terror Networks in the Twenty-First Century (Philadelphia: University of Pennsylvania Press, 2008), 116.

24 Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

25 Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

26 Aly et al., "Terrorist Online Propaganda and Radicalization," 5.

27 "Islamic terrorist propaganda student Mohammed Gul jailed," BBC News, accessed March 25, 2019, http://www.bbc.co.uk/news/uk-england-london-12576973.

28 Julia Carrie Wong, "8chan: the far-right website linked to the rise in hate crimes," The Guardian, accessed October 1, 2019, https://www.theguardian.com/technology/2019/aug/04/mass-shootings-el-paso-texas-dayton-ohio-8chan-far-right-website.

discussion groups about a number of different topics from anime and cryptocurrency to politics and video games.[29] *8chan*'s /pol/ board was considered as 'a gathering place for extremely online neo-Nazis', and its purpose was, as described by its members, to radicalise anonymous members to carry out acts of violence in the physical world.[30]

One of the Christchurch attackers posted a manifesto on *8chan*, which was titled 'The Great Replacement' referring to 'white genocide' conspiracy theories.[31] He also posted link on this platform to his live-streamed attack on Facebook Live. His aim was to show his brutal attack to spread fear of his terrorism, and perhaps, to inspire other extremists to carry out their own attacks.[32] His live-streamed attack posted in *8chan* attracted a number of members of this platform, and his manifesto was translated to different languages.[33] It was reported that the attacker's live-streamed video was watched by fewer than 200 people on Facebook before it was taken down by the social media site. However, the live footage posed on *8chan* allowed 'the grisly footage to reach millions'.[34] The El Paso shooter, who killed 22 people and injured 24 others, also

---

29 "What is 8chan?," BBC News, accessed October 1, 2019, https://www.bbc.co.uk/news/blogs-trending-49233767.

30 Robert Evans, "Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board," Bellingcat, accessed October 1, 2019, https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/.

31 Kathy Gilsinan, "How White-Supremacist Violence Echoes Other Forms of Terrorism," The Atlantic, accessed October 1, 2019, https://www.theatlantic.com/international/archive/2019/03/violence-new-zealand-echoes-past-terrorist-patterns/585043/.

32 Isaac Stanley-Becker et al., "Primary Suspect, One Alleged Accomplice Identified in Terrorist Attack That Killed 49 in New Zealand," The Washington Post, accessed May 10, 2019, https://www.washingtonpost.com/nation/ 2019/03/15/ shootings-reported-mosques-christchurch-new-zealand/.

33 Evans, "Pay Attention To 8chan's /pol/ Board."

34 Rachel Siegel, "8chan Is Back Online, This Time as 8kun," The Washington Post, accessed November 18, 2019, https://www.washingtonpost.com/technology/2019/11/04/chan-is-back-online-this-time-kun/.

posted an anti-immigrant manifesto decrying Hispanic migrants on *8chan*, which also expressed support for the gunman who killed 51 people in Christchurch, New Zealand.[35] Similarly, the attacker in Poway, California was also a user of this website to spread his hate speeches before conducting his attack.[36] Although 8chan was knocked offline, its extremist users appeared to move other websites.[37]

It is also important to note that the Internet has contributed to the radicalisation of 'lone wolves'. Ramón Spaaij defines a lone wolf terrorist as someone who carries out attacks 'individually and independently' from the terrorist groups he or she sympathises with or supports.[38] Similarly, Gabriel Weimann suggests that 'a lone wolf is someone who commits violent acts in support of some group, movement or ideology, but does so alone, outside of any command structure'.[39] However, it is sometimes questioned whether lone wolves are really alone in their radicalisation and operation process. It is argued that although lone wolves carry out their attacks individually and independently, they are radicalised and supported through the Internet.[40] Weimann states that '[l]one wolves connect, communicate and share information, know-how and guidance — all online — on the "Dark Web"'.[41] Regarding the role played by the

---

35 "Texas Walmart Shooting: El Paso Attack 'Domestic Terrorism'," BBC News, accessed September 12, 2019, https://www.bbc.co.uk/news/world-us-canada-49226573.

36 Jill Cowan, "What to Know About the Poway Synagogue Shooting," The New York Times, accessed September 12, 2019, https://www.nytimes.com/2019/04/29/us/synagogue-shooting.html.

37 Joshua Fisher-Birch, "Users of 8chan's /Pol Board Move to Other Websites," Counter Extremism Project, accessed September 10, 2019, https://www.counterextremism.com/blog/users-8chan%E2%80%99s-pol-board-move-other-websites.

38 Ramón Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," Studies in Conflict & Terrorism 33, no. 9 (2010): 854.

39 Gabriel Weimann, "Lone Wolves in Cyberspace," Journal of Terrorism Research 3, no. 2 (2012): 77.

40 Weimann, "Lone Wolves in Cyberspace," 76.

41 Weimann, "Lone Wolves in Cyberspace," 76.

Internet in lone wolves' radicalisation, Pantucci suggests that the Internet is 'an incubator or accelerator of the Lone Wolf phenomenon'.[42] Additionally, that the Internet has considerable impact on the radicalisation of and attacks by lone wolves was shown in the report conducted by the General Intelligence and Security Service in the Netherlands (AIVD).[43]

Dissemination may also take the form of terrorists broadcasting their activities in order to evoke sympathy or support from their intended targets and this phenomenon has increasingly become prevalent with the advent of online live-streaming platforms that are not subjected to the rigors of editorial processes.[44] This phenomenon is particularly attractive to lone wolf terrorists who may draw inspiration from terrorist organisations in jurisdictions beyond their reach or who may be radicalised by ideologies pursued by groups at a local level.

Terrorist use of the Internet is not only limited to the dissemination of terrorist propaganda or radicalisation of individuals. Terrorists also utilise the Internet to recruit new supporters.[45] Before the Internet, terrorist groups recruited individuals from certain geographic areas as communication with others from different countries or territories was too much of a challenge.[46] With the use of the Internet, the world is getting smaller for terrorist groups since they can contact others irrespective of where they live.[47] Today, terrorist groups can communicate with

---

42 Raffaello Pantucci, "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists," Developments in Radicalisation and Political Violence, International Centre for the Study of Radicalisation and Political Violence (ICSR) (2011): 34.

43 Netherlands: General Intelligence and Security Service (AIVD), Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age (The Hague, 2012), 20-21.

44 Maura Conway and Joseph Dillon, "Future Trends: Live-Streaming Terrorist Attacks?," VOX-Pol, accessed October 8, 2019, https://www.voxpol.eu/download/vox-pol_publication/Live-streaming_FINAL.pdf.

45 Weimann, "How Modern Terrorism Uses the Internet," 8-9.

46 Macdonald and Mair, "Terrorism Online," 16.

47 Tom Holt et al., "Political Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos," Dynamics of Asymmetric Conflict 8, no. 2 (2015): 108-109.

people in countries and territories which were closed to them before the Internet.[48] For instance, ISIS used the Internet to recruit people from Europe, North America, Australia and the Muslim countries.[49] It appears that the Internet allows terrorist groups to live in a visible world in which there are no boundaries to prevent them from accessing people. This is also the case for sympathisers because they can easily contact these groups and join them via the Internet.[50]

The Internet is more frequently used by young individuals than the older generation.[51] Among young individuals, those who are socially deprived, angry and/or marginalised are online more often than others.[52] By engaging these individuals, who are the major target for terrorist groups, and introducing terrorist literature to them, terrorist groups create new extremists and supporters.[53] This is another reason why terrorist groups exploit the Internet for recruitment purposes.[54] For example, PKK targeted young individuals aged between 15 and 25 in order to recruit them through social media. Ali Sahin, a Turkish MP, stated that 'the terrorist organization [PKK] uses it as a hunting field to recruit fighters for its mountain crew'. He noted that the average age of the PKK members 'has fallen to ages considered children' as young people are more vulnerable to be deceived, especially with the help of social media.[55]

---

48 Macdonald and Mair, "Terrorism Online," 16.

49 Rudner, "Electronic Jihad," 16.

50 Macdonald and Mair, "Terrorism Online," 16.

51 William H. Dutton, Grant Blank, and Darja Groselj, "Cultures of the Internet: The Internet in Britain, Oxford Internet Survey 2013 Report," Oxford Internet Surveys, accessed September 24, 2019, http://oxis.oii.ox.ac.uk/wp-content/uploads/2014/11/OxIS-2013.pdf.

52 Tina Frieburger and Jeffrey S. Crane, "A Systematic Explanation of Terrorist Use of the Internet," International Journal of Cyber Criminology 2, no. 1 (2008): 313-314.

53 Macdonald and Mair, "Terrorism Online," 17.

54 Macdonald and Mair, "Terrorism Online," 16.

55 "AKP Warns on PKK Activities on Internet," Hurriyet Daily News, accessed September 14, 2019, http://www.hurriyetdailynews.com/akp-warns-on-pkk-activities-on-internet-37572.

IV. Online Training & Attack

In addition to radicalisation and recruitment, terrorist groups use the Internet for online training for their supporters and for planning and preparing for attacking their targets.[56] In *Inspire*, the Al-Qaeda web-based magazine, Al-Malahem, in an article entitled 'Make a bomb in the kitchen of your Mom', wrote the following:

> My Muslim brother: we are conveying to you our military training right into your kitchen to relieve you of the difficulty of traveling to us. If you are sincere in your intentions to serve the religion of Allah then all what you have to do is enter your kitchen and make an explosive device that would damage the enemy if you put your trust in Allah and then use this explosive device properly.[57]

It is obvious that the purpose of the extract above was to train and equip terrorist supporters with a desire to engage with 'leaderless jihad'.[58] Holbrook wrote that two individuals obtained some bomb-making materials and tried to make a homemade bomb to carry out an attack in the UK.[59] From the evidence, which was seized from the suspects' properties during the investigation, it was understood that they had downloaded many manuals and searched information online to make a bomb in their house.[60] Indeed, some researchers claim that the Internet is an 'online terrorism university' for people who seek this kind of information.[61] For instance, Stenersen argues that many forums include some sub-forums dedicated solely to online training, and, in these sub-forums,

---

56 Macdonald and Mair, "Terrorism Online," 17.

57 Donald Holbrook, "A Critical Analysis of the Role of the Internet in the Preparation and Planning of Acts of Terrorism," Dynamics of Asymmetric Conflict 8, no. 2 (2015): 131.

58 Rudner, "Electronic Jihad," 16.

59 Holbrook, "A Critical Analysis of the Role of the Internet," 123-124.

60 Holbrook, "A Critical Analysis of the Role of the Internet," 126.

61 Gabriel Weimann, Terror on the Internet: The New Arena, the New Challenges (Washington, D.C.: United States Institute of Peace, 2006) 127.

members can ask questions and share their knowledge and experience with each other.[62] Moreover, there are 'manuals and encyclopaedias, instruction videos, series and periodicals', which may be helpful for the online training of terrorists.[63]

Some have contested that the Internet does not have an important role in the terrorists' training process because training requires hands-on experience along with technical information, and online materials may include misleading and incorrect information.[64] However, there have been some empirical examples of successful online training. For example, David Copeland and Anders Behring Breivik — the London 1999 and Oslo 2011 attackers, respectively — utilised the Internet to make their explosives, and they were successful in their attacks, even though they had no previous experience of making explosive devices.[65] These arguments also overlook the extent to which online training has facilitated acquisition of skills by mass shooters who have carried out acts of terrorism in different places.[66] Therefore, it can be argued that, notwithstanding the prevalence of wrong information on the Internet in terms of training, even an amateur attacker may obtain accurate information that he or she can use to make an explosive and carry out his or her attack.

The Internet can also be useful for terrorist groups in terms of planning an operation and attack. For example, Weimann wrote that

---

62 Anne Stenersen, "The Internet: A Virtual Training Camp?," Terrorism and Political Violence 20, no. 2 (2008): 228.

63 Stenersen, "The Internet: A Virtual Training Camp?," 228.

64 Michael Kenney, "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists," Terrorism and Political Violence 22, no. 2 (2010): 179.

65 Gilbert Ramsay, "Relocating the Virtual War," Defence against Terrorism Review 2, no. 1 (2009): 45.

66 Jillian Peterson and James Densley, "Op-Ed: We have Studied every Mass Shooting since 1966. Here's what we've Learned about the Shooters," Los Angeles Times, accessed September 22, 2019, https://www.latimes.com/opinion/story/2019-08-04/el-paso-dayton-gilroy-mass-shooters-data.

'Al Qaeda operatives relied heavily on the Internet in planning and coordinating the September 11 attacks'.[67] It was discovered that, in the 9/11 attack, Al-Qaeda was gathering information about the targets and sending messages through the Internet.[68] Terrorists planning the 9/11 attack used thousands of encrypted messages on a website that was accessed by password.[69] According to the United States Department of Justice: Office of Public Affairs, Najibullah Zazi, who tried to carry out an attack on the New York subway system in 2009, wrote 'Marriage is ready' to his contact in Pakistan via e-mail. 'Marriage', the word in his e-mail, refers to the attack and explosives.[70] Similarly, the members of Gülenist Terror Organisation (FETÖ) in Turkey used a messaging smartphone application, *ByLock*, to communicate via a private, encrypted connection.[71]

Planning an attack may require some preparatory acts such as 'target selection; reconnaissance; selection of entrance and exit routes; gaining knowledge of local peak times; and acquiring information on emergency service response times and effectiveness'.[72] These kinds of preparatory acts require multiple visits to the possible target, which is highly risky, costly and time consuming. However, the Internet allows terrorists to decrease these risks and costs and to save time.[73] For example, in its twelfth issue,

---

67 Weimann, "How Modern Terrorism Uses the Internet," 10.

68 Keene, "Terrorism and the Internet," 363.

69 Weimann, "How Modern Terrorism Uses the Internet," 10.

70 The United States Department of Justice: Office of Public Affairs, "Charges Unsealed Against Five Alleged Members of Al-Qaeda Plot to Attack the United States and United Kingdom," The United States Department of Justice, accessed September 28, 2019, https://www.justice.gov/opa/pr/charges-unsealed-against-five-alleged-members-al-qaeda-plot-attack-united-states-and-united.

71 İsmail Saymaz, "ByLock use is an evidence of Gülen network links: Owner," Hurriyet Daily News, accessed September 3, 2019, http://www.hurriyetdailynews.com/bylock-use-is-an-evidence-of-gulen-network-links-owner-105284. For the analysis of 'Bylock' by the Republic of Turkey Court of Cassation, see General Criminal Division of the Republic of Turkey Court of Cassation, E.2019/312, K.2019/514, 02.07.2019.

72 Macdonald and Mair, "Terrorism Online," 21.

73 Macdonald and Mair, "Terrorism Online," 21.

Al-Qaeda's magazine, *Inspire,* showed a 'country-by-country list of targets' and provided detailed information about these targets and how to carry out an attack on them.[74] Similarly, in the attack on British bases in Basra, attackers used photographs taken from Google Earth that showed the building and vulnerable areas in detail.[75] It has also been established that the Al Shaabab have in the past used social media platforms to generate propaganda and control the narrative during the course of an attack.[76] Part of the strategy has been to shape public opinion during an attack and to appeal to their perceived sympathisers. A similar strategy has been deployed by the Boko Haram in West Africa, who have not only employed the use of the Internet for propaganda, but also as a recruitment tool and to coordinate its activities.[77]

The empirical evidence has shown the importance of the Internet in preparation for terrorist attacks. For example, Gill et. al. examined the cases of 223 convicted terrorists in the United Kingdom.[78] They found that terrorists used the Internet for a variety of activities including radicalisation and/or attack planning in 61 percent of these 223 cases.[79] More than half of the terrorists in their study specifically

---

[74] "Al-Qaeda urges followers to bomb the Savoy," The Telegraph, accessed September 29, 2019, http://www.telegraph.co.uk/news/worldnews/al-qaeda/10704708/Al-Qaeda-urges-followers-to-bomb-the-Savoy.html.

[75] "Terrorists use Google maps to hit UK troops," The Telegraph, accessed September 15, 2019, http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

[76] David Mair, "#Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack," Studies in Conflict & Terrorism 40, no. 1 (2017): 24-43, https://doi.org/10.1080/1057610X.2016.1157404.

[77] Kate Cox et al., Social Media in Africa: A Double-edged Sword for Security and Development (UNDP, 2018), 22, https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf.

[78] Paul Gill et al., "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes," Criminology & Public Policy 16, no. 1 (2017): 99-117, https://doi.org/10.1111/1745-9133.12249.

[79] Gill et al., "Terrorist Use of the Internet by the Numbers," 107.

employed the Internet to learn about their intended terrorist activities.[80] Importantly, more than a third used the Internet in preparation for their attacks, including watching bomb-making videos, reading poison manuals and assassination guidebooks, downloading plans for the London Underground, Buckingham Palace, and other symbolic landmarks and terrorist training manuals.[81]

V. Terrorist Financing

The Internet presents a platform where terrorists can easily obtain financing for acts of terrorism. The United Nation Office on Drugs and Crime has identified four different ways which terrorists use the Internet to obtain financing, to wit; direct solicitation, e-commerce, exploitation of online payment tools, and through charitable organisations.[82] The Internet's attractiveness arises from the ease in which the platform offers a broad reach, timely efficiency, and a degree of anonymity and security to both the donor and recipient of the funds.[83] These considerations particularly become relevant within a context where access to properly regulated banking services is limited and where other alternatives such as mobile payments are prevalent. The situation is further exacerbated by the fact that few countries possess the technical know-how to detect and investigate online terrorist activities which means that this remains an area that will for a long time be attractive to terrorists and terrorist organisations.[84] To this end, it becomes challenging to assess the scale and impact of terrorist financing through the Internet, especially where encryption tools are deployed by the individuals.[85] Such complexities have heightened calls to

---

80 Gill et al., "Terrorist Use of the Internet by the Numbers," 107.

81 Gill et al., "Terrorist Use of the Internet by the Numbers," 107.

82 United Nations Office on Drugs and Crime, The Use of the Internet for Terrorist Purposes (UNODC, 2012), 7, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

83 Michael Jacobson, "Terrorist Financing on the Internet," CTC Sentinel 2, no. 6 (2009): 17-20.

84 Jacobson, "Terrorist Financing on the Internet," 19.

85 Tom Keatinge and Florence Keen, Social Media and Terrorist Financing: What are the Vulnerabilities and how Could Public and Private Sectors Collaborate

ensure collaboration amongst States and various stakeholders to collectively develop interventions for the threats occasioned from the use of the Internet for terrorist financing.[86] Efforts should particularly be driven towards expanding the capacities of low-income countries to be able to detect and investigate the use of the Internet for terrorist activities. Similarly. Efforts should be directed at strengthening the financial systems within these countries to ensure that financial transactions are monitored and regulated to prevent abuse of cash transfer platforms by terrorists and terrorist organisations. In Kenya for instance, the State vide The Kenya Information and Communications (Registration of SIM-CARDS) Regulations, 2015 has placed stringent regulations requiring proper records to be kept by telecommunication operators or their agents to keep in place a record of all the registered subscribers made by the telecommunications operator and to submit these records to the Communication Authority on a quarterly basis.[87] Such regulations essentially ensure that the regulatory agencies keep a record of all the users of communication devices utilising SIM cards and can enable the authorities monitor suspicious activities. Privacy and illegal surveillance concerns however cannot be overlooked whenever such interventions are deployed.

VI. Conclusion

The Internet has enormous importance for terrorists because it enables them to be independent from mainstream media, increase the size of their audience and benefit from the use of digitalised information, which is almost impossible to be blocked and removed from circulation. It also allows terrorist groups to shift their focus for radicalising people from public areas to online platforms such as websites, chatrooms and forums. In addition to radicalisation purposes, the Internet is also used by terrorist groups for the

Better? (Royal United Services Institute for Defence and Security Studies, 2019), 6, https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

86 Keatinge and Keen, Social Media and Terrorist Financing, 2.

87 The Kenya Information and Communications (Registration of SIM-CARDS) Regulations, 2015. Section 3.

purposes of consolidating their sympathisers and inciting 'lone wolves' to carry out terrorist attacks. Importantly, it enables terrorist groups to access and potentially recruit those living in different countries where were not closed to them prior to the existence of the Internet. The Internet is seen as a library or even an 'online terrorism university' for terrorists to acquire knowledge and information. It is a source for planning and coordinating a terrorist attack. Although it includes a great deal of misleading or wrong information, there is empirical evidence that shows that even amateur attackers were able to successfully carry out attacks thanks to online training. This paper concludes that the Internet is a vital tool for today's terrorist organisations, especially in terms of disseminating their propaganda, radicalising people, recruiting new supporters, providing online training materials for their followers and planning and preparing terrorist attacks and terrorist financing.

Bibliography

Aly, Anne, Stuart Macdonald, Lee Jarvis, and Thomas M. Chen. "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 1–9. https://doi.org/10.1080/1057610X.2016.1157402.

Awan, Akil N. "The Virtual Jihad: An Increasingly Legitimate Form of Warfare." *CTC Sentinel* 3, no. 5 (2010): 10-13.

BBC News. "Islamic terrorist propaganda student Mohammed Gul jailed." Accessed March 25, 2019. http://www.bbc.co.uk/news/uk-england-london-12576973.

BBC News. "Texas Walmart Shooting: El Paso Attack 'Domestic Terrorism'." Accessed September 12, 2019. https://www.bbc.co.uk/news/world-us-canada-49226573.

BBC News. "What is 8chan?." Accessed October 01, 2019. https://www.bbc.co.uk/news/blogs-trending-49233767.

Benson, David C. "Why the Internet Is Not Increasing Terrorism." *Security Studies* 23, no. 2, (2014):293–328.

Conway, Maura and Joseph Dillon. "Future Trends: Live-Streaming Terrorist Attacks?." VOX-Pol. Accessed October 8, 2019. https://www.voxpol.eu/download/vox-pol_publication/Live-streaming_FINAL.pdf.

Conway, Maura. "Terrorism and the Internet: New Media - New Threat?." *Parliamentary Affairs* 59, no. 2 (2006): 283–298.

Cowan, Jill. "What to Know About the Poway Synagogue Shooting." The New York Times. Accessed September 12, 2019. https://www.nytimes.com/2019/04/29/us/synagogue-shooting.html.

Cox, Kate, William Marcellino, Jacopo Bellasio, Antonia Ward, Katerina Galai, Sofia Meranto, and Giacomo Persi Paoli. *Social Media in Africa: A Double-edged Sword for Security and Development*. UNDP, 2018. https://www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pdf.

Davis, Benjamin R. "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance." *Commlaw Conspectus* 15, no. 1 (2006): 119-135.

Denning, Dorothy E. "Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services US House of Representatives." May 23, 2000. https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm.

Dutton, William H., Grant Blank, and Darja Groselj. "Cultures of the Internet: The Internet in Britain, Oxford Internet Survey 2013 Report." Oxford Internet Surveys. Accessed September 24, 2019. http://oxis.oii.ox.ac.uk/wp-content/uploads/2014/11/OxIS-2013.pdf.

Edwards, Charlie and Luke Gribbon. "Pathways to Violent Extremism in the Digital Era." *The RUSI Journal* 158, no. 5 (2013): 40–47.

Evans, Robert. "Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board." Bellingcat. Accessed October 01, 2019. https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/.

Fisher-Birch, Joshua. "Users of 8chan's /Pol Board Move to Other Websites." Counter Extremism Project. Accessed September 10, 2019. https://www.counterextremism.com/blog/users-8chan%E2%80%99s-pol-board-move-other-websites.

Frieburger, Tina and Jeffrey S. Crane. "A Systematic Explanation of Terrorist Use of the Internet." *International Journal of Cyber Criminology* 2, no. 1 (2008): 309-319.

Gill Paul, Emily Corner, Maura Conway, Amy Thornton, Mia Bloom, and John Horgan. "Terrorist Use of the Internet by the Numbers: Quantifying Behaviors, Patterns, and Processes." *Criminology & Public Policy* 16, no. 1 (2017): 99-117. https://doi.org/10.1111/1745-9133.12249.

Gilsinan, Kathy. "How White-Supremacist Violence Echoes Other Forms of Terrorism." The Atlantic. Accessed October 1, 2019. https://www.theatlantic.com/international/archive/2019/03/violence-new-zealand-echoes-past-terrorist-patterns/585043/.

Holbrook, Donald. "A Critical Analysis of the Role of the Internet in the Preparation and Planning of Acts of Terrorism." *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 121–133.

Holt, Tom, Joshua D. Freilich, Steven Chermak, and Clark McCauley. "Political Radicalization on the Internet: Extremist Content, Government Control, and the Power of Victim and Jihad Videos." *Dynamics of Asymmetric Conflict* 8, no. 2 (2015): 107–120.

Hurriyet Daily News. "AKP Warns on PKK Activities on Internet." Accessed September 14, 2019. http://www.hurriyetdailynews.com/akp-warns-on-pkk-activities-on-internet-37572.

Jacobson, Michael. "Terrorist Financing on the Internet." *CTC Sentinel* 2, no. 6 (2009): 17-20.

Janbek, Dana and Valerie Williams. "The Role of the Internet Post-9/11 in Terrorism and Counterterrorism." *Brown Journal of World Affair* 20, no. 2 (2014): 297–309.

Jarvis, Lee and Stuart Macdonald. "What Is Cyberterrorism? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27, no. 4, (2015): 657-678. https://doi.org/10.1080/09546553.2013.847827.

Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. "Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat." *European Journal of International Security* 2, no. 1 (2017): 64-87. https://doi.org/10.1017/eis.2016.14.

Keatinge, Tom and Florence Keen. *Social Media and Terrorist Financing: What are the Vulnerabilities and how Could Public and Private Sectors Collaborate Better?*. Royal United Services Institute for Defence and Security Studies, 2019. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf.

Keene Shima D. "Terrorism and the Internet: A Double-edged Sword." Journal of Money Laundering Control 14, no. 4 (2011): 359–370.

Kenney, Michael. "Beyond the Internet: Mētis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." *Terrorism and Political Violence* 22, no. 2 (2010): 177–197.

Klausen, Jytte. "Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq." *Studies in Conflict & Terrorism* 38, no. 1 (2015): 1-22.

Macdonald, Stuart and David Mair. "Terrorism Online: A New Strategic Environment." in *Terrorism Online: Politics, Law and Technology*, edited by Lee Jarvis, Stuart MacDonald, and Thomas M. Chen, 10-34. Abingdon: Routledge, 2015.

Mair, David. "#Westgate: A Case Study: How al-Shabaab used Twitter during an Ongoing Attack." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 24-43. https://doi.org/10.1080/1057610X.2016.1157404.

Netherlands: General Intelligence and Security Service (AIVD). *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age*. The Hague, 2012.

Pantucci, Raffaello. "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists." *Developments in Radicalisation and Political Violence, International Centre for the Study of Radicalisation and Political Violence (ICSR)* (2011): 1–39.

Peterson, Jillian and James Densley. "Op-Ed: We have Studied every Mass Shooting since 1966. Here's what we've Learned about the Shooters." Los Angeles Times. Accessed September 22, 2019. https://www.latimes.com/opinion/story/2019-08-04/el-paso-dayton-gilroy-mass-shooters-data.

Ramsay, Gilbert. "Relocating the Virtual War." *Defence against Terrorism Review* 2, no. 1 (2009): 31-50.

Rudner, Martin. "'Electronic Jihad': The Internet as Al-Qaeda's Catalyst for Global Terror." *Studies in Conflict & Terrorism* 40, no. 1 (2017): 10-23.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia: University of Pennsylvania Press, 2008.

Saymaz, İsmail. "ByLock use is an evidence of Gülen network links: Owner." Hurriyet Daily News. Accessed September 3, 2019. http://www.hurriyetdailynews.com/bylock-use-is-an-evidence-of-gulen-network-links-owner-105284.

Siegel, Rachel. "8chan Is Back Online, This Time as 8kun." The Washington Post. Accessed November 18, 2019. https://www.washingtonpost.com/technology/2019/11/04/chan-is-back-online-this-time-kun/.

Spaaij, Ramón. "The Enigma of Lone Wolf Terrorism: An Assessment." *Studies in Conflict & Terrorism* 33, no. 9 (2010): 854–870.

Stanley-Becker, Isaac, Eli Rosenberg, Alex Horton, and Michael Brice-Saddler. "Primary Suspect, One Alleged Accomplice Identified in Terrorist Attack That Killed 49 in New Zealand." The Washington Post. Accessed May 10, 2019. https://www.washingtonpost.com/nation/2019/03/15/shootings-reported-mosques-christchurch-new-zealand/.

Statista. "Number of social Media users worldwide from 2010 to 2021 (in billions)." Accessed March 20, 2019. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users.

Stenersen, Anne. "The Internet: A Virtual Training Camp?." *Terrorism and Political Violence* 20, no. 2 (2008): 215–233.

The Telegraph. "Al-Qaeda urges followers to bomb the Savoy." Accessed September 29, 2019. http://www.telegraph.co.uk/news/worldnews/al-qaeda/10704708/Al-Qaeda-urges-followers-to-bomb-the-Savoy.html.

The Telegraph. "Terrorists use Google maps to hit UK troops." Accessed September 15, 2019. http://www.telegraph.co.uk/news/worldnews/1539401/Terrorists-use-Google-maps-to-hit-UK-troops.html.

The United States Department of Justice: Office of Public Affairs. "Charges Unsealed Against Five Alleged Members of Al-Qaeda Plot to Attack the United States and United Kingdom." The United States Department of Justice. Accessed September 28, 2019. https://www.justice.gov/opa/pr/charges-unsealed-against-five-alleged-members-al-qaeda-plot-attack-united-states-and-united.

The World Bank. "Individuals using the Internet (% of population)." Accessed September 20, 2019. https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2017&start=1960&view=chart.

United Nations Office on Drugs and Crime. *The Use of the Internet for Terrorist Purposes*. UNODC, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

Vidino, Lorenzo. "The Evolution of Jihadism in Italy: Rise in Homegrown Radicals." *CTC Sentinel* 6, no. 11 (2013): 17-20.

Weimann, Gabriel. "www.terror.net - How Modern Terrorism Uses the Internet." *USIP Special Report*, no. 116 (2004): 1–12.

Weimann, Gabriel. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3, no. 2 (2012): 75–90.

Weimann, Gabriel. *Terror on the Internet: The New Arena, the New Challenges*. Washington, D.C.: United States Institute of Peace, 2006.

Wong, Julia Carrie. "8chan: the far-right website linked to the rise in hate crimes." The Guardian. Accessed October 01, 2019. https://www.theguardian.com/technology/2019/aug/04/mass-shootings-el-paso-texas-dayton-ohio-8chan-far-right-website.

ÇEVİRİ
BÖLÜMÜ

CEZA MUHAKEMESİNDE VİDEOKONFERANS YÖNTEMİNİNİN (SEGBİS) KULLANIMI*

"Videokonferenz Im Türkischen Strafprozessrecht"

Çev.: Erdal YERDELEN**

ÖZET

Gelişen teknoloji, hukuk alanında kolaylıkları beraberinde getirmekle birlikte bazı dezavantajları da bünyesinde taşımaktadır. Videokonferans (SEGBİS) yönteminin ceza muhakemesi alanında kullanılması, özellikle işlemi yapan makam ile muhatabın farklı yerlerde olduğu durumlarda büyük avantajlar sağlamaktadır. Ancak ifade alma sırasında muhatabın ifadeyi alan makamın fiziken karışısında olmaması yüzyüzelilik ilkesi bakımından tartışmalara neden olmaktadır. Videokonferans (SEGBİS) yönteminin ceza muhakemesindeki hukuki niteliğinin ne olduğu tartışılmaktadır. Bu sistemin (SEGBİS) kullanılmasının; istinabe (talimat) yerine geçtiği, duruşmada bulunma ile aynı olduğu şeklinde iki görüş mevcuttur. Ayrıca bu ikisinden başka kendine özgü bir sistem olduğu da kabul edilmektedir. Bu makalede videokonferans (SEGBİS) yönteminin hukuki niteliği ve ceza muhakemesinde kullanılmasının meşruiyeti ortaya konulacaktır.

---

* Bu makale, Kriminalpolitische Zeitschrift Dergisi'nin 2018/4 sayısında yayınlanmış olan "Videokonferenz Im Türkischen Strafprozessrecht" başlıklı Almanca makalenin çevirisidir.

** Doç. Dr. Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Öğretim Üyesi, erdalyerdelen@hotmail.com, ORCID: 0000-0002-8796-2186.

Makale Gönderim Tarihi: 28.11.2019.

Makale Kabul Tarihi: 13.12.2019.

I. GİRİŞ

Video konferans teknolojileri birçok alanda kullanılabilmektedir; çünkü her alanda ve meslekte insan etkileşimi söz konusudur. Farklı yerlerdeki insanların görüntülü görüşmesi, evden çalışma, şirket toplantıları, teletıp denilen uzaktan verilen sağlık hizmetleri, uzaktan eğitim ve TV canlı yayın katılımı gibi çok farklı alanlarda çok farklı kullanımlarla gerçekleşebilmektedir.[1]

Video konferansın yaygın kullanımı, insanların görüntülü haberleşme ve birlikte çalışma ihtiyaçlarını karşılayarak, evden/uzaktan çalışmanın ve çok farklı mekânlardan katılımcıların olduğu toplantı, konferans, eğitim vb. etkinliklerin gerçekleşmesine imkân vermektedir.[2] Video konferans yöntemi, uzaktan çalışma olanağı sağladığı gibi yargılama hukukunda da uzaktaki kişi ile adli makam arasında irtibat kurmaktadır. Son dönemde bu sebeplerle değişik ülkelerde yargılama hukukunda sıkça kullanılmaktadır.[3]

---

1 Bilgin Yazar, Görüntülü İletişim–Video Konferans Teknolojilerinin Kullanım Alanları (Etgi Grup, 2012), 2, https://www.etgigrup.com/wp-content/uploads/2016/04/video_konferans_ab_2013-1.pdf.

2 Yazar, Görüntülü İletişim, 3.

3 Mahkemelerde videokonferans usulünün uygulanmasına ilişkin düzenleme; Ceza muhekemesinde tanığın korunması amacıyla Alman Ceza Muhakemesi Kanunu (StPO) m.247a'da düzenlenmiştir. Bu madde 30.4.1998'de yürürlüğe girmiştir (BGBl. I S. 820). 2004 yılında ceza muhakemesinde delillerin korunması amacına yönelik olarak videokonferans uygulaması genişletilmiştir. Duruşma salonunda videokonferans usulünün kullanılması şu haller için meşru kabul edilmektedir:

– Bir tanık, ilgili veya suça iştirak eden kişinin uzun veya belirsiz bir süre duruşma salonunun bulunduğu yere getirilmelerinin mümkün olmaması,

– Bir tanık veya ilgilinin uzaklık nedeniyle duruşma salonunda bulunmalarının onlardan beklenemeyecek olması,

– Aynı şekilde savcılık, müdafii veya sanığın kabul etmiş olması (§ 247a i. V. m. § 251 Abs. 2 StPO, eingefu̇gt durch das Opfer-rechtsreformgsetz vom 24. Juni 2004, BGBl. I S. 1354, und das Justizmodernisierungsgesetz vom 24. August 2004, BGBl. I S. 2198).

II. Sesli ve Görüntülü Bilişim Sistemi (SEGBİS)

Ses ve Görüntü Bilişim Sistemi (SEGBİS), UYAP Bilişim Sisteminde ses ve görüntünün aynı anda elektronik ortamda iletildiği, kaydedildiği ve saklandığı çoklu bir ortam (multimedya) sistemidir.[4] Sistem, görüntü ile sesin aynı anda, güvenli bir şekilde iletilebilmesini ve kaydedilebilmesini gerektirmektedir. Görüntü kalitesi, ilgilinin yüz ifadelerini, vücut hareketlerini, tavır ve davranışlarını gözlemlemeye yeterli olmalıdır. Ses, ilgilinin duygularını anlamaya ve söylediklerini anlaşılır bir şekilde dinlemeye imkân verecek nitelikte olur. Bilgi, belge ve delillerin elektronik ortamda anında iletilebilmesi gerekir. SEGBİS ile elde edilen kayıtlar, nitelikli elektronik imza ile imzalanarak güvenli bir şekilde, talep eden makam tarafından saklanır.[5]

III. SEGBİS'in Yargı Alanında Sunduğu Olanaklar

SEGBİS ile ifadeler ve duruşma; video kaydına alınacak, tutanaklar bu kayıtlara göre düzenlenecek, video kayıtları Cumhuriyet savcısı, hâkim ve mahkemece tekrar tekrar izlenebilecektir.[6] Cumhuriyet savcısı ve hâkimin; unutmadan, atlamadan ve hata yapmadan ilgili kişinin ifadesini tutanağa geçirmesi kolaylaşacaktır. Dolayısıyla öncelikle iddialar ve şikâyetler ciddi oranda azalacak, video kayıtlarıyla gerçek kolaylıkla ortaya çıkarılabilecektir.[7] Cumhuriyet savcısı, hâkim veya mahkeme, ifadelerin özetlenmesine ve tutanağa geçirilmesine yoğunlaşmak zorunda kalmayacaktır. Video konfe-

---

4 "Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik," Mevzuat Bilgi Sistemi, erişim tarihi 21 Ağustos 2017, http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.15315&sourceXmlSearch=&MevzuatIliski=0.

5 RG. 20.09.2011, S. 28060.

6 Arif Gözel, "Yargılamada Ses ve Görüntü Bilişim Sistemi (SEGBİS) Kullanımı," Academia, erişim tarihi 21 Ağustos 2017, https://www.academia.edu/12580753/Yarg%C4%B1lamada_Ses_ve_G%C3%B6r%C3%BCnt%C3%BC_Bili%C5%9Fim_Sistemi_SEGB%C4%B0S_Kullan%C4%B1m%C4%B1.

7 Turan Açıkmeşe ve Ulvi Karaşahin, "Sesli Görüntülü Bilişim Sistemi (SEGBİS)," UYAP Bilişim Dergisi, no. 5 (2012): 25.

rans sistemiyle yargılamanın süjeleri (özneleri) ve ifade veren kişiler, huzurdaymış gibi yüz yüze getirilebileceklerdir. Video kayıtları, soruşturma veya kovuşturma işleminin yapıldığı sırada hazır bulunmayan yargılama süjeleri tarafından, sonradan izlenebilecek ve böylece yüz yüzelik ilkesi nispeten uygulanmış olacaktır. Örneğin; soruşturma aşamasında alınan ifadeler mahkemece izlenebilecektir. Bunun sonucunda mahkeme, söz konusu ifadenin doğruluğunu daha iyi takdir edebilecektir.[8]

SEGBİS ile savcılık veya ilk derece mahkemelerce video kaydına alınan ifadeler, kanun yolu mercilerince izlenebilmektedir. SEGBİS video konferans yöntemi sayesinde, ilgililerin huzuru dışında dinlenen tanıkların ses ve görüntüleri, ilgililerin huzuruna aktarılabilmektedir. Bu sayede aktarma sırasında ses ve görüntü bozmak suretiyle tanıkların korkmadan ve etki altında kalmadan beyanda bulunabilmeleri, kimliklerinin saklı tutulması ve aynı zamanda "*silahların eşitliği*" ve "*yüz yüzelik*" ilkelerinin uygulanması sağlanmaktadır.[9]

Kişileri sistem sayesinde huzurlarında gibi görmekte, bunların hâl ve hareketlerini izleyebilmektedirler. İfade alma veya sorgu işlemini de bizzat yaparak ellerindeki asıl dosya içeriğine göre ihtiyaç duydukları beyanları daha kolay alabilmektedirler. Yargılamanın tarafları da sistem sayesinde, ifadeleri alınacak veya sorgusu yapılacak kişileri huzurlarında görebilmektedir. Bunların hâl ve hareketlerini izleyebilecekler ve ifade alma veya sorgu işlemine katılarak soru sorabileceklerdir.[10]

SEGBİS video konferans sistemiyle, yargılamanın süjeleri yüz yüze getirilerek asıl yetkili soruşturma veya kovuşturma makamlarının kendi işlemlerini bizzat yapmaları sağlanmaktadır. Uzakta bulunan ve ifadeleri alınacak veya sorgusu yapılacak kişiler, sistem sayesinde o dosya için esas yetkili olan yargılama makamı huzuruna

---

8 Açıkmeşe ve Karaşahin, "Sesli Görüntülü," 26.

9 Açıkmeşe ve Karaşahin, "Sesli Görüntülü," 27.

10 Sami Acar ve Hülya Gürsoy, "Türk Mahkemelerinde Sesli ve Görüntülü Kayıt ve Videokonferans Sistemi Uygulamasına Geçiş, Ceza Mahkemeleri Örneği," Ankara Barosu Dergisi 70, no. 4 (2012): 131.

çıkmaktadırlar.[11] Bu yargılama makamları, bunların hâl ve hareketlerini izleyebilmekte; ifade alma, sorgu ve tutuklama işlemini bizzat yapmaktadır. Bunun sonucunda "*doğrudan doğruyalık-yüz yüzelik*" ve "*silahların eşitliği*" ilkelerinin uygulanması sağlanmış olmaktadır. Ayrıca istinabe ve naip hâkim uygulaması ile yok tutuklaması[12] işlemleri büyük oranda azalacaktır. Bu bağlamda özellikle yol tutuklamasından kaynaklanan mağduriyetler ortadan kalkmaktadır. Ceza infaz kurumlarında bulunan tutuklu ve hükümlülerin SEGBİS video konferans sistemi ile ceza infaz kurumundan duruşmalara katılmaları ve ifadelerinin alınmaları sağlanmaktadır.[13] Yol tutuklaması sonucu ortaya çıkan nakil masrafları da önemli ölçüde azalmaktadır.[14]

IV. SEGBİS Mevzuatı

5271 sayılı CMK'nın 52, 58, 147, 180, 196 ve 219. maddelerinde, SEGBİS yönteminin kullanılmasına izin verilmiş ve bazı durumlarda zorunlu kılınmıştır.[15] SEGBİS ile ilgili 20 Eylül 2011 tarih ve 28060 sayılı Resmi Gazetede yayınlanarak SEGBİS Yönetmeliği yürürlüğe konulmuştur. Adalet Bakanlığı Bilgi İşlem Dairesi Başkanlığı 14.12.2011 tarih ve 150 no' lu genelge[16] ile SEGBİS yönteminin kullanılmasını adli makamlara tavsiye etmiş ve nasıl kullanılacağına dair usul ve esasları belirlemiştir.

CMK 52 ve 58. maddelerinde tanık ifadelerinin alınmasında sesli ve görüntülü bilişim sisteminin (Videokenferans) kullanımı dü-

---

11 Ali Kaya ve Meral Güneş, Ulusal Yargı Ağı Projesi-I (Eskişehir: Anadolu Üniversitesi Yayınları, 2011), 4.

12 Yol tutuklaması, esas yetkili mahkemesi huzuruna getirilmek üzere sanığın başka bir yer hâkimi tarafından geçici olarak tutuklanmasıdır.

13 Halil Güner, "SEGBİS Sisteminin Ceza Evi Uygulamasının Adil Yargılanma Hakkı Yönünden Değerlendirilmesi," Terazi Hukuk Dergisi 9, no. 99 (Kasım 2014): 88.

14 Acar ve Gürsoy, "Türk Mahkemelerinde Sesli ve Görüntülü," 133.

15 Ali İhsan İpek, İfade Almanın Teknik ve Taktikleri (Ankara: Adalet Yayınevi, 2015), 106.

16 "Ses ve Görüntü Bilişim Sistemi (SEGBİS) Genelge No: 150," Adalet Bakanlığı, erişim tarihi 20 Ağustos 2017, www.adalet.gov.tr/genelgeler/genelge_pdf/segbis.pdf.

zenlenmiştir. CMK m.147, 196'da sanık ifadesinin alınmasında SEGBİS kullanımı, CMK 180. Maddesinde tanık ve bilirkişinin dinlenmesinde istinabe ve SEGBİS, CMK 219. Maddesinde ise duruşmada yapılan işlemlerin kayda alınması düzenlenmiştir.

V. Sanığın Duruşmada Hazır Bulunması

Yargılamanın yapıldığı yargı çevresi dışında tutulan sanık, iki şartla huzura getirilmeyebilir; öncelikle sorgusunun daha öncesinde yapılmış olması ve niteliği itibariyle hazır bulundurulmasına gerek görülmeyen bir celsede, sanığın huzura getirilmemesine karar verilebilecek olunmasıdır.[17] CMK m.196/5'e göre; *"Hastalık veya disiplin önlemi ya da zorunlu diğer nedenlerle, yargılamanın yapıldığı yargı çevresi dışındaki bir hastane veya tutukevine nakledilmiş olan sanığın, sorgusu yapılmış olmak koşuluyla, hazır bulundurulmasına gerek görülmeyen oturumlar için getirilmemesine mahkemece karar verilebilir".*

Bu hüküm, Yargıtay Ceza Genel Kurulu'nun 10.06.2008 tarihli, 2008/9-148 E. ve 2008/169 K. sayılı kararında şöyle yorumlanmaktadır; *"CMK m.196/5 hükmünün, 'sanık hazır bulunmayı açıkça istemedikçe' şeklinde yorumlanması gerekir".* İlgili kararda Ceza Genel Kurulu, davanın görüldüğü yer mahkemesinin yargı çevresi dışında başka bir suçtan cezası infaz edilmekte olan sanık hakkında hüküm vermiştir. Sanık, bu olayda duruşmada hazır bulunmak istediğini yazılı olarak mahkemeye iletmiştir. Sanığın duruşmada hazır edilip müdafii huzurunda bozmaya karşı diyecekleri sorulmadan direnme kararı verilmesini, savunma hakkının açıkça kısıtlanması olarak değerlendirmiştir. Bu nedenle hükmün bozulmasına karar vermiştir.[18]

---

[17] Feridun Yenisey ve Ayşe Nuhoğlu, Ceza Muhakemesi Hukuku (Ankara: Seçkin Yayıncılık, 2016), 741-744; Nur Centel ve Hamide Zafer, Ceza Muhakemesi Hukuku (İstanbul: Beta Basım Yayın, 2016), 712-716; Veli Özer Özbek, Ceza Muhakemesi Hukuku (Ankara: Seçkin Yayıncılık, 2016), 666.

[18] Ersan Şen, "Sanığın Mahkemeye Çıkma Hakkı," Haber7, erişim tarihi 5 Mart 2017, http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1830305-sanigin-mahkemeye-cikma-hakki.

Yargıtay 16. Ceza Dairesi, üç kararla[19] tartışma konusu netleştirilmiştir. Kararlarda özetle; sanık ve müdafii sesli ve görüntülü iletişim tekniğinin kullanılması suretiyle savunma yapılmasını istememişlerdir. Bu sistemin kullanılmasına muhalefet etmişlerdir. Sanık ve müdafii duruşmada hazır bulunmayı ısrarla talep etmişler; buna rağmen SEGBİS aracılığıyla sanık savunması alınmıştır. Sanık hakkında mahkûmiyet hükmü kurmuştur. Yargıtay bu kararlarında bu şartlar altında sanığın savunma hakkının kısıtlandığına karar vermiştir.

Bu kararlarda "sanık olmaksızın yargılama olmaz" ilkesi üç başlıkta açıklanmıştır. Bunlar;

1. Genel kural, sanığın duruşmada hazır bulundurulmasıdır. Bu hak, ancak somut ciddi nedenlere dayalı olarak mahkeme kararı ile sınırlandırılabilir.
2. İlk ve son savunmanın yapıldığı, esasa ilişkin delillerin toplandığı oturumlara, sanığın SEGBİS yolu ile katılması açık kabulüne dayalı olmalıdır.
3. Sesli ve görüntülü yöntemle savunma alınması hâlinde, talebi doğrultusunda sanığın yanında da müdafi bulunması olanağının sağlanması koşulları gerçekleştiğinde, savunma hakkının kısıtlanmadığı kabul edilebilecektir.

Bunların dışında; sanığın SEGBİS yoluyla ifadesinin alınabilmesi için, huzurda bulundurulmasının mümkün olmaması gerekmektedir.[20] Deyim yerinde ise SEGBİS, savunma hakları çerçevesinde sanığa tanınan "ikincil asgari hak" niteliğindedir. Yargıtay Ceza Genel Kurulu da Haziran 2017 tarihinde verdiği kararında 16. Ceza Dairesinin kararını benimsemiştir. Yargıtay daireleri arasında var olan içtihat farklılığı bu sayede ortadan kalkacaktır. Yukarıda zikredilen üç kriter artık daha geniş uygulama alanı bulacaktır.

---

[19] Yar. 16. CD, E.2015/1076, K.2015/1932 19.06.2015; Yar. 16. CD, E.2015/1078, K.2015/1930 19.06.2015; Yar. 16. CD, E.2015/1083, K.2015/1926 19.06.2015.

[20] Erşan Şen, "Uzakta Olan Sanığın Sorgusu," Haber7, erişim tarihi 19 Temmuz 2017, http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1875201-uzakta-olan-sanigin-sorgusu.

Yargıtay kararları ile de sabit olduğu üzere, esas olan kovuşturma aşamasında sanığın huzura gelmesi ve duruşma salonunda bulunmasıdır. Bu usul, "delillerin doğrudan doğruyalığı" ve "yüz yüzelik" ilkeleri ile de uyumludur. Sanığın, SEGBİS yöntemi ile duruşmalara uzaktan katılmasını gerektirecek haklı gerekçe veya delil söz konusu değilse duruşma salonuna bizzat getirilmesi gerekir. Sanık, yanında müdafii olmaksızın ve duruşma salonunda yüz yüzelik sağlanmaksızın sorguya alınmamalıdır. Kapalı cezaevi koşullarında tutulan sanığın, güvenlik veya ulaşım zorluğu gibi kabulü mümkün olmayan gerekçelerle mahkemeye getirilmemesi, savunma hakkının kısıtlanmasına ve adil yargılanma hakkının ihlal edilmesine yol açacaktır.[21]

VI. Avrupa İnsan Hakları Mahkemesi'nin Yaklaşımı

AİHM'in özellikle Marcello Viola–İtalya kararı[22] bu konuda kriterlerin ortaya konulduğu en önemli kararıdır. Başvurucu Marcello Viola, ceza yargılamasının ikinci setindeki, yani istinaf mahkemesinde yapılan yargılamada üç duruşmaya rızası olmaksızın video konferans yoluyla (işitsel ve görsel sistemler kullanılarak) katılarak, tutuklu bulunduğu hapishaneden duruşma salonuna getirilmemiştir. Başvurucu "usuli" sebeplere dayanarak (istinaf mahkemesinin kararına karşı) temyiz başvurusunda bulunmuştur. Yüksek Mahkeme (Yargıtay) başvurucunun temyiz talebini reddetmiştir.

Hükümetin görüşü; mevcut davada, dürüst yargılanma hakkı ile ilgili tüm koşulların sağlandığı, sanığın tutuklu bulunduğu yerde kalmasına izin veren gelişmiş bir teknik alet olan ve önemli gecikmelerin önüne geçen video konferans sisteminin sanığın duruşmalara etkili bir şekilde katılımını sağladığı yönündedir. Sanığın aynı tarihlerde farklı mahkemelerde davası görülmektedir. Hükümet; başvurucunun, yargılama süresine zarar vermeyecek şekilde yargılamaya katılımını sağlayacak en iyi sistemin sesli ve görüntülü bağlantı usulü olduğu kanaatindedir. Ayrıca sanık, duruşma salonunda

---

21 Güner, "Adil Yargılanma Hakkı Yönünden," 84-86.

22 AİHM Üçüncü Dairesi'nin 2004/45106 sayılı ve 05.10.2006 tarihli kararı.

bulunan müdafii dışarıdan bir üçüncü kişi tarafından herhangi bir dinleme teşebbüsüne karşı önlem alınmış bir telefon bağlantısı ile özel olarak danışabilme imkânına sahiptir. Müdafii, video konferans yapılan salona kendisinin yerine bir müdafii gönderebilir veya aksine kendisi müvekkilinin yanında bulunarak duruşma salonunda savunma yapması için kendisi tarafından görevlendirilen bir müdafii de gönderebilmektedir.

Somut davada İHAM; başvurucunun, müdafii ile üçüncü kişiler tarafından dinlenilmeden görüşme hakkının ihlal edilmediğini tespit etmiştir. Zira başvurucunun, duruşma salonunda bulunan müdafiine dışarıdan bir üçüncü kişi tarafından herhangi bir dinleme teşebbüsüne karşı önlem alınan telefon bağlantısı ile özel olarak danışabilme imkânına sahiptir. Başvurucu müdafiinin, müvekkilinin bulunduğu yerde hazır olma ve onunla mahremiyet içerisinde görüşme hakkının bulunduğunu kabul ederek İHAS m.6'nın ihlal edilmediğine karar vermiştir.[23]

Marcello Viola - İtalya kararının, SEGBİS usulünün tatbik edildiği yargılamalarda emsal teşkil edebilmesi için; yargılama makamının SEGBİS usulünün kullanımına ilişkin kararının, öncelikle İHAS m.6 ile korunan dürüst yargılanma hakkına ilişkin usuli güvencelerin özünü ortadan kaldırmaması ve sanığın savunma hakkına orantısız müdahale içermemesi gerekmektedir. Bir başka anlatımla; Marcello Viola kararı veya emsal gösterilecek herhangi bir karar, bireyin mahkemede hazır bulunma hakkını bertaraf edecek şekilde her celse için uygulanabilecek bir yol olarak algılanmamalıdır.[24]

---

[23] Cankat Taşkın, "Müdafinin Ve Vekilin Hukuki Yardımı, Sınırları İle Uygulamada Karşılaşılan Sorunların Aihm İçtihatları Işığında Değerlendirilmesi," Türkiye Barolar Birliği Dergisi, no. 69 (Mart-Nisan 2007): 211-241.

[24] Şen, "Sanığın Mahkemeye Çıkma Hakkı."

VII. Marcelo Viola-İtalya Kararında İhlale Hükmedilmemesinin Nedenleri

1. İtalyan Ceza Muhakemesi Kanununda Var Olan Usuli Güvenceler:

   a) Videokonferans (SEGBİS) uygulamasına, ancak sanığın duruşmaya getirilmesinin kamu düzeni ve güvenliği açısından ciddi problemler oluşturuyor ve zorunluluk arz ediyorsa başvurulabilir. Türkiye'de, daha çok kamu güvenliği veya düzeni değil, sevklerin masraflı olması veya ceza infaz kurumlarının dolu olması gerekçesiyle yapılmaktadır.

   b) Bu yöntem, kargaşa ve suçun önlenmesi, mağdurların ve tanıkların yaşam, özgürlük, güvenlik haklarının korunması ve adli işlemlerde makul süre gerekliliklerine uyulması hususları sebebiyle kullanılabilir. Bu da ancak çok hızlı gelişen durumlarda, örneğin yakalama infazlarında bunu meşru kılmaktadır.

   c) Bu yönteme başvurulması, sanığın farklı mahkemelerde duruşmasının veya başka işlemlerinin bulunması sebebiyle gecikmeyi önleyecekse başvurulabilir. Özellikle bulunduğu yerdeki mahkemede de yakın tarihte duruşmasının olması hâlinde bu yöntem meşru hâl almaktadır.

   d) Bu yönteme başvurulması hâkim kararına bağlıdır ve bunun taraflara ve müdafiine 10 gün önceden bildirilmesi gerekir. CMK m.196'daki istinabe yasağı SEGBİS yasağı anlamına da gelmektedir. Her somut olayda hâkime takdir yetkisi vermek gerekir. Ancak uygulamada bu yol zaten zorlanmaktadır. Mevzuat ile kuralları koymak gerekir.

   e) Videokonferans yöntemi uygulanırken duruşma salonu ile sanığın bulunduğu yerdeki herkes, herkesi görebilecek durumda olmalıdır. Duruşmalarda sıklıkla teknik sorunların yaşandığı gözlenmektedir.

f) Sanık müdafii, her zaman sanığın yanında hazır bulunmalıdır.

g) Müdafii, sanığın yanında yer almıyor, duruşma salonunda bulunuyorsa sanık ile müdafi arasında gerekli teknik vasıtalarla özel ve gizli konuşmayı sağlayacak iletişim hattı bulunmalıdır. Bu hukuki yardım sağlanması bakımından vazgeçilemez bir haktır. Ancak şu anda bunu sağlayan mahkeme sayısı çok azdır. Bu iletişimin, denetlenmeden sağlandığının güvenceye alınması gerekir.[25]

h) Sanığın bulunduğu yer duruşma salonunun uzantısı sayılacak şekilde düşünülmelidir; teknik olarak aksamaların bulunmaması ve anlık iletişimin sağlanması gerekir. Uzaktan katılım kararı verildiğinde, duruşmanın yapılacağı mahkeme salonu ile tutuklunun bulunduğu yer arasında görsel ve işitsel bir bağlantı kurularak iki mekânda da hazır bulunan kişilerin birbirlerini eş zamanlı ve net olarak görmeleri ve söylenenleri duymaları sağlanacaktır. Farklı davalılar da farklı mekânlarda birbirlerini görebilecektir.

i) Sanığın kimliğini tespit açısından, mutlaka bir mahkeme yetkilisinin sanığın yanında bulunması sağlanır. Hâkime yardım ile görevli bir mahkeme yetkilisi sanığın yanında bulunarak sanığın kimliği, hak ve yetkilerini kullanmakta hiçbir şekilde kısıtlamaya maruz kalmadığını tasdik edecektir. SEGBİS yönetmeliğinde infaz kurumu görevlisine bu yetkinin verilmiş olması yeterli değildir.

2. İtalya Anayasa Mahkemesi, Videokonferans uygulamasını Anayasaya aykırı bulmamıştır.

3. CİKAYAS (Cezai Konularda Adli Yardımlaşma Avrupa Sözleşmesi) m.9-11 bu yönteme belli şartlarda izin vermektedir.

---

[25] Gizem Dursun, "Sanığın Duruşmada Hazır Bulunma Hakkı ve Bu Kapsamda Sesli ve Görüntülü Bilişim Sisteminin (SEGBİS) Değerlendirilmesi," Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi 11, no. 143-144 (Temmuz-Ağustos 2016): 127-157.

4. Temyiz (Somut olayda istinaf) aşamasında delillerin tartışılması söz konusu olmadığından bu yöntemin yargılamaya etkisi sınırlı kalmaktadır.

VIII. Anayasa Mahkemesi'nin Yaklaşımı

Erdal Korkmaz ve Diğerleri Kararı,[26] bu konuda Anayasa Mahkemesi'nin değerlendirme yaptığı önemli bir karardır. Başvurucular, devlet memuru olmakla birlikte Kamu Emekçileri Sendikasına (KESK) bağlı Eğitim ve Bilim Emekçileri (Eğitim-Sen) üyesidirler. İstanbul Cumhuriyet Başsavcılığı, başvurucularla ilgili olarak *DHKP-C silahlı terör örgütüne üye olma* nedeniyle soruşturma başlatmıştır. DHKP-C'nin silahlı bir terör örgütü olup BM Güvenlik Konseyi, AB (2002), ABD (1997), Almanya (1998), İngiltere Birleşik Krallığı (2001) nezdinde terör örgütleri listesinde yer almış olması nedeniyle başvurucular hakkında tutuklama kararı alınmıştır. Başvuruculaların tutukluluk süreci içerisinde yapmış oldukları tüm itirazlar reddedilmiştir. SEGBİS usulüyle tutukluluk incelemesi yapılmış ve müdafilerin hazır bulundurulması ve dinlenilmesi talebi de CMK m. 108/1; *şüpheli veya müdafii* dinlenilmesini öngördüğü için reddedilmiştir.

Bu karara da itiraz üzerine, İstanbul 1 No'lu Hâkimliğine göre;

SEGBİS'in beyan almada yeterli bir sistem olup şüphelilerin iradeleriyle beyanda bulunmamış olmaları tutukluluk hâlinin devamına karar vermede bir engel olarak değerlendirilmemiştir. Yasal mevzuat açısından tutukluluk incelemesinin duruşmalı olarak yapılması zorunlu değildir. Taraflar itiraz ve taleplerini her zaman dosyaya sunabileceklerdir. SEGBİS ile cezaevine bağlanarak gerekli ortam ve imkânın sağlandığı belirtilmektedir.

Başvurucu iddialarından biri; tutukluluk incelemelerinin duruşmalı olması istenmesine karşın SEGBİS usulüyle yapılması Anayasa m.36'da düzenlenen adil yargılanma hakkının ihlalidir.

---

[26] AYM, B.2013/2653, 18.11.2015.

Anayasa Mahkemesi değerlendirmesinde; AY m.19/8 kapsamında tutukluluğa yapılan her itirazda başvurucunun dinlenilmesinin gerekli olmadığını yalnızca tutukluluğun gözden geçirilmesinde "çelişmeli yargı" ve "silahların eşitliği" ilkelerine riayet edilmesi noktasındaki hassasiyetlerini *Firas Aslan ve Hebat Aslan kararı*nı atıf yaparak belirtmiştir. SEGBİS' in ifade alma ve sorgu işlemlerinde ve duruşmalarda, Cumhuriyet başsavcılığı veya mahkemenin yargı çevresi dışında bulunan veya mahkemede hazır bulunmayan kişilerin (şüpheli, tanık, şikâyetçi) video konferans yoluyla dinlenilmesini ve ifadelerin kayda alınmasını sağlayan bir imkân olduğu üzerinde durulmuştur.

Bu kayıtların daha sonra yazılı olarak tutanağa dönüştürüldüğü de sistemin güvencesi olarak ifade edilmiştir. Mahkeme yine *Aslan kararı*na atıf yaparak tutukluluğun incelenmesinin ve tahliye talebi değerlendirmesinin SEGBİS vasıtasıyla yapılmasını ve başvuruculara o anda herhangi bir beyanda bulunmayışını hatta Cumhuriyet savcısının da sözlü beyanda bulunmak üzere mahkemeye çağrılmamış olmasını "silahların eşitliği" ilkesine aykırı bulmamıştır.[27] CMK m.147/1-h uyarınca, SEGBİS' in kullanılmasının emredici hükme bağlandığı da belirtilerek bu sistemin *yüz yüzelik ilkesi*ni sağladığı avantajı vurgulanmaktadır.

Buna gerekçe olarak AY m.19/8 gereğince tutuklama ile ilgili kısa sürede karar verilmesinin gerekliliği fakat her incelemede de duruşma yapılmasının ceza yargılamasını sistemini sekteye uğratacağını vurgulamaktadır. SEGBİS vasıtasıyla yapılan incelemede, makul sürede değerlendirme maksadı taşındığı da yine bu çerçevede hem güvenlik hem de kişi haklarının ihlaline engel olması bakımından önem arz ettiği de belirtilmiştir. Mevcut davada duruşma yapılmasını gerektirecek özel bir durum olmadığı da yine belirtilmektedir. Son olarak Mahkeme, *AİHM Marcello Viola/İtalya 2007* kararına atıf yaparak, sanıkların duruşmaya video konferans yöntemiyle katılımının sağlanmasını, savunmanın diğer taraflara nazaran ciddi bir şekilde dezavantajlı bir konuma düşürülmediği durumlarda -

[27] Şen, "Sanığın Mahkemeye Çıkma Hakkı."

bilhassa burada karşı tarafın pozisyonu üzerinde durulmaktadır-sanığın mahkemede hazır bulunma şartının gerçekleşmiş sayılacağını belirtmektedir. SEGBİS vasıtasıyla yapılan tutukluluk incelemelerinde, başvuruculara tutukluluk hâlleriyle ilgili itirazlarını dile getirme, Mahkeme önünde sözlü savunma yapma fırsatının verilmiş olması, herhangi bir hak ihlalinin olmadığının tespiti vurgulanmaktadır. Aynı zamanda başvuruculaların itirazlarının dosya üzerinden vaktinde incelenmiş olması nedeniyle de makul aralıklarla dinlenme noktasında bir ihlal görülmemektedir. Anayasa Mahkemesi'nin bu değerlendirmelerine, AİHM'nin Marcelo Viola-İtalya Kararındaki kriterler sebebiyle katılmamız mümkün değildir.

IX. Sonuç

Ülkemizde tatbik edilen SEGBİS usulünün; teknik aksaklıklar (elektrik kesintileri veya sistem arızaları) sebebiyle sistemin kullanımını zorlaştırdığı, duruşma salonu ile tutuklunun bulunduğu yer arasında ses ve görüntü bağlantısının kopukluğu, ses iletiminde yaşanan zorluklar bilinmektedir. Özellikle sanık beyanlarının mahkeme heyeti, sanık müdafii, tanıklar, diğer sanıklar ve hatta duruşma tutanağını düzenleyen kâtip tarafından bazı zamanlarda anlaşılamaz hâl aldığı görülmektedir. Beyanların "ilk ağızdan" değil, SEGBİS olarak adlandırılan sistemden mahkemeye yansıdığı kadarıyla "dolaylı" yollarla duyulması, sanığın somut olayı anlatırken sergilediği mimiklerinin doğrudan görülememesi gibi gerekçelerle, yargılamanın sıhhatini, saygınlığını ve dürüstlüğünü azalttığı bir gerçektir.

Sanığın savunma hakkını kısıtlayan bu usulün, salt teknik aksaklıklar sebebiyle değil, hakkın özünü zedeleyen hatalı uygulamalar sebebiyle de dürüst yargılanma hakkını ihlal etmektedir. Yalnızca somut gerekçelerle ve "istisnai" olarak başvurulabilen SEGBİS usulünün, uygulamada "zorunlu" addedildiği görülmektedir. SEGBİS odasında bekleyen tutuklu sanığın yanında isteğe bağlı veya zorunlu olarak müdafii (zorunlu müdafi sıfatıyla) bulundurulmamaktadır. Tutuklu sanığın, mahkemede hazır bulunan müdafii ile üçüncü kişilerin duyamayacağı şekilde görüşebileceği, göz tema-

sı kurup etkili hukuki yardım alabileceği herhangi bir sesli veya görüntülü iletişim ağı yoktur.

SEGBİS odasında bekletilen tutuklu sanıklar, yaşanan teknik aksaklıklar sebebiyle duruşmayı kaldığı yerden takip edememektedir. Cezaevi personelinin SEGBİS sistemi konusunda yeterli teknik bilgi ve hâkimiyeti bulunmamaktadır. Bağlantı kopuklukları eş zamanlı olarak giderilmemektedir. Bu nedenlerle sık sık celse arası verildiği gibi duruşmanın başka tarihlere ertelenmesi de söz konusu olmaktadır. Söz konusu koşullarda yaşanan mağduriyetin önlenememesi, teknik aksaklık sırasında sistemi yeniden kurabilecek donanıma sahip personellerin yetersiz olması gibi esasında hakkın kullanımına etki ve katkısı tartışılmaz olan bu eksikliklerin giderilmesi ve "SEGBİS" sisteminin yenilenmesi gerekmektedir.

Özellikle son dönemde SEGBİS Yönetmeliğinde değişiklik yapılarak usuli güvenceler getirilmesi gündemdedir. Bu maksatla SEGBİS Yönetmeliği üzerinde çalışılmaktadır. Marcelo Viola-İtalya Kararında zikredilen İtalya Ceza Muhakemesi Kanunu'nda yer alan usuli güvencelerin sağlanarak SEGBİS yönteminin bu şartlar altında etkin kullanılması gerekmektedir.

KAYNAKÇA

Acar, Sami ve Hülya Gürsoy. "Türk Mahkemelerinde Sesli ve Görüntülü Kayıt ve Videokonferans Sistemi Uygulamasına Geçiş, Ceza Mahkemeleri Örneği." Ankara Barosu Dergisi 70, no. 4 (2012): 109-137.

Açıkmeşe, Turan ve Ulvi Karaşahin. "Sesli Görüntülü Bilişim Sistemi (SEGBİS)." UYAP Bilişim Dergisi, no. 5 (2012): 25-35.

Adalet Bakanlığı. "Ses ve Görüntü Bilişim Sistemi (SEGBİS) Genelge No: 150." Erişim tarihi 20 Ağustos 2017. www.adalet.gov.tr/genelgeler/genelge_pdf/segbis.pdf.

Centel, Nur ve Hamide Zafer. Ceza Muhakemesi Hukuku. İstanbul: Beta Basım Yayın, 2016.

Dursun, Gizem. "Sanığın Duruşmada Hazır Bulunma Hakkı ve Bu Kapsamda Sesli ve Görüntülü Bilişim Sisteminin (SEGBİS) Değerlendirilmesi." Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi 11, no. 143-144 (Temmuz-Ağustos 2016): 127-157.

Gözel, Arif. "Yargılamada Ses ve Görüntü Bilişim Sistemi (SEGBİS) Kullanımı." Academia. Erişim tarihi 21 Ağustos 2017. https://www.academia.edu/12580753/Yarg%C4%B1lamada_Ses_ve_G%C3%B6r%C3%BCnt%C3%BC_Bili%C5%9Fim_Sistemi_SEGB%C4%B0S_Kullan%C4%B1m%C4%B1.

Güner, Halil. "SEGBİS Sisteminin Ceza Evi Uygulamasının Adil Yargılanma Hakkı Yönünden Değerlendirilmesi." Terazi Hukuk Dergisi 9, no. 99 (Kasım 2014): 84-86.

İpek, Ali İhsan. İfade Almanın Teknik ve Taktikleri. Ankara: Adalet Yayınevi, 2015.

Kaya, Ali ve Meral Güneş. Ulusal Yargı Ağı Projesi-I. Eskişehir: Anadolu Üniversitesi Yayınları, 2011.

Mevzuat Bilgi Sistemi, "Ceza Muhakemesinde Ses Ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik." Erişim tarihi 21 Ağustos 2017. http://www.mevzuat.gov.tr/Metin.Aspx?MevzuatKod=7.5.15315&sourceXmlSearch=&MevzuatIliski=0.

Özbek, Veli Özer, Koray Doğan, Pınar Bacaksiz, ve İlker Tepe. Ceza Muhakemesi Hukuku. Ankara: Seçkin Yayıncılık, 2016.

Şen, Ersan. "Sanığın Mahkemeye Çıkma Hakkı." Haber7. Erişim tarihi 5 Mart 2017. http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1830305-sanigin-mahkemeye-cikma-hakki.

Şen, Ersan. "Uzakta Olan Sanığın Sorgusu." Haber7. Erişim tarihi 19 Temmuz 2017. http://www.haber7.com/yazarlar/prof-dr-ersan-sen/1875201-uzakta-olan-sanigin-sorgusu.

Taşkın, Cankat. "Müdafinin Ve Vekilin Hukuki Yardımı, Sınırları İle Uygulamada Karşılaşılan Sorunların Aihm İçtihatları Işığında Değerlendirilmesi." Türkiye Barolar Birliği Dergisi, no. 69 (Mart-Nisan 2007): 211-241.

Yazar, Bilgin. Görüntülü İletişim–Video Konferans Teknolojilerinin Kullanım Alanları. Etgi Grup, 2016. https://www.etgigrup.com/wp-content/uploads/2016/04/video_konferans_ab_2013-1.pdf.

Yenisey, Feridun ve Ayşe Nuhoğlu. Ceza Muhakemesi Hukuku. Ankara: Seçkin Yayıncılık, 2016.

Düzeltme

Erratum

Bilişim Hukuku Dergisi Cilt:1 – Sayı: 1'de 113. sayfada yazar Cemre Çise KADIOĞLU'na ait ORCID numarasında 1 rakam sehven yanlış yazılmıştır. Yazara ait ORCID numarası: 0000-0002-9573-727X.