BİLİŞİM HUKUKU DERGİSİ

DIGITAL LAW REVIEW

Cilt: 4 Sayı: 1 | Vol: 4 Issue: 1 | 2022

BİLİŞİM HUKUKU DERGİSİ

DIGITAL LAW REVIEW

Cilt: 4 **Sayı**: 1 **Haziran 2022**

Vol.: 4 Issue: 1 **June 2022**

ASBÜ Yayınevi

Ankara 2022

BİLİŞİM HUKUKU DERGİSİ
DIGITAL LAW REVIEW

e-ISSN: 2667-6109
Cilt: 4 **Sayı**: 1 **Vol**.: 4 Issue: 1
Haziran 2022 **June 2022**

Dergi İletişim Bilgileri/Review Contact Information:
ASBÜ Hukuk Fakültesi Dekanlığı
Hükümet Meydanı No: 2, 06030 Ulus, Altındağ, ANKARA
Tel: +90 312 596 44 44–45 **Fax**: +90 312 311 86 00
E-mail: bilisimhukukudergisi@asbu.edu.tr
https://dergipark.org.tr/bilisimhukukudergisi

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

Baskı: Dijital Yayın
Sertifika No: 33365
Tel: 596 46 12

Prof. Dr. Cemil KAYA	İstanbul Üniversitesi Hukuk Fakültesi
Prof. Dr. Leyla KESER BERBER	İstanbul Bilgi Üniversitesi Hukuk Fakültesi
Prof. Dr. Yücel OĞURLU	İstanbul Ticaret Üniversitesi Hukuk Fakültesi
Prof. Dr. Erdal YERDELEN	Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi
Doç. Dr. Gülsün Ayhan AYGÖRMEZ UĞURLUBAY	İstanbul Gedik Üniversitesi Hukuk Fakültesi
Doç. Dr. Armağan Ebru BOZKURT YÜKSEL	Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi
Doç. Dr. Barış ERMAN	Yeditepe Üniversitesi Hukuk Fakültesi
Doç. Dr. Hasan SINAR	Altınbaş Üniversitesi Hukuk Fakültesi
Dr. Öğr. Üyesi Erman BENLİ	Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi
Dr. Öğr. Üyesi Fatih KAPLANHAN	İstanbul Sabahattin Zaim Üniversitesi İşletme ve Yönetim Bilimleri Fakültesi
Dr. Öğr. Üyesi Mehmet Bedii KAYA	İstanbul Bilgi Üniversitesi Hukuk Fakültesi
Dr. Ahmet KILIÇ	Bilgi Teknolojileri ve İletişim Kurumu
Dr. Mustafa KÜÇÜKALİ	Bilgi Teknolojileri ve İletişim Kurumu
Dr. Yuhanif YUSOF	Universiti Utara Malaysia School of Law

YAZIM KURALLARI

Başlangıç

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

Metin

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

Dipnotlar

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

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

Kaynakça

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

Yazım-İmla Kuralları ve Atıf Usulü

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

3. Eserin yayın dilinin Türkçe olması halinde atıf yapılırken;

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

◊ Mahkemenin/kurumun adı varsa dairesi, E. esas numarası K. karar numarası tarih [gün.ay.yıl formatında], (kararın ulaşıldığı kaynak, varsa ulaşıldığı kaynaktaki sayfa numarası veya URL veya DOI numarası).
◊ Yabancı kararlarda ilgili mahkemenin veya kurumun kendisinin benimsemiş olduğu karar atıf usulü kullanılabilir. Tercih edilirse Türk kararları için kullanılan sistem de uygun düştüğü ölçüde uygulanabilir. Ancak, bir eserde aynı mahkemenin veya kurumun bir kararı için hangi sistematik kullanılmışsa diğer kararlarında aynı sistematiğin kullanılması gerekir.

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

Örnekler:

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

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

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

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

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

WRITING FORMAT

Beginning

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

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

Bibliography

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

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

Spelling and Footnotes

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

İÇİNDEKİLER/CONTENTS

Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.1114305**

SOSYAL MEDYAYA YÖNELİK YENİ DÜZENLEMELERİN HUKUKEN DEĞERLENDİRİLMESİ

The Legal Analysis of New "Social Media Law"

Merve Ayşegül KULULAR İBRAHİM*

Öz

Bireylerin içerik oluşturup paylaşıp yorumlayabildikleri online platformlara ilgi artmıştır. Twitter, YouTube, Facebook, bloglar, forumlar gibi platformlar üzerinden kişilerin, bizzat kendilerince paylaştıkları içerikler gerek kendi kişilik haklarına gerek başkalarının kişilik haklarına zarar verici nitelikte olabilmektedir. Örneğin sosyal medya platformlarında yapılan paylaşımlar bireyler üzerinde sonradan telafisi mümkün olmayan zararlara neden olabilmekte, kamu düzenini ihlal ederek kişileri suça teşvik edebilmektedir. Sosyal medyaya yönelik yapılan düzenlemeler, sosyal medya üzerinden işlenen suçlar karşısında veya sosyal medyada gerçekleşen hak ihlallerini engellemede yeterli olamamıştır. Bu yetersizlik; teknik

* Dr Öğr Üyesi, Ankara Sosyal Bilimler Üniversitesi, Hukuk Fakültesi, Bilişim ve Teknoloji Hukuku Abd. Bşk. aysegul.kulular@asbu.edu.tr, ORCID ID: 0000-0001-6556-0269.

Bu çalışma, 10-13 Şubat 2022 Hukukun Güncel Meseleleri Erzincan Sempozyumu'nda *Yeni Sosyal Medya Düzenlemelerinin Hukuken Değerlendirilmesi* şeklinde sözlü olarak sunulmuştur

Makale Gönderim Tarihi/Received: 09.05.2022.

Makale Kabul Tarihi/Accepted: 23.06.2022.

Atıf/Citation: Kulular İbrahim, Merve Ayşegül. "Sosyal Medyaya Yönelik Yeni Düzenlemelerin Hukuken Değerlendirilmesi" *Bilişim Hukuku Dergisi* 4, no. 1 (2022): 1- 32.

imkansızlıklar, hukuk kuralarının ülke hudutları ile sınırlı olmasına karşın internetin ülke hudutlarını aşan yapısı, hukuka aykırılıkların gerçekleştiği sosyal medya platformlarının ticari menfaatlerini önemseyerek ihlalleri giderme konusunda isteksiz davranmaları, mevcut düzenlemelerin bilgi teknolojilerindeki hızlı ilerlemelerin gerisinde kalması gibi nedenlerden kaynaklanmıştır. Bu nedenle Almanya başta olmak üzere Avrupa Birliği üyesi ülkelerde ve ülkemizde sosyal medya platformlarında hukuka aykırılıkları giderici iyileştirme çalışmaları gündeme gelmiştir. Bu kapsamda sosyal medya platformlarının sorumluluklarının artırılmasına ilişkin olarak ülkemizde 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da değişiklik yapılmıştır. Yapılan değişiklikler sosyal ağ sağlayıcılarının temsilci ataması, uyarı yöntemi ile içeriğin yayından çıkarılması başvurusu, verilerin Türkiye'deki sunucularda saklanması şeklinde sosyal ağ platformlarının hukuka aykırı içerikler karşısında sorumluluk ve yükümlülüklerinin belirlenmesine yöneliktir. Yeni düzenlemelerin sosyal medya platformları üzerindeki etkisi zamanla kendini gösterecektir. Sosyal medya şirketlerinin hukuka aykırılıkları önlememesi halinde yeni yaptırımların öngörülmesi ya da mevcut yaptırımların ağırlaştırılması gerekecektir.

Anahtar Kelimeler: Sosyal Medya, Bilişim Hukuku, İnternet Hukuku, Sosyal Ağ, Facebook.

Abstract

Interest in online platforms where individuals can create, and share content or comment on content has increased. Content shared by individuals on platforms such as Twitter, YouTube, Facebook, blogs, or forums might infringe both their own and others' personal rights. For example, posts made on social media platforms may cause irreparable harm to individuals, and may encourage people to commit crimes by violating public order. Regulations made for social media have not been sufficient to

prevent infringement on private rights or crimes committed through social media. Technical impossibilities, blurred borders, social media platforms' focus on their commercial interests and their ignorance on infringements, lagging of law behind technological innovations are some of reasons of insufficient protection. To eliminate illegality in social media platforms many countries including Turkey and European Union, in particular Germany, started arguments on amendments to the social media law. In this context, amendments in Turkish Law on Publications on the Internet and Suppression of Crimes Committed by Means of such Publications, No. 5651, several amendments were made to increase the responsibilities of social networking platforms, such as the appointment of representatives for social network providers, application for the removal of content by warning method, and the storring data servers in Turkey. The impact of the new amendments on social media platforms will be revealed as time progresses. If social media companies do not wish to comply with new regulations to prevent unlawful contents, new sanctions should be envisaged or existing sanctions should be aggravated.

Keywords: Social Media, Cyberspace Law, Internet Law, Social Network, Facebook.

GİRİŞ

İnternet altyapısının her türlü yerleşim birimine ulaştırılarak insanların online ortama teşviki sonrasında özellikle bireylerin kendilerinin içerik oluşturup paylaşıp yorumlayabildikleri ağlara ilgi artmıştır. Twitter, YouTube, Facebook, Skype, Tiktok ya da bloglar, forumlar gibi platformlar, kullanıcıların kişisel intikamları için kullandıkları ya da çeşitli otoritelerin gerek ticari çıkarları için gerekse siyasi çıkarları için toplumları yalan haber ya da farklı bilişim yöntemleriyle kendi istekleri doğrultusunda yönlendirme amacıyla kullandıkları ortamlara dönüşmüştür. Sosyal medya sosyal bir medya ağı olmaktan ziyade hukuka aykırı içeriklerin özgürce paylaşılarak kişilik haklarının ihlal edildiği, toplumda kin, nefret ve

ayrımcılığın perçinlendiği, başka devletlerin ulus devletlerin içişlerine karıştığı bir mecra haline gelmiştir. Bu şekilde hukuka aykırılık ağında hukuka aykırı eylem ve söylemleri gerçekleştiren kişilerin kimlik tespitinin zorluğu, teknik nedenlerden dolayı hukuka aykırılıkların giderilememesi, hudutsal nedenlerden dolayı mahkeme kararlarının uygulanamaması, internetin sunduğu kolaylık sonucu hukuka aykırı içeriklerin saniyeler içinde milyonların erişimine sunulabilmesi gibi sorunlar mevcut düzenlemelerin hukuka aykırılıkların giderilmesinde etkili olamadığını göstermiştir. Bu nedenle Almanya, İngiltere, Avustralya, Yeni Zelanda gibi yabancı ülkelerde ve ülkemiz Türkiye'de hukuka aykırılıkları giderebilecek teknik yeterliğe sahip olan sosyal medya şirketlerinin sorumluluklarının artırılmasına ilişkin düzenlemeler yapılmıştır.

Bu makalede öncelikle sosyal medyaya yönelik iyileştirici düzenlemeye duyulan ihtiyaç açıklanmış ve yurt dışı örnekleri belirtilmiştir. Ardından sosyal medya ile sosyal ağ platformları tanımlanmış ve Tortuk davası üzerinden iyileştirici düzenlemeler öncesinde sosyal medyada gerçekleşen ihlallerinin neden olabileceği zararlara dikkat çekilmiştir. Sosyal ağ platformlarının sorumluluklarının artırılmasına yönelik 5651 sayılı Kanun'da yapılan iyileştirmeler sosyal ağ sağlayıcılarının temsilci ataması, uyarı yöntemi ile içeriğin yayından çıkarılması başvurusu, verilerin Türkiye'deki sunucularda saklanması şeklinde ayrı başlıklar altında analiz edilmiştir. Bu çalışma ile yeni düzenlemelerin sosyal medya platformları üzerinden gerçekleşen ihlalleri önlemeye yönelik etkisinin incelenmesi amaçlanmıştır.

I. SOSYAL MEDYANIN DÜZENLEMESİNDE İYİLEŞTİRME ÖRNEKLERİ

Sosyal medya çeşitli hukuka aykırı uygulamalara konu olması nedeniyle düzenlenmesi gereken önemli bir alan olarak gündeme gelmiştir. Türkiye'de 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla

İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da, Almanya'da ise Telemediengesetz (Telemedya Kanunu)'nda sosyal medyaya yönelik düzenlemelere yer verilmiştir. Fakat bu düzenlemeler sosyal medyada hukuka aykırı uygulamaların engellenmesinde etkili ve yeterli olamamıştır. Yayınlanan hukuka aykırı içeriklerle ilgili olarak yeterli şekilde erişim engelleme gerçekleşmemiştir.[1] Sosyal medyada; kişisel verilerin hukuka aykırı işlenmesi, özel hayatın gizliliğinin ihlal edilmesi, iftira, hakaret gibi suçların işlenmesi, onur kırıcı şeref ve saygınlığı incitici eylemlerde bulunulması[2] gibi kamu düzeninin bozulmasına yönelik olarak suça teşvik gibi ihlaller yaşanmaya devam etmektedir. İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da Değişiklik Yapılmasına Dair Kanun'un gerekçesinde belirtildiği üzere sosyal ağ sağlayıcıları, hukuki düzenlemelere direnç göstererek önleyici ve koruyucu mekanizmaları geliştirmemekte yahut bu tür mekanizmaları etkin kullanmamaya devam etmektedir. İnsanlar özellikle takma isim (nick name) lerle yahut gerçek olmayan kompleks profiller oluşturarak internet üzerindeki bir çok ortamda duygu ve düşüncelerini anonim şekilde paylaşabilmektedir.[3] Sonuç olarak sosyal medya; sahte isimlerle hukuka aykırı içerikleri geniş

---

1 Bülent Kent, "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu," *Bilişim Hukuku Dergisi (BHD)* 2, no. 1 (2020) : 9.

2 Filiz Akar, "Okula Yansıyan Siber Zorbalık: İdari ve Hukuki Önleme Yolları,"içinde *Prof. Dr. Emine Akyüz'e Armağan - Akademisyenlikte 50 Yıl, Çocuk Hakları, Eğitim Hukuku, Vatandaşlık Eğitimi*, düzenleyen: Yasemin Karaman Kepenekci ve Pelin Taşkın (Ankara: Pegem Akademi, 2018), 472, 473.

3 Zakir Avşar ve Gürsel Öngören, *Bilişim Hukuku*, (İstanbul: Türkiye Bankalar Birliği, 2010), 13. Shuzhe Yang, Anabel Quan-Haase, Andrew D Nevin, ve Yimin Chen, "The Role of Online Reputation Management, Trolling, and Personality Traits in the Crafting of the Virtual Self on Social Media," içinde *Social Media Research Methods*, düzenleyen: Luke Sloan ve Anabel Quan-Haase, (London: SAGE, 2017), 76.

kitlelere ulaştıran, fikri mülkiyet haklarının kolayca ihlal edilerek haksız kazanç elde edilen, karşıt siyasi görüşteki kişilere, eski eş veya sevgiliye, rakip şirketlere, bunların ürün ve hizmetlerine, memuriyeti değiştirilenlerce müdürlerine, derslerinde zorlanan öğrencilerce veya akademisyenlere karşı kişilik haklarını ihlal eden içerikler paylaşılarak şahsi hesaplaşma aracı olarak kullanılan bir ortam haline gelmiştir. Bu tür hukuka aykırılıklara ortam sağlayan sosyal medya düzenlenmesi gerekli bir alandır.[4] Sosyal medyada kişilik hakkı ihlalleri, haksız rekabet, iftira, tehdit veya hakaret gibi suç oluşturan eylemler devam etmektedir.[5] Sosyal medya, kişilerin özel alanlarını kontrol edemedikleri bir ortam haline gelmiştir[6]. İnternetin devlet egemenliklerini aşan, ülke sınırlarını ortadan kaldıran etkisi nedeniyle sosyal medyadaki hukuka aykırılıklara ilişkin ulusal mahkeme kararlarının uygulanabilirliği sınırlı kalmaktadır. Mahkeme kararı ile erişimin engellenmesi gereken içeriklere yalnızca Türkiye'den erişim engellenmektedir. Bu durum, Türkiye'deki kullanıcıların bu hesaba erişimini ortadan kaldırmamaktadır. Zira VPN kullanılarak yahut ayna siteler (mirror sites) veya vekil sunucular (proxy servers) üzerinden Türkiye tarafından erişime engelleme kararı verilen ve

---

[4] John Woodhouse, *Commons Library Briefing, Social Media Regulation* (London: Pexels Licence, 2020), 3.; Mine Kaya, "*Elektronik Ortamda Kişilik Hakkı İhlalleri ve Korunması"* (Doktora tezi, Ankara Üniversitesi, 2015), 170.

[5] Cesim Parlak. "*Yeni Sosyal Medya Düzenlemesi."* 23 Temmuz 2020, 2, https://www.hukukihaber.net/yeni-sosyal-medya-duzenlemesi-makale,8114.html; Güney Nair ve Emine Balta, "Bilgi İletişim Teknolojileri Kullanımında sınırları Aşan Bir Sosyal Sorun Alanı Olarak Unutulma Hakkı," *Cumhuriyet Üniversitesi Sosyal Bilimler Dergisi* 41, no. 2 (2017): 117.

[6] Kişilerin kişiliklerini geliştirebilmeleri için gereken özel alanları üzerindeki hâkimiyetini kaybettiği bir ortam haline gelen sosyal medyada kendine yönelik verilerini tümüyle kontrol edebilmeleri için unutulma hakkı düzenlenmiştir. Bayram Doğan ve Emine Baysak. "Kişisel Verilerin Korunması Bağlamında Unutulma Hakkı." İç. *USVES Uluslararası Sosyal Bilimler ve Eğitim Bilimleri Sempozyumu* (Elazığ: Asos Yayınevi, 2021), 126.

uygulanan içeriklere erişim mümkün olmaktadır.[7] Örneğin Twitter kişisel ayarlar kısmından kullanıcılar ülke bölmesinde "worldwide" seçeneğini veya Türkiye dışında bir ülkeyi seçerek Türk mahkemelerinin erişim engelleme kararı verdiği hesaplara erişim sağlamaya devam edebilmektedir.[8] Bir diğer sosyal medya platformu Youtube'da sayfa altında yer alan 'ülke' bölmesine Türkiye dışındaki herhangi bir ülke yazılarak mahkeme kararı ile erişimin engellenmesi gereken hukuka aykırı içeriklere erişim devam etmektedir.[9] Sosyal medya şirketleri, kullanıcıların nasıl etkileşimde bulunacağının belirlenmesi ve içerik kontrolünün sağlanmasında ulusal otoritelerden gelen bildirimler, mahkeme kararları yahut kullanıcı şikayetlerine göre hukuka aykırı yahut kullanım politikalarına uygun olmayan içerikleri kaldırabilecek veya bunlara erişimi engelleyecek teknolojiye sahiptir. Ayrıca yapay zeka kullanılarak zararlı olduğu otomatik olarak belirlenen içeriklerin sosyal medya platformlarına yüklenmeleri engellenebilmektedir.[10] Bu şekilde ulusların teknik ve egemenlik yetkisinden kaynaklı sınırlamalar nedeniyle engelleyemedikleri hukuka aykırı içerikler teknolojik üstünlüğe sahip olmaları dolayısıyla sosyal medya şirketlerince internetten kaldırılabilmekte ve hatta henüz sosyal medya platformuna yüklenmeden tespit edilmesi halinde yüklenmesi engellenebilmektedir. Buna rağmen sosyal medya şirketleri,

---

7 Alp Öztekin, *Sosyal Medya Alanında Yapılması Gereken Hukuki Düzenlemeler Üzerine Düşünceler*, Temmuz 3, 2020, 3, https://www.hukukihaber.net/sosyal-medya-alaninda-yapilmasi-gereken-hukuki-duzenlemeler-uzerine-dusunceler-makale,8062.html.; Güven Köse ve Kerem Özen. "İnternet'te Sansür Üzerine Bir Değerlendirme," içinde *2. Uluslararası Değişen Dünyada Bilgi Yönetimi Sempozyumu* (Ankara: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü, 2010), 118.

8 *Recep Tayyip Erdoğan Başvurusu*. 2014/5376 (Anayasa Mahkemesi, 28 Ocak) 2020.

9 *Erdoğan Başvurusu*.

10 *Erdoğan Başvurusu*.

zararlı ve uygunsuz içeriklerin paylaşımını engellememektedir. Ticari kar için faaliyet gösteren sosyal medya şirketleri nihayetinde toplumsal iyiliğe değil, kendi mali çıkarlarına dayalı kararlar almaktadır.[11]

İnternetteki zararlı içeriklerle etkin mücadele için sosyal medya platformlarının sorumlu tutulması gereklidir. Buna yönelik olarak 2017 yılında Netzwerkdurchsetzungsgesetz (NetzDG) adlı Kanun ile Almanya'da ve 2019 yılında İngiltere'de kanun tasarısı çalışması ile sosyal medya şirketlerinin zararlı içerikle mücadelede etkin mekanizma kurup uygulamaları düzenlenmiştir.[12]

---

[11] Open Rights Groups, *ORG Policy Responses to Online Harms White Paper*, Mayıs 2019, 1 https://modx.openrightsgroup.org/assets/files/reports/report_pdfs/ORG_Policy_Lines_Online_Harms_WP.pdf.

[12] Sosyal medya platformları, kullanıcıların platforma katılırken kabul etmek zorunda oldukları 'topluluk standartları' yahut 'kullanım şartları' kapsamında suç teşkil etmemekle birlikte zararlı yahut uygunsuz olan içerik paylaşımının yasak olduğunu belirtmektedir. Sosyal medya platformları topluluk standartları' yahut 'kullanım şartları'nda yasakladıkları zarar verici, rahatsız edici, şiddeti teşvik edici yahut yanıltıcı uygunsuz içerikler kullanıcılar tarafından bu platformlara yüklenmekte ve yasak ihlal edilmektedir. Örneğin Yeni Zelanda'da gerçekleştirilen terör saldırısında topluluk standartlarına uymayan videolar YouTube'da paylaşılarak geniş kitlelere ulaştırılmıştır. Yeni Zelanda Christchurch şehrinde Cuma namazı sırasında iki camiye gerçekleştirilen terör saldırısına yönelik videolarla ilgili olarak Türkiye'den Bilgi Teknolojileri Kurumu camideki terör saldırısı içerikli 70 videonun YouTube'den kaldırılması talebinde bulunmuş, bu talep kapsamındaki 8 video YouTube'un Topluluk Kurallarını ihlal gerekçesiyle kaldırılmıştır.; Yaman Akdeniz ve Ozan Güven, *Engelli Web Buz Dağının Görünmeyen Yüzü* (İstanbul: İfade Özgürlüğü Derneği, 2019), 49. Google raporuna göre talepte yer alan 62 videoyu ise YouTube talep öncesinde kaldırmıştır.; Akdeniz ve Güven , *Engelli Web Buz Dağının Görünmeyen Yüzü*, 49. Sosyal medya platformlarının genel tutumu sosyal medya ağlarında yer alan içeriklerin denetimini sağlamada isteksiz ve yetersiz kalma yönündedir. Bu tutumun engellenmesi için İngiltere'de E-Ticaret Direktifi'nde değişiklik yahut

Almanya'daki düzenleme ile sosyal medya platformlarının kullanıcıların yasa dışı içerik hakkında şikayette bulunmaları için bir mekanizma sağlaması gerekmiştir. Sosyal medya şirketlerine şikayet edilen içeriğin kaldırılması için içeriğin açıkça yasaya aykırı olması halinde 24 saat, yasadışı olduğu açıkça anlaşılmayan içerikler için ise 7 gün süre verilmiştir. Kanun'a aykırı hareket edilmesi halinde 50 milyon Euro'ya kadar para cezası öngörülmüştür.[13]

Ülkemizde Kişisel Verilerin Korunması Kanunu'nun 12. maddesi ile veri sorumlusuna kişisel verilerin hukuka aykırı işlenmesini engelleme ve kişisel verilere hukuka aykırı şekilde erişimi engelleme yükümlülüğü getirilmiştir.[14] Bu yükümlülük

---

eklemeler yapılarak internet servis sağlayıcıları, telekomünikasyon operatörleri ve sosyal medya platformlarından oluşan çevrimiçi aracıların sorumluluklarının artırılması yönünde çağrıda bulunulmuştur. Woodhouse, *Commons Library Briefing*, 4, 6. Graham Smith, "Time to Speak up for Article 15," *Cyberleagle*, 21 Mayıs 2017, https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html. Benzer şekilde 2017'de Dijital Ekonomi Yasası'nda İngiltere Hükümetinin sosyal medya platformları için kurallar ve asgari standartları ortaya koyan ve uygulamada düzenli inceleme ve denetim sağlayan bir kanun hazırlaması gerektiği belirtilmiştir. Woodhouse, *Commons Library Briefing*, 9.

13 Heidi Tworek ve Paddy Leerssen, *An Analysis of Germany's NetzDG Law* (Amsterdam: Transatlantic High Level Working and Freedom of Expression, 2019), 2.

14 Kişisel Verilerin Korunması Kanunu 3. maddesine göre veri sorumlusu: "*Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder."* Bu bağlamda verilerin nasıl işleneceği, gerçek veya tüzel kişi veri sorumlusu tarafından belirlenmektedir. Bayram Doğan, *Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı* (Ankara: Adalet Yayınevi, 2022), 54, 55. Veri sorumlusunun sorumluluklarını belirleme yetkisi ise Kişisel Verileri Koruma Kurumu'na verilmiştir. Esin Gürsel ve Fatih Düğmeci, "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme." *R&S - Research Studies Anatolia Journal* 1, no. 2 (2018): 323, 324.

kapsamında veri sorumlusu, kişisel verilerin muhafazasını sağlamak ve bunlara hukuka aykırı şekilde erişimi engellemek üzere her türlü teknik ve idari tedbiri almak durumundadır. Buna rağmen veri ihlalinin gerçekleşmesi durumunda Kişisel Verileri Koruma Kurumu'nca veri sorumlusunun bu ihlali ilgilisine ve Kişisel Verileri Koruma Kurumu'na 72 saat içinde bildirme zorunluluğu getirilmiştir. Burada 72 saatlik süre, Avrupa Birliği Genel Veri Koruma Tüzüğü'nde (GDPR) belirtilen veri sorumlusunun ihlalden haberdar olduktan itibaren 72 saat içinde veri ihlalinden denetim makamlarını haberdar etmesini öngören 33. maddesi dikkate alınarak belirlenmiştir. Türkiye'de veri işleyen yurt dışında yerleşik veri sorumluları düşünüldüğünde bu düzenlemelerin uygulanması güçlük arz etmektedir. Örneğin Facebook, Twitter, Youtube gibi sosyal medya şirketleri kullanıcılardan elde ettikleri verileri işleme amaçlarını açık ve kesin şekilde belirlemelidir. Kuşkusuz bu amaç meşru ve hukuka uygun olmalıdır. Meşru amaç, yapılan iş veya hizmetle ilgili amaç anlamındadır.[15] Bu amaca aykırı veri işlenmesini veri sorumlusu olan bu şirketlerin engelleme yükümlülüğü bulunmaktadır. Ancak şirketler, bu yükümlülüklerini yerine getirmemektedir. Örneğin 2019 yılında Yeni Zelanda cami saldırılarında bulunan teröristin masum insanları öldürürken başına taktığı kamera ile bunu Facebook hesabından canlı olarak yayınlamasında sosyal medya şirketi Facebook'un sorumluluğu tartışması gündeme gelmiştir. Bu olay üzerine Avustralya Ceza Kanunu'nda 2019 yılında yapılan değişiklikle Facebook, Youtube, Twitter gibi yer sağlayıcı sosyal medya şirketlerinin nefret uyandırıcı şiddet barındıran içerik bulundurmaları halinde bu içeriği derhal durdurmamaları

[15] KVKK, *Kişisel Verilerin Korunması Hukuku Bilgilendirme Rehberi,* Hasan Kalyoncu Üniversitesi, 2019, https://www.hku.edu.tr/wp-content/uploads/2019/04/kvkk-kitapcik.pdf.

halinde suç işlemiş olacakları 474.34. maddede belirtilmiştir.[16] Benzer şekilde nefret uyandırıcı şiddet barındıran içeriğe erişim için kullanılan içerik hizmeti sağlayıcının bu materyalin içerik sağlayıcıdan derhal kaldırılacağı güvencesini vermezse suç işlemiş olacağı hükme bağlanmıştır.[17] Bu hükümlerin uygulanabilmesi için ülkenin sosyal medya şirketlerinden muhatap bulması gerekmektedir. Ülkemizdeki yeni yapılan düzenleme ile temsilci bulundurma yükümlülüğü, temsilci bilgilerinin açıkça belirtilmesi ve veri sorumlularının mernise kayıt olma zorunluluğu hukuki düzenlemelerin muhatap bulunarak uygulamaya aktarılabilmesi için önemli bir gerekliliktir.[18]

II. SOSYAL MEDYA TANIMI

Bireylerin sanal hesap oluşturmalarını mümkün kılarak özgürlüklerini sınırsız hale getiren sosyal medyanın tanımlanması, sosyal medyaya yönelik düzenlemelerin kapsam

---

[16] The Parliament of the Commonwealth of Australia, "A Bill for an Act to amend the Criminal Code Act 1995, and for related purposes," *Criminal Code Amendment (Sharing of Abhorrent Violent Material)* 2019, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf.

[17] The Parliament of the Commonwealth of Australia, "A Bill for an Act."

[18] Faruk Bilir, *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Kanunu,* Web Panel, SETA, Ankara, 18 Kasım 2020, https://www.setav.org/guncel-gelismeler-isiginda-kisisel-verilerin-korunmasi-kanunu/. Veri sorumlularının mernise kayıt olma yükümlülüğü kapsamında yurtdışında yerleşik olan yaklaşık 550 veri sorumlusu mernise kayıt olmuştur. Türkiye'de veri işleyen yurt dışında yerleşik veri sorumlularının mernis kayıtları 30 Eylül 2020'de sona ermiştir. Yurt içinde yerleşik veri sorumluları için ise 30 Eylül 2020'den itibaren mektup gönderilmekte ve bu mektubun ulaşmasından itibaren 30 günlük ek süre verilmiştir. Ana faaliyet konusu hassas veri işleyen veri sorumlularının ve kamu sorumlusu veri sorumlularının mernise kayıt süresi 31 Mart 2021 tarihine kadar belirlenmiştir. Bilir, *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Kanunu.*

ve muhatabının belirlenmesi açısından önemlidir.[19] Sosyal medyanın genel kabul görmüş bir tanımı bulunmamaktadır.[20] Sosyal medya; bloglar, iş ağları, ortak projeler, kurumsal sosyal ağlar, sosyal oyunlar, forumlar, fotoğraf yahut video paylaşımı, ürün incelemesi ve yorumları da içine alan bir şemsiye terim olarak kullanılmaktadır.[21] Sosyal medya, Web 2.0 üzerine inşa edilmiş ve kullanıcı tarafından oluşturulan içeriğin ihdasına, değiş tokuşuna izin veren internet tabanlı bir uygulama grubu şeklinde tanımlanabilir.[22] 5651 sayılı Kanun'da internet

---

19 Ahmet Altındiş, "Sosyal Medya Ağları ve Sosyal Görünüm Anksiyetesi," *The Journal of Academic Social Science Studies* no. 64 (2017): 234.

20 Caleb T Carr ve Rebecca A Hayes, "Social Media: Defining, Developing, and Divining," *Atlantic Journal of Communication* 23, no. 1 (2015): 46.

21 Thomas Aichner, Matthias Grünfelder, Oswin Maurer, ve Deni Jegeni, "Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019," *Cyberpsychology, Behavior, and Social Networking* (2020): 1, https://www.liebertpub.com/doi/pdfplus/10.1089/cyber.2020.0134.

22 Andreas M Kaplan ve Michael Haenlein, "Users of the World, Unite! The Challenges and Opportunities of Social Media," *Business Horizons* 53, no. 1 (2010): 61. Muhammed Süheyl Karakaya, "5651 sayılı Kanun'un 9. Maddesi ve Erişimin Engellenmesi: Koyun Postunda Kurt Hükmü," *Türkiye Barolar Birliği Dergisi* no. 137 (2018): 101. Bünyamin Atıcı ve Serkan Yıldırım, "Web 2.0 Uygulamalarının E-Öğrenmeye Etkisi," içinde *Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri*, düzenleyen: Mustafa Akgül, Ethem Derman, Ufuk Çağlayan, Attila Özgit ve Tuğrul Yılmaz (Muğla: Muğla Üniversitesi Basımevi, 2010), 370. Fehmi Şener Gülseren, "İnternet Ortamında İşlenen Hakaret Suçları," *Lefke Avrupa Üniversitesi Sosyal Bilimler Dergisi* 4, no. 1 (2013): 16. Sinan Sami Akkurt, "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlali Halinde Ortaya Çıkacak Cezai Sorumluluğa Medeni Hukuk Bağlamında Bir Bakış," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 25, no. 2 (2017): 335. Bu tanım 1996- 2019 yılları arasında akademik çalışmalarda yer alan sosyal medya tanımlarına yapılan Google akademik atıflarını kıyaslayan araştırmada sosyal medyayı tanımlayan ve 19656 atıf alarak en yüksek kabul gören tanım olarak belirtilmiştir. Ayrıca ilgili çalışmada yapılan atıf sayısının belirlendiği akademik çalışmalarda yer alan sosyal medya tanımları incelendiğinde sosyal medya ve sosyal ağ kavramlarının akademik çalışmalarda aynı

ortamındaki yayınların düzenlenmesine yönelik ilgili terimler tanımlanmış olmakla birlikte sosyal medyanın tanımı yapılmamıştır. Sosyal medya, isminde yer alan *medya*da bulunmayan kendine özgü nitelikleri haizdir.[23] Örneğin medyada insanların tüketmeye istekli olduğu içerikler oluşturma işi ancak yayıncılar tarafından gerçekleştirilebilirken sosyal medyada kişiler Twitter, bloglar, forumlar gibi platformlar üzerinden içeriği bizzat kendileri oluşturmakta ve medyadan farklı olarak diğer kişilerle doğrudan iletişim kurabilme ve etkileşimde bulunma olanağına sahiptirler.[24] Sosyal medyanın en önemli özelliklerinden biri bu şekilde kullanıcılarına fikir ve bilgi, fotoğraf ve video paylaşımı gibi karşılıklı etkileşimde bulunma olanağı tanımasıdır.[25] Benzer şekilde web tabanlı hizmetler olan sosyal ağlar da kullanıcıların kendileri için profil oluşturarak fikirlerini ve çeşitli içerikleri paylaşabilmelerine, diğer kullanıcıların oluşturduğu içerikleri okuyup izleyebilmelerine, kendi yorumlarını yaparak birbirleriyle etkileşimde bulunmalarına imkan sağlamaktadır.[26]

---

anlamda kullanıldığı gözlemlenmiştir. Aichner ve diğerleri, "Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019," 5.

23 Başak Solmaz, Gökhan Tekin, Züleyha Herzem, ve Muhammed Demir, "İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama," *Selçuk İletişim* 7 no. 4 (2013): 25.

24 David Meerman Scott, *The New Rules of Marketing and PR, How to Use Social Media, Online Video, Mobile Applications, Blogs, News Releases, and Viral Marketing to Reach Buyers Directly* (New Jersey: Wiley, 2015), 61. Zekiye Beril Akıncı Vural ve Mikail Bat, "Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma," *Journal of Yasar University* 20, no. 5 (2010): 3349, 3350.

25 Solmaz ve diğerleri, "İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama," 24.

26 Ercüment Büyükşener, "Türkiye'de Sosyal Ağların Yeri ve Sosyal Medyaya Bakış," iç. *Inet-tr ' 09: 12-13 Aralık 2009 : XIV. "Türkiye'de İnternet" Konferansı Bildirileri*, düzenleyen: Mustafa Akgül, Ethem Derman, M Ufuk Çağlayan ve Attila Özgit (İstanbul: İnternet Teknolojileri Derneği, 2014), 19.

Bu hizmetleri sunan sosyal ağ sağlayıcıları ise 5651 Sayılı Kanun'da gerçek ve tüzel kişileri kapsayacak şekilde internet üzerinden görüntülü, sesli veya yazılı içeriklerin oluşturulup paylaşılmasını sağlayan kişiler olarak tanımlanmıştır.[27] Tanımda oluşturulmasına, görüntülenmesine veya paylaşılmasına imkan sağlanan içeriklerden biri de konum olarak belirtilmiştir. Kullanıcıların kendi oluşturdukları hesapları üzerinden gerek metin gerek konum paylaşımı düşünüldüğünde Whatsapp, belirtilen tanıma uygun olarak sosyal ağ sağlayıcısı olarak kabul edilmelidir.[28] Facebook, Instagram, TikTok gibi sosyal medya

---

[27] 5651 sayılı Kanun'a sosyal ağ sağlayıcı tanımı eklenmeden önce YouTube, Facebook gibi sosyal medya platformları aynı Kanun'da "Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler" şeklinde tanımlanan yer sağlayıcı olarak nitelenmekte ve yer sağlayıcının sorumluluk ve yükümlülüklerine tabi tutulmaktaydı.

[28] Almanya'da Sosyal Medya Ağları Uygulaması Yasası'nda (Almanca Netzwerkdurchsetzungsgesetz) yer alan tanımda 5651 sayılı Kanun'dan farklı olarak sosyal ağ sağlayıcısı olma iki şarta bağlanmıştır. Bunlar; kar amacı gütmek ve oluşturulan içeriği başka kullanıcılarla paylaşmak yahut içeriği herkese açık hale getirmektir. Almanya'daki bu tanımın dikkate alınması gerektiği ve bu bağlamda Whatsapp'ın sosyal ağ sağlayıcısı kabul edilmemesi gerektiği yönündeki görüş için bakınız: Murat Volkan Dülger ve Onur Özkan, *Sosyal Medya Yasası Meclis'ten Geçti: Peki, Şimdi?* 15 Aralık 2020, 2, 3, https://www.academia.edu/43746570/Sosyal_Medya_Yasas%C4%B1_Meclisten_Ge%C3%A7ti_Peki_%C5%9Eimdi.

Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanun (Almanca (Das deutsche Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken kısaca Netzwerkdurchsetzungsgesetz - NetzDG) 1. maddesinde Kanun kapsamı belirtilirken konular 3 kısımda sınıflandırılmıştır. Kent, "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu," 13. Buna göre 1. grup kullanıcıların içerik paylaşımında bulunabilecekleri kar getiren sosyal medya platformlarıdır -ki bunlar Kanun'da "sosyal ağ" olarak isimlendirilmişlerdir-. 2. grup gazetecilik editoryal işlevi olan platformlardır. 3. grup ise kişisel iletişim platformları ile yalnızca belirli bir içerik dağıtımını sağlayan platformlardan oluşmuştur. Bundesamt für Justiz (Alman Federal Adalet Bürosu). *Gesetz zur Verbesserung der*

platformlarında oluşturulan içeriğin görüntülenmesinde sınırsız sayıda kullanıcıya ulaşılabilmesi mümkündür. Diğer taraftan Whatsapp, Skype gibi dijital mecralarda da kullanıcıların oluşturdukları profilleri üzerinden metin görüntü veya konum gibi içerik paylaşımları mümkündür. Benzer şekilde Whatsapp durum paylaşımında paylaşılan içerik kullanıcıda kayıtlı ve yasaklı olmayan herkes tarafından görülebilmektedir. Bu mecralarda içerikler ayrıca bireysel olarak kullanıcılarla yahut grup şeklinde çoklu kitlelerle paylaşılabilmektedir. Facebook, Instagram veya TikTok gibi platformlara kıyasla Whatsapp yahut Skype'ta oluşturulan içeriklerin genellikle daha az sayıda kullanıcı ile paylaşılması, Kanun'daki tanım düşünüldüğünde bunların sosyal ağ sağlayıcısı niteliğini haiz olmasına bir engel teşkil etmemektedir.

III. SOSYAL MEDYADA GERÇEKLEŞEN İHLAL ÖRNEKLERİ

Anayasa Mahkemesi'nin bireysel başvuru kararları içerisinde yer alan 2013/9660 başvuru numaralı davada sosyal medya üzerinden özel hayatın gizliliğinin ihlali tartışması gündeme gelmiştir. Gülhane Askeri Tıp Akademisi Sağlık Meslek Yüksek Okulu mezunu olarak aynı kurumda sivil memur hemşire olan Serap Tortuk'un açtığı davada Anayasa Mahkemesi'nce_özel hayatın gizliliğinin korunması hakkını düzenleyen Anayasa'nın 20. maddesinin ihlal edildiğine karar verilmiştir. Tortuk, kendi adı kullanılarak oluşturulan Facebook profilinde cinsel içerikli görüntü yayınlandığını, sosyal medya hesabının ve görüntülerin kendisine ait olmadığını, kendisinin bu tür paylaşımlarda bulunmadığını ileri sürmüştür. Bir bayanın

Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)(Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanun). 1 Eylül 2017. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html. Buradan hareketle Alman kanunları uyarınca Skype, Telegram, Whatsapp veya e-postalar 3. grupta değerlendirilebilir. Murat Volkan Dülger ve Mustafa Temmuz Oğlakcıoğlu, "Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanuna İlişkin Değerlendirme," *Ceza Hukuku Dergisi* 13, no. 37 (2018): 89.

kendisine dair cinsel içerikli görüntülerini paylaşmasının hayatın olağan akışına aykırı olduğunun da göz önünde bulundurularak Milli Savunma Bakanlığı Yüksek Disiplin Kurulu'nca verilen devlet memurluğundan çıkarma cezasında takdir yetkisinin doğru kullanılmadığını belirtmiştir. Buna karşın Milli Savunma Bakanlığı Yüksek Disiplin Kurulu, sosyal medya hesabında bu tür görüntülerin yayınlanmasının Türk Silahlı Kuvvetleri'nin itibarını derinden sarsacak nitelikte ve memurluk sıfatıyla bağdaşmayacak derecede yüz kızartıcı ve utanç verici bir fiil oluşturduğuna karar vererek Serap Tortuk için devlet memurluğundan çıkarma cezasına hükmetmiştir.[29] Bunun üzerine yürütmenin durdurulması talebiyle başvurulan Askeri Yüksek İdare Mahkemesi, cinsel içerikli görüntülerin Serap Tortuk'un iddia ettiği şekilde "*hukuka aykırı olarak yayınlandığı değerlendirilebilecek ise de, … başvurucunun disiplin soruşturmasına konu eylemleri memuriyet sıfatı ile bağdaşmayacak nitelik ve derecede yüz kızartıcı ve utanç verici eylemler olduğundan, savunmasında belirttiği hususların hukuki bir geçerliliği bulunmadığı*"nı belirtmiştir.[30] Bu şekilde internet üzerinden hukuka aykırı olarak başkası tarafından yayınlanan içerikler nedeniyle çalışma hayatının olumsuz etkilenmesinde hukuka aykırılığın dikkate alınması gerekir. Ayrıca sosyal medyada gerçekleşen cinsel içerikli görüntü paylaşımı, Tortuk'un iş hayatından ziyade özel hayatını ilgilendiren bir eylem olarak özel hayatın gizliliğinin korunması hakkının ihlal edilip edilmediği tartışmasını gündeme getirmiştir.[31] Bundan başka, sosyal medya kullanılarak hukuka aykırı eylemlerde bulunulması, yalnızca kişilik hakkı ihlali, özel hayatın ihlali gibi

---

29 *Serap Tortuk Kararı*. 2013/9660 (Anayasa Mahkemesi, 21 Ocak) 2015.

30 *Serap Tortuk Kararı.*

31 Merve Ayşegül Kulular İbrahim, "Protection of Privacy Against IT," iç. *The Palgrave Handbook of Global Social Problems*, düzenleyen: Sajid S., Przeperski J., Nadesan V., Rezaul I., Gao J. Baikady R. (Cham: Palgrave Macmillan, 2022), 8 https://doi.org/10.1007/978-3-030-68127-2.

aykırılıklara değil ayrıca ilgili olayda görüldüğü şekilde kamu otoritesinin sarsılması, kamu düzeninin bozulması gibi sorunlara da neden olabilmektedir. Mevcut düzenlemeler, sosyal medyada uzun süredir yaşanmakta olan mağduriyetlerin giderilmesinde etkili olmamaktadır.[32] Sosyal medya üzerinden gerçekleşen hukuka aykırılıkların sonlandırılarak gerek kişilerin bireysel olarak haklarının korunması gerekse toplu olarak kamu düzeninin sağlanması için sosyal ağ sağlayıcıların sorumluluklarının artırılması gerekmektedir.

IV. SOSYAL AĞ SAĞLAYICILARINA YÖNELİK YENİ DÜZENLEMELER

A. Sosyal Ağ Sağlayıcılarının Temsilci Ataması

5651 sayılı Kanun'da yapılan değişiklikle merkezi yurt dışında olan sosyal ağ sağlayıcılarına Türkiye'den erişimi günlük bir milyonu geçenler için Türkiye'de bir temsilci atama zorunluluğu getirilmiştir. 5651 sayılı Kanun'da Türkiye'den erişimi günlük bir milyonu geçen yurt dışı merkezli sosyal ağ sağlayıcılarının Türkiye'de bulundurmakla yükümlü kılındıkları temsilciliklerin hukuki niteliğine yönelik bir sınırlama yapılmamıştır. Dolayısıyla yabancı sosyal medya şirketleri 4875 sayılı Doğrudan Yabancı Yatırımlar Kanunu Uygulama Yönetmeliği uyarınca Sanayi ve Teknoloji Bakanlığı'ndan izin alarak, Türkiye'de irtibat bürosu açma yahut 6102 sayılı Türk Ticaret Kanunu'na göre şube açma ve bu şubelere ticari mümessil atanması gibi müesseseler ile Türkiye'de muhatap alınacak bir temsilci bulundurabileceklerdir.[33] Türkiye'de temsilci bulundurma

---

[32] Öztekin, *Sosyal Medya Alanında Yapılması Gereken Hukuki Düzenlemeler Üzerine Düşünceler*, 1. Mustafa Tırtır, *Sosyal Medya Yasası Üzerine Değerlendirmeler*, 29 Temmuz 2020, 1, https://www.hukukihaber.net/sosyal-medya-yasasi-uzerine-degerlendirmeler-makale,8129.html.

[33] Dülger ve Özkan, Sosyal Medya Yasası Meclis'ten Geçti: Peki, Şimdi? 3. Daha İyi Yargı Derneği, *Türkiye Büyük Millet Meclisi'ne Sunulan Sosyal Medya Yasa Tasarısı Hakkında Görüşümüz*, 28 Temmuz 2020, 6, http://www.dahaiyiyargi.org/gundem-notlari/sosyalmedyatasari2020/.

yükümü ile yurt dışı kaynaklı sosyal ağ sağlayıcılarının Bilgi Teknolojileri ve İletişim Kurumu'nun yahut ilgili diğer mercilerin isteklerinin yahut bildirimlerin gerçekleştirilebilmesi için muhatap bulundurması amaçlanmıştır. Bu nedenle temsilcinin kimlik ve iletişim bilgilerinin Bilgi Teknolojileri ve İletişim Kurumu'na bildirilmesi ve sosyal ağ sağlayıcının internet sitesinde belirtilerek erişime sunulması zorunlu kılınmıştır. Bu yükümlülüğü yerine getirmeyen sosyal ağ sağlayıcıları için kademeli olarak yaptırımlar öngörülmüştür. Bu yaptırımlar on milyon TL idari para cezasından başlayıp Türkiye'den bu sosyal ağ sağlayıcısına reklam verilmesinin yasaklanması, sosyal ağ sağlayıcısının internet trafiğinin azaltılması için bant genişliğinin yüzde doksana kadar daraltılması şeklinde belirlenmiştir. Burada dikkat çekilmesi gereken konulardan biri, bu yaptırımların yurt dışı kaynaklı sosyal ağ sağlayıcısı tarafından Türkiye'de temsilci bulundurma yükümü ihlaline yönelik olduğudur. Nitekim Türkiye'de temsilci bulundurmakla birlikte 5651 sayılı Kanun ile getirilen yükümlülükleri yerine getirmeyenler için yalnızca idari para cezası söz konusudur.[34] Yükümlülüklerini yerine getirmeyen sosyal ağ sağlayıcıları, yalnızca temsilci atayarak bant genişliğinin daraltılması yahut Türkiye'deki vergi yükümlülerince bu sosyal ağ sağlayıcılarına reklam vermelerinin yasalanarak reklam gelirlerinin düşürülmesi gibi yaptırımlardan kurtulabileceklerdir. Dolayısıyla sosyal ağ sağlayıcılarını Kanun'da getirilen yükümlülüklerini yerine getirmeye yöneltmek için etkili başka yaptırımlar öngörülmesi gerekmektedir.

B. Sosyal Ağ Sağlayıcılarına Uyarı Yöntemi ile İçeriğin Yayından Çıkarılması Başvurusu

Sosyal medya üzerinden kişilik hakkı ihlallerinin önlenmesi yahut özel hayatın gizliliğinin korunması için sosyal ağ

---

34 Pelin Ünker, *Sosyal Medyada Yeni Dönem: Ağ Sağlayıcılar Neden Suskun?* 07 Temmuz 2020, https://p.dw.com/p/3g8Vs.

sağlayıcıların platformlarında paylaşılan içerik hakkında sorumlulukları artırılmıştır. Buna yönelik olarak Türkiye'den bir gün içerisinde erişimi bir milyonu geçen sosyal ağ sağlayıcılarına, hak ihlallerinin bildirilmesi için bir şikayet mekanizması oluşturarak yapılan başvuruları 48 saat içinde cevaplama yükümlülüğü getirilmiştir.[35] Kişilik hakkı yahut özel hayatın gizliliğini ihlal eden içeriklerin yayından çıkarılması talebinin olumsuz cevaplanması halinde sosyal ağ sağlayıcıların gerekçelerini belirtmeleri gerekir. Bu şekilde doğrudan şikayet sistemine yönelik yükümlülüğünü yerine getirmeyen sosyal ağ sağlayıcısı için beş milyon TL yaptırım öngörülmüştür. Ayrıca sosyal ağ sağlayıcılarına bu başvuruların 6 aylık periyotlar halinde raporlanarak Bilgi Teknolojileri ve İletişim Kurumu'na bildirilmesi ve kişisel veriler çıkarıldıktan sonra kendi internet sitelerinde yayınlanması yükümü getirilmiştir.[36] Bu yüküm ile doğrudan başvuruların hem istatistiksel kategorik analizi yapılabilecek hem de sosyal ağ sağlayıcılarının bu başvurulara karşı uyguladıkları aktiviteler belirlenerek doğrudan şikayet

---

[35] Sosyal ağ sağlayıcılara 5651 sayılı Kanun 9. ve 9/A maddelerince başvuruda bulunulabilmesine yönelik gerekli düzenlemeleri yapmaları için Mayıs 2021 tarihine kadar süre tanınmıştır. Buna rağmen yükümlülüklerini yerine getirmeyenler için idari yaptırımlar söz konusu olmuştur. Ancak özellikle sosyal medya şirketlerinin Türkiye'de muhatap bulundurmaması hukukun uygulanabilirliğini aksatmaktadır. Bu hususta yurt dışında faaliyet gösteren sosyal medya şirketlerinden özellikle Türkiye'de temsilci bulundurma yükümlülüğünü yerine getirmeyenler için 5651 sayılı Kanun'un 3. maddesinin 3. fıkrası kapsamında internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir. Bildirimin bu şekilde yapılması durumunda bu bildirim aynı zamanda tebligat hükmüne geçecektir. Bu şekilde yurt dışı merkezli sosyal medya şirketlerinin tebligattan ve bağlı hukuki sonuçlardan kurtulmalarının önüne geçilmesi amaçlanmıştır.

[36] 5651 sayılı Kanun'a göre ilk raporun Haziran 2021 tarihinde Bilgi Teknolojileri ve İletişim Kurumu'na bildirilmesi ve sosyal ağ sağlayıcının internet sitesinde yayınlanması gerekmektedir.

sisteminin denetimi sağlanmış olacaktır. Bu sistemin işlemesi için yaptırım olarak rapor yükümünün ihlal eden sosyal ağ sağlayıcıya on milyon TL idari para cezası öngörülmüştür.

Doğrudan şikayet sistemi haricinde hakim yahut mahkeme kararı ile içeriğin kaldırılması yahut erişim engelleme de mümkün kılınmıştır.[37] Buna göre hakim yahut mahkeme kararıyla hukuka aykırı olduğu sosyal ağ sağlayıcıya bildirilmesine rağmen bildirimden itibaren 24 saat içinde içeriği kaldırmayan yahut içeriğe erişimi engellemeyen sosyal ağ sağlayıcı bu hukuka aykırı içerikten kaynaklı zararı tazminle sorumlu tutulmuştur. Erişim engelleme kararı zarar görenin zararını tazmine yönelik yahut zarar verene yaptırım uygulanmasına yönelik olmayıp hukuka aykırılığın devam etmesini önlemeye yöneliktir. Bir başka ifadeyle erişim engelleme kararları yaptırım değil tedbir olarak değerlendirilmelidir.[38] 5651 sayılı Kanun'da adli makamlarca verilen ve koruma tedbiri olarak isimlendirilen erişim engelleme kararlarına aykırı hareket edenler için bu fiilin daha ağır bir suç oluşturmaması halinde beş yüz günden üç bin güne kadar adli para cezası öngörülmüştür. İdari tedbir niteliğindeki idari makamların vermiş olduğu erişim engelleme kararını yerine

---

[37] Erişim engelleme kararının sulh ceza mahkemelerince alınması yerine bilişim hukuku alanında ihtisaslaşmış mahkemeler kurulması gerektiği ve bu mahkemelerin bilirkişilerle desteklenerek kararların gerekçelendirilmesinin toplumsal hukuka güvenilirliği artıracağı düşünülmektedir. Köse ve Özen, "İnternet'te Sansür Üzerine Bir Değerlendirme," 119, 120. Her ne kadar 5651 sayılı Kanun uyarınca sulh mahkemelerine müracaat edilmekteyse de kişilik hakkı ihlalinin söz konusu olduğu hallerde 4721 sayılı Türk Medeni Kanunu 24 ve 25. maddelerine dayanarak sosyal medya üzerinden kişilik hakkı ihlal edilen kişinin asliye hukuk mahkemesine başvurması da mümkündür. Yar. 4. HD, E.2013/17358, K.2013/19417, 09.12.2013.

[38] Bu tedbirin amacı delil korumaya yönelik olmayıp hak ihlalinin sonlandırılmasına ilişkindir. Turan Atlı, "Kişi Haklarının İhlali Durumunda İnternet Erişiminin Engellenmesi," *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* 3, no. 1 (2020): 17, 18.

getirmeyen içerik, yer ve erişim sağlayıcının karşılaşacağı yaptırım ise on bin TL'den yüz bin TL'ye kadar idari para cezasıdır. Erişim sağlayıcı için ayrıca para cezası verildikten sonra 24 saat içinde hala erişim engelleme kararını yerine getirmemesi durumunda faaliyette bulunabilmesi için Bilgi Teknolojileri ve İletişim Kurumu'nca verilmiş olan yetkilendirmenin yine Bilgi Teknolojileri ve İletişim Kurumu'nca iptal edilebileceği belirtilmiştir.

5651 sayılı Kanun'un 9. maddesine dayanarak erişimin engellenmesi kararının uygulanması sonrasında hukuka aykırı eylemin faillerine karşı adli soruşturma açılabilir veya açılmayabilir. Kanun'un 9. maddesi uyarınca sosyal medya üzerinden kişilik hakkı ihlalinde bulunanlar hakkında soruşturma yahut kovuşturma başlatılması durumunda bunun sonucuna göre erişim engelleme tedbirinin devamına yahut kaldırılmasına karar verilebilir. Ancak herhangi bir soruşturmanın başlamaması durumunda erişim engelleme kararı devam edecek ve dolayısıyla burada aslında tedbir niteliğinde olan erişim engelleme kararı kesin hüküm gibi erişimin süresiz olarak engellenmesine neden olabilecektir.[39]

İçeriğin kaldırılması ile içeriğe erişimin engellenmesi farklı faaliyetlerdir. İçeriğe erişimin engellenmesi farklı yöntemlerle yapılabilen bir uygulamadır. Bu yöntemler Radyo, Televizyon ve İsteğe Bağlı Yayınların İnternet Ortamından Sunumu Hakkında Yönetmelik'te alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi şeklinde örneklendirilmiştir. Bu ve benzeri yöntemlerle erişimin engellenmesi durumunda içerik yalnızca Türkiye veri tabanından kaldırılmakta, Türkiye'den ilgili içeriğe

[39] *Ali Kıdık Kararı*. 2014/5552 (Anayasa Mahkemesi, 26 Ekim) 2017.

ulaşılması engellenmektedir.[40] Buna rağmen söz konusu erişimi engellenen içeriklere Türkiye sınırları içinden erişim yurt dışındaki ülkeler üzerinden VPN bağlantısı sağlanması yahut ayna siteler (mirror sites) veya vekil sunucular (proxy servers) üzerinden mümkün olmaktadır.[41] Her ne kadar 5651 sayılı Kanun'un 6. maddesinde erişim sağlayıcılara erişimi engelleme kararı olan içeriklere alternatif yollardan erişimi engelleyici tedbirleri alma yükümlülüğü getirilmiş olsa da gerek teknik yetersizlikler gerek erişim sağlayıcıların isteksiz tutumları nedeniyle alternatif yollar tamamen önlenememektedir.[42] Dolayısıyla içeriğe erişimin engellenmesi Türkiye hudutları ile sınırlı bir uygulama olup içerik internet ortamında var olmaya devam etmekte olduğundan Türkiye hududu içindeki kullanıcıların erişimi dahi tam olarak önlenememektedir. İçeriğin kaldırılmasında ise içerik ülkesel bir sınırlama olmaksızın erişime kapatılmaktadır.[43] Bu nedenle içeriğin kaldırılması, bireylerin haklarının korunması bağlamında erişimin engellenmesinden daha etkili bir yöntemdir. Ancak bu durumda toplumun haber alma hürriyeti ya da ifade hürriyeti sınırlanmış olacağından her bir somut olaya göre hakların dengelenmesi gerekmektedir. İfade hürriyeti ya da haber alma hürriyetinin sağladığı fayda ile hakkı ihlal edilen kişinin gördüğü zarar birlikte değerlendirilmelidir. Diğer taraftan, ihlal engellenerek kişilik hakkının korunmasının kişiye sağladığı fayda ile haber alma hürriyeti veya ifade hürriyetinin

---

40 Dülger ve Oğlakcıoğlu, Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanuna İlişkin Değerlendirme, 99. Köse ve Özen, "İnternet'te Sansür Üzerine Bir Değerlendirme," 120.

41 Köse ve Özen, "İnternet'te Sansür Üzerine Bir Değerlendirme," 118. Öztekin, *Sosyal Medya Alanında Yapılması Gereken Hukuki Düzenlemeler Üzerine Düşünceler*, 3.

42 Merve Ergüney, "RTÜK'ün İnternet Denetimi: İlgili Mevzuat Üzerine Bir Değerlendirme," *AJIT-e: Bilişim Teknolojileri Online Dergisi* 11, no. 41 (2020): 107, 108.

43 Dülger ve Oğlakcıoğlu, Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanuna İlişkin Değerlendirme, 99.

kısıtlanmasının doğurduğu zarar birlikte değerlendirilmelidir. Her bir somut olayda bu değerlendirmelere göre kâr zarar analizi yapılarak karar verilmelidir.

C. Verilerin Türkiye'de Tutulması

5651 sayılı Kanun ile yeni getirilen düzenlemelerden bir diğeri verilerin Türkiye'de saklanması şartıdır. Bu şart günlük erişimi bir milyonu aşan sosyal ağ sağlayıcılar için öngörülmüş ve Türkiye'deki kullanıcıların verileriyle sınırlı tutulmuştur. Verilerin Türkiye'de tutulması, bilgi isteme başlığı altında düzenlenen 5271 sayılı Ceza Muhakemesi Kanunu 332. maddesinin işlerliğini sağlamaya yöneliktir. Buna göre sosyal medya üzerinden işlenen bir suçla ilgili savcı, hakim yahut mahkemece istenen bilgileri sosyal ağ sağlayıcı, Kanun gereğince 10 gün içinde bildirmekle yükümlüdür. Talep edilen bilginin 10 gün içinde verilmesinin mümkün olmaması durumunda nedeniyle birlikte en geç ne zaman bildirileceğine yönelik bilgi verilmesi gerekir. Bu düzenleme ile sosyal ağ sağlayıcılarına sosyal medya üzerinden hukuka aykırı eylemde bulunan kişilerin IP verilerini adli makamlara bildirme yükümlülüğü getirilmektedir. Bu sayede suç işlediği iddia edilen Facebook gibi sosyal medya hesaplarından delil toplanabilmesi için arama ve el koyma kararı alınmasının beklenmesi ve bu kararlar ile evine gidilen şüphelinin suç işlediği iddia edilen hesabı kapatmış olması ve suçu da inkar etmiş olması halinde suçun cezasız kalması engellenmiş olacaktır.[44] Talep edilen verilerin Kanun'da belirtilen 10 günlük süre içinde bildirilmemesi durumunda temsilci 5326 sayılı Kabahatler Kanunu'nun 32. maddesi uyarınca emre aykırı davranışta bulunmuş olacaktır.[45] Ancak emre aykırılık

---

[44] Tırtır, *Sosyal Medya Yasası Üzerine Değerlendirmeler*, 1.

[45] Dülger ve Özkan, Sosyal Medya Yasası Meclis'ten Geçti: Peki, Şimdi? 3. Şirket yetkililerinin kamu görevlisi olmamalarından ötürü bu tür hukuka

kabahatinin cezası aynı maddede yalnızca 100 TL olarak belirlenmiştir. Bu şekilde güçlü bir yaptırım öngörülmemesi nedeniyle kabahat işlenerek Türkiye'deki sunucularda tutulmasına rağmen talep edilen verinin adli makamlarla paylaşılmasından kaçınılması mümkündür. Bu durumda 5651 sayılı Kanun'da yapılan düzenleme ile sosyal medya kullanıcılarının verilerinin Türkiye'de depolanması, hukuka aykırılıkları önlemek için gerekli veri paylaşımını sağlamada yetersiz kalmaktadır. Kanun hükümlerinin uygulanabilirliğinin sağlanabilmesi için ya emre aykırılık kabahatinde öngörülen idari para cezasının artırılması yahut sosyal ağ sağlayıcısı temsilcilerinin adli makamlarla ilgili verileri paylaşmaması durumuna yönelik etkili başka bir yaptırım öngörülmesi gerekmektedir.

---

aykırı eylemlerinin emre aykırılık kabahati oluşturacağı yönündeki Yargıtay kararı için bakınız: Y5.CD, 3.5.2017, E. 2017/1400, K. 2017/1864.

Bu durumun aynı zamanda temsilci açısından 5237 sayılı Türk Ceza Kanunu 257. maddesi uyarınca görevi kötüye kullanma suçu oluşturabileceği yönünde görüş için bakınız: Daha İyi Yargı Derneği, *Türkiye Büyük Millet Meclisi'ne Sunulan Sosyal Medya Yasa Tasarısı Hakkında Görüşümüz*, 6. Kanun'da görevinin gereklerini yerine getirmeyerek, kamuya veya kişilere zarar veren yahut haksız menfaat elde eden kamu görevlisi kişiler için altı aydan iki yıla kadar hapis cezası öngörülmüştür. Kanun'da bu suçun açıkça kamu görevlileri ile sınırlandığı görüldüğünden sosyal ağ sağlayıcısı temsilcileri kamu görevlisi olmamaları nedeniyle bu suçun muhatabı olmayacaklardır. Nitekim görevi kötüye kullanma suçu özgü suç niteliğinde olup, sadece çalışmakta olduğu görevinin verdiği yetkilerini kötüye kullanan kamu görevlisi tarafından işlenmesi mümkündür. Bir başka ifadeyle bu suçun faili sadece kamu görevlisi olabilir. Handan Yokuş Sevük, "Görevi Kötüye Kullanma Suçu (TCK m. 257)," *Dicle Üniversitesi Hukuk Fakültesi Dergisi* 23, no. 39 (2018): 262. Dülger ve Özkan, Sosyal Medya Yasası Meclis'ten Geçti: Peki, Şimdi? 3. Yargıtay'ın özel şirket çalışanlarının eylemlerinin görevi kötüye kullanma suçu oluşturamayacağı yönündeki görüşü için bakınız: Yar. 15.CD, E. 2017/14316, K. 2017/7499, 14.3.2017.

SONUÇ

Bilişim teknolojilerindeki gelişmeler ve internet kullanımının yaygınlaşması sonucu sosyal medya sitelerinin kullanımı artmıştır. Sosyal medya sitelerinin kullanımı bir taraftan sosyal medya şirketlerinin kârlarını artırırken bir taraftan kişilerin haklarını ihlal eden, toplumların değer yargılarını ve iradelerini etkileyip yönlendiren, kamu düzenini tehdit eden bir boyut kazanmıştır. Sosyal medya şirketlerinin ticari kar odaklı hareket etmeleri,[46] bilişim hukuku alanında ihtisaslaşmış mahkemeler bulunmaması,[47] hukuki düzenlemelerin bilişim teknolojilerindeki gelişmelerin gerisinde kalması[48] gibi nedenler, insanlara hem kişi temelinde hem kamusal düzeyde zarar vermektedir. Sosyal medya paylaşımlarından doğan zararların önlenebilmesi için sosyal medya şirketlerinin sorumluluklarının artırılması gerekmiştir. Avustralya, Yeni Zelenda, İngiltere, Almanya gibi ülkeler sosyal medya şirketlerine çeşitli yükümlülükler getirerek kişilik haklarını ihlal eden veya kamu düzenini bozan içeriklerin tespiti ve önlenmesi, paylaşılması ya da kaldırılmasında konularında sosyal medya şirketlerini aktif rol oynamaya yönlendirmiştir. Benzer şekilde Türkiye'de de 5651 sayılı Kanun'da sosyal medya şirketlerinin sorumluluklarını artırıcı değişiklikler yapılmıştır. Bunlardan başlıcaları uyarı yöntemi ile içeriğin yayından çıkarılması, verilerin Türkiye'deki sunucularda saklanması, faaliyetlerin raporlanmasıdır. Bu yükümlülüklerin yerine getirilmesini sağlamak için muhatap bulunması gerekmektedir. Zira sosyal medya şirketleri, Türkiye Cumhuriyeti mahkemelerinin verdiği kararların gereğini yerine getirerek erişimi engellemek yerine karara konu ihlali gerçekleştiren içerikleri yayınlamaya devam ederek kendi çıkarlarını temel

---

46 Open Rights Groups, *ORG Policy Responses to Online Harms White Paper*, 1.

47 Köse ve Özen, "İnternet'te Sansür Üzerine Bir Değerlendirme," 119, 120.

48 Merve Ayşegül Kulular İbrahim, *Modern Teknolojinin Hukuki Temelleri Telgraf Örneği*, (Ankara: Adalet, 2021), 13.

insan haklarının dahi üzerinde tutabilmektedir. Toplum refahının sağlanması, kamu düzeninin korunması, kişilerin sırf insan olarak doğmalarından ötürü sahip oldukları kişilik haklarının korunması için sosyal medya şirketlerinin yeni düzenlemelerle getirilen yükümlülüklere uyması gerekmektedir. Bu amaçla öngörülmüş yeni düzenlemelerin uygulamaya yansıması takip edilmelidir. Zira ihlalleri engellemede başarılı olunmaması durumunda yaptırımların artırılması veya yeni yükümlülükler öngörülmesi gerekebilir. Sosyal medya şirketlerinin en az ticari çıkarları kadar kişilerin temel hakları ve kamu refahının korunmasını önemsemesi sağlanmalıdır.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.

KAYNAKÇA

Aichner, Thomas, Matthias Grünfelder, Oswin Maurer, ve Deni Jegeni. "Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019." *Cyberpsychology, Behavior, and Social Networking* (2020):1 - 8. https://www.liebertpub.com/doi/pdfplus/10.1089/cyber.2020.0134.

Akar, Filiz. "Okula Yansıyan Siber Zorbalık: İdari ve Hukuki Önleme Yolları."İçinde *Prof. Dr. Emine Akyüz'e Armağan - Akademisyenlikte 50 Yıl, Çocuk Hakları, Eğitim Hukuku, Vatandaşlık Eğitimi*, düzenleyen: Yasemin Karaman Kepenekci ve Pelin Taşkın, 466 - 476. Ankara: Pegem Akademi, 2018.

Akdeniz, Yaman, ve Ozan Güven. *Engelli Web Buz Dağının Görünmeyen Yüzü.* İstanbul: İfade Özgürlüğü Derneği, 2019.

Akıncı Vural, Zekiye Beril, ve Mikail Bat. "Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma." *Journal of Yasar University* 20, no. 5 (2010): 3348 - 3382.

Akkurt, Sinan Sami. "Kişilik Hakkının Sosyal Medya Kullanıcıları Tarafından İhlali Halinde Ortaya Çıkacak Cezai Sorumluluğa Medeni Hukuk Bağlamında Bir Bakış." *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 25, no. 2 (2017): 329 - 373.

Ali Kıdık Kararı. 2014/5552 (Anayasa Mahkemesi, 26 Ekim) 2017.

Altındiş, Ahmet. "Sosyal Medya Ağları ve Sosyal Görünüm Anksiyetesi." *The Journal of Academic Social Science Studies* no. 64 (2017): 227 - 235.

Atıcı, Bünyamin, ve Serkan Yıldırım. "Web 2.0 Uygulamalarının E-Öğrenmeye Etkisi." İçinde *Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri*, düzenleyen: Mustafa Akgül, Ethem Derman, Ufuk Çağlayan, Attila Özgit ve

Tuğrul Yılmaz, 369 - 374. Muğla: Muğla Üniversitesi Basımevi, 2010.

Atlı, Turan. "Kişi Haklarının İhlali Durumunda İnternet Erişiminin Engellenmesi." *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi* 3, no.1 (2020): 4 - 32.

Avşar, Zakir, ve Gürsel Öngören. *Bilişim Hukuku.* İstanbul: Türkiye Bankalar Birliği, 2010.

Bilir, Faruk. *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması.* Web Panel. SETA. Ankara, 18 Kasım 2020 https://www.setav.org/guncel-gelismeler-isiginda-kisisel-verilerin-korunmasi-kanunu/.

Bundesamt für Justiz (Alman Federal Adalet Bürosu). *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)(Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanun).* 1 Eylül 2017. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

Büyükşener, Ercüment. "Türkiye'de Sosyal Ağların Yeri ve Sosyal Medyaya Bakış." İçinde *Inet-tr ' 09: 12-13 Aralık 2009 : XIV. "Türkiye'de İnternet" Konferansı Bildirileri*, düzenleyen: Mustafa Akgül, Ethem Derman, M Ufuk Çağlayan ve Attila Özgit, 19 - 23. İstanbul: İnternet Teknolojileri Derneği, 2014.

Carr, Caleb T, ve Rebecca A Hayes. "Social Media: Defining, Developing, and Divining." *Atlantic Journal of Communication* 23, no. 1 (2015): 46 - 65 .

Daha İyi Yargı Derneği. *Türkiye Büyük Millet Meclisi'ne Sunulan Sosyal Medya Yasa Tasarısı Hakkında Görüşümüz.* 28 Temmuz 2020. http://www.dahaiyiyargi.org/gundem-notlari/sosyalmedyatasari2020/.

Doğan, Bayram. *Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı .* Ankara: Adalet, 2022.

Doğan, Bayram ve Emine Baysak. "Kişisel Verilerin Korunması Bağlamında Unutulma Hakkı." İçinde *USVES Uluslararası*

Sosyal Bilimler ve Eğitim Bilimleri Sempozyumu, 116 - 140. Elazığ: Asos Yayınevi, 2021.

Dülger, Murat Volkan, ve Mustafa Temmuz Oğlakcıoğlu. "Alman Sosyal Ağlarda Hukuk Uygulamasının İyileştirilmesi Hakkında Kanuna İlişkin Değerlendirme." *Ceza Hukuku Dergisi* 13, no. 37 (2018): 87 - 109.

Dülger, Murat Volkan, ve Onur Özkan. *Sosyal Medya Yasası Meclis'ten Geçti: Peki, Şimdi?* 15 Aralık 2020. https://www.academia.edu/43746570/Sosyal_Medya_Yasas%C4%B1_Meclisten_Ge%C3%A7ti_Peki_%C5%9Eimdi.

Ergüney, Merve. "RTÜK'ün İnternet Denetimi: İlgili Mevzuat Üzerine Bir Değerlendirme." *AJIT-e: Bilişim Teknolojileri Online Dergisi* 11, no. 41 (2020): 96 - 122.

Gülseren, Fehmi Şener. "İnternet Ortamında İşlenen Hakaret Suçları." *Lefke Avrupa Üniversitesi Sosyal Bilimler Dergisi* 4, no. 1 (2013): 15 - 33.

Gürsel, Esin ve Fatih Düğmeci. "Yapısal Anlamda Türkiye Kişisel Verileri Koruma Kurumu'na İlişkin Bir Değerlendirme." *R&S - Research Studies Anatolia Journal* 1, no. 2 (2018): 318 - 329.

Kaplan, Andreas M ve Michael Haenlein. "Users of the World, Unite! The Challenges and Opportunities of Social Media." *Business Horizons* 53, no. 1 (2010): 59 - 68.

Karakaya, Muhammed Süheyl. "5651 Sayılı Kanun'un 9. Maddesi ve Erişimin Engellenmesi: Koyun Postunda Kurt Hükmü." *Türkiye Barolar Birliği Dergisi* no. 137 (2018): 97 - 132.

Kaya, Mine. *Elektronik Ortamda Kişilik Hakkı İhlalleri ve Korunması.* Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Özel Hukuk Anabilim Dalı, Doktora Tezi, 2015.

Kent, Bülent. "Alman Hukukunda Sosyal Ağların Düzenlenmesi ve Alman Sosyal Ağ Kanunu." *Bilişim Hukuku Dergisi (BHD)* 2, no. 1 (2020): 1 - 46.

Köse, Güven, ve Kerem Özen. "İnternet'te Sansür Üzerine Bir Değerlendirme." İçinde *2. Uluslararası Değişen Dünyada Bilgi Yönetimi Sempozyumu*, 113 - 122. Ankara: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü, 2010.

Kulular İbrahim, Merve Ayşegül. "Protection of Privacy Against IT." İçinde *The Palgrave Handbook of Global Social Problems*, düzenleyen: Sajid S., Przeperski J., Nadesan V., Rezaul I., Gao J. Baikady R. Cham: Palgrave Macmillan. 2022. https://doi.org/10.1007/978-3-030-68127-2.

Kulular İbrahim, Merve Ayşegül. *Modern Teknolojinin Hukuki Temelleri Telgraf Örneği.* Ankara: Adalet, 2021.

KVKK. *Kişisel Verilerin Korunması Hukuku Bilgilendirme Rehberi.* Hasan Kalyoncu Üniversitesi. 2019. https://www.hku.edu.tr/wp-content/uploads/2019/04/kvkk-kitapcik.pdf.

Nair, Güney, ve Emine Balta. "Bilgi İletişim Teknolojileri Kullanımında sınırları Aşan Bir Sosyal Sorun Alanı Olarak Unutulma Hakkı." *Cumhuriyet Üniversitesi Sosyal Bilimler Dergisi* 41, no. 2 (2017): 113 - 126.

Open Rights Groups. *ORG Policy Responses to Online Harms White Paper.* Mayıs 2019. https://modx.openrightsgroup.org/assets/files/reports/report_pdfs/ORG_Policy_Lines_Online_Harms_WP.pdf.

Öztekin, Alp. *Sosyal Medya Alanında Yapılması Gereken Hukuki Düzenlemeler Üzerine Düşünceler.* 3 Temmuz 2020. https://www.hukukihaber.net/sosyal-medya-alaninda-yapilmasi-gereken-hukuki-duzenlemeler-uzerine-dusunceler-makale,8062.html.

Parlak, Cesim. *Yeni Sosyal Medya Düzenlemesi.* 23 Temmuz 2020. https://www.hukukihaber.net/yeni-sosyal-medya-duzenlemesi-makale,8114.html.

Scott, David Meerman. *The New Rules of Marketing and PR, How to Use Social Media, Online Video, Mobile Applications, Blogs,*

News Releases, and Viral Marketing to Reach Buyers Directly. New Jersey: Wiley, 2015.

Smith, Graham. "Time to Speak up for Article 15." *Cyberleagle.* 21 Mayıs 2017. https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html.

Solmaz, Başak, Gökhan Tekin, Züleyha Herzem, ve Muhammed Demir. "İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama." *Selçuk İletişim* 7 no. 4 (2013): 23 - 32.

The Parliament of the Commonwealth of Australia. "A Bill for an Act to amend the Criminal Code Act 1995, and for related purposes." *Criminal Code Amendment (Sharing of Abhorrent Violent Material).* 2019. https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/s1201_first-senate/toc_pdf/1908121.pdf;fileType=application%2Fpdf.

Tırtır, Mustafa. *Sosyal Medya Yasası Üzerine Değerlendirmeler.* 29 Temmuz 2020. https://www.hukukihaber.net/sosyal-medya-yasasi-uzerine-degerlendirmeler-makale,8129.html.

Tok, Gökhan. *İnternette Unutulma Hakkı.* Ankara: Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, İnsan Hakları Anabilim Dalı, Yüksek Lisans Tezi, 2020.

Tworek, Heidi, ve Paddy Leerssen. *An Analysis of Germany's NetzDG Law.* Amsterdam: Transatlantic High Level Working and Freedom of Expression, 2019.

Ünker, Pelin. *Sosyal Medyada Yeni Dönem: Ağ Sağlayıcılar Neden Suskun?* 07 Temmuz 2020. https://p.dw.com/p/3g8Vs.

Woodhouse, John. *Commons Library Briefing, Social Media Regulation.* London: Pexels Licence, 2020.

Yang, Shuzhe, Anabel Quan-Haase, Andrew D Nevin, ve Yimin Chen. "The Role of Online Reputation Management, Trolling, and Personality Traits in the Crafting of the Virtual Self on Social Media." İçinde *Social Media Research Methods*, düzenleyen: Luke Sloan ve Anabel Quan-Haase, 74 - 89. London: SAGE, 2017.

Yokuş Sevük, Handan. "Görevi Kötüye Kullanma Suçu (TCK m. 257)." *Dicle Üniversitesi Hukuk Fakültesi Dergisi* 23, no. 39 (2018): 257 - 316.

Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.1132645**

KRİPTO PARALARIN TERÖRÜN FİNANSMANI SUÇUNDA KULLANILMASI

Use of Cryptocurrency for the Crime of Financing of Terrorism

Rümeysa GENÇCELEP*

Öz

Kripto para sistemleri, teknolojik yeniliğinin yanısıra büyük ölçekli para transferlerini kolaylaştırıcı özellikleri nedeniyle faydalı olsa da kullanıcısının kimlik bilgileri saklayarak kullanıcılarına gizli alan sunması nedeniyle suçlular için cazip bir alan oluşturmaktadır. Kripto paraların üretimi, transferi ve korunmasında kullanılan blokzincir teknolojisinin herhangi bir otoriteden bağımsız olması devletlerin veya kurumların gözetiminden ve denetiminden uzak olmasına neden olmaktadır. Sistemin bu özelliği suçluları iz sürülmesi zor olan bu alana itmekte ve kripto paralar hırsızlık, dolandırıcılık, yağma, uyuşturucu ve uyarıcı madde ticareti, silah ticareti, karapara aklama ve terörün finansmanı gibi birçok suçun işlenmesinde kullanılabilmektedir.

Çalışmamızda öncelikle Türk mevzuatında düzenlenen terörün finansmanı suçu unsurları ile açıklanacak, ardından kripto paraların "ne olduğu" sorusuna cevap aranarak

* Cumhuriyet Savcısı Adayı, Adalet Bakanlığı; rumeysagenccelep@gmail.com , ORCID: 0000-0003-1115-7399.

Makale Gönderim Tarihi/Received: 18.06.2022.

Makale Kabul Tarihi/Accepted: 26.06.2022.

Atıf/Citation: Gençcelep, Rümeysa. "Kripto Paraların Terörün Finansmanı Suçunda Kullanılması." *Bilişim Hukuku Dergisi* 4, no. 1 (2022): 33-80.

terörizmin finansmanı suçunun konusunu oluşturup oluşturmayacağı belirlenecektir. Bu belirlemeler ışığında kripto paraların fon olarak kabul edilmeleri halinde terörizmin finansmanı suçunun işlenmesinde kullanılmaları değerlendirilecektir.

Anahtar Kelimeler: Kripto Para, Blokzincir, Terörün Finansmanı Suçu, Terör Örgütüne Yardım Suçu.

Abstract

Although cryptocurrency systems are useful because of their technological innovations as well as their facilitating features for large-scale money transfers, they create an attractive area for criminals because they provide a confidential area to their users by hiding their user's identity information. The fact that the blockchain technology used in the production, transfer and protection of cryptocurrencies is independent of any authority causes it to be away from the surveillance and control of states or institutions. This feature of the system pushes criminals to this area, which is difficult to trace, and cryptocurrencies can be used to commit many crimes such as theft, fraud, looting, drug and stimulant drug trade, arms trade, money laundering and terrorist financing.

In this study, first of all, the elements of the crime of financing of terrorism, which is regulated in the Turkish legislation will be explained. Then the answer to the question of "what is cryptocurrency" will be sought in order to determine whether cryptocurrencies will constitute the subject of the crime of financing of terrorism. In the light of these, if cryptocurrencies are accepted as a funds, their use in committing the crime of financing of terrorism will be evaluated.

Keywords: *Cryptocurrency, Blockchain, The Crime of Financing of Terrorism, The Crime of Aiding a Terrorist Organization.*

GİRİŞ

Herhangi bir otoriteye bağlı olmadan sistemdeki kullanıcılar tarafından üretilen kripto paralar, aynı zamanda kısmen veya tamamen anonimlik sağladığından yasadışı aktivitelerde kullanılmak için adeta biçilmiş bir kaftandır. Kullanıcı sahip olduğu kripto para ile kullanımı yasak olan uyuşturucu veya uyarıcı madde temin edebilir, silah satın alabilir, çocuk pornografisi görüntüleri izleyebilir ya da başka birçok suçu işlemek için kripto para kullanabilir.

Çalışmamızın konusunu oluşturduğu üzere kripto paralar üyesi veya sempatizanı olunan terör örgütüne yardım etmek için de kullanılabilir. Bu kapsamda Türk mevzuatında müstakil bir suç olarak düzenlenen terörizmin finansmanı suçunun kripto paralarla işleniş biçimi ve delillendirilmesi açıklanacaktır.

I. TERÖRÜN FİNANSMANI SUÇU

A. Genel Olarak

Latince'de "*terrorem*" ismi ve "*terrere*" fiilinden türeyen terör kelimesi Fransızca'da "*terreur"*, İngilizce ve Almanca'da "*terror"* olarak, Türkçe'de ise ürkütmek, korkutmak, kaçırmak anlamlarına gelen "*tedhiş"* kelimesi ile aynı anlamda kullanılmaktadır.[1]

Türk hukukunda 3713 sayılı Terörle Mücadele Kanunu'nun **(TeMK)**[2] 1.maddesinde uluslararası alana uyum sağlanarak terör kavramı kullanılmıştır. Düzenlemeye göre cebir ve tehdit kullanarak ülkenin siyasi, hukuki, sosyal, laik ve ekonomik düzenini ve Cumhuriyetin niteliklerini değiştirmek, devletin

---

[1] Mehmet Gödekli, *Terörizmin Finansmanı Suçu*, (Ankara: Seçkin Yayıncılık, 2017), 29-30; Faruk Yasin Turinay, "Ceza Hukukunda Terör Örgütü Kavramı", *TBB Dergisi 27*, no. 116 (2015): 40; Burak Boz, "Türk Ceza Hukukunda Terör Örgütü ve Terör Örgütüne Üye Olma Suçu", *ASBÜ Hukuk Fakültesi Dergisi* 2, no. 1 (2020): 136.

[2] RG. 12.04.1991, S. 20843.

güvenliğini ve bölünmez bütünlüğünü bozmak ve varlığını tehlikeye düşürmek, otoriteyi zaafa uğratmak, yıkmak, ele geçirmek, temel hak ve hürriyetleri yok etmek, kamu düzenini veya genel sağlığı bozmak amaçlarıyla örgüt mensuplarınca gerçekleştirilecek suç teşkil eden her türlü eylem terör eylemidir.[3]

Terörizmin "*politik amaçlara ulaşabilmek için yasadışı kuvvet kullanımı"* şeklinde genel ve kısa bir tanımı da yapılmaktadır. Her iki tanımına göre; tanımlanabilir bir grup tarafından, terör örgütünün nüfuzunu artırmak ve politik amaçlı olarak, şiddet kullanarak devlet dışı unsurların şiddet mağduru yapılması veya şiddet kullanılacağına dair tehditte bulunarak hedeflenen bazı gruplar üzerinde etki oluşturulması eylemleri terörizm olarak adlandırılmaktadır.[4]

Uluslararası alanda Birleşmiş Milletler ve Avrupa Konseyi bünyesinde hazırlanarak yürürlüğe konulan birçok terörizm karşıtı antlaşmada yalnızca terör eylemleri belirlenerek terörizm tanımı yapılmaktan kaçınılmıştır.[5] Bu durumun sebebi olarak devletlerin siyasal sistem, ideoloji ve siyasi çıkarlarının farklılık göstermesi, savaş ve terörizm kavramlarının ayrıştırılmaması,

---

[3] *TeMK Madde 1: Terör; cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir*.

[4] Ahmet Caner Yenidünya, Olgun Değirmenci, *Mukayeseli Hukuk ve Türk Hukukunda Terörizmin Finansmanı Suçu, Ord. Prof. Dr. Sulhi Dönmezer Armağanı*, (Ankara: Türk Ceza Hukuku Derneği ve Atatürk Araştırma Merkezi Yayını, 2008), 5.

[5] Turinay, "Ceza," 42.

self determinasyon hakkı ile ulusal kurtuluş savaşlarının yapılmış ve yapılacak olması gösterilmektedir.[6]

Terör örgütlerinin, benimsedikleri ideolojinin yayılması, devletin ve toplumun zarar görmesi veya devlete veya topluma gözdağı vermek veya onları korkutmak amacıyla faaliyetlerde bulunmaları için mali olarak desteklenmeleri gerekmektedir. Finansal kaynak olmaksızın örgüt üyelerinin toplanmaları, barındırılmaları, eğitilmeleri ve eylem yapılacak yerlere ulaştırılmaları sekteye uğrayabilir, örgütün devamlılığı tehlikeye düşebilir.[7] Bu nedenle terör örgütlerinin asıl amaçları bir gelir elde etmek olmasa da eylemlerinin ve ideolojilerinin devamlılığını sağlayarak örgütün varlığını devam ettirmek üzere finans kaynakları edinmek zorundadırlar.

Her ne kadar uluslararası alanda kabul görmüş bir terör veya terör örgütü kavramı bulunmasa da ülkeler iç hukuk düzenlemeleriyle terör örgütü kabul ettikleri örgütlerin mali kaynaklarını kesmeyi, böylelikle terörizmle etkin bir şekilde mücadele etmeyi amaçlamaktadırlar. Türkiye de bu amaçla 6415 sayılı Terörizmin Finansmanının Önlenmesi Hakkında Kanun[8] **(Kanun)** ile terörizmin finansmanı suçunu ve bu suç kapsamında malvarlığının dondurulması usulünü düzenlemiştir.

Kanun, 3.maddesinde yasakladığı fon sağlama ve toplama fiillerinin bir terörist veya bir terör örgütüyle ilişkilendirilmesini daha ağır cezayı gerektiren başka bir suçu oluşturmaması

---

6 Mehmet Akça, "Terörizmin Kendine Özgü (Suı Generis) Niteliği: Kavramı Tanımlamada Metodoloji Sorunu, *İstanbul Barosu Dergisi 88*, no. 1 (2014): 32-33.

7 Yenidünya, Değirmenci, "Mukayeseli," 7; Deniz Turan, Eser Gemici; "Terörizmin Finansman Kaynakları ve Karapara Aklamanın Terörizmin Finansmanındaki Rolü", *Anadolu Üniversitesi Sosyal Bilimler Dergisi* 20, no. 2 (2020): 263.

8 RG. 16.02.2013, S. 28561.

halinde suç olarak kabul etmektedir. Kanun ile BM'nin 1999 tarihli Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşmenin[9] **(Sözleşme)** ve Güvenlik Konseyinin bu kapsamındaki kararlarının uygulanması da amaçlamaktadır. 9 Aralık 1999 tarihinde Genel Kurul tarafından kabul edilen Sözleşmeye, 2000 yılında imzaya açılmasının ardından 189 ülke taraf olmuştur.[10] Türkiye de 27 Eylül 2001'de imzaladığı Sözleşmeyi 10 Ocak 2002 tarih ve 4738 sayılı Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşmenin Onaylanmasının Uygun Bulunduğu Hakkında Kanun[11] ile iç hukukuna dahil etmiştir.

B. Suçla Korunan Hukuki Değer

Failin gerçekleştirdiği eylem ile ihlal ettiği hukuki varlık veya menfaat suçla korunan hukuki değeri oluşturmaktadır.[12] Terörizmin finansmanı suçu ile terör örgütüne maddi kazanç sağlayan eylemler engellenerek örgütün zayıflatılması, terör eylemlerinin engellemesi ve toplumun mal ve can güvenliğinin

---

9 International Convention for the Suppression of the Financing of Terrorism (New York, 9 December 1999), erişim tarihi: Nisan 12, 2022; https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf, Sözleşmenin Türkçe Metni için bkz. erişim tarihi: Nisan 12, 2022, https://diabgm.adalet.gov.tr/arsiv/adli_yardimlasma/adli_isbirligi_ceza/suclularin_iadesi_ek/terorizmin_finansmanının_önlenmesine_ilişkin%20BM%20sözlesmesi.pdf,

10 Sözleşmeye taraf ülkelerin isimleri ve beyannameleri için bkz. erişim tarihi: Nisan 12, 2022, https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&clang=_en#EndDec.

11 RG. 17.01.2002, S. 24643.

12 İzzet Özgenç, *Türk Ceza Hukuku Genel Hükümler*, (Ankara: Seçkin Yayıncılık, 2021), 220.

sağlanması amaçlanmaktadır.[13] Terör eylemleri ile devletin siyasi, sosyal, askeri ve ekonomik düzeni, güvenilirliği zarar görmektedir. Bu bakımdan teröre sağlanan mali desteğin kesilmesi ile kamu düzeninin ve güvenliğinin de korunan hukuki değer olduğunu söylemek mümkündür.[14]

Bu bakımından terörizmin finansmanı suçunda birden çok korunan hukuki değer vardır. Hem devletin anayasal düzeni hem de bireylerin anayasal hak ve hürriyetleri kapsamında devletin bütünlüğü, güvenliği, birliği, toplumun düzeni, güvenliği ve bireylerin hukuki güvenliği suçla korunan hukuki değeri oluşturmaktadır.[15]

C. Suçun Maddi Unsurları

1. Suçun Maddi Konusu

Suçun maddi konusunu failin eylemlerinin yöneldiği kişi veya şey oluşturmaktadır. Fail suçu işleyerek suçun konusuna zarar vermekte veya suçun konusunu tehlikeye maruz bırakmaktadır.[16] Terörizmin finansmanı suçunda suçu oluşturan fon sağlama veya fon toplama eylemleri fon üzerinde gerçekleştirildiği için suçun maddi konusunu da "fon" oluşturmaktadır.[17]

Kanunda terör örgütlerinin finansal kaynağını tanımlamak üzere "fon" kavramı kullanılmıştır ve "*para, değeri para ile temsil edilebilen taşınır veya taşınmaz, maddi veya gayri maddi her türlü mal, hak, alacak ile bunları temsil eden her türlü belge"* olarak

---

[13] Ümit Kocasakal, *Terörizmin Finansmanı –18. Uluslararası Ceza Hukuku Kongresi*, (İstanbul: Türk Ceza Hukuku Derneği Yayınları, 2009), 134.

[14] Yeşim Yılmaz, "Terörizmin Finansmanı Suçu", *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 3*, no. 3 (2020); 209.

[15] Gödekli, *Terörizmin, 290.*

[16] Özgenç, *Türk*, 220.

[17] Ersan Şen ve H. Sefa Eryıldız, *Suç Örgütü*, (Ankara: Seçkin Yayıncılık, 2022), 570.

tanımlanmıştır. Sözleşme ise Kanundan daha geniş bir tanıma yer vererek her türlü kıymeti ve bu kıymetlerin üzerindeki mülkiyet hakkı veya çıkarı kanıtlayan, elektronik veya dijital şekilleri de fon kavramına dahil etmiştir ve bu tanımı sınırlayıcı tutmamıştır.[18] Her iki tanımda da fon kavramı için belirleyici olan fonun "para ile ölçülebilir" niteliğine sahip olmasıdır.[19]

Fonun yasal yollardan hukuka uygun olarak elde edilmesi veya hukuka aykırı olarak haksız bir şekilde ele geçirilmiş olması önemli değildir, her halükarda fon tanımına dahil olabilecek niteliğe sahip meşru veya gayrimeşru her şey suçun maddi konusunu oluşturacaktır.[20]

2. Fail ve Mağdur

Faile göre bir özellik göstermeyen terörizmin finansmanı suçu herkes tarafından işlenebilen bir suçtur. Kanunun 4. maddesinde de "*…fon sağlayan veya toplayan kişi…*" şeklinde düzenlenme yapılmıştır. "*Kişi*" kelimesi gerçek kişi olarak algılanmalı ve yalnızca gerçek kişilerin fail olabileceği kabul edilmelidir. Zira TCK'nın 20. maddesine göre ceza sorumluluğu şahsidir.

Suçun tüzel kişiliğin faaliyeti çerçevesinde veya bir özel hukuk tüzel kişisi yararına işlenmiş olması halinde yine TCK'nın 20/2. maddesi gereğince tüzel kişi hakkında cezaya hükmolunamayacaktır. Bu halde Kanun'un 4/4. maddesinin

---

[18] *TFÖDUS Madde 1/1: "Fon" her ne suretle edinilmiş olursa olsun, maddi veya gayri maddi, menkul veya gayrimenkul, her türlü kıymeti ve bu kıymetler üzerinde bir mülkiyet hakkı veya çıkarı kanıtlayan, elektronik veya dijital şekilleri dahil olmak üzere, her türlü görünüşteki belge ve yasal araçları ve bu çerçevede banka kredilerini, seyahat çeklerini, para havalelerini, hisse senetlerini, teminatları, tahvilleri, kredi mektuplarını, işbu tadat sınırlayıcı olmaksızın kapsar.*

[19] Gödekli, *Terörizmin*, 306; Şen, Eryıldız, *Suç*, 571.

[20] Kocasakal, *Terörizmin*, *136.*

yollamasıyla tüzel kişilik hakkında TCK'nın 60. maddesinde sayılan güvenlik tedbirlerine hükmolunacaktır.[21]

Failin hem örgüt üyesi veya mensubu olup hem de örgüte finans sağlaması halinde failin finans sağlama eylemlerinin örgüt faaliyeti çerçevesinde değerlendirilmesi ve örgüt kuruculuğundan veya üyeliğinden cezalandırılması gerekmektedir. Yargıtay Ceza Genel Kurulu kararında da terörizmin finansmanı suçunun silahlı terör örgütüne yardım suçunun özel bir hali olduğuna dikkat çekilerek genel uygulama örgüt kurucusu, yöneticisi veya mensubu olmayan tüm gerçek kişilerin finansman suçunun faili olabileceği yönündedir.[22]

Terörizmin finansmanı suçu, toplum düzenine karşı işlenen bir suç olduğu için suçun mağduru terör örgütünün doğrudan hedef aldığı ve fonun sağlandığı ülkede yaşayan herkestir. Ayrıca terör eylemleri sonucunda doğrudan hakları ihlal edilen kişiler de mağdur olmaktadır.[23] Modern ceza hukuku yorumuna göre devlet mağdur olarak kabul edilmeyecektir. Devlet tüzel kişiliği, uluslararası toplum ve tüzel kişiliğe haiz uluslararası kuruluşlar suçtan zarar gören olacaklardır.[24]

---

21 *TeMK Madde 4/4: Suçun bir tüzel kişinin faaliyeti çerçevesinde işlenmesi hâlinde, bunlara özgü güvenlik tedbirlerine hükmolunur*

TCK Madde 60- (1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkûmiyet halinde, iznin iptaline karar verilir.

(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.

(3) Yukarıdaki fıkralar hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebilir.

(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır.

22 Yar. CGK., 13.2.2018, 2017/9-692 E., 2018/41 K.

23 Yılmaz, "Terörizmin," 215.

24 Gödekli, *Terörizmin*, *306.*

3. Fiil ve Netice

Sözleşme 2. maddesinde sayılan eylemlerin gerçekleştirilmesi için dolaylı veya doğrudan, hukuka aykırı olarak ve isteyerek fon sağlanmasını veya toplanmasını yasaklamakta,[25] 4. maddesi ile de bu kişilerin cezalandırılması için taraf devletlere sayılan eylemleri iç hukuklarında suç olarak düzenlemeleri yükümlülüğü getirmektedir.

Bu yükümlülüğe uygun olarak Türkiye, Sözleşmenin 2/1) a maddesi gereğince ek kısmında atıf yapılan sözleşmeleri[26]

---

[25] *TFÖDUS Madde 2: Herhangi bir kişi, her ne suretle olursa olsun, tümüyle veya kısmen, aşağıda tadat edilen eylemlerin gerçekleştirilmesinde kullanılması niyetiyle veya kullanılacağını bilerek, doğrudan veya dolaylı olarak, yasa dışı bir şekilde ve kasten, fon sağlamakta veya toplamakta ise, bu Sözleşmeyi ihlal eder:*

a) Ekte tadat olunan antlaşmaların herhangi biri kapsamında ve vazettiği tanım çerçevesinde suç teşkil eden eylem,

*b) Niteliği veya kapsamı itibariyle, bir halkı korkutmak, ya da bir hükümeti veya uluslararası örgütü herhangi bir eylemi gerçekleştirmeye veya gerçekleştirmekten kaçınmaya zorlamak amacını gütmesi halinde, bir sivilin ya da bir **silahlı çatışma durumunda** muhasemata doğrudan katılmayan herhangi başka bir kişiyi öldürmeye veya ağır şekilde yaralamaya yönelik diğer tüm eylemler.*

[26] *1. Uçakların Yasadışı Ele Geçirilmesinin Önlenmesi Sözleşmesi (16 Aralık 1970, Lahey)- ICAO*

2. Sivil Havacılık Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesi Sözleşmesi (23 Eylül 1971, Montreal)- ICAO

3. Diplomatik Ajanlar Dahil Uluslararası Korunan Kişilere Karşı Suçların Önlenmesi ve Cezalandırılması Sözleşmesi (14 Aralık 1973, New York)- BMGK

4. Rehin Almalara Karşı Uluslararası Sözleşme (17 Aralık 1979, New York)- BMGK

5. Nükleer Maddelerin Fiziki Korunması Sözleşmesi (3 Mart 1980, Viyana)

6. Uluslararası Sivil Havacılığa Hizmet veren Havalimanlarında Yasadışı Şiddet Eylemlerinin Önlenmesi Protokolü¨, Sivil Havacılık Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesi Sözleşmesine Ek Protokol (24 Şubat 1988, Montreal)- ICAO,

7. Denizcilik Seferyollarının Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesi Sözleşmesi (10 Mart 1988, Roma)- IMO,

Kanunun 3. maddesiyle aynen tatbik etmiş ve bu sözleşmelerde yasaklanan ve suç sayılan fiillerin gerçekleştirilmesi amacıyla fon sağlanmasını veya toplanmasını suç olarak kabul etmiştir. Ayrıca Türkiye, Sözleşmeyi imzalarken 2/1) b maddesine göre "silahlı çatışma" durumunu suçun unsuru olarak kabul etmediğini, silahlı çatışma kavramının ceza hukuku kapsamında farklı bir durumu betimlediğini beyan etmiştir.[27]

Bu beyanın sonucu olarak; silahlı çatışmanın varlığı aramaksızın herhangi bir eylemi gerçekleştirmesi veya bundan kaçınması için bir hükümeti veya kuruluşu zorlamak, ya da bir halkı korkutmak, sindirmek için kasten öldürme veya ağır yaralama fiillerinin işlenmesi amacıyla fon sağlanması veya toplanması 3. madde kapsamında suç olarak düzenlenmiştir.[28] Kanun koyucu, Sözleşmeden farklı olarak 3713 sayılı Terörle Mücadele Kanunu'nda[29] terör suçu olarak sayılan fiillerin gerçekleştirilmesi amacıyla fon sağlanmasını veya toplanmasını da suç olarak Kanun kapsamına dahil etmiştir.

Fon sağlamak terör örgütünün finansmanında kullanılacak fonun fail tarafından temin edilmesi iken fon toplanması fonun

---

8. Kıta Sahanlığında Kurulu Sabit Platformların Güvenliğine Karşı Yasadışı Eylemlerin Önlenmesi Hakkında Protokol (10 Mart 1988, Roma)-IMO,

9. Terörist Bombalamaların Önlenmesi Sözleşmesi (15 Aralık 1997, New York)-BMGK

[27] *Türkiye Cumhuriyeti, Sözleşmenin 2nci maddesinin 1(b) paragrafının uygulanmasının bir silahlı çatışmanın varlığına işaret etmeyeceğini, silahlı çatışma tabirinin, örgütlü¨ bir biçimde olsun veya olmasın, ceza hukuku kapsamında terörizm suçunu oluşturan fiillerin işlenmesinden farklı olan bir durumu betimlediğini beyan eder.*

[28] *TFÖHK Madde3: (1) Aşağıda sayılan fiillerin gerçekleştirilmesi amacıyla fon sağlanması veya toplanması yasaktır:*

a) Bir halkı korkutmak veya sindirmek ya da bir hükümeti veya uluslararası kuruluşu herhangi bir eylemi gerçekleştirmeye veya gerçekleştirmekten kaçınmaya zorlamak amacıyla, kasten öldürme veya ağır yaralama fiilleri.

[29] RG. 12.04.1991, S.20843.

aynı amaçla üçüncü kişilerden sağlanmasıdır.[30] Üçüncü kişilerin finansman amacıyla fonun toplandığını bilip bilmemeleri toplama fiilini gerçekleştiren failin cezalandırılabilirliği bakımından önem arz etmemektedir. Üçüncü kişinin finansman amacını bilmesi halinde fon sağlamak eylemi bakımından cezai sorumluluğu doğacaktır. Her iki halde de yasal dayanağı olan parasal değerin veya yasadışı yollarla veya bir suç kapsamında temin edilen parasal değerin fon olarak kullanılması mümkündür.[31] Sırf hareket suçu olan finansman suçu fon sağlandığı ya da toplandığı anda gerçekleşmiş olur. Fonun örgütünün eline geçmesi veya örgüt tarafından kullanılması gerekmemektedir.[32] Bu hususta Kanunun 4/3 maddesinde fonun bir suçun işlenmesinde kullanılmasının aranmadığı düzenlenmiştir.[33]

D. Suçun Manevi Unsuru

Kanunun 4. maddesiyle failin *"…teröriste veya terör örgütlerine…"* fon sağlaması veya toplaması eylemlerini cezalandırmıştır. O halde failin örgüte finans sağladığı halde örgütün, yukarıda açıklandığı üzere TeMK'nın 1.maddesinde sayılan amaçları taşıyan bir terör örgütü olduğunu bilmesi gerekmektedir. Failin gerçek bir kişiye fon sağlaması veya toplaması halinde ise gerçek kişinin bir terörist olduğunu bilmesi gerekecektir. Terör suçlusu, TeMK 1'deki terör eylemlerini tek başına veya başkalarıyla gerçekleştiren ya da bu amaçları gerçekleştirmek amacıyla kurulan terör örgütüne

---

30 Nurullah Bodur ve Eshat Özkul, *Uygulamada Terör Örgütü ve Terör Suçları*, (Ankara: Seçkin Yayıncılık, 2022), 237-238.

31 Şen ve Eryıldız, *Suç*, 571.

32 Yenidünya ve Değirmenci, "Mukayeseli," 21.

33 *TFÖHK Madde 4/3: Birinci fıkra hükmüne göre ceza verilebilmesi için fonun bir suçun işlenmesinde kullanılmış olması şartı aranmaz.*

mensup kişi olarak tanımlanmıştır.[34] Düzenlemeye göre yalnızca terör örgütüne üye olmakla, örgüte üye olmadan örgüt adına suç işlemekle veya hem örgüte üye olup hem de örgüt adına suç işlemekle terör suçlusu olunabilecektir.

Failin fon sağlarken veya toplarken *"…tümüyle veya kısmen kullanılması amacıyla veya kullanılacağını bilerek ve isteyerek belli bir fiille ilişkilendirilmeden dahi…"* hareket etmesi aranmıştır. Buna göre failin fonu sağladığı veya topladığı anda suç konusu fonun terör örgütünü finanse etmek amacıyla sağlandığını veya toplandığını bilmesi ve istemesi gerekmektedir. Bu bakımdan finansman suçu doğrudan kastla işlenebilecek bir suçtur.

Failin Kanunun 3. maddesindeki yasak eylemleri gerçekleştirdiği sırada bilme manevi unsurunu taşımadığı yani sağlanan veya toplanan fonun terör örgütünü finanse etme amacıyla kullanılacağını bilmemesi durumunda doğrudan kastı bulunmayan fail bakımından suç oluşmayacaktır.[35]

Kanun, 3.maddesiyle *"aşağıdaki fiillerin gerçekleştirilmesi amacıyla fon sağlanması veya toplanması yasaktır"* düzenlemesi ile finansman suçunu oluşturan eylemleri sınırlı olarak saydığı için failin ayrıca bu eylemlerin gerçekleşmesi amacını da taşıyan özel kastla hareket etmesi gerekmektedir. Failin 3.maddede yasaklanan terör eylemlerini gerçekleştirmek dışında başka amaçlarla fon toplaması veya sağlaması durumunda özel kastı bulunmayan failin finansman suçunda sorumluluğu gündeme gelmeyecektir.[36] Ancak sağlanan fona göre failin TCK m. 220/7

---

[34] *TeMK Madde 2: Birinci maddede belirlenen amaçlara ulaşmak için meydana getirilmiş örgütlerin mensubu olup da bu amaçlar doğrultusunda diğerleri ile beraber veya tek başına suç işleyen veya amaçlanan suçu işlemese dahi örgütlerin mensubu olan kişi terör suçlusudur. Terör örgütüne mensup olmasa dahi örgüt adına suç işleyenler de terör suçlusu sayılır.*

[35] Engin Akın, *Terörizmin Finansmanı Suçu*, (Ankara: Adalet Yayınevi, 2009), 402.

[36] Gödekli, *Terörizmin*, 319.

gereğince terör örgütüne yardım suçundan veya TCK m. 315 gereğince silahlı terör örgütüne silah sağlama suçundan sorumluluğu gündeme gelebilecektir.[37]

TCK'nın 22. maddesi gereğince terörizmin finansmanı suçunun ayrıca taksirli hali düzenlenmediği için failin taksirle hareket ettiği hallerde suç oluşmayacaktır. Örneğin terör örgütünün adının gizlenerek fon toplandığı hallerde kendisinden fon sağlanan 3. kişinin terör örgütü adına fon toplandığını öngörmesi kendisinden beklenemeyecek ise bu durumunda kastı bulunmayan 3. kişi hakkında suç oluşmayacaktır.[38]

E. Teşebbüs

Suçun oluşması için failin fon sağlaması veya toplaması eylemlerini gerçekleştirmesi yeterli olduğu için bu eylemlerin süreklilik arz etmesi gerekmemektedir. Bu yönüyle suçun neticesi harekete bitişik-sırf hareket suçu olarak kabul edilmesi gerekmektedir. Sırf hareket suçlarında suçu oluşturan icrai hareketlerin bölünebiliyor olması halinde suça teşebbüs olmaktadır.[39]

Terörizmin finansmanı suçunda failin fon toplamak üzere kişilerle iletişime geçerek icrai hareketlere başladığı ancak elinde olmayan sebeplerle fonları temin edemediği hallerde suç teşebbüs aşamasında kalmış olacaktır. Örneğin bağış, yardım veya etkinlik gibi hukuka uygun bir görünüm altında veya doğrudan örgüt adına mağdurlara para konulacak zarf dağıtıdığı ancak bu zarfların geri toplanmadan failin yakalandığı olayda suç teşebbüs aşamasında kalmış olacaktır.[40] Bu halde failin cezası TCK m. 35 gereğince indirim yapılarak belirlenecektir. Ancak bu durumda somut olaya göre failin

---

37 Şen ve Eryıldız, *Suç*, 578.

38 Gödekli, *Terörizmin*, 316-317.

39 Yılmaz, "Terörizmin," 239.

40 Bodur ve Özkul, *Uygulamada*, 240.

hareketlerinin icra hareketi seviyesine ulaşıp ulaşmadığının değerlendirilmesinin iyi yapılması gerekmektedir. Eğer failin eylemleri hazırlık hareketleri kapsamında kalmış ise artık teşebbüsten bahsedilemeyecek ve fail finansman suçundan cezalandırılamayacaktır.

F. İştirak

Suça iştirak edilmesi bakımından bir özellik arz etmeyen terörizmin finansmanı suçu bakımından TCK'nın 37 ila 39. maddelerine göre değerlendirme yapılması gerekmektedir.

Müşterek faillik bakımından, faillerin birden çok olması, her failin terör örgütünü finanse etme amacını bilerek veya isteyerek fon sağlaması veya toplaması, faillerin terörizmin finansmanı suçunun işlenmesi hususunda anlaşmaları ve fiil üzerinde ortak hakimiyet kurmuş olmaları gerekmektedir.

Her ne kadar Kanunda dolaylı olarak finans eylemlerine katılmış olmak suç kapsamında düzenlenmemiş ise de şeriklik hükümleri kapsamında bu durum mümkündür.[41] Şeriklik için yardım edenlerin bizzat fon sağlama veya toplama eylemleri gerçekleştirmeseler de fonların sağlanması toplanması veya örgüte iletimi hususunda davranışlarda bulunması ve bu davranışların suçla nedensel bir bağa sahip olması gerekmektedir.[42]

Yargıtay, kişinin terör örgütüne iletilmek üzere yurtdışından kendi banka hesabına gelen parayı çekerek örgüte ileten kişiyi bir kararında parayı gönderen ile müşterek fail olarak değerlendirmişken[43] bir kararında suça iştirak olarak[44] kabul etmiştir. Failin sorumluluğunu belirlemek için somut

---

41 Zeki Yıldırım, *Türk Hukukunda Terörizmin Finansmanı Suçu ve Malvarlıklarını Dondurma*, (Ankara: Adalet Yayınevi, 2013), 95.

42 Gödekli, *Terörizmin*, 325.

43 Yar. 9. CD, 2012/6766 E., 2013/12505 K., 11.10.2013.

44 Yar. 9. CD, 2014/5464 E., 2014/12447 K., 22.12.2014.

olaya göre suç üzerinde ortak hakimiyetinin bulunup bulunmadığı veya suça etkisinin nedensel bir katkı seviyesinde olup olmadığının değerlendirilmesi gerekmektedir.[45]

G. İçtima

Kanunun 4. maddesiyle fon sağlama veya toplama eylemlerinin *daha ağır cezayı gerektiren başka bir suçu oluşturmaması* halinde madde kapsamında cezalandırılabileceği düzenlenerek suç tali norm olarak ihdas edilmiştir.[46] Bu düzenleme ile Kanun koyucu finans suçunu oluşturan eylemin aynı zamanda başka bir suçu oluşturabileceğini ve bu halde TCK 44. maddesi gereğince fikri içtima hükümlerinin uygulanmasının gerekebileceğini öngörmektedir.[47] Bu bakımdan failin fon toplama veya sağlama eylemlerinin finansman suçunu oluşturup oluşturmadığının denetiminin yapılması büyük önem arz etmektedir.

Terörizmin finansmanı suçu bakımından gerçek içtima kuralları geçerli olabilmektedir. Terör örgütünün finanse edilmesi için gerekli olan fonun sağlanması için öncü başka bir suçun işlenmesi halinde fail her iki suçtan da ayrı ayrı sorumlu olacaktır. Örneğin uyuşturucu ve uyarı madde ticareti, insan ticareti, hırsızlık, zimmet gibi maddi kazanç sağlayan suçların öncü suç olarak işlenmesi halinde fail hakkında iki farklı iddianame düzenlenerek iki farklı dava açılması gerekmektedir.

Failin sağladığı veya topladığı fonun getirisi ile örgütün bir suç işlemesi halinde, örneğin bomba teçhizatı alınarak bombalı eylem yapılması halinde, nedensellik bağı ve objektif isnadiyet

---

45 Yılmaz, "Terörizmin," 243.

46 Soner Hamza Çetin "Terörizmin Finansmanı Suçu", *Ceza Hukuku Dergisi* 11, no. 31 (2016): 154; Yılmaz, "Terörizmin," 246.

47 Şen ve Eryılmaz, *Suç*, 572.

teorileri gereğince finansman suçunun failinin işlenen bombalı saldırı eyleminden bir sorumluluğu doğmayacaktır.[48]

H. Yaptırım ve Muhakeme

Beş yıldan on yıla kadar hapis cezası öngören suç resen soruşturulan ve kovuşturulan suçlardan olup 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 12. maddesine göre ağır ceza mahkemeleri görevlidir.[49]

Ancak Kanunun 4/5. maddesine[50] göre suçun yabancı devlet veya uluslararası bir kuruluş aleyhine işlenmesi halinde Adalet Bakanının talebi üzerine soruşturma ve kovuşturma yapılabilmektedir. Kanunda geçen "talep" kelimesinin izin olarak algılanmaması gerekmektedir. Zira izin savcılık makamının soruşturma yapmak üzere Adalet Bakanının iznini istemesi iken talep Adalet Bakanının soruşturma yapılması için savcılık makamına başvurması anlamına gelmektedir.[51] Suçun aynı zamanda Türkiye Cumhuriyeti Devleti aleyhine işlenmesi

---

48 Gödekli, *Terörizmin, 329.*

49 *AYİDMBAMKGYHK Madde 12: "Kanunların ayrıca görevli kıldığı haller saklı kalmak üzere, Türk Ceza Kanununda yer alan yağma (m. 148), irtikap (m. 250/1 ve 2), resmi belgede sahtecilik (m. 204/2), nitelikli dolandırıcılık (m. 158), hileli iflas (m. 161) suçları, Türk Ceza Kanununun İkinci Kitap Dördüncü Kısmının Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar (318, 319, 324, 325 ve 332 nci maddeler hariç) ve 12/4/1991 tarihli ve 3713 sayılı Terörle Mücadele Kanununun kapsamına giren suçlar dolayısıyla açılan davalar ile ağırlaştırılmış müebbet hapis, müebbet hapis ve on yıldan fazla hapis cezalarını gerektiren suçlarla ilgili dava ve işlere bakmakla ağır ceza mahkemeleri görevlidir. Anayasa Mahkemesi ve Yargıtay'ın yargılayacağı kişilere ilişkin hükümler, askerî mahkemelerin görevlerine ilişkin hükümler ile çocuklara özgü kovuşturma hükümleri saklıdır."*

50 *TFÖHK Madde 4/5: Suçun, yabancı bir devlet veya uluslararası bir kuruluş aleyhine işlenmesi hâlinde, soruşturma ve kovuşturma yapılması Adalet Bakanının talebine bağlıdır.*

51 Yılmaz, "Terörizmin," 256.

halinde ise artık Bakanının talebine gerek kalmayacak, suç resen soruşturulacaktır.[52]

Suçun soruşturulması ve kovuşturulması kapsamında Kanunun 4/7. maddesi gereğince şartlarının varlığı halinde kayyım tayini (CMK m. 133), iletişimin tespiti, dinlenmesi ve kayda alınması (CMK m.135), gizli soruşturmacı (CMK m. 139) ve teknik araçlarla izleme (CMK m.140) koruma tedbirlerine başvurulabilecektir.

İ. Terör Örgütüne Yardım Sağlama Suçu ile Karşılaştırılması

Terör örgütüne yardım suçu TCK'nın 220/7. maddesinde örgütün hiyerarşik yapısına dahil olmadan örgüte *bilerek ve isteyerek* yardım eden kişilerin cezalandırılması öngören genel yardım suçu olarak düzenlenmektedir.[53] Bu bakımdan failin örgütün suç örgütü olduğu veya yardım ettiği kişilerin örgüt üyesi olduğu hususunu bilmesi, dolayısıyla bu suç bakımından doğrudan kastla hareket etmesi gerekmektedir.[54]

Kanun koyucu genel yardım suçuyla *örgüt kurucusu, yöneticisi veya üyesi olmayan* ancak bilerek ve isteyerek terör örgütüne yadım eden kişilerin yardım eylemlerinin cezalandırılmasını amaçlamıştır.[55] Yardım eden failin aynı zamanda yardım ettiği örgütün kurucusu, yöneticisi veya üyesi olması halinde ise TCK 220/1-2. maddeleri gereğince terör örgütü kurma, yönetme veya örgüte üye olma suçlarından sorumluluğu doğacaktır. Örgütün silahlı olması halinde ise fail

---

52 Çetin, "Terörizmin," 159.

53 *TCK 220/7: Örgüt içindeki hiyerarşik yapıya dahil olmamakla birlikte, örgüte bilerek ve isteyerek yardım eden kişi, örgüt üyesi olarak cezalandırılır. Örgüt üyeliğinden dolayı verilecek ceza, yapılan yardımın niteliğine göre üçte birine kadar indirilebilir.*

54 Yar. CGK., E. 2018/437, K. 2019/203, 12.03.2009.

55 Bodur ve Özkul, *Uygulamada*, 139.

hakkında TCK 314/1-2. maddelerinin uygulanması gerekecektir.[56]

Yardım; örgüte üye sağlamak, örgütün amaçlarını gerçekleştirmesi için plan ve program sağlamak veya yol ve yöntem göstermek,[57] maddi bir değer sağlamak veya malzeme ve araç-gereç temin etmek, üyeleri saklama, üyelere yemek yedirmek veya belli konularda bilgi vermek gibi eylemler olabilmektedir.[58] Kanun, 7. maddenin ikinci cümlesi ile sağlanan yardımın niteliğine göre hakime vereceği cezada üçte birine kadar indirim yapma hususunda takdir hakkı da vermektedir.

Yargıtay 16. Ceza Dairesince örgüt mensuplarını evinde barındırma, diş tedavilerini sağlama,[59] gıda malzemesi sağlama, şoförlük yapma, bilgi aktarma,[60] sınırdan geçmelerine yardım etme,[61] örgüt üyeleri arasında kuryelik yapma, örgüt bildirilerini dağıtmak, örgüte ait malzemeleri muhafaza etme[62] eylemleri örgüte yardım etme suçu kapsamında değerlendirilmiştir.

Sağlanan yardımın maddi bir değer taşıması halinde ise failin yardım suçundan mı yoksa finansman suçundan mı ya da her iki suçtan mı sorumlu olacağı sorusu gündeme gelecektir. Kanunun, fon sağlama veya toplama eylemlerini daha ağır cezayı gerektiren başka bir suçu oluşturmaması halinde finansman suçu olarak kabul etmesi, finansman suçunun özel norm, TCK'nın 220/7. maddesinde düzenlenen yardım suçunun ise genel norm olduğunu göstermektedir.[63] Ayrıca 5 ila 10 yıl hapis cezası öngören finansman suçunun 2 ila 4 yıl hapis cezası

---

56 İzzet Özgenç, *Suç Örgütleri*, (Ankara: Seçkin Yayıncılık, 2022), 53.

57 Şen ve Eryıldız, *Suç*, 571.

58 Özgenç, *Suç*, 49.

59 Yar. 16. CD, E. 2019/2837, K.2020/1306, 13.02.2020.

60 Yar. 16. CD, E. 2020/1306, K.2020/2410, 08.06.2020.

61 Yar. 16. CD, E. 2020/1314, K.2020/2141, 01.06.2020.

62 Mikael Lyngbo, Feridun Yenisey, Namık Kemal Topçu, Önder Tozman, Kemal Şahin, Örgütlü Suçlar ve Terör Suçları Eğitim Modülü; 162.

63 Bodur ve Özkul, *Uygulamada*, 235.

öngören genel yardım suçundan daha fazla hapis cezasını öngörmesi de bu halde somut olayda öncelikle finansman suçunun oluşup oluşmadığının değerlendirilmesi gerektiğini göstermektedir. Değerlendirilme yapılırken failin bu suç bakımından hem doğrudan hem de özel kastla hareket edip etmediği tespit edilmeye çalışılacaktır. Zira yukarıda açıklandığı üzere Kanun, finansman suçu için failin finans sağladığı örgütün 3. maddede sayılan yasak eylemleri gerçekleştirmek amacıyla hareket ettiğini bilmesini yani bu hususta özel kastla hareket etmesini aramaktadır. Değerlendirme sonucunda failin özel kastının bulunmadığı sonucuna varıldığı hallerde artık finansman suçu oluşmayacak, failin genel kastla işlenen yardım suçundan sorumluluğu gündeme gelecektir.[64]

Yargıtay Ceza Genel Kurulu'nun kararına göre belli aralıklarla örgüt mensuplarına ekmek, un, tereyağı, şeker, çay, peynir, bulgur, deterjan gibi yaşam malzemelerinin, koyun, kitap, dijital kamera gibi eşyaların ve bir kere 3000 TL paranın temin edilmesi eylemleri sağlanan malzemelerin niteliğine göre fon kavramı kapsamına değerlendirilerek eylemin terörizmin finansmanı suçunu oluşturduğu kabul edilmiştir.[65]

---

64 Gödekli, *Terörizmin*, 319.

65 Yar. CGK, E.2017/692, K. 2018/41, 13.02.2018: …*PKK silahlı terör örgütünün varlığını koruması, 6415 sayılı Kanun'un 3. maddesinde fon sağlanması veya toplanması yasaklanan fiilleri gerçekleştirebilmesi ve bu hususta örgütsel faaliyetlerini sürdürülebilmesi amaçlarına uygun olarak, örgütün kırsalda faaliyet gösteren mensuplarına, sanıklardan ...'nin 2009 yılı bahar aylarında iki kez ekmek ile diğer erzak ve yaşam malzemesi, sanık ...'ın 2009 yılı Mayıs ayında un, tereyağı, şeker, çay ve ekmek, 2010 yılı Nisan ayında on kg un, 3-4 kg peynir, dört kg bulgur ve deterjan gibi erzak ve yaşam malzemesi, sanık ...'ün de 2009 yılına kadar yiyecek, koyun, kitap ile iki adet dijital kamera ve 3.000 TL temin ettiği olayda; sanıklar tarafından temin edilen para ve diğer eşyanın niteliği itibarıyla 6415 sayılı Kanun'un 2. maddesinin (c) bendinde tanımlanan "fon" kapsamında olduğu, dolayısıyla sanıkların terör örgütü mensuplarına fon sağlamaları şeklinde gerçekleşen eylemlerinin, aynı Kanun'un 4. maddesinde düzenlenen terörizmin finansmanı suçunu oluşturduğunun kabulü gerekmektedir.*

Failin silah, roketatar veya bomba gibi mühimmat yardımında bulunması halinde de genel yardım suçuna göre özel norm niteliğinde olan finansman ve silah yardımı suçları değerlendirilecek ve 10 ila 15 yıl hapis cezası öngören, ceza miktarı bakımından daha ağır cezayı gerektiren silahlı yardım suçunun oluştuğu kabul edilecektir.[66]

II. BLOKZİNCİR SİSTEMİ VE KRİPTO PARALAR

İlk olarak 2009 yılında Bitcoin ile gündeme gelen kripto paralar gün geçtikçe çeşitlenmekte ve birçok farklı alanda kullanılmaktadır. Bitcoin dışındaki kripto paralar altcoin olarak adlandırılmakta ve şu an 18.847 adet kripto para birimi bulunmaktadır.[67] Ethereum, Tether, Binance Coin, USD Coin, XRP gibi her birinin kendi blokzincir sistemlerini kullandıkları altcoinlerin kaç adet üretilebilecekleri kuruluş aşamasında belirlenmektedir. 21 milyon adet üretilmek üzere sınırlandırılmış olan Bitcoin'in ve diğer altcoinlerin altın gibi sınırlı sayıda olmaları kripto paraları maddi olarak değerli kılmaktadır.[68]

Aslında kripto paralardan çok daha önce, David Chaum tarafından 1982 yılında merkezi otoriteye bağlı olarak üretilen elektronik paranın yine bu merkezi otoriteler aracılığıyla şifrelenerek iletilebilmesi amacıyla elektronik para kavramı kullanılmıştır.[69] Chaum'un kullandığı e-cash sistemi

---

66 Bodur ve Özkul, *Uygulamada*, 237.

67 Coinmarketcap, erişim tarihi: Nisan 12, 2022, https://coinmarketcap.com/tr/.

68 Fatma Ulucan Özkul ve Ece Baş, "Dijital Çağın Teknolojisi Blokzincir ve Kripto Paralar: Ulusal Mevzuat ve Uluslararası Standartlar Çerçevesinde Mali Yönden Değerlendirme", *Muhasebe ve Denetime BAKIŞ 20,* no. 60 (2020): 61, 64.

69 David Chaum, *Blind Signatures for Untraceable Payments, Advances in Cryptology Proceedings of Crypto 82*, (New York: Plenum, 1983), 202, https://www.chaum.com/publications/Chaum-blind-signatures.PDF, erişim tarihi: Nisan 12, 2022; Umut Evlimoğlu, Umut Tolga Gümüş, "İtibari

kullanıcıların paralarının varlığını güvenilir bir otorite tarafından teyit edilmesini zorunlu kıldığı için çok tercih edilmemiştir.[70]

2008 yılında Satoshi Nakamoto isimli kişi veya kişilerce yazılan "Bitcoin: A Peer-to-Peer Electronic Cash System"[71] isimli makalede ise blokzincir sistemi kullanılarak kripto paraların üretimi, transferi ve depolanması anlatılmaktadır. Blokzincir sistemi, herhangi bir merkez tarafından kontrol edilmeyen halka açık bir ağ içerisinde bulunan bilgileri kullanmaya ve paylaşmaya imkan veren dijital bir veri tabanıdır.[72] Makaleye göre blokzincir sistemi Chaum'un sisteminin aksine herhangi merkezi otorite olmadan, her bir katılımcının birbiri ile eş konumda sistemin denetleyicisi ve işletimcisi olarak çalışmasına dayanmaktadır. Blokzincir, birbirlerine bağlanarak doğrusal ve eklemeli bir zincir yapısını oluşturan bloklardan oluşmaktadır. Bir bloğun içindeki işlemler metadata, girdi ve çıktı olmak üzere üç kısımda bulunmaktadır. İşleme ait genel bilgiler metadata kısmında, Bitcoinleri temsil eden indeksler girdi kısmında, Bitcoin'lerin gönderileceği dijital adres bilgisi ise çıktı kısmında bulunmaktadır.[73]

Paranın Kullanımdan Kaldırılmasına Yönelik Teorik Bir Değerlendirme", *LAÜ Sosyal Bilimler Dergisi 9*, no. 2 (2018): 172; Merve Can Kuş Khalilov, Mücahit Gündebahar, İrfan Kurtulmuşlar, Bitcoin ile Dünya ve Türkiye'deki Dijital Para Çalışmaları Üzerine Bir İnceleme, AB 2017 XIX. Akademik Bilişim Konferansı, Aksaray Üniversitesi, https://ab.org.tr/ab17/bildiri/100.pdf, erişim tarihi: Nisan 12, 2022.

70 Deniz Turan ve Cem Demircan, "Kripto Paralar ile Terör ve Diğer İllegal Aktivitelerin Finansmanı," *Anadolu Akademi Sosyal Bilimler Dergisi* 3, no: 1, 2021; 164.

71 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf, erişim tarihi: Nisan 12, 2022.

72 Turan ve Demircan, "Kripto," 162.

73 Ersin Ünsal ve Ömer Kocaoğlu, "Blokzincir Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri," *Avrupa Bilim ve Teknoloji Dergisi*, no. 13 (2018): 56-57.

Her bir blok, kendinden önceki bloğun içindeki bu verilerin şifreleme algoritmalarıyla şifrelenmiş hash değerini (özet değer) ve kendi bloğundaki verilerin hash değerini içermektedir. Bu şekilde ilk bloktan son bloğa kadar var olan tüm blokların hash değerleri zincir boyunca son bloğa kadar aktarılmaktadır. Hash değerleri, "kriptografik karma işlev" (cryptographic hash function, CHF) olarak adlandırılan matematiksel fonksiyon işlemleri ile oluşturulmaktadır.[74] CHF ile zincir sistemine yazılan her bir girdi verisi şifrelenmiş ve sadece o girdi verisine özel olarak çıktı haline dönüştürülmektedir. Kriptoloji sayesinde herhangi bir bloğun içindeki verilere müdahale edilip değiştirilmesi halinde hash değeri de değişmektedir. Bu halde dağıtık sistemdeki diğer eş bloklar kendilerindeki hash değerinden farklı olan yeni hash değeri içeren bu işlemi onaylamazlar ve işlem gerçekleştirilmez. Merkezi olmayan blokzincir sistemini oluşturan her bloğun, CHF ile yapılan işlemleri doğrulama yetkisine sahip olması sistemin ve verilerin güvenliği sağlamaktadır.

Blokzincir sisteminin süreklilik arz edebilmesi için yeni blokların ardı sıra üretilmesi ve üretilen yeni bloğun diğer bloklarca onaylanarak zincirin geliştirilmesi gerekmektedir. Yeni bloklar, madenciler (miner) tarafından kripto bulmacalarının bir dizi hesaplamalarla çözülmesi ile oluşturulmaktadır. Bu bulmacanın doğru olarak çözülüp çözülmediği sistemdeki diğer bloklarca denetlenmektedir. Her yeni blok eklenmesinden sonra bir sonraki bloğu oluşturmak için çözülmesi gereken yeni bir kripto bulmacası oluşmaktadır.[75] Bitcoin yeni blokların üretilmesi için teşvik prosedürünü uygulayarak yeni blok üreten madenciye ödül olarak Bitcoin vermektedir.

---

74 Turan ve Demircan, "Kripto," 163.

75 Makato Yano, Chris Dai, Kenichi Masuda, Yoshio Kishimoto, Blokchain and Crypto Currency, *Economics, Law, and Institutions in Asia Pacific*, (Tokyo: Springer Open, 2020), 6.

A. Kripto Paraların Fon Kavramı Kapsamında Değerlendirilmeleri

Elektronik ortamda saklanması ve transfer edilmesi nedeniyle kripto paraların elektronik para olarak değerlendirilip değerlendirilemeyeceğinin ele alınması gerekmektedir. Avrupa Birliği Parlamentosunun 2009/110/EC numaralı Elektronik Para Kuruluşlarının Kurulması, Faaliyetlerinin Sürdürülmesi, Denetimi[76] isimli ikinci elektronik para direktifinde elektronik paranın tanımı yapılmıştır. Direktife göre elektronik para; gerçek ve tüzel kişilerce ödeme aracı olarak kabul edilen, manyetik veya elektronik olarak yüklenip saklanabilen parasal bir değerdir. E-para, e-para ihraç yetkisi olan kredi kuruşlarından alınarak ihraç edene karşı ileri sürülebilir.[77]

Türk Hukukunda ise 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun'un[78] 3-ç maddesine göre elektronik para, elektronik para ihraç yetkisine sahip kuruluş tarafından fon karşılığında ihraç edilerek elektronik ortamda saklanan, ödeme aracı olarak kabul edilen parasal değer olarak tanımlanmıştır.

Her iki tanıma göre elektronik para kanunla yetkilendirilmiş kuruluş tarafından bir fon karşılığında ihraç edilmelidir, elektronik ortamda saklanabilmelidir ve ihraç kuruluşu dışında gerçek veya tüzel kişilerce de ödeme aracı

---

76 "Directive 2009/110/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: Mart 21, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0110&%20from=EN.

77 Turgay Geçer, "Elektronik Para ve Elektronik Para Kuruluşları," *Journal of Social Sciences, Istanbul Sabahattin Zaim University* 3, no. 5 (2014): 201.

78 RG. 27.06.2013, S. 28690.

olarak kabul edilmelidir.[79] Kişilerin banka hesaplarına bağlı olarak banka kartları üzerinden kullandıkları Dolar, Euro veya Türk Lirası gibi devletlerce tedavüle sunulan para birimleri elektronik paraların en bilinen örneğidir.[80] Elektronik paralar devletlerin karşılığını vadettiği itibari paraların elektronik ortamda temsilini sağlamaktadırlar.[81] Kripto paraların ise merkezi olmayan blokzincir ağı üzerinde herhangi bir fona bağlı olmadan merkezsiz olarak herkes tarafından üretilebilmesi kripto paraları bu düzenlemelerin dışında tutmaktadır ve kripto paraların elektronik para olmadıkları sonucunu ortaya çıkarmaktadır.[82]

Türk hukukunda ise TCMB'nin çıkarmış olduğu, 16 Nisan 2021 tarihli Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmeliğin[83] 3.maddesi ile ilk kez kripto varlıkların tanımı yapılarak kripto paraların *ne olmadıkları* hukuken belirlenmiştir. Yönetmeliğe göre kripto varlıklar; itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen, sanal ortamlarda dağıtık defter sistemi veya benzer teknolojiler

---

79 Abdüssamet Kahraman, "Elektronik Paraya İlişkin Avrupa Birliği ve Türk Düzenlemeleri," *Bilişim Hukuku Dergisi*, no. 2 (2019): 160.

80 Alican Mert, *Deniz Kabuğundan Kripto Paraya: Bitcoin'in Vergisel Boyutu, Sekizinci Genç Vergi Hukukçuları Sempozyumu* (Bildiri Kitabı), (İstanbul: Oniki Levha Yayınları, 2018), 304; Armağan Ebru Bozkurt Yüksel, "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış Açısı," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* 73, no. 2 (2015): 197.

81 Adem Yelmen, "Bitcoinin Satış Sözleşmesinin Bedel Unsuru Açısından Değerlendirilmesi," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 28, no. 1 (2020): 270.

82 Bitcoin ve Elektronik paraların karşılaştırılmalı değerlendirilmesi için bkz. Sarah Rotman, *Bitcoin Versus Electronic Money*, CGAP (Consultative Group to Assist the Poor) 2014, erişim tarihi: Mart 8, 2022, https://www.cgap.org/sites/default/files/Brief-Bitcoin-versus-Electronic-Money-Jan-2014.pdf .

83 RG. 16.04.2021, S. 31456

kullanılarak oluşturulan ve dijital ağlarla dağıtımları sağlanan gayri maddi varlıklardır.[84] Tanımda kullanılan kripto varlık kavramı kripto paraları da kapsayan şemsiye bir terimdir ve bu tanım Yönetmeliğin uygulanma alanı ile sınırlı olarak algılanmalıdır. Keza yönetmelik sadece TCMB'nin yetki alanına giren ödeme konuları hakkında düzenleme yapılması amacıyla çıkarılmıştır.[85] Bu nedenle kripto paraların para olarak kabul edilip edilemeyeceği hususu bu düzenlemeden ayrı olarak tartışılmalıdır.

Para, bir ülkenin egemenlik hakkının göstergesi olarak kanunlarla yetkilendirilmiş Merkez Bankaları tarafından mal veya hizmet karşılığında kullanılan ödeme aracı olarak tanımlanmaktadır. Ülkelerin çıkarmış oldukları resmi paralar değerlerini o ülkenin ekonomik ve teknolojik gücünden almaktadırlar.[86] Ancak kripto paraların devlet veya başkaca otoritelere bağlı olmaksızın üretilmeleri ve bu anlamda devletlerin kripto paraların maddi değerinin karşılığını vadetmiyor olması, kripto paraların değerlerinin kullanıcıların taleplerine ve kullanılan blokzincir sisteminin güvenilirliğine göre değişkenlik göstermesi, günümüzde herkes tarafından ödeme aracı olarak kabul edilmemeleri kripto paraların para olarak değerlendirilemeyeceğini göstermektedir. Dünya devletleri bakımından; Almanya kripto paraları yasal ödeme aracı olarak kabul etmeksizin hukuken yabancı ülke paralarıyla

---

84 *Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik Madde 3: Bu Yönetmeliğin uygulanmasında kripto varlık, dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder.*

85 Gençer Özdemir, "Kripto Paraların Eşya Niteliği," *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* 11, no. 1 (2021): 295.

86 Evlimoğlu ve Gümüş, "İtibari," 168.

aynı statüde tutarken, İngiltere kripto paraları hem özel bir para birimi olarak hem de varlık olarak kabul etmektedir.[87]

Bizim de katıldığımız görüşe göre, öncelikle madenciler tarafından devlet egemenliğinden ayrı olarak kendine has blokzincir sistemi üzerinden kriptografik bulmacaların çözülmesi ile elektronik ortamda üretiliyor olmaları, değerlerinin insanların taleplerine ve bu paraların kullanımının kabul edilmesine göre değişiyor olması kripto paraları güvenilir ve garanti edilmiş itibari para kavramından uzaklaştırmaktadır. Diğer yandan kullanımının sınırlı olması, parasal değerinin bir devletin egemenlik hakkını kullanarak yetkilendirdiği güvenilir herhangi bir otorite tarafından sağlanmaması, kişilerin taleplerine göre parasal değerinin değişkenlik göstermesi nedenleriyle de kripto paralar para olarak kabul edilemezler.[88]

Bu halde para veya elektronik para olarak kabul edilmeyen kripto paraların fon olarak kabul edilip edilmeyeceği hususu Yargıtay Ceza Genel Kurulu'nun kararının[89] yorumu ile belirlenebilecektir. İlgili kararda fonun para veya eşya olmasının zorunlu olmadığı, ekonomik değer ihtiva eden ancak eşya niteliği taşımayan şeylerin de fon olarak kabul edileceği belirtilmiştir. Ülkelerin para birimlerine göre değişkenlik göstermekle birlikte yatırım amaçlı, sanal dünyalarda veya fiziki dünyada alım-satım işlemlerinde parasal bir değer olarak veya diğer kripto para birimleri ile değiş-tokuş işlemlerinde kullanılan kripto paraların sahibinin malvarlığında aktif bir parasal değer olarak yer aldıkları kabul edilmelidir.[90] Sonuç olarak bir malvarlığı değeri olan kripto paraların terör

---

87 Özkul ve Baş, "Dijital," 71.

88 Evlimoğlu ve Gümüş, "İtibari," 168; Asuman Turanboy, "Kripto Paraların Ortaya Çıkmaları ve Hukuki Nitelikleri," *Banka ve Ticaret Hukuku Dergisi* 35, no. 3 (2019); 48, 52.

89 Yar. CGK, E.2017/692, K. 2018/41, 13.02.2018.

90 Taner Emre Yardımcı, "İcra Takibi Yoluyla Bitcoin Alacağının İleri Sürülmesi ve Borçlunun Bitcoininin Haczedilmesi", *Ankara Hacıbayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 23, no. 3 (2019); 98.

örgütlerine finansman sağlamak amacıyla örgüte aktarılmaları Kanun kapsamında fon aktarımı olarak kabul edilecektir.

III. KRİPTO PARALAR KULLANILARAK TERÖRİZMİN FİNANSMANI SUÇUNUN İŞLENİŞ BİÇİMLERİ VE SUÇUN DELİLLENDİRİLMESİ

Kripto paraların finansman suçunda nasıl kullanıldığını tespit etmek için kripto para türlerinin ve bu paralara nasıl sahip olunduğu hususunun açıklanması gerekmektedir. Kripto para kullanıcıları yatırım, alım-satım, değiş-tokuş veya ödeme işlemlerinde kullanmak üzere kripto para edinebilirler.

İlk olarak madencilik işlemi ile kripto para üretilerek kripto para sahibi olunabilir. İkinci olarak satılan mal veya verilen hizmet karşılığında veya hediye olarak kripto para birimlerinin kabul edilmesi ile kripto para edinilebilir. Üçüncü olarak devletlerin para birimleri karşılığında kripto para alımına imkan sağlayan merkezi borsalar üzerinden itibari para (fiat) karşılığında kripto para alınabilir. Son olarak merkezi olmayan kripto para borsalarında, mevcut kripto para birimleri arasında değiş-tokuş sağlaması ile farklı kripto para birimlerine sahip olunabilir.[91]

Dijital olarak bilgisayar programları ile üretilen kripto paralar yine dijital ortamdaki cüzdanlarda saklanırlar. Kripto para sahibi olmak isteyen bir kişi o kripto para biriminin sistem yazılımını mobil cihazına veya bilgisayarına yüklemelidir. Bitcoin "bitcoin.com", Ethereum "ethereum.org" ve Tether "tehter.to" isimli internet sitelerinden hesap oluşturup cüzdan sağlama ve kripto para satın alma hizmetleri sunmaktadırlar. Bunun yanısıra Binance.com, Coinbase.com, BtcTurk.com gibi kripto para borsaları da kullanıcılara cüzdan sağlamakta ve kripto paraların değiş tokuşu hizmetini sunmaktadırlar. Cüzdanlar, kripto paraların sahiplerinin dijital imzaları ile imzalanarak saklandıkları bilgisayar yazılımlarıdır. Sürekli

[91] Turan ve Demircan," Kripto," 165.

olarak çevrimiçi borsalarda bilgisayar veya diğer mobil cihazlar üzerinde bulunan cüzdanlar sıcak cüzdan (online cüzdan) olarak adlandırılırlar.[92]

Her ne kadar anti virüs yazılımları ile sıcak cüzdanların çevrimiçi siber saldırılara karşı korunması mümkün ise de her zaman bir saldırı ihtimalinin olması soğuk cüzdanların geliştirilmesine neden olmuştur. Nitekim 2011 yılında Bitcoin sistemine yapılan siber saldırı ile 17.50 Amerikan doları olan Bitcoin'in kur değeri 0.01 Amerikan doları olarak değiştirilmiştir. 2012 yılında da bir kripto para borsası olan Mt.Gox'a yapılan siber saldırı ile kullanıcıların tüm kişisel verileri ele geçirilmiştir.[93] Son olarak 23 Mart 2022 tarihinde Ronin sistemine siber saldırı yapılarak olay tarihinde değeri 540 milyon dolar olan kripto paralar çalınmıştır.[94] Siber saldırı sonucu kripto paraların çalınması borsa sistemine yapılan saldırı ile kullanıcıların açık cüzdan anahtarlarına erişilmesi ve bu cüzdanlardan saldırganların sahip oldukları cüzdanlara aktarım yapılmasıyla gerçekleşmektedir.[95] Soğuk cüzdanların sadece kullanılmak istendiklerinde çevrimiçi ortama bağlanmaları bu cüzdanları güvenlik açısından daha avantajlı kılmaktadır. Fiziken taşınabilir donanımsal bir cihaz olan soğuk cüzdanlar da kaybolma veya çalınma risklerine karşı korunma gerektirmektedirler.[96] Barındırdıkları kripto para çeşidine göre değişiklik göstermekle birlikte günümüzde en çok kullanılan

---

92 Beyhan Yaslıdağ, *Kripto Paralar,* (Ankara: Seçkin Yayıncılık, 2022), 60.

93 Bozkurt Yüksel, "Elektronik Para," 203.

94 Euronews, erişim tarihi: Nisan 3, 2022, https://tr.euronews.com/2022/03/30/dunyan-n-en-buyuk-ikinci-kripto-para-h-rs-zl-g-615-milyon-dolar-degerinde-sanal-para-cal-n.

95 Turan ve Demircan, "Kripto," 173.

96 Ünsal ve Kocaoğlu, "Blokzincir," 57; Mert, *Deniz,* 319

soğuk cüzdanlar sırasıyla MetaMask, TrustWallet, Coinbase, Binance Wallet, Ledger'dir.[97]

Cüzdanlar kripto para transferini sağlamak için ihtiyaç olan açık ve kapalı anahtarı barındırmaktadırlar. İlk olarak cüzdanın açık anahtarı üretilir, bu anahtar bankanın IBAN numarası veya kişinin el yazısı imzası gibi cüzdana sahiplik kazandırır ve herkes tarafından bilinebilir. Açık anahtarın karşılığı olarak oluşturulan gizli anahtar ise banka hesabına erişmek için kullanılan şifre gibi cüzdan hesabıyla yapılacak işlemleri onaylamak için kullanılır ve kesinlikle gizli tutulması gerekmektedir.[98] Transfer işlemi yapılırken alıcı taraf açık anahtarını gönderici tarafa iletir, gönderici taraf işleme konu olan kripto para miktarını ve alıcının açık anahtarını kendi gizli anahtarı ile şifreleyerek alıcıya geri gönderir. Alıcı taraf, kendi gizli anahtarı ile göndericiden gelen şifreli metni açarak işleme konu kripto paraları kendi cüzdanına aktarır. Bu transfer işleminde kullanılan açık ve gizli anahtarın birbirleri ile uyumlu olup olmadıkları sistemdeki diğer eşler tarafından kontrol edilerek işlem güvenliği sağlanmaktadır. Onay işleminden sonra söz konusu transfer işlemi zincire yeni bir blok olarak eklenmekte ve zincir büyümektedir.

A. Merkezi Kripto Para Borsaları (CEX)

BtcTurk, Binance, CoinBase, Huobi Global gibi merkezi kripto para borsaları (Centralized Exchange-CEX), itibari paralar karşılığında kripto para birimlerinin alımının ve satımının yapılmasını sağlarlar. Bu borsalar geleneksel bir hiyerarşik şirket düzeninde çalışan, güvenilir aracı kurum işlevi gören, devlet destekli ve yasal düzenlemelere tabi olan borsalardır.

---

[97] Aksiyon, erişim tarihi: Mart 21, 2022, https://www.aksiyon.com.tr/haber-en-guvenilir-5-kripto-para-cuzdani-2184.

[98] Fatih Bilgili ve M. Fatih Cengil, "Bitcoin Özelinde Kripto Paraların Ticaret Şirketlerine Sermaye Olarak Getirilmesi," *Ankara Hacıbayram Veli Üniversitesi Hukuk Fakültesi Dergisi* 23, no. 3 (2019): 6; Yardımcı, "İcra," 100.

Bu borsalar sisteme kaydolmak için Müşterini Tanı (Know Your Customer-KYC) ilkesi gereği olarak kullanıcılardan e-posta adresi, kimlik ve adres bilgisi, alımın yapılacağı banka hesap numarası talep etmektedirler. KYC ilkesi Kara Para Aklamayla Mücadele (Anti Money Laundering-AML) ve Terörizmin Finansmanıyla Mücadele (Combating the Financing of Terrorism-CFT) kapsamında kripto para kullanıcıları hakkında bilgi sahibi olmayı ve onların gerçek kimliklerini tespit etmeye yarayan bir müşteri tanımlama programıdır.

Böylelikle kullanıcıların kimlikleri dış verilerle birlikte incelenerek kara para aklama eylemlerinde bulunup bulunmayacakları adli sicillerine göre de belirlenmeye çalışılmaktadır[99] Fransa, İsrail, Amerika gibi ülkeler kripto para borsalarına KYC ilkesini uygulama yükümlülüğü getirmişlerdir.[100] Türkiye'de ise Mali Suçları Araştırma Kurulu (MASAK), çıkarmış olduğu Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik[101] ile kripto varlık hizmet sağlayıcılarını finansal kuruluş olarak kabul etmiş ve Kurulun denetimine tabi kılmıştır. O halde Türkiye'de faaliyet gösteren kripto varlık hizmet sağlayıcı olan Binance, Paribu, BtcTurk gibi merkezi kripto para borsaları CEX'ler de Kurumun getirdiği yükümlülüklere uymak zorundadır.

Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklere İlişkin Temel Esaslar isimli rehber bu

---

99 Jesse Bryan Crawford, Knowing Your Bitcoin Customer: A Survey of Bitcoin Money Laundering Services and Technical Solutions for Anti-Money Laundering Compliance, Iowa State University, 2019; 25-26.

100 Zeynep Esra Tarakçıoğlu, "Kripto Varlıkların Ceza Hukuku Sorumluluğu," *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi* 11, no. 12 (2021); 313.

101 RG. 01.05.2021, S. 31471.

yükümlülükleri detaylı olarak açıklamıştır.[102] BtcTurk[103] ad, soyad, telefon numarası, e-posta adresi ve ayrıca T.C. kimlik numarası da girilerek hesap oluşturulmasına izin vererek KYC ilkesinin gereklerini yerine getirmektedir. Binance[104] ve Paribu[105] borsaları ise hem sadece ad, soyad, telefon numarası, e-posta adresi bilgilerini talep edip T.C. kimlik numaralarını sisteme girmeyerek KYC ilkesine uyum sağlamamakta hem de kullanıcıların verdikleri kişisel bilgilerin doğruluğundan kullanıcının sorumlu olduğu belirleterek bu hususta bir kontrol etme yükümlülüklerinin olmadıklarını belirtmektedirler. Ancak bu durum hem suç işlenmesini kolaylaştıracak hem de kullanıcıların gerçek kimliklerinin tespiti zorlaştıracaktır.[106]

MASAK 2021 yılında Türkiye'de faaliyet gösteren kripto varlık hizmet sağlayıcısı CEX'lere dair yapmış olduğu denetimler sonucu rehberde sayılan yükümlülükleri ihlal eden Paribu ve BtcTürk'ün de aralarında bulunduğu şirketlere toplam 18 milyon 800 bin lira TL değerinde idari para cezası kesmiştir.[107]

Merkezi borsalar, kullanıcıların kripto varlıkları üzerindeki tasarruflarını devralarak, bu varlıkları işlemek ve saklamak için komisyon almaktadırlar. Görüldüğü üzere merkezi borsalarda sistemin güvenilirliği blokzincir sistemi ile değil, aracı borsaya duyulan güven ile sağlanmaktadır. Ayrıca borsaya kaydolurken

---

[102] Erişim tarihi: Nisan 12, 2022, https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf.

[103] BtcTurk, erişim tarihi: Nisan 3, 2022, https://sso.btcturk.com/k/account/register.

[104] Binance, erişim tarihi: Nisan 3, 2022, https://accounts.binance.com/tr/register.

[105] Paribu, erişim tarihi: Nisan 3, 2022, https://www.paribu.com.

[106] Eylül Balıkçı, "Dava ve Takip Konusu Olmaları Bakımından Kripto Paralar", *Erciyes Üniversitesi Hukuk Fakültesi Dergisi 16*, no.2 (2021); 289-290.

[107] Bloomberght, erişim tarihi: Nisan 12, 2022, https://m.bloomberght.com/masak-4-kripto-borsasina-ceza-kesti-2299107.

verilen kişisel bilgiler blokzincir sisteminin vadettiği anonimlik özelliğinden uzaklaşmaktadır.[108]

B. Merkezi Olmayan Kripto Para Borsaları (DEX)

Merkezi olmayan kripto para borsaları (Decentralized Exchange-DEX) ise blokzincir yazılımı tarafından kontrol edilen, sadece kripto para satıcıları ile alıcılarını bir araya getiren borsalardır. Aslında Bitcoin ve diğer kripto para birimlerinin üzerine inşa edildiği eşler arası dağıtık veri sistemini kullanan yazılım sistemlerine bu ad verilmektedir.

CEX'ler sadece fiyat karşılığında kripto para birimlerinin satın alınmasına imkân sağlarken, DEX'ler kullanıcının sahip olduğu kripto para birimini veya birimlerini direkt olarak diğer kripto para birimleri ile değiş-tokuş edilmesine imkan sağlamaktadırlar. DEX'lerde güvenilir aracı kurum yoktur, işlemler akıllı sözleşmeler ile sistem kullanıcıları tarafından gerçekleştirilir ve blokzincire kaydedilir. Dolayısıyla KYC, AML ve CFT ilkeleri işletilmez ve vadedilen anonimlik tam olarak sağlanır.

Bu halde CEX'lerin aksine kullanıcının özel anahtarı DEX sistemi ile paylaşılmamakta ve kullanıcısına özel olarak kalmaktadır. Bu durum kripto paraların illegal faaliyetlerde kullanımın tespit edilmesine engel oluşturmaktadır. Sıcak cüzdanlara sahip olmayan bu borsalarda kripto paralara sahiplik soğuk cüzdanlar ile sağlanmaktadır.[109] Soğuk cüzdanların sadece kullanılmak istendiklerinde çevrimiçi ortama bağlanmaları bu cüzdanları siber saldırılara karşı güvenlik açısından daha avantajlı kılmaktadır. Güncel olarak en

---

[108] Ertuğrul Şimşek, Merkezi Olan ve Olmayan Borsalar: DEX ve CEX: Genel Bir Bakış, medium.org, erişim tarihi: Nisan 12, 2022, https://medium.com/@iublocktech/merkezi-olan-ve-olmayan-borsalar-281342ac2406.

[109] Bitlo.com, erişim tarihi 12 Nisan 2022, https://www.bitlo.com/rehber/merkeziyetsiz-borsa-dex-nedir.

iyi DEX'ler dYdX, UnisWap, PancakeSwap olarak sayılmaktadır.[110] Bu DEX'ler Ethereum, EOS, TRON, Binance Chain gibi çeşitli blokzincir sistemlerini kullanabilmektedirler.[111]

C. Suçun İşleniş Biçimleri

Terör örgütlerinin mali kaynakları sempatizan yardımları, suçtan elde edilen gelirler, hukuka uygun ticari faaliyet gelirleri ve diğer devlet yardımları olmak üzere dört gruba ayrılmaktadır.[112]

1. Sempatizan Yardımları

Sempatizan yardımları; örgütün kuruluş amacına ve faaliyetlerini destekleyen kişi veya topluluklarca düzenlenen örgüte yardım toplama kampanyaları ile elde edilen gelirlerin örgüt kasasına aktarılmasıdır. Sempatizanlar bazen kar amacı gütmeyen kuruluşların arkasına saklanarak kuruluşlarında belirlenen yasal amaçlar için bağış toplayarak gelirlerini örgüte aktarmaktadırlar. Yine örgüt üyeleri veya sempatizanları korkutma yoluyla veya gönüllü olarak aidat adı altında para toplayarak bunları örgüte iletebilmektedirler. Ayrıca yardım kampanyaları dışında zengin örgüt sempatizanları bireysel olarak direkt bir şekilde örgütün belirttiği kasaya da para yardımı yapabilmektedirler.[113]

Günümüzde paranın türü kripto para ve örgüt kasasının da kripto cüzdanlar olarak belirlendiği yardım kampanyaları artış göstermektedir. DEAŞ terör örgütü darkwebdeki sayfasında gizlilik odaklı kripto para birimi olan Monero (XMR) üzerinden

---

[110] Coinmarketcap, erişim tarihi: Nisan 12, 2022, https://coinmarketcap.com/tr/rankings/exchanges/dex/.

[111] Merkezi olmayan kripto para borsaları hakkında bkz., Coinbalina.com, erişim tarihi: Nisan 12, 2022, https://coinbalina.com/merkezi-olmayan-borsalar/.

[112] Yenidünya ve Değirmenci, "Mukayeseli," 7.

[113] Gödekli, *Terörizmin*, 59-60.

yardımları kabul edeceğini açıklamıştır. Bu kripto para türlerinde aktarılan tutar, gönderici ve alıcı adresleri kriptografik olarak şifrelenir ve kamuoyuna açıklanmaz.[114] Bu konuda ABD Adalet Bakanlığı 2020 yılında terör örgütlerinin finansmanı ile bağlantılı olan 155 adet Bitcoin hesabını ele geçirmiş ve bu hesaplarla düzenlenen üç farklı yardım kampanyası ile İzzeddin el-Kassam Tugayları, El-Kaide ve DEAŞ terör örgütlerine blokzincir sistemleri üzerinden finansman sağlandığını tespit etmiştir.[115]

ABD'de yaşayan bir Twitter kullanıcısı, kişisel bloğunda yazdığı "Bitcoin ve Cihada Bağış" isimli yazısını hesabında paylaşarak Bitcoin kullanılarak IŞID terör örgütüne fon sağlanması amacıyla yardım kampanyası başlatmıştır. Fon sağlayacaklara "dark wallet" isimli cüzdanın kullanılmasını tavsiye eden fail sonuç olarak 11 yıl hapis cezasına mahkum edilmiştir.[116]

Bu şekilde yardım kampanyaları, aidat veya bağış yollarıyla elde edilen kripto paraların örgüte aktarılmaları fon toplama suretiyle terörizmin finansmanı suçunu oluşturmaktadır. Suç, yardımlar sonucu elde edilen itibari paranın CEX'ler üzerinden kripto paralara çevrilerek örgüte iletilmesiyle de işlenebilecektir.

2. Suçtan Elde Edilen Gelirler

Örgütler gelir getirici herhangi bir suçu işleyerek elde edilen geliri mali finansmanları için kullanabilirler. Bu suçlar insan kaçakçılığı, sahtecilik, haraç toplama, fidye alma gibi suçlar olabilmektedir.[117] Türkiye'de PKK terör örgütü uyuşturucu,

---

[114] Turan ve Demircan," Kripto," 168.

[115] Turan ve Demircan," Kripto," 171-172.

[116] Umut Balcı, "Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri," *TBB Dergisi 34*, no. 155 (2021): 226.

[117] MASAK, erişim tarihi: Nisan 12, 2022, https://masak.hmb.gov.tr/terorun-finans-kaynaklari.

silah ve canlı hayvan kaçakçılığı, tehdit suçları ile kazanç elde etmektedir.[118]

Örgüt, itibari para olarak elde ettiği bu geliri kripto paralara dönüştürerek kripto para cüzdanında tutabilir veya yine aynı şekilde faaliyetleri için gerekli olan harcamaları kripto para üzerinden yapabilir. Ayrıca örgütün kripto para borsaları üzerinden gerçekleştirdiği siber saldırılarla dolandırıcılık, hırsızlık, yağma gibi suçlar işlenerek elde edilen kripto paralar örgütün finansmanı için kullanabilir. Bu halde örgüt üyesi olarak suç işleyerek fon sağlayanlar Kanun'un 4/2. maddesinin yollamasıyla TCK'nın 220. maddesine göre örgüte üye olma suçundan cezalandırılacaklar ve cezaları artırılacaktır.

3. Hukuka Uygun Ticari Faaliyet Gelirleri ve Yabancı Devlet Yardımları

Örgüt üyesi, örgütten ayrılmış kişi veya görünüşte örgütle bağlantısı olmayan kişilerin hukuka uygun olarak yerine getirdikleri ticareti faaliyetleri ile elde ettikleri gelirleri örgüte aktarmaları fon sağlayarak finansman suçunu oluşturacaktır. Ayrıca terör örgütünün ihtiyacı olan malların nakliyesini sağlayan ticari işletmelerin kurulması, ya da örgütün uyuşturucu ticaretinde kullanacağı uyuşturucuyu var olan nakliye şirketleri üzerinden taşınmasıyla da örgütünün finanse edilmesi mümkündür.[119] El Kaide terör örgütü, ABD'deki 11 Eylül olaylarını gerçekleştirmek için ihtiyacı olan mali kaynağı yasal işletmeler ve sempatizan yardımları üzerinden sağlamıştır.[120]

Örgüt, ideolojilerini yaymak için yayınladığı gazete, dergi ve kitapları sempatizanlarına satarak ya da konser, sergi, gösteri gibi sosyal etkinlikler düzenleyerek elde ettiği hukuka uygun

---

118 Yenidünya ve Değirmenci, "Mukayeseli," 8.

119 Gödekli, *Terörizmin*, 60.

120 Yenidünya ve Değirmenci, "Mukayeseli," 8.

gelirleri de örgüte fon sağlamak için kullanabilmektedir.[121] Örgüt, elektronik ortamlarda yayınladığı eserlerin ya da sanal dünyalarda düzenlediği sosyal etkinliklerin bedellerini kripto paralar üzerinden belirleyip bu bedellerin direkt olarak örgütün kripto para cüzdanına gönderilmesini de talep edebilir.

Yabancı devletlerin genel olarak dış politika aracı olarak ilgili ülkede faaliyet gösteren terör örgütlerine beslenme, barınma, silah ve mühimmat sağlama şeklinde yardım edilmesi ile veya örgütün yakın olduğu dernek veya vakıflara para yardımı sağlaması ile örgüt eylemleri desteklenmektedir.[122]

D. Suçun Delillendirilmesi

Çeşitli şekillerde elde edilen fonların örgüte ulaştırılması için geleneksel olarak alternatif bankacılık sistemleri kullanılmaktaydı. Bu sistemlerden en yaygın olanı Hawala sistemidir.[123] Fon miktarının fazla olması ve blokzincir sistemlerinin anonimlik özelliği sunması nedenleriyle kripto

---

121 Gödekli, *Terörizmin*, 60

122 Gödekli, *Terörizmin*, 61.

123 Burcu Gediz Oral, "Gayri Resmi Değer Transfer Sistemlerinin Kara Para Aklama ve Terörizmin Finansmanındaki Rolü: Hawala Sistemi," *Optimum Ekonomi ve Yönetim Bilimleri Dergisi* 8, no. 2 (2021): 332; *Gayri Resmi Değer Transfer Sistemlerinden (Informal Value Transfer Systems-IVTS) biri olan Hawala sistemi, bir fonun veya değerin ülkeler veya coğrafi bölgeler arasında kişisel bir ağ aracılığıyla herhangi bir kayıt bırakmadan taşınmasını sağlayan finansal hizmet sistemidir. Sistem, bulunduğu ülke veya coğrafi bölgedeki fonu hedef yabancı ülke veya coğrafi bölgeye transfer etmek isteyen kişinin Hawaladar 1 olarak isimlendirilen kişiye ulaşması ile işlemeye başlamaktadır. Gönderici kişi kendisi ile aynı ülkede veya coğrafi bölgede bulunan Hawaladar 1' e hedef lokasyona göndermek istediği fon miktarını nakit olarak verir. Hawaladar 1, bu havale işlemine özel bir havale kodu oluşturarak, gönderici kişiye ve hedef lokasyonda bulunan Hawaladar 2'ye bu kodu bildirir. Nihai alıcı Hawaladar 2 ile iletişime geçer, doğru havale kodunu bildirir ve havale konusu fon miktarını nakit olarak Hawaladar 2'den alır. Böylelikle banka veya benzeri kurumlar kullanılmaksızın fiziki veya elektronik olarak bir para transferi yapılmadan hedef yabancı ülkede veya coğrafi bölgede bulunan nihai alıcıya bir nevi takas yoluyla fon iletimi sağlanmış olur.*

paralar ve kripto para sistemleri aktarım aşamasında son yıllarda oldukça fazla kullanılmaya başlanmıştır.

Yukarıda bahsedildiği üzere her ne suretle elde edilmiş olursa olsun kripto paraların izlerinin sürülebilmesi ve bir terör örgütüne fon sağlamak veya toplamak amaçlı kullanıldığının tespit edilebilmesi kripto paranın türüne ve işlem yapılan borsaya göre değişiklik göstermektedir.

Örgütün kripto para cüzdanının CEX'lerde bulunması ve fonun oraya aktarılması halinde faillerin ve aktarılan fonun miktarı ilgili borsalar aracılığı ile kolayca tespit edilebilecektir. Ancak örgütlerin faaliyetlerinin başlı başına yasa dışı olması, bu örgütlerin finansmanlarını da otorite denetiminden uzak DEX'ler üzerinden yapmalarına neden olmaktadır. Bu nedenle terörizmin finansmanı suçunun delillendirilmesi DEX'ler üzerinden yapılan fonlama işlemleri kapsamında incelenecektir.

Kripto paralar, yapılan işlemlerin kamuoyuna açık olup olmamalarına göre şeffaf kripto paralar ve gizlilik odaklı kripto paralar olarak sınıflandırılmaktadırlar. Bitcoin, Ethereum gibi şeffaf kripto para sistemlerinde kullanıcıların adres bilgileri ve aktarılan tutar herkesçe izlenebilmektedir. Bu sistemler bir CEX olmadığı için kullanıcıların gerçek kimlik bilgilerine sahip olunamasa da fonlama amaçlı yapılan işlemlerin ait olduğu hesapları takip etme imkanı vermekte, bu yönüyle suçun delillendirilmesinde kolaylık sağlamaktadır. Nitekim ABD Adalet Bakanlığı da 2020 yılındaki olayda para aktarımlarını şüpheli bulduğu Bitcoin adreslerini takip ederek örgütlere yardım kampanyalarına ulaşmış ve faaliyetlerini sona erdirmiştir. Bu hesaplarla bağlantılı olarak fonlanan DAEŞ, bu olaydan sonra artık gizlilik odaklı kripto para birimi olan Monero üzerinden fon kabul edeceğini açıklamıştır. Diğer bir gizlilik odaklı kripto para olan Verge'nin de (XVG) Monero gibi gizlilik, izlenemezlik, bağlantısızlık, kullanıcı anonimliği özelliklerine sahip olması bu para türlerinin kullanıldığı işlemlerin izlenmesini ve kara listeye alınmasını olanaksız kılmaktadır. Amerika Birleşik Devletleri Gelirler İdaresinin (IRS)

Monero'nun takip edilmesine imkân verecek teknolojik çalışmaların yapılması yönünde attığı adımları bulunmaktadır.[124]

Kripto para borsalarından önce, ulaşılan başka delillerle de fonlama fiilleri tespit edilebilir. 2020 yılında ABD'de yapılan operasyonların kaynağı bilgisayarlarda yapılan aramalara, Telegram veya sosyal medya platformları aracılığıyla yapılan iletişimlere ve istihbari bilgilere dayanmaktadır.[125]

Türkiye bakımından Adalet Bakanlığı Ceza İşleri Genel Müdürlüğünce yayınlanan 23.02.2021 tarih ve 155/1 nolu Genelge ile Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama ve Terörizmin Finansmanı Suçlarının Soruşturma Sürecine İlişkin Temel Esaslar düzenlenmiştir.[126] Genelgede de belirtildiği üzere 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun'un 17.maddesine göre terörizmin finansmanı suçunun işlendiği hususunda kuvvetli şüphe bulunması halinde CMK'nın 128 maddesine göre elkoyma kararı verilebilecektir. Ayrıca finansman suçunun ve bağlantılı diğer suçların ve suç ağlarının, müsadereye konu olabilecek terör fonlarının belirlenmesi, maddi olayın aydınlatılması için eş zamanlı mali soruşturma da yapılacaktır. Kuvvetli şüphe bulunması halinde CMK 133, 135, 139, 140 maddelerinde düzenlenen koruma tedbirlerine başvurularak soruşturma genişletilebilecektir.

---

124 Turan ve Demircan," Kripto," 168-170.

125 Turan ve Demircan," Kripto," 171-172.

126 Adalet Bakanlığı, Ceza İşleri Genel Müdürlüğü, 23.02.2021, 155/1, erişim tarihi: Nisan 12, 2022, https://cigm.adalet.gov.tr/Resimler/SayfaDokuman/2322021173124155-1%20Sayılı%20Genelge.pdf.

MASAK, Bankalara İlişkin Şüpheli İşlem Bildirim Rehberine[127] göre tespit ettiği şüpheli işlemler sonucu FETÖ terör örgütü ile bağlantılı olarak Türkiye'den Amerika borsalarına gönderilmek istenen 100 milyon lira değerindeki kripto paraların yüzde kırkına sahip olan şirketin hesaplarına bloke koymuştur ve soruşturmanın yapılması için adli mercilere bildirimde bulunulmuştur.[128]

SONUÇ

Kripto paraların kullanılması finansal teknolojinin gelişmesine katlı sağlamış ise de bu para sistemlerinin anonimlik özelliğine sahip olması yasadışı faaliyetlerde kullanılmalarına da neden olmuştur. Terör örgütüne fon sağlayarak veya toplayarak terörizmin finansmanı suçunu işleyen failler örgütün faaliyetlerine devam etmesi ve ideolojisinin yayılması için gerekli olan maddi desteğin sağlanmasını amaçlamaktadırlar. Çoğu zaman merkezi bilinmeyen ve dağınık şekilde faaliyet gösteren terör örgütlerine maddi yardımların ulaştırılması kripto paraların zamandan ve mekandan bağımsız olan sistemleri sayesinde oldukça kolaylaşmıştır. Bu suçun takibi ve delillendirilmesi bakımından kullanılan kripto para birimi ve borsa türü önem arz etmektedir.

Kripto para fonlarının CEX'ler üzerinden temin edilmesi ve transfer edilmesi halinde KYC, AML, CFT ilkeleri gereğince ilgili borsalar aracılığıyla faillerin kimlik ve adres bilgilerine ulaşılabilecektir. Bitcoin gibi şeffaf kripto paraların kendi blokzincir sistemleri (DEX) üzerinden fon olarak transfer

---

127 MASAK, Bankalara İlişkin Şüpheli İşlem Bildirim Rehberi hakkında bkz. erişim tarihi: Nisan 12, 2022, https://ms.hmb.gov.tr/uploads/2020/11/SIB-REHBERI-DIGER-YUKUMLULER.pdf.

128 Balcı, "Kripto,"251: *Müşteri hesaplarından kripto para alımı amacıyla yurtiçi ve yurtdışı kripto para borsalarına ya da gerçek veya tüzel kişi hesaplarına müşteri profiline uymayacak sıklık ve tutarda para transferi yapılması" ve "Kaynağı bilinmeyen veya şahsın mali profili ile uygun olmayan şekilde yapıldığından şüphelenilen kripto para satımı sonucunda müşteri hesaplarına transfer gelmesi" şüpheli işlem olarak kabul edilmektedir.*

edilmesi hallerinde de transferin tarafları ve tutarı ağda paylaşıldığı için failler belirlenebilecektir. Türkiye bakımından MASAK'ın denetimine tabi olan CEX'ler de KYC, AML, CFT ilkelerince kullanıcı kaydı tutmak zorundadırlar. Suçun delillendirilmesinde ise Adalet Bakanlığının genelgesine ve diğer mevzuat hükümlerine göre CMK kapsamındaki koruyucu tedbirlere başvurulabilecektir. Yargılama sonunda kripto paralarla fon sağlamak veya toplamak suretiyle terörizmin finansmanı suçunu işleyen sanık hakkında cezaya hükmolunacaktır.

Ancak Monera, Verge gibi gizlilik odaklı kripto paraların merkezsiz borsalar üzerinden terör örgütlerinin finanse edilmesi hallerinde suçun delillendirilmesinde sorunlar oluşmaktadır. Bu borsalar tutar ve taraflar hakkında hiçbir bilgi vermeyerek tamamen anonimlik oluşturduğu için faillerin ve fon olarak kullanılan tutarların belirlenmesi oldukça zorlaşmaktadır. Çözüm olarak gizlilik odaklı bu yazılımlar hakkında yasal düzenleme yapılarak hukuken tanımlanmaları ve bu yazılımlar üzerinden delil etme yöntemleri gösterilmelidir.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.

KAYNAKÇA

Akça, Mehmet. "Terörizmin Kendine Özgü (Suı Generis) Niteliği: Kavramı Tanımlamada Metodoloji Sorunu." *İstanbul Barosu Dergisi 88*, no.1 (2014): 16-63.

BIBLIOGRAPHY Akın, Engin.*Terörizmin Finansmanı Suçu.* Ankara: Adalet Yayınevi, 2009.

Balcı, Umut. "Kripto Paraların Ceza Hukuku Boyutu ve Türk Mevzuatındaki Muhtemel Düzenlenme Yeri." *TBB Dergisi 34*, no.155 (2021): 203-259.

Balıkçı, Eylül. "Dava ve Takip Konusu Olmaları Bakımından Kripto Paralar." *Erciyes Üniversitesi Hukuk Fakültesi Dergisi 16*, no.2 (2021): 273-312.

Bilgili, Fatih, ve M. Fatih Cengil. "Bitcoin Özelinde Kripto Paraların Ticaret Şirketlerine Sermaye Olarak Getirilmesi." *Ankara Hacıbayram Veli Üniversitesi Hukuk Fakültesi Dergisi 23*, no.3 (2019): 3-23.

Bodur, Nurullah, ve Eshat Özkul. *Uygulamada Terör Örgütü ve Terör Suçları.* Ankara: Seçkin Yayıncılık, 2022.

Boz, Burak. "Türk Ceza Hukukunda Terör Örgütü ve Terör Örgütüne Üye Olma Suçu." *ASBÜ Hukuk Fakültesi Dergisi 2*, no. 1 (2020): 131-186.

Bozkurt Yüksel, Armağan Ebru. "Elektronik Para, Sanal Para, Bitcoin ve Linden Doları'na Hukuki Bir Bakış Açısı." *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 73*, no.2 (2015): 173-220.

Chaum, David. *Blind Signatures for Untraceable Payments. Advances in Cryptology Proceedings of Crypto 82* içinde, yazan David Chaum, Ronald L. Rivest ve Alan L. Sherman, 199-203. New York: Plenum, 1983.

Crawford, Jesse Bryan. *Knowing Your Bitcoin Customer: A Survey of Bitcoin Money Laundering Services and Technical Solutions for Anti-Money Laundering Compliance.* Iowa State University, 2019.

Çetin, Soner Hamza. "Terörizmin Finansmanı Suçu." *Ceza Hukuku Dergisi 11*, no. 31 (2016): 125-171.

Evlimoğlu, Umut, ve Umut Tolga Gümüş. "İtibari Paranın Kullanımdan Kaldırılmasına Yönelik Teorik Bir Değerlendirme." *LAÜ Sosyal Bilimler Dergisi 9*, no.2 (2018): 167-183.

Geçer, Turgay. "Elektronik Para ve Elektronik Para Kuruluşları." *Journal of Social Sciences Istanbul Sabahattin Zaim University 3*, no.5 (2014): 197-207.

Gödekli, Mehmet. *Terörizmin Finansmanı Suçu.* Ankara: Seçkin Yayıncılık, 2017.

Kahraman, Abdüssamet. "Elektronik Paraya İlişkin Avrupa Birliği ve Türk Düzenlemeleri." *Bilişim Hukuku Dergisi,* no.2 (2019): 149-184.

Khalilov Kuş, Merve Can, Mücahit Gündebahar, ve İrfan Kurtulmuşlar. "Bitcoin ile Dünya ve Türkiye'deki Dijital Para Çalışmaları Üzerine Bir İnceleme." *AB 2017 XIX. Akademik Bilişim Konferansı.* Aksaray: Bilgi Kitapevi ve Kırtasiye Ltd. Şti., 2017: 59-65.

Kocasakal, Ümit. "Terörizmin Finansmanı." *18. Uluslararası Ceza Hukuku Kongresi.* İstanbul: Türk Ceza Hukuku Derneği Yayınları, 2009.

Lyngbo, Mikael, Feridun Yenisey, Namık Kemal Topçu, Önder Tozman, ve Kemal Şahin. *Örgütlü Suçlar ve Terör Suçları Eğitim Modülü.* Ankara: Adalet Bakanlığı.

Mert, Alican. *Deniz Kabuğundan Kripto Paraya: Bitcoin'in Vergisel Boyutu, Sekizinci Genç Vergi Hukukçuları Sempozyumu.* İstanbul: Oniki Levha Yayıncılık, 2018.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System.", 2008.

Oral Gediz, Burcu. "Gayri Resmi Değer Transfer Sistemlerinin Kara Para Aklama ve Terörizmin Finansmanındaki Rolü: Hawala Sistemi." *Optimum Ekonomi ve Yönetim Bilimleri Dergisi 8*, no.2 (2021): 331-350.

Özgenç, İzzet. *Suç Örgütleri.* Ankara: Seçkin Yayıncılık, 2022.

Özgenç, İzzet. *Türk Ceza Hukuku Genel Hükümler.* Ankara: Seçkin Yayıncılık, 2021.

Özdemir, Gençer. "Kripto Paraların Eşya Niteliği." *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi 11*, no.1 (2021): 289-306.

Rotman, Sarah. *Bitcoin Versus Electronic Money.* CGAP (Consultative Group to Assist the Poor), 2014.

Şen, Ersan, ve H. Sefa Eryıldız. *Suç Örgütü.* Ankara: Seçkin Yayıncılık, 2022.

Tarakçıoğlu, Zeynep Esra. "Kripto Varlıkların Ceza Hukuku Sorumluluğu." *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi 11*, no.12 (2021): 295-352.

Turan, Deniz, ve Cem Demircan. "Kripto Paralar ile Terör ve Diğer İllegal Aktivitelerin Finansmanı." *Anadolu Akademi Sosyal Bilimler Dergisi 3*, no.1 (2021): 161-176.

Turan, Deniz, ve Eser Gemici. "Terörizmin Finansman Kaynakları ve Karapara Aklamanın Terörizmin Finansmanındaki Rolü." *Anadolu Üniversitesi Sosyal Bilimler Dergisi 20,* no.2 (2020): 257-278.

Turanboy, Asuman. "Kripto Paraların Ortaya Çıkmaları ve Hukuki Nitelikleri." *Banka ve Ticaret Hukuku Dergisi 35*, no.3 (2019): 47-62.

Turinay, Faruk Yasin. "Ceza Hukukunda Terör Örgütü Kavramı." *Türkiye Barolar Birliği Dergisi 27*, no. 116 (2015): 39-84.

Ulucan Özkul, Fatma, ve Ece Baş. "Dijital Çağın Teknolojisi Blokzincir ve Kripto Paralar: Ulusal Mevzuat ve Uluslararası Standartlar Çerçevesinde Mali Yönden Değerlendirme." *Muhasebe ve Denetime BAKIŞ 20*, no.60 (2020): 57-74.

Ünsal, Ersin, ve Ömer Kocaoğlu. "Blokzincir Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri." *Avrupa Bilim ve Teknoloji Dergisi* no.13 (2018): 54-64.

Yano, Makato, Chris Dai, Kenichi Masuda, ve Yoshio Kishimoto. *Blokchain and Crypto Currency.* Tokyo: Springer Open, 2020.

Yardımcı, Taner Emre. "İcra Takibi Yoluyla Bitcoin Alacağının İleri Sürülmesi ve Borçlunun Bitcoininin Haczedilmesi." *Ankara Hacıbayram Veli Üniversitesi Hukuk Fakültesi Dergisi 23*, no.3 (2019): 97-128.

Yaslıdağ, Beyhan. *Kripto Paralar.* Ankara: Seçkin Yayıncılık, 2022.

Yelmen, Adem. "Bitcoinin Satış Sözleşmesinin Bedel Unsuru Açısından Değerlendirilmesi." *Selçuk Üniversitesi Hukuk Fakültesi Dergisi 28*, no.1 (2020): 265-294.

Yenidünya, Ahmet Caner, ve Olgun Değirmenci. *Mukayeseli Hukuk ve Türk Hukukunda Terörizmin Finansmanı Suçu. Ord. Prof. Dr. Sulhi Dönmezer Armağanı*, 2008.

Yıldırım, Zeki. *Türk Hukukunda Terörizmin Finansmanı Suçu ve Malvarlıklarını Dondurma.* Ankara: Adalet Yayınevi, 2013.

Yılmaz, Yeşim. "Terörizmin Finansmanı Suçu." *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 3*, no.3 (2020): 177-267.

İNTERNET KAYNAKLARI

Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü. *Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme.* Erişildi: Nisan 12, 2022. https://diabgm.adalet.gov.tr/arsiv/adli_yardimlasma/adli_isbirligi_ceza/suclularin_iadesi_ek/terorizmin_finansmanının_önlenmesine_ilişkin%20BM%20sözlesmesi.pdf.

Adalet Bakanlığı Ceza İşleri Genel Müdürlüğü. *Suçtan Kaynaklanan Malvarlığı Değerlerini Aklama ve Terörizmin Finansmanı Suçlarının Soruşturma Sürecine İlişkin Temel Esaslar.* 23 Şubat 2021. Erişildi: Nisan 12, 2022. https://cigm.adalet.gov.tr/Resimler/SayfaDokuman/2322021173124155-1%20Sayılı%20Genelge.pdf.

Aksiyon.com. *En Güvenilir 5 Kripto Para Cüzdanı.* 17 Şubat 2022. Erişildi: Mart 21, 2022. https://www.aksiyon.com.tr/haber-en-guvenilir-5-kripto-para-cuzdani-2184 .

Binance. https://accounts.binance.com/tr/register.

Bitlo.com. https://www.bitlo.com/rehber/merkeziyetsiz-borsa-dex-nedir.

Bloomberght. *Masak 4 Kripto borsasına Ceza Kesti.* 17 Şubat 2022. Erişildi: Nisan 12, 2022. https://m.bloomberght.com/masak-4-kripto-borsasina-ceza-kesti-2299107.

BtcTurk. https://sso.btcturk.com/k/account/register.

Coinbalina.com. https://coinbalina.com/merkezi-olmayan-borsalar/.

Coinmarketcap. https://coinmarketcap.com/tr/rankings/exchanges/dex/.

Euronews.com. *Dünyanın en büyük ikinci kripto para hırsızlığı: 615 milyon dolar değerinde sanal para çalındı.* 3 Mart 2022. Erişildi: Nisan 3, 2022. https://tr.euronews.com/2022/03/30/dunyan-n-en-buyuk-ikinci-kripto-para-h-rs-zl-g-615-milyon-dolar-degerinde-sanal-para-cal-n .

European Union. *Directive 2009/110/EC of The European Parliament and of the Council of 16 Semptember 2009* . Erişildi: Mart 21, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0110&%20from=EN.

MASAK. *Kripto Varlık Hizmet Sağlayıcıları İçin Suç Gelirlerinin Aklanmasının ve Terörizmin Finansmanının Önlenmesine Dair Yükümlülüklere İlişkin Temel Esaslar.* https://ms.hmb.gov.tr/uploads/sites/12/2021/05/Kripto-Varlik-Hizmet-Saglayicilar-Rehberi.pdf.

MASAK. *Bankalara İlişkin Şüpheli İşlem Bildirim Rehberi.* https://ms.hmb.gov.tr/uploads/2020/11/SIB-REHBERI-DIGER-YUKUMLULER.pdf.

Paribu. https://www.paribu.com.

Şimşek, Ertuğrul. *Merkezi Olan ve Olmayan Borsalar: DEX ve CEX: Genel Bir Bakış.* 11 Ekim 2021. Erişildi: Nisan 12, 2022.

https://medium.com/@iublocktech/merkezi-olan-ve-olmayan-borsalar-281342ac2406.

United Nations Treaty Collection. *11. International Convention for the Suppression of the Financing of Terrorism.* https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-11&chapter=18&clang=_en#EndDec.

Unodc.org. *International Convention for the Supression of the Financing of Terrorism.* Erişildi: Nisan 12, 2022. https://www.unodc.org/documents/treaties/Special/1999%20International%20Convention%20for%20the%20Suppression%20of%20the%20Financing%20of%20Terrorism.pdf

Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.932106**

5651 SAYILI KANUN KAPSAMINDA SUÇ İŞLENMESİNİN ÖNLENMESİ AMACIYLA İNTERNET ERİŞİMİNİN ENGELLENMESİ

Blocking Internet Access to Prevent Crime within Scope of Law Nr. 5651

Yunus ÖZKAYA[*]

Öz

Günümüzde internet en yaygın kullanılan kitle iletişim araçlarından birisi haline gelmiştir. Bireylerin yaşantısına sağladığı pek çok katkının yanı sıra internet kullanımından meydana gelen sorunlar da söz konusudur. Özellikle internetin, kötü amaçlarla kullanılması halinde başkalarının hak ve özgürlüklerine yapılan saldırıların bir aracı olduğu görülmektedir. Devletler tarafından yapılan hukuki düzenlemeler çerçevesinde; internet kullanımı ile meydana gelen hukuka aykırılıkların önlenmesi amacıyla bazı tedbirlere başvurulmaktadır. Bu tedbirlerden bir tanesi de internet ortamında yayınlanan hukuka aykırı içeriklere erişimin engellenmesidir. Özü itibariyle bir tedbir kararı olan internet erişiminin engellenmesi suç işlenmesinin önlenmesi gibi çeşitli sebeplere dayalı olarak verilmektedir. Bu çalışmada öncelikle

[*] Sanayi ve Teknoloji Uzmanı, Sanayi ve Teknoloji Bakanlığı, av.yunusozkaya@outlook.com, ORCID: 0000-0001-7796-8691.

Makale Gönderim Tarihi/Received: 03.05.2021.

Makale Kabul Tarihi/Accepted: 27.12.2021.

Atıf/Citation: Özkaya, Yunus. "5651 Sayılı Kanun Kapsamında Suç İşlenmesinin Önlenmesi Amacıyla İnternet Erişiminin Engellenmesi." *Bilişim Hukuku Dergisi* 4, no. 1 (2022): 81-140.

genel olarak internet erişiminin engellenmesi kavramı üzerinde durulmakta; akabinde 5651 sayılı Kanunun 8 ve 8/A maddelerinde düzenlenen internet erişiminin engellenmesi kararlarının hukuki niteliği, kararların alınması ve uygulanması ile kararlara karşı başvurulabilecek hukuki yollar değerlendirilmektedir.

Anahtar Kelimeler: Erişim Engelleme, 5651 sayılı Kanun, Koruma Tedbiri, İdari Tedbir.

Abstract

Internet has become one of the most widely used mass media today. In addition to its many contributions to the lives of individuals, there are also problems arising from internet use. It is seen that the internet is a means of attacks on the rights and freedoms of others, especially if it is used for malicious purposes. Within the framework of the legal regulations made by the states; some measures are taken in order to prevent the illegality of the internet usage. One of these measures is to prevent access to illegal content published on the internet. The blocking of internet access, which is a precautionary decision in essence, is given based on various reasons such as the prevention of crime. In this study, first of all, the concept of blocking internet access is focused on; subsequently, the legal nature of the decisions to block internet access regulated in Articles 8 and 8/A of the Law Numbered 5651, the making and implementation of the decisions and the legal remedies to be applied against the decisions are evaluated.

Keywords: Blocking Access, Law No. 5651, Protection Measure, Administrative Measure.

GİRİŞ

İnternet çağımızın en önemli kitle iletişim aracıdır. Türkiye İstatistik Kurumu tarafından yayımlanan 26 Ağustos 2021 tarihli ve 37437 sayılı çalışmaya göre; internet kullanım oranı 2021

yılında 16-74 yaş arası bireylerde %82,6 olarak belirlenmiştir[1]. Bu verilerden de anlaşılacağı üzere günümüzde internet, yaşamın kaçınılmaz bir unsuru haline gelmiştir. İnternetin bu kadar yaygın kullanılmasının nedeni elbette ki bireylere sağladığı faydalardır. Bu faydaların başında hiç kuşkusuz haberleşme ve bilgiye erişimde sağladığı hız ve pratiklik gelmektedir[2].

İnternet, sağladığı faydaların yanı sıra kötü niyetli kullanımlar nedeniyle bireyler üzerinde olumsuz sonuçlar doğurmaya da uygun bir araçtır. İnternet üzerinde var olan bir veri saniyeler içerisinde bir ülkeden başka bir ülkeye gönderilebilmekte ya da internet ortamında yayınlanan bir içeriğe saniyeler içerisinde milyonlarca insan tarafından ulaşılabilmektedir. İşte bu hızlılık ve kolaylık kötü niyetli kişilerin elinde başka amaçlarla kullanılabilmektedir. Örneğin; suç teşkil eden bir fiilin internetin sağladığı kolaylıklar kullanılarak işlenmesi, başkasının kişilik veyahut özel hayatının gizliliğini ihlal eden bir içeriğin internet ortamında yayınlanması gibi hallerde internet, başkalarına zarar veren bir araç haline dönüşmektedir.

İnternet kullanımı; haberleşme hürriyeti, ifade hürriyeti, bilgiye erişim hakkı gibi pek çok temel hak ve özgürlükle ilişkili bir kavramdır. Avrupa İnsan Hakları Mahkemesi içtihatlarında demokratik toplumlarda internete son çare olarak müdahalede bulunulması gerektiği belirtilmektedir. Ancak internetin kullanım alanının genişlemesi ve bu alanda ortaya çıkan zararlı

---

1 Bkz. "Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2021," Türkiye İstatistik Kurumu, erişim tarihi: 19 Kasım, 2021, https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2021-37437.

2 Mehmet Bedii Kaya, "İnsan Hakları Ekseninde İnternetin Kontrolü ve Hukuki Sorumluluk Rejimi," *Anayasa Yargısı Dergisi*, no.2 (2020): 162; Yasin Söyler, *Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi* (Ankara: Savaş Yayınevi, 2014), 6.

faaliyetlerin artması nedeniyle Devletlerin bu alana müdahalesi zorunlu hale gelmiştir. Gerek ulusal hukukta gerekse uluslararası alanda internet ortamının düzenlenmesi ve bu alana müdahale edilmesi tartışılan bir mesele haline gelmiştir[3].

Günümüzde pek çok Devlet tarafından yapılan hukuki düzenlemelerle internet ortamı düzenlenmiştir[4]. Yapılan düzenlemelerde internet ortamının bireyler ve Devletler üzerinde doğuracağı olumsuz sonuçları gidermeye yönelik bazı tedbirlere yer verilmiştir. Bu tedbirlerden bir tanesi de "internet erişiminin engellenmesi"dir. İnternet erişiminin engellenmesi; internet ortamında var olan hukuka aykırı bir içeriğe bu hukuka aykırılık hali sona erene kadar ulaşılmamasını sağlayan teknik bir tedbir.

Ülkemiz mevzuatı açısından internet erişiminin engellenmesi 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümleri çerçevesinde düzenlenmektedir. Kanunda erişim engelleme kararlarının hangi nedenlere dayalı olarak kim tarafından verileceği, bu kararların uygulanması ve bu kararlara karşı başvurulabilecek hukuki yollar detaylı bir biçimde düzenlenmektedir. Kanun kapsamında erişim engelleme kararının verilebileceği hallerden birisi de "suç işlenmesinin önlenmesi"dir. Burada "önleme" ibaresi ile kastedilen esas itibariyle suç teşkil eden bir içeriğin internet ortamındaki etkilerinin sonlandırılmasıdır. Ancak bazı hallerde erişim engelleme yöntemiyle henüz işlenmemiş bir suçun işlenmesinin önüne geçilebilmesi de mümkündür.

Suç işlenmesinin önlenmesi amacıyla erişimin engellenmesi 5651 sayılı Kanunun 8 ve 8/A maddeleri çerçevesinde düzenlenmektedir. Söz konusu düzenlemeler çalışmanın temel

---

3 Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 58.

4 Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 65.

inceleme noktasını oluşturmakla birlikte hükümlerin daha iyi anlaşılabilmesi ve konu bütünlüğünün sağlanması amacıyla çalışma kapsamında öncelikle internet erişiminin engellenmesi konusu incelenmiştir. Bu başlık altında internet erişiminin engellenmesinin kavramsal boyutu ve engelleme yöntemlerinin neler olduğu üzerinde durulmaktadır. Ardından suç işlenmesinin önlenmesi amacıyla internet erişiminin engellenmesi hususu Kanuni düzenlemeler ve ilgili yargı kararları çerçevesinde etraflıca ele alınmaktadır.

I. İNTERNET ERİŞİMİNİN ENGELLENMESİ

A. Genel Olarak

Günümüzde internet en önemli iletişim araçlarından birisi haline gelmiştir. Dünyadaki milyarlarca insan tarafından kullanılan internetin her geçen gün etki alanı giderek genişlemektedir.[5] İnternetin insan yaşamına sağladığı pek çok katkı bulunmaktadır. Bu yönüyle internetin olumlu özellikleri bulunan bir araç olduğu söylenebilecektir. Ancak buna karşın bazı hallerde internetin olumsuz sonuçlara da yol açtığı görülmektedir. Bu olumsuz sonuçlar genellikle internetin kötü niyetli kullanımından kaynaklanmaktadır.[6]

İnternet vasıtasıyla ortaya çıkan olumsuz durumları gidermek amacıyla her Devlet kendi içerisinde birtakım yöntemlere başvurmaktadır. Bu yöntemlerden bir tanesi de internet erişiminin engellenmesidir.[7] İnternet erişiminin engellenmesi; internet üzerinden yayımlanan haber, video, fotoğraf, yazı vb. içeriklerde Devletlerce belirlenen durumların

---

5 Ahmet Buğra Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," (Yüksek Lisans Tezi, Selçuk Üniversitesi, 2017), 80.

6 Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 80.

7 Bülent Kent, *Türkiye'de İnternet Sitelerine Erişimin Engellenmesi* (Ankara: Adalet Yayınevi, 2019), 51; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 197.

ortaya çıkması halinde (kişilik haklarının ihlali, özel hayatın gizliliği, suç işlenmesinin önlenmesi, kamu yararı, kamu düzeninin korunması vb.) bu içeriğin bulunduğu internet sitesine erişimin Devlet gücü ile birtakım yöntemlerle (IP adresinden ya da URL adresinden engelleme gibi) engellenmesini ifade etmektedir.[8]

İnternet erişiminin engellenmesi ile internetten içeriğin kaldırılması birbirinden farklı kavramlardır. İnternet erişiminin engellenmesi içeriğin yayınladığı web sitesine girilememesi sonucunu doğuruyor iken; internetten içeriğin kaldırılması söz konusu içeriğin silinerek tamamen ortadan kaldırılmasını ifade eder. Dolayısıyla internet erişiminin engellenmesi içeriğe ulaşmanın önüne geçen bir fonksiyona sahiptir. Yani aslında o içerik varlığını korumakta yalnızca ona ulaşım engellenmektedir. İçeriğin kaldırılması halinde ise söz konusu içerik tamamen ortadan kaldırılmakta; dolayısıyla o içeriğe ulaşılması mümkün olmamaktadır. Öte yandan internet erişiminin engellenmesi yalnızca o engellemeyi yapan Devletin ülke sınırları içerisinden bu içeriğe ulaşmayı engellerken; içeriğin kaldırılması halinde söz konusu içeriğe dünyadaki hiçbir ülkeden ulaşılamamaktadır.[9]

B. Yöntemleri

İnternet erişiminin engellenmesi bazı teknik yöntemler kullanılarak gerçekleştirilmektedir. Devletler kendi iç mevzuatlarında bu tekniklerden birini ya da birkaçını tercih etmektedir.

---

[8] Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 51; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 197.

[9] Kemal Gözler, "Erişimi Engellenen Bir Web Sayfasının İçerik Sağlayıcı Tarafından Yayından Çıkarılması Ne İşe Yarar? Erişim Sağlayıcıları Birliğinin 3 Eylül 2019 Tarihli Bir E-Postasının Düşündürdükleri (İçerik Sağlayıcıları İçin Bir Uyarı)" ANAYASA.GEN.TR, erişim tarihi Kasım 30, 2020, https://www.anayasa.gen.tr/esbnin-epostasi.htm.

Erişim engellemede kullanılan her bir tekniğin ortaya çıkardığı sonuçlar da farklı olmaktadır. Bunlarla sınırlı olmamak kaydıyla erişim engelleme teknikleri arasında ön plana çıkan üç adet teknik bulunmaktadır[10]. Bunlar; alan adından (DNS/Domain Name System) erişim engelleme ve IP (İnternet Protocol) adresinden erişim engelleme ve nesne tabanlı (URL/Uniform Resource Locator) erişimi engellemedir.[11]

1. Alan Adından Erişim Engelleme

Bu yöntemde alan adı (DNS) sunucularındaki söz konusu internet sitesine ait alan adı kapatılarak internet sitesine erişim engellenmektedir[12]. Alan adları (domain name), web sitelerinin internette tanımlanmasını sağlayan IP adresine göre daha basitleştirilmiş ve kelimelerle ifade edilen isimlerdir.[13]

Bu engelleme yönteminde; alan adı engellenen bir web sitesine kişi ulaşmak istediğinde öncelikle sunucuya bu alan adını girmekte; bunun karşılığında tarayıcı tarafından söz konusu siteye ait IP adresi DNS sunucusuna sorulduğunda DNS sunucu tarafından o internet sitesine ait IP adresi değil de sitenin

---

10 Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 198.

11 Sevgi Türkmen, "5651 sayılı Kanuna Göre Erişimin Engellenmesi". REHBERHUKUK.NET, erişim tarihi Kasım 30,2020,https://rehberhukuk.net/uploads/files/SEVGİ%20TÜRKMEN%205651%20sayılı%20kanuna%20göre%20erişimin%20engellenmesi%20.pdf.

12 Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 83; Türkmen, "5651 sayılı Kanuna Göre Erişimin Engellenmesi," 27.

13 Ali Osman Özdilek, *İnternet ve Hukuk* (İstanbul: Papatya Yayıncılık, 2002), 128; Burcu Görkemli. *Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi* (Ankara: Adalet Yayınevi, 2015), 69; Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 60.

engellenmiş olduğunu belirten sayfaya ait IP adresi verilerek siteye erişim engellenmektedir.[14]

Alan adından erişim engelleme yönteminin olumsuz yönü söz konusu içeriğin bulunduğu internet sitesi içerisinde yer alan tüm verilere erişimin engellenmesi sonucunu doğurmasıdır[15]. Bu yöntem ile yapılan engelleme neticesinde engellemeye neden olan içerik dışındaki diğer içeriklere de ulaşılması engellenmektedir. Bu yönüyle bu yöntemin uygulanması halinde ceza sorumluluğunun şahsiliği ve ölçülülük ilkelerinin ihlal edileceği belirtilmektedir.[16]

2. IP Adresinden Erişim Engelleme

IP adresi; internet iletişimi içerisinde bulunan cihazların birbirinden ayırt edilmesini sağlayan, internet protokolü standartlarına göre verilen ve rakamlarla ifade edilen belirleyici bir kimlik olarak tanımlanabilecektir. Nitekim 30.11.2007 tarihli ve 26716 sayılı Resmi Gazetede yayımlanarak yürürlüğe giren İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin Tanımlar başlıklı 3 üncü maddesinin h bendinde; IP adresi: *"Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adresi ifade eder."* şeklinde tanımlanmaktadır. Dolayısıyla internete bağlanan her bir bilgisayarın mutlaka bir IP adresiAmerigo Md BTbulunmaktadır. IP adresi birbirinden

---

[14] Görkemli, "Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi," 106; Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," .83; Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 61; Özdilek, "İnternet ve Hukuk," 128.

[15] Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 61; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 198.

[16] Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 61; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 198.

noktalarla ayrılan dört adet rakamsal gruplamalardan oluşmaktadır.[17]

Bu yöntem ile erişimin engellenmesinde; IP adreslerini ulaşılabilir kılan sistemde söz konusu siteye ait IP adresi ulaşılamaz hale getirilerek bu IP adresi devre dışı bırakılmaktadır. Bu işlem neticesinde söz konusu IP adresi üzerinden kullanılan sistem kullanıma kapatılmaktadır.[18]

Bir IP adresi sunucusu üzerinden birden fazla web sitesinin ya da farklı web sitelerine ait içeriklerin yayınlanması mümkün olduğundan; bu yöntemin kullanılması bazı durumlarda olumsuz sonuçlara yol açabilmektedir. Örneğin; suç teşkil eden bir içeriğin engellenmesi amacıyla bu yöntemin tercih edilmesi halinde aslında hiçbir hukuka aykırılık teşkil etmeyen başkaca bir içeriğin de engellenmesi sonucu ortaya çıkacaktır. Dolayısıyla bu hallerde söz konusu yöntemin uygulanması ceza sorumluluğunun şahsiliği ilkesine de aykırı bir uygulama olacaktır.[19]

3. Nesne Tabanlı Erişim Engelleme

İnternet sitelerinin resmi ismi *"Uniform Resource Locator (URL)"* olarak adlandırılmaktadır.[20] Bu terim "Standart Kaynak Bulucu" olarak Türkçeye çevrilebilecektir. URL bir internet sitesinin adresini ifade eden adıdır. Örneğin;

---

17 Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," .82; Türkmen, "5651 sayılı Kanuna Göre Erişimin Engellenmesi," .27.

18 Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 63.

19 Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," .83; Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 63; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 198.

20 Görkemli, "Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi," 105; Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 83.

"https://sbe.asbu.edu.tr/tr/duyurular" bir URL'dir. Bu yönüyle URL, söz konusu içeriğin yer aldığı internet adresine gitmemizi sağlayan açık adres olarak karşımıza çıkmaktadır[21].

Bu yöntem ile erişimin engellenmesinde; DNS sunucusundan doğru adresi alınarak doğru IP adresine bağlanılmasına karşın tarayıcı tarafından yöneltilen talepler internet servis sağlayıcı tarafından sürekli incelenmektedir[22]. Yapılan bu incelemelerde hukuka aykırı içeriğin bulunduğu adrese ilişkin talepler engellenerek kişinin bu içeriğe ulaşması önlenmektedir.[23]

Bu yöntem ile yalnızca engellenmeye neden olan içeriğe erişim engellendiği için uluslararası metinlerde bu yöntemin hukuki olarak kullanılması tavsiye edilmektedir.[24] Söz konusu internet sitesinin tamamına değil de yalnızca zararlı içeriğin bulunduğu sayfasının yer aldığı bölüme yönelik erişim engeli uygulanması hakkaniyet ve ölçülülük ilkesinin bir gereğidir.[25] Aksi takdirde; bireylerin internet kullanımı ile bağlantılı temel hak ve özgürlüklerinin orantısız ve ölçüsüz biçimde sınırlandırılması söz konusu olacaktır.

---

21 Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 63.

22 Görkemli, "Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi," 105.

23 Görkemli, "Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi," 105.

24 Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 83; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 198.

25 Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 64.

II. 5651 SAYILI KANUN AÇISINDAN İNTERNET ERİŞİMİNİN ENGELLENMESİ

A. Genel Olarak

İnternet kullanımının yaygınlaşması ve etki alanının giderek genişlemesi nedeniyle her Devlet internet ortamındaki hukuka aykırı faaliyetlerin önlenmesi ve ortadan kaldırılması amacıyla kendi iç mevzuatlarında düzenlemeler yapma ihtiyacı duymuştur.[26] Bu kapsamda ülkemizde de 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hazırlanarak 23.05.2007 tarihli Resmi Gazetede yayımlanarak yürürlüğe sokulmuştur.[27] Akabinde Kanunda yer alan düzenlemelere ilişkin usul ve esasların belirlendiği İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik 30.11.2007 tarihli ve 26716 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

Kanunun genel gerekçesinde; *"Dünyada yaşanan gelişmelere paralel olarak, ülkemizde de, internet dahil hızla yaygınlaşan elektronik iletişim araçlarının sağladığı imkânların suiistimal edilmesi suretiyle işlenen suçlarla mücadele konusunda etkin ve doğru bir yapılanmayı mümkün kılabilecek özel bir kanun çıkartılması zorunlu hale gelmiş bulunmaktadır."* ifadelerine yer verilmektedir. Ayrıca gerekçede Devletin aileyi, çocukları ve gençleri korumakla görevli olduğundan bahisle; internetin kötüye kullanılmasıyla bu kimselere karşı kolayca suç işlenmesinin önlenmesine yönelik gerekli tedbirlerin alınmasının amaçlandığı belirtilmektedir.[28]

---

[26] Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 94; Ferhat Tuna Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı" (Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi, 2019), 40.

[27] Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 94; Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 40.

[28] Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 36.

Kanunda yer, içerik, erişim sağlayıcıları gibi internet süjeleri tanımlanarak bunların yükümlülükleri düzenlenmiştir.[29] Aynı şekilde yükümlülüklerini ihlal eden internet süjelerine uygulanacak yaptırımlar da Kanun kapsamında yer almıştır. Öte yandan Kanun ile erişim engelleme kararlarının uygulanması ve erişim sağlayıcıları arasında koordinasyonun sağlanması ile görevli olan Erişim Sağlayıcıları Birliği adında bir kuruluş oluşturulmuştur. Kanunda yer alan hükümler ile ülkemizde internet erişiminin engellenmesinin hangi hallerde ve nasıl uygulanacağı detaylı bir şekilde düzenlenmiştir.

Kanunda yer alan düzenlemelere bütünsel olarak bakıldığında; adli para cezasına ilişkin düzenlemeleri içermesi bakımından özel bir ceza kanunu niteliğini, idari para cezasına ilişkin düzenlemeleri bakımından kabahatlere ilişkin özel bir kanun niteliğini, ceza muhakemesine ilişkin getirdiği düzenlemeler bakımından ise ceza yargılamasına ilişkin düzenlemeler içeren özel bir kanun niteliğini taşıdığı görülmektedir.[30] Doktrinde Kanunun hukuki niteliğine ilişkin çeşitli görüşler ileri sürülmüştür. Bu görüşlerden bir tanesi; Kanunun yeni suç tipleri ortaya koymaması nedeniyle özel bir ceza kanunu olarak nitelendirilemeyeceğini; içerdiği düzenlemeler bakımından ancak ceza hukukuna yardımcı özel bir kitle iletişim Kanunu niteliğinde olabileceğini belirtmiştir.[31] Bir başka görüş ise Kanunun idare hukuku ve ceza muhakemesi hukukuna ilişkin düzenlemeler içeren kendine özgü bir Kanun niteliğinde olduğunu belirtmektedir. Katıldığımız bir başka görüşe göre ise; Kanun, idare hukuku, kabahatler hukuku, ceza hukuku, ceza muhakemesi hukuku ve özel hukuka ilişkin düzenlemeleri bünyesinde barındıran kendine özgü (sui generis) bir Kanun niteliğindedir.

---

29 Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 40.

30 Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 40.

31 Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 40.

Kanunun konumuz açısından önemli olan düzenlemeleri internet erişiminin engellenmesine ilişkin hükümleridir. İnternet erişiminin engellenmesi Kanunun 8, 8/A, 9 ve 9/A maddelerinde yer alan hükümler ile detaylı bir şekilde düzenlenmiştir. Söz konusu maddelerde yer alan düzenlemelere bakıldığında her hüküm açısından internet erişiminin engellenmesi nedenleri, karar vermeye yetkili mercii ve uygulanacak usulün farklı olduğu görülmektedir. Kanunun 8 ve 8/A maddeleri suç işlenmesinin önlenmesi amacıyla internet erişiminin engellenmesi usulünü düzenliyorken; 9 uncu maddesi kişilik haklarının ihlali nedeniyle, 9/A maddesi ise özel hayatın gizliliğini ihlal nedeniyle erişimin engellenmesi usulünü düzenlemektedir.

B. Kanunun 8 inci Maddesine Göre Erişimin Engellenmesi

1. Maddenin İncelenmesi

Kanunun 8 inci maddesi kapsamında internet ortamında suç teşkil edecek bir içeriğin bulunması halinde internet erişiminin engellenmesine ilişkin bir düzenleme yapıldığı görülmektedir. Maddenin ilk fıkrasında, hükümde yer verilen katalog suçların işlendiğine ilişkin yeterli şüphenin bulunması halinde internet üzerinden yayınlanan içeriğe erişimin engellenmesine karar verileceği belirtilmektedir. Hükmün lafzı esas alındığında belirtilen katalog suçların işlendiği hususunda yeterli şüphenin varlığı halinde erişimin engellenmesine karar verilmek durumundadır. Dolayısıyla burada karar vermeye yetkili merciiye bir takdir yetkisi bırakılmamıştır.

Kanunun 8 inci maddesinin ikinci ve üçüncü fıkrasında ise birinci fıkra çerçevesinde verilecek erişim engelleme kararının hangi usul çerçevesinde verileceği ve bu kararın nasıl uygulanacağı belirtilmektedir. Dördüncü fıkrada ise bir idari makam olan BTK Başkanının resen erişim engelleme kararı verebileceğine ilişkin bir hüküm yer almaktadır. On ve on birinci fıkra hükümlerinde erişim engelleme kararlarının yerine getirilmemesi halinde uygulanacak olan yaptırımlar; on iki ve on üçüncü fıkra hükümlerinde ise bu yaptırımlara karşı

başvurulacak hukuki yol düzenlenmektedir. Maddenin on dördüncü fıkra hükmünde 5602 sayılı Şans Oyunları Hâsılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanuna atıf yapılarak belirtilen kamu kurum ve kuruluşları tarafından da erişimin engellenmesi kararı verilebileceği belirtilmektedir.

Kanunun 8 inci maddesine 10.09.2014 tarihli ve 6527 sayılı Kanun ile sonradan eklenen on altıncı fıkra hükmü Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli kararı ile iptal edilmiştir. Maddenin on yedinci fıkrası ile de bu madde kapsamında verilecek erişimin engellenmesi kararının uygulanma yönteminin düzenlendiği görülmektedir.

2. Engelleme Kararlarının Hukuki Niteliği

Kanunun 8 inci maddesinin sistematiğine bakıldığında internet erişiminin engellenmesinin koruma tedbiri ve idari tedbir olmak üzere ikili bir ayrımla düzenlendiği görülmektedir.[32] Nitekim maddenin; ikinci fıkrasının son cümlesinde *"Koruma tedbiri olarak verilen içeriğin çıkarılmasına ve/veya erişimin engellenmesine ilişkin karara 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hü-kümlerine göre itiraz edilebilir"*, onuncu fıkrasında yer alan *"koruma tedbiri olarak verilen…"*, ve on birinci fıkrasında yer alan *"idari tedbir olarak verilen…"* ifadelerinden kanunkoyucunun bu yönde bir nitelendirme yapmayı tercih ettiği anlaşılmaktadır. Maddenin sistematiğinden hareket edildiğinde kanunkoyucunun adli merciler tarafından verilen erişim engelleme kararlarını "koruma tedbiri"; idari merciler tarafından verilen erişim

[32] Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 56; Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 41; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 213.

engelleme kararını ise "idari tedbir" olarak nitelendirdiği sonucuna ulaşılmaktadır.[33]

Her ne kadar kanunkoyucu tarafından bu şekilde bir nitelendirme yapılmış olsa da doktrinde bu kararların hukuki niteliğine ilişkin farklı görüşler ileri sürülmüştür. Koruma tedbiri adlandırılmasına ilişkin olarak doktrinde bir görüş; her ne kadar bir suç şüphesi nedeniyle ve adli merciler tarafından veriliyor olsa da bu kararın ceza muhakemesi hukuku anlamında bir koruma tedbiri olarak nitelendirilemeyeceğini belirtmektedir.[34] Söz konusu görüşe göre; madde kapsamında alınan erişim engellenmesi kararı ceza muhakemesi hukukunda yer alan koruma tedbiri kavramının klasik amaçlarından farklı bir amacı ihtiva etmektedir. Bu kapsamda verilen erişim engellenmesi kararının temel amacı ve fonksiyonu maddede sayılan katalog suçların işlenmesini önlemektir. Dolayısıyla bu tedbirin temel amacı esas itibariyle bir suçun işlenmesini önlemektir.[35] Bu yönüyle söz konusu erişim engellenmesi kararı klasik anlamda bir koruma tedbiri olarak nitelendirilemeyecektir. Görüşe göre; bu kapsamda verilen erişim engelleme kararı ancak internet aracılığıyla bazı suçların önlenmesi amacını taşıyan kendine özgü bir tedbir olarak nitelendirilmelidir. Bir başka görüşe göre ise; söz konusu tedbir ile bir delilin korunmasından ziyade suç işlenmesinin önlenmesi

---

33 Görkemli, "Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi," 119; Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 56; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 213.

34 Murat Volkan Dülger ve Yasin Beceni, *Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler* (Ankara: TÜSİAD Yayınları, 2011), 38; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 215.

35 Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 41.

ve kamunun zarar görmemesi amaçlandığından bu tedbirin "önleyici tedbir olarak" nitelendirilmesi gerekmektedir.[36]

Koruma tedbiri kavramı doktrinde çeşitli şekillerde tanımlanmıştır. Bir tanıma göre koruma tedbiri; ceza muhakemesinin gecikmeksizin yapılabilmesini, uyuşmazlığın konusunu oluşturan somut olaya uygun karar verilebilmesini ve verilen kararın uygulanabilmesini sağlamaya yönelik tedbirlerdir.[37] Bir başka tanımda ise koruma tedbiri; ceza muhakemesinde maddi gerçeğe ulaşabilmek ve sonuçta verilen kararların uygulanabilmesini sağlamak amacıyla başvurulması gereken tedbirler olarak tanımlanmaktadır.[38] Bu tanımlardan da anlaşılacağı üzere koruma tedbiri, ceza yargılamasının yürütülebilmesi ve yargılama neticesinde verilen hükmün uygulanabilmesi amacıyla alınan tedbirler olarak karşımıza çıkmaktadır.[39] Bu yönüyle bakıldığında ceza muhakemesi anlamında koruma tedbiri kavramının bir suçun işlenmesinin önlenmesi amacını taşımadığı açıktır. Kanaatimizce; ceza yargılamasının yürütülmesi amacıyla alınabilecek haller dışında (örneğin; delillerin yok edilmesi ihtimali gibi) sırf bu kararın adli merciler tarafından verilmesi nedeniyle bu kararların koruma tedbiri olarak nitelendirilmesi hukuken yerinde olmayacaktır. Her bir karar özelinde kararın alınmasının temelinde yatan amaç göz önünde bulundurularak hukuki nitelendirme yapılmasının daha uygun olacağı düşünülmektedir.

---

36 Görkemli, "Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi," 119.

37 Nevzat Toroslu ve Metin Feyzioğlu, *Ceza Muhakemesi Hukuku* (Ankara: Savaş Yayınevi, 2020), 214.

38 Yener Ünver ve Hakan Hakeri, *Ceza Muhakemesi Hukuku* (Ankara: Yetkin Yayınları, 2020), 313.

39 Dülger ve Beceni, "Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler," 41; Kent, "Türkiye'de İnternet Sitelerine Erişimin Engellenmesi," 58; Söyler, "Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi," 214.

Kanunun 8 inci maddesi kapsamında idari merciler tarafından verilen kararlar ise "idari tedbir" olarak nitelendirilmektedir. Bu nitelendirmede yine kararı veren mercilerin idari nitelikte olmalarından hareket edilmiştir. Madde kapsamında karar vermeye yetkili idari mercilerin; Bilgi Teknolojileri ve İletişim Kurumu Başkanı ve 5602 sayılı Şans Oyunları Hâsılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3. maddesinin birinci fıkrasının ç bendinde tanımlanan kurum ve kuruluşlar olduğu görülmektedir. Her ne kadar bu kararı veren kişiler idari merciler olsa da bu nitelendirmenin ayrıca idarenin hangi faaliyeti kapsamında verildiği açısından da değerlendirilmesi gerekmektedir.[40]

İdari tedbir kavramı doktrinde; asıl amacı cezalandırma olmamakla birlikte kamu düzeni, güvenliği ya da sağlığını korumak amacıyla ortaya çıkması muhtemel bir tehlikeyi önlemek için idare tarafından alınan önlemler şeklinde tanımlanmaktadır.[41] Örneğin; kamu sağlığının korunması amacıyla bir işyerinin geçici olarak kapatılmasına ilişkin idarece alınan karar bir idari tedbir olarak nitelendirilebilecektir. Madde kapsamında idari mercilerce verilen kararların alınmasının altında yatan amaca bakıldığında bu kararların idarelerce söz konusu suçun işlenmesinin sona erdirilmesi ve dolayısıyla da o suçun yol açtığı kamusal zararları ortadan kaldırma amacıyla alındığı anlaşılmaktadır. Nitekim suç niteliğinde olan bir içeriğin internet ortamında yayınlanmaya devam etmesi gerek toplumsal gerekse bireylerin hakları üzerinde olumsuz sonuçları olan bir durumdur. Kanaatimizce, bu durumu ortadan

---

40 Melikşah Çırakoğlu, "5651 sayılı Kanun Çerçevesinde İnternet Erişiminin Engellenmesi ve Erişim Sağlayıcıları Birliği" (Yüksek Lisans Tezi, Yıldırım Beyazıt Üniversitesi, 2015), 34.

41 Ali Ulusoy, *İdari Yaptırımlar* (İstanbul: On İki Levha Yayıncılık, 2013), 175; Mustafa Karabulut, *İdari Yaptırımların Hukuki Rejimi* (Ankara: Turhan Kitabevi, 2008), 14; Yücel Oğurlu, *İdari Yaptırımlar Karşısında Yargısal Korunma* (Ankara: Seçkin Yayıncılık, 2001), 86/ Dipnot 386.

kaldırmaya yönelik alınan kararın idari tedbir olarak nitelendirilmesi kavramsal açıdan bir sorun teşkil etmeyecektir.

3. Engelleme Kararlarının Alınması

a. Koruma Tedbiri Olarak Verilen Kararlar

Kanunun 8 inci maddesinin birinci fıkrasında yer alan hüküm uyarınca; internet ortamında yer alan içeriğin sayılan katalog suçlardan birisini oluşturduğu hususunda yeterli şüphenin bulunması halinde soruşturma evresinde hâkim, kovuşturma evresinde ise mahkeme tarafından internet erişiminin engellenmesine karar verilecektir. Soruşturma evresinde gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı tarafından da erişimin engellenmesi kararı verilebilecektir. Ancak bu halde Cumhuriyet Savcısı tarafından alınan kararın, en geç 24 saat içerisinde hâkimin onayına sunulması ve hâkim tarafından da en geç 24 saat içerisinde bu kararın onaylanması gerekmektedir. Aksi durumda bu karar Cumhuriyet Savcısı tarafından derhal kaldırılacaktır. Maddenin on beşinci fıkrasında yer alan hüküm uyarınca; soruşturma evresinde verilecek kararlar bakımından, birden fazla sulh ceza mahkemesinin bulunduğu yerlerde bu kararlar Hâkimler ve Savcılar Kurulu tarafından belirlenen sulh ceza mahkemesi tarafından verilecektir.

Kanunun 8 inci maddesinin ikinci fıkrasında; bu kapsamda verilecek erişimin engellenmesi kararı amacı gerçekleştirecek nitelikte görülmesi halinde belirli bir süreyle sınırlı olarak da verilebileceği belirtilmektedir. Doktrinde; bu hükümden hareketle erişim engelleme kararlarının koruma tedbiri niteliğine de uygun olarak geçici süreliğine verilmesi gerektiği savunulmaktadır.[42] Erişim engelleme kararının kişiler üzerinde cezai bir sonuç doğurmaması için kural olarak belirli bir süreyle

[42] Kalender, "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi," 97.

sınırlı olarak verilmesi gerektiği belirtilmektedir. Görüşe göre tedbir bir amaç değil araç olmalıdır.

Bu kapsamda internet erişiminin engellenmesine yönelik bir kararın verilebilmesi için öncelikle maddede sayılan katalog suçlara ilişkin olarak adli mercilerce başlatılmış bir ceza soruşturmasının ya da kovuşturmasının bulunması gerekmektedir. Ceza soruşturmasının ya da kovuşturmasının bulunması kararın verilmesi bakımından tek başına yeterli olmayıp aynı zamanda bu engelleme kararına konu içerik ile sayılan suçların işlendiğine yönelik yeterli suç şüphesi bulunmak zorundadır. Şüphe, ceza yargılaması bakımından önemli bir kavram olarak karşımıza çıkmaktadır. En genel tabirle şüphe, bir olay hakkında duyulan kuşku halidir. Ceza muhakemesi hukukunda şüphe, maddi gerçeği ne olduğu hususunda var olan belirsizliğin yoğunluğuna göre derecelendirilmiştir.[43] Bu kapsamda şüphe; basit şüphe, makul şüphe, yeterli şüphe ve kuvvetli şüphe olmak üzere dört dereceli olarak ifade edilmektedir. Doktrinde yeterli şüphenin, yargılama dosyasında yer alan delillere bakıldığında şüphelinin ya da sanığın mahkûm olma ihtimalinin beraat etme ihtimalinden daha yüksek olduğu hallerde var olacağı ifade edilmektedir.[44]

Erişimin engellenmesi kararının verilebilmesi için madde kapsamında sayılan katalog suçlar; 1- İntihara yönlendirme (TCK md.84), 2- Çocukların cinsel istismarı (TCK md.103/1), 3- Uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma (TCK md.190), 4- Sağlık için tehlikeli madde temini (TCK md.194), 5-Müstehcenlik (TCK md.226), 6-Fuhuş (TCK md.227), 7- Kumar oynanması için yer ve imkân sağlama (TCK md.228),

---

[43] Özkan Gültekin, *Öğreti ve Uygulamada İddianame ve İddianamenin İadesi*, (Ankara: Seçkin Yayıncılık, 2011), 117.

[44] Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku*, (İstanbul: Beta Basım, 2015), 83; Bahri Öztürk, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, (Ankara: Seçkin Yayıncılık, 2012), 485; Ş. Cankat Taşkın, *İnternete Erişim Yasakları*, (Ankara: Seçkin Yayıncılık, 2016), 214.

8- 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar ve 9- 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlar şeklinde karşımıza çıkmaktadır. Söz konusu suç tiplerinin, kanunun genel gerekçesinde belirtilen internet gibi elektronik araçların kötüye kullanılması ile özellikle çocukların, ailenin ve gençlerin zarar görmelerini önlemeye yönelik koruyucu tedbirlerin alınması amacına uygun olarak belirlendiği görülmektedir. Söz konusu suçlar kanunda sınırlı bir şekilde sayılmış olup yorum yoluyla bu suçların genişletilmesi mümkün değildir.[45]

Koruma tedbiri olarak verilen internet erişiminin engellenmesi kararında yer alması gereken hususlar İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 15 inci maddesinde düzenlenmektedir. Hükme göre erişim engellenmesi kararında; kararı veren merciin adı, karar tarihi, soruşturma numarası ya da mahkeme esas numarası, tedbirin hangi suç için istendiği ve bu suç için yeterli şüphe sebeplerinin neler olduğu açıkça belirtilmek zorundadır.

b. İdari Tedbir Olarak Verilen Kararlar

Kanunun 8 inci maddesinde bir idari merci tarafından engelleme kararının alınması hali idari tedbir olarak erişimin engellenmesi şeklinde nitelendirilmektedir. Bu kapsamda; dördüncü fıkra hükmü çerçevesinde BTK başkanının ve on dördüncü fıkra hükmü çerçevesinde ise 5602 sayılı Şans Oyunları Hâsılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3. maddesinin birinci fıkrasının ç bendinde tanımlanan kurum ve kuruluşlarının erişim engelleme kararı alma hususunda yetkilendirildiği görülmektedir.

---

[45] Tekin Memiş, "Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri," *Erzincan Üniversitesi Hukuk Fakültesi Dergisi*, no. 3-4 (2009): 166.

BTK başkanının erişim engelleme kararı verebileceği hal ikili bir ayrıma tabi tutularak düzenlenmektedir. Birinci halde; maddenin birinci fıkrasında sayılan katalog suçları (bu suçlardan herhangi birisi) oluşturan yayınların içerik veya yer sağlayıcısı yurt dışında ise, BTK başkanı, resen bu içeriğe ilişkin yayınlara erişim engelleme kararı vermekle yetkilendirilmiştir. İkinci halde; suç konusu yayınların içerik veya yer sağlayıcısı yurt içinde ise; yayınlanan içerikle yalnızca çocukların cinsel istismarı (TCK md.103/1), müstehcenlik (TCK md.226), fuhuş (TCK md.227), kumar oynanması için yer ve imkân sağlama (TCK md.228) ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanunda yer alan suçlara ilişkin olması halinde BTK başkanı resen erişimin engellenmesi kararı verme yetkisine sahip kılınmıştır. Görüldüğü üzere suç konusu oluşturan yayının içerik veya yer sağlayıcısının yurt dışında ya da yurt içinde olmasına göre ikili bir ayrım yapılarak BTK başkanına tanınan yetki farklılaşmaktadır. İçerik veya yer sağlayıcının yurt içinde olduğu hallerde ancak içeriğin belirtilen suçlardan birisine ilişkin olması halinde BTK başkanı resen erişimin engellenmesi kararı verebilecektir.

Ekim 2021 tarihi itibariyle BTK tarafından verilen resen erişim engelleme kararlarının suç türlerine göre dağılımı; müstehcenlik %49,94, fuhuş %19,60, kumar oynanması için yer ve imkân sağlama %28,46, çocukların cinsel istismarı %1,54, yasadışı bahis %0,22, sağlık için tehlikeli madde temini %0,07, uyuşturucu ve uyarıcı madde %0,12, Atatürk aleyhine işlenen suçlar %0,03, intihara yönlendirme %0,02 şeklindedir.[46] BTK tarafından verilen erişim engelleme kararlarının % 99,76'sı çocukların cinsel istismarı, fuhuş, müstehcenlik, yasadışı bahis ve kumar suçlarına ilişkindir.

---

[46] Bkz. "Erişimin Engellenmesi Tedbiri İstatistikleri", Bilgi Teknolojileri ve İletişim Kurumu, erişim tarihi Kasım 10, 2021, https://www.guvenliweb.org.tr/dosya/brEi5.pdf.

Her ne kadar Kanun metninde hâlihazırda yer alıyor olsa da BTK başkanına tanınan bu yetki Anayasa Mahkemesinin E.2015/76, K.2017/153 sayılı ve 15.11.2017 tarihli kararı ile müstehcenlik (TCK md.226) suçu yönünden iptal edilmiştir. Söz konusu iptal kararı gereğince BTK başkanı, içerik veya yer sağlayıcının yurt dışında bulunması halinde müstehcenlik suçu bakımından resen erişim engelleme kararı verme yetkisini kullanamayacaktır. Anayasa Mahkemesinin söz konusu iptal kararı incelendiğinde; Danıştay Onüçüncü Dairesi tarafından yürütülen bir yargılama neticesinde davada uygulanacak olan normun Anayasaya aykırılık iddiasıyla yapılan bir somut norm denetimi neticesinde verilen bir karar olduğu görülmektedir. Söz konusu kararda Anayasa Mahkemesi 5651 sayılı Kanunun 8. maddesinin dördüncü fıkrasına ilişkin değerlendirmelere de yer vermektedir. Bu değerlendirmelerde Anayasa Mahkemesi, kanunla haberleşme ve ifade hürriyetine getirilen bu sınırlama yetkisinin idareye tanınırken kapsam ve sınırlarının yeterli açıklıkta çizilmediğinden bahisle belirlilik ilkesi ile bağdaşmadığı, öte yandan bu yetkinin hâkim onayına sunulmadan kullanılması göz önüne alınarak bu düzenlemenin Anayasanın 13,22 ve 26 ncı maddelerine aykırı olması nedeniyle iptali gerektiğini belirtmiştir.[47] Anayasa Mahkemesi tarafından somut norm denetimi ile bir inceleme yapıldığından sonuç itibariyle yalnızca davaya uygulanmakta olan 5651 sayılı Kanun md.8/4 hükmünün müstehcenlik suçuna ilişkin BTK başkanına yetki veren kısmının içerik veya yer sağlayıcının yurt dışında bulunması haliyle sınırlı olmak üzere iptaline karar verilmiştir.

BTK başkanına resen erişim engelleme yetkisi tanıyan bu hüküm doktrinde de eleştirilmektedir. Temel hak ve özgürlüklerin sınırlandırılmasına ilişkin bu yetkinin herhangi bir yargısal denetime tabi kılınmaksızın doğrudan bir idari merci tarafından kullanılması bu hükme yöneltilen en temel

[47] AYM, E.2015/76, K.2017/153, 15.11.2017.

eleştirilerden birisidir.[48] Koruma tedbiri olarak verilen erişim engelleme kararında yargısal süje olan Cumhuriyet Savcısı tarafından verilen kararın bile yirmi dört saat içerisinde hâkim onayına sunulması öngörülmüşken BTK başkanına verilen bu yetkinin hâkim onayına tabi tutulmaksızın tek taraflı olarak kullanılması kanaatimizce de hukuka uygun değildir. Nitekim haberleşme hürriyetinin düzenlendiği Anayasanın 22. maddesinde bu özgürlüğün ancak belirtilen sebeplere dayalı olarak hâkim kararıyla sınırlanabileceği belirtilmektedir. Haberleşme hürriyeti çerçevesinde söz konusu düzenlemenin Anayasaya aykırı olduğu zaten açıktır.

Kanuni düzenlemeden farklı olarak İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte BTK başkanına tanınan yetkinin daha sınırlı bir şekilde düzenlendiği görülmektedir. Yönetmeliğin "İdari tedbir olarak erişimin engellenmesi kararı" başlıklı 14 üncü maddesinin birinci fıkrasında; *"İçeriği 12 nci maddede belirtilen suçları oluşturan yayınlarda, içerik sağlayıcının veya yer sağlayıcının yurt dışında bulunması halinde veya içerik sağlayıcı veya yer sağlayıcı yurt içinde bulunsa bile, içeriği Türk Ceza Kanununun 103 üncü maddesinin birinci fıkrasında yer alan çocukların cinsel istismarı veya aynı Kanunun 226 ncı maddesinde yer alan müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak erişimin engellenmesine Başkanlıkça re'sen karar verilir. Türk Ceza Kanununun 103. maddesinin birinci fıkrasında yer alan çocukların cinsel istismarı veya aynı Kanunun 226 ncı maddesinde yer alan müstehcenlik suçlarını oluşturan yayınlara ilişkin olarak içerik veya yer sağlayıcının yurt içinde bulunması durumunda bu karar, yirmidört saat içinde hâkimin onayına sunulur ve hâkim kararını en geç yirmidört saat içinde verir. Bu süre içinde kararın onaylanmaması halinde tedbir, Başkanlık tarafından derhal kaldırılır ve erişim sağlayıcılara bildirilerek gereğinin yerine getirilmesi istenir."* hükmüne yer verilmiştir.

---

[48] Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 47.

Söz konusu Yönetmelik hükmü içerik veya yer sağlayıcının yurt dışında bulunması halinde BTK başkanına tanınan resen erişim engelleme kararı verme yetkisi Kanuni düzenleme ile paraleldir. Ancak içerik veya yer sağlayıcının yurt içinde bulunduğu halde BTK başkanınca resen kullanılacak yetki Yönetmelikte daha da sınırlandırılmıştır. Yönetmelik hükmüne göre bu halde BTK başkanı içeriğin yalnızca çocukların cinsel istismarı (TCK md.103/1) ve müstehcenlik (TCK md.226) suçuna ilişkin olması halinde resen erişimin engellenmesi kararı verebilecektir. Bu halde BTK başkanınca resen alınan erişimin engellenmesi kararı yirmi dört saat içinde hâkimin onayına sunulacak ve hâkim tarafından da en geç yirmi dört saat içinde karar verilecektir. Hâkim tarafından bu kararın onaylanmaması halinde karar Başkanlıkça derhal kaldırılacaktır. Her ne kadar Yönetmelik ile alınan karara ilişkin hâkim güvencesi öngörülmüş olsa da bu denetimin yalnızca içerik veya yer sağlayıcının yurt içinde bulunması halinde alınan kararlara ilişkin getirildiği gözden kaçırılmamalıdır. Kanaatimizce, kanunda öngörülmemiş olan hâkim güvencesinin Yönetmelikte öngörülmesi normlar hiyerarşisi bakımından sakıncalı bir durumdur. Bir başka açıdan söz konusu Yönetmelik hükmü mahkemelerin görevlerinin ancak kanunla düzenlenebileceğini öngören Anayasanın 142. maddesinin birinci fıkra hükmüne de aykırılık teşkil etmektedir. Bu kapsamda gerek Kanuni düzenlemede gerekse Yönetmelik hükmünde yapılacak düzenleme ile BTK başkanı tarafından resen verilen erişim engelleme kararlarının tümü bakımından hâkim onayı şartının getirilmesi Anayasaya uygunluğun sağlanması bakımından yerinde olacaktır.

Kanunun 8. maddesinin altıncı fıkra hükmüne göre; başkan tarafından verilen içeriğin çıkarılması ve/veya erişimin engellenmesi kararının konusunu oluşturan yayını yapanların kimliklerinin belirlenmesi halinde, Başkan tarafından Cumhuriyet başsavcılığına suç duyurusunda bulunulacaktır. Doktrinde söz konusu hüküm, ceza muhakemesi mevzuatıyla

uyumlu olmadığı nedeniyle eleştirilmektedir[49]. Hükmün lafzına göre; erişim engelleme kararına konu yayını yapanların kimliklerinin belirlenmesi halinde ancak BTK başkanı tarafından suç duyurusunda bulunulacağı şeklinde bir anlam ortaya çıkmaktadır. Oysa 5271 sayılı Ceza Muhakemesi Kanununa göre bir suç ihbarında bulunmak için failin kimliğinin belirlenmesi gibi bir şart getirilmemiştir. Bir suçun işlendiğine ilişkin bilgi sahibi olan herkes gerekli soruşturmanın yapılması amacıyla Cumhuriyet başsavcılığına suç ihbarında bulunabilmektedir. Suçun failini tespit etmek de ceza soruşturmasının bir parçasıdır. Bu nedenle doktrinde, BTK başkanına getirilen yükümlülüğün böyle bir şarta tabi tutulmasının hukuk mantığı ile uyumlu olmadığı belirtilmektedir.[50]

Kanunun 8 inci maddesinin on dördüncü fıkra hükmüne göre; 5602 sayılı Şans Oyunları Hâsılatından Alınan Vergi, Fon ve Payların Düzenlenmesi Hakkında Kanunun 3. maddesinin birinci fıkrasının ç bendinde tanımlanan kurum ve kuruluşları kendi görev alanlarına giren suçların internet ortamında işlendiğini tespit etmeleri halinde bu yayınlarla ilgili olarak erişim engelleme kararı vermekle yetkilidir. Kanunun 3. maddesinin birinci fıkrasının ç bendinde; ilgili kurum ve kuruluş: *"ilgili mevzuat çerçevesinde şans oyunu tertip etme hak ve yetkisine sahip kurumlar ile bu hak ve yetkinin devredildiği kurum, kuruluş ve özel hukuk tüzel kişilerini"* şeklinde tanımlanmaktadır. Söz konusu tanımdan hareketle; ilgili mevzuat çerçevesinde şans oyunu tertip etme hak ve yetkisine sahip kurumlar ile bu yetkinin devredildiği kurum, kuruluş ve özel hukuk tüzel kişileri kendi görev alanlarına giren suçlara ilişkin bu suça ilişkin

---

[49] Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 47; Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin Yayıncılık, 2018), 741.

[50] Dülger, "Bilişim Suçları ve İnternet İletişim Hukuku," 741.

yayın hakkında erişim engelleme kararı verme yetkisine sahip olacaktır.

Hükümde "kendi görev alanlarına giren suçlar" ifadesi kullanılmış olup bu suçların neler olduğu açıkça belirtilmemiştir.[51] Kanaatimizce temel hak ve özgürlüklere ilişkin sınırlayıcı bir yetkiyi düzenleyen bu hüküm belirlilik ilkesi yönünden Anayasanın 13. maddesine aykırıdır. Nitekim Avrupa İnsan Hakları Mahkemesinin 18.12.2012 tarihli Ahmet Yıldırım&Türkiye kararında da bu yetkinin açıklıkla tanınması gerektiği belirtilmektedir.[52] Öte yandan söz konusu hükümle yargı mercileri tarafından kullanılması gereken bir yetkinin idari mercilere ve hatta özel hukuk tüzel kişilerine bırakıldığı görülmektedir. Doktrinde hükmün bu yönüyle hukuk devletinde olması gereken temel hak ve özgürlüklerin yargıç kararı ile sınırlandırılması ilkesiyle bağdaşmadığı ifade edilmektedir.[53] Özellikle hükümde yer alan "suç işlendiğini tespit etmeleri halinde" ifadesinden hareket edildiğinde; bir idari kurum ya da özel hukuk tüzel kişisi tarafından suç işlendiğinin nasıl tespit edileceği izaha muhtaçtır. Üstelik yapılacak bu tespitin bir yargı merci tarafından denetlenmeden doğrudan uygulanması bir başka sorundur[54]. Bu kararların

---

51 Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 44; Taşkın, "İnternete Erişim Yasakları," 226.

52 "59. AİHM'in yerleşik içtihadına göre, bu koşullara uymak için, Sözleşme ile güvence altına alınan haklara kamu gücü tarafından keyfi biçimde zarar verilmesi halinde iç hukukta şüphesiz bir koruma imkânı sunulmalıdır. Temel haklara zarar veren fiiller söz konusu olduğunda, şayet bu duruma ilişkin takdir yetkisi kullanmakta idare organları açısından bir sınır belirlenmemişse, kanun, Sözleşme ile korunan, demokratik toplumun temel ilkelerinden birini oluşturan hukukun üstünlüğü ilkesine aykırı düşmektedir. Dolayısıyla, kanunda böyle bir yetkinin kullanılmasına ilişkin kapsam ve usullerin yeterli açıklıkla tanımlanması gerekmektedir (bkz, diğer birçok karar arasında, anılan Sunday Times, § 49 ve Maestri v. İtalya [BD], no 39748/98, § 30, AİHM 2004-I)"

53 Taşkın, "İnternete Erişim Yasakları," 226.

54 Taşkın, "İnternete Erişim Yasakları," 226.

hâkim denetimi ve onayından geçmeden uygulanması temel hak ve özgürlüklerin antidemokratik yöntemlerle sınırlandırılması sonucunu doğuracaktır.

4. Kararların Uygulanması

Kanunun 8 inci maddesi kapsamında alınan erişim engelleme kararları, BTK başkanınca karar alınması haricinde, gereği yapılmak üzere BTK'ya gönderilmektedir. Söz konusu erişimin engellenmesine ilişkin kararı alan BTK, gereği yapılmak üzere kararı ilgili içerik ve yer sağlayıcılar ile erişim sağlayıcısına bildirmektedir. Maddenin beşinci fıkra hükmüne göre; içeriğin çıkarılması ve/veya erişimin engellenmesi kararının gereği, derhal ve en geç kararın bildirilmesi anından itibaren dört saat içinde yerine getirilmek zorundadır.

Yönetmelik md. 16/4 hükmüne göre; erişim sağlayıcılar, BTK ile aralarındaki bağlantıdan aktarılacak erişimin engellenmesi kararlarının, kendi sistemlerinde derhal uygulanabilmesi için gerekli olan donanım ve yazılımı kurarak lazım olan düzenlemeleri yapmak zorundadır. BTK Başkanı tarafından resen erişimin engellenmesine karar verildiği hallerde bu karar; BTK tarafından hazırlanan ve mevcut sayfa yerine kararı veren merciin adı ile karar tarih ve sayısını belirten uyarı sayfasına yönlendirilmek suretiyle uygulanacaktır.

Kanunun 8 inci maddesinin 17 nci fıkra hükmüne göre; erişimin engellenmesinde; kural olarak nesne tabanlı erişim engelleme yöntemi kullanılacaktır. Nitekim söz konusu hükümde; *"…erişimin engellenmesi kararları ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilir."* denmektedir. Ancak teknik olarak bu yöntemin uygulanmasının mümkün olmadığı hallerde (örneğin; https sisteminin kullanılması gibi) internet sitesinin tamamına erişimin engellenmesi söz konusu olabilecektir.

Koruma tedbiri olarak verilen bir erişim engelleme kararı söz konusu ise; kişi hakkında kovuşturmaya yer olmadığına dair karar ya da beraat hükmü verilmesi ile erişim engelleme kararı

kendiliğinden hükümsüz hale gelmektedir. Bu hallerde ilgili kararlar BTK'ya gönderilerek daha önceden uygulanan erişimin engellenmesi kararının kaldırılması için gereği ivedilikle yapılmaktadır. Erişimin engellenmesi kararı verilmesine neden olan içeriğin yayından çıkarılması halinde kararı veren merci tarafından erişimin engellenmesinin kaldırılmasına karar verilecektir. Erişimin engellenmesinin kaldırılması kararı BTK'ya gönderilerek gereği BTK tarafından ivedilikle yapılacaktır.

Erişimin engellenmesi kararının gereğinin yerine getirilmemesi halinde Kanunda (md.8/10-11) kararın niteliğine göre adli ve idari para cezasına hükmedilmesi öngörülmüştür. Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen içerik, yer ve erişim sağlayıcıları sorumluları; fiil daha ağır bir cezayı gerektiren başka bir suç oluşturmadığı takdirde beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılacaktır.

İdari tedbir olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen içerik, yer ve erişim sağlayıcıları sorumluları hakkında; BTK başkanı tarafından on bin Türk lirasından yüz bin Türk lirasına kadar idari para cezasına hükmedilecektir. Söz konusu idari para cezasının verildiği andan itibaren yirmi dört saat içerisinde kararın gereğini yerine getirmeyen erişim sağlayıcının yetkilendirilmesi BTK tarafından iptal edilecektir. Bu kapsamda ilgililer hakkında verilen kararlara (idari para cezası veya yetkilendirmenin iptali) karşı 2577 sayılı İYUK çerçevesinde kanun yoluna başvurulabilecektir.

5. Kararlara Karşı Başvuru Yolları

Kararlara karşı başvurulabilecek hukuki yolların koruma tedbiri olarak verilen erişim engelleme kararı ve idari tedbir olarak verilen erişim engelleme kararı olmak üzere ikiye ayrılarak incelenmesi gerekmektedir.

Koruma tedbiri olarak erişimin engellenmesi kararı adli merciler tarafından verilmektedir. Kural olarak bu karar soruşturma evresinde hâkim; kovuşturma evresinde ise mahkeme tarafından verilmektedir. İstisnai olarak soruşturma evresinde gecikmesinde sakınca bulunan hallerde bu karar yirmi dört saat içerisinde hâkim onayına sunulmak üzere Cumhuriyet Savcısı tarafından da verilebilmektedir. Maddenin ikinci fıkrasının son cümlesinde bu kapsamda verilen erişim engelleme kararlarına karşı 5271 sayılı Ceza Muhakemesi Kanununa göre itiraz yoluna başvurulabileceği belirtilmektedir.

CMK'nın 267-271 inci maddeleri arasında itiraz, olağan kanun yolu olarak düzenlenmektedir. CMK'nın 267 nci maddesine göre hâkim kararları ile kanunun gösterdiği hâllerde, mahkeme kararlarına karşı itiraz yoluna gidilebilmektedir. Kanun yollarına başvurma hakkı ise CMK'nın 260 ıncı maddesinin birinci fıkrasında düzenlenmektedir. Söz konusu hükümde; *"Hâkim ve mahkeme kararlarına karşı Cumhuriyet savcısı, şüpheli, sanık ve bu Kanuna göre katılan sıfatını almış olanlar ile katılma isteği karara bağlanmamış, reddedilmiş veya katılan sıfatını alabilecek surette suçtan zarar görmüş bulunanlar için kanun yolları açıktır."* denmektedir. Bu hükümden hareket edildiğinde erişim engelleme kararlarına karşı; soruşturma evresinde şüpheli (içeriği oluşturan veya yayan) ve cumhuriyet savcısı tarafından; kovuşturma evresinde ise, sanık (içeriği oluşturan veya yayan), cumhuriyet savcısı ile katılan (suçtan zarar görüp katılan sıfatını alan kişi) tarafından itiraz edilmesi mümkün olacaktır.[55]

CMK'nın itiraz kanun yoluna ilişkin düzenlemelerine ek olarak 5651 sayılı Kanunda da özel birtakım düzenlemelerin yer aldığı görülmektedir. Bu kapsamda; Kanunun 8 inci maddesinin on üçüncü fıkra hükmü ile koruma tedbiri olarak verilen erişim engellenmesi kararlarına karşı BTK'nın da itiraz kanun yoluna başvurabileceği öngörülmüştür. Söz konusu özel düzenleme

[55] Çırakoğlu, "5651 sayılı Kanun Çerçevesinde İnternet Erişiminin Engellenmesi ve Erişim Sağlayıcıları Birliği," 37.

gereğince gereği yapılmak üzere kendisine gönderilen engelleme kararlarına karşı BTK tarafından da itiraz kanun yoluna başvurabilecektir. CMK'nın 268 inci maddesinin birinci fıkra hükmüne göre başvuru hakkı bulunanlar engelleme kararını öğrendikleri günden itibaren yedi gün içerisinde kararı veren mercie bir dilekçe vermek suretiyle ya da zapta geçirerek karara itiraz edebilecektir.

İdari tedbir olarak erişimin engellenmesine ise idari merciler tarafından karar verilmektedir. Bu kapsamdaki erişim engelleme kararlarının BTK başkanı ve 5602 sayılı Kanun md.3/1-ç de tanımlanan kamu kurum ve kuruluşları tarafından verildiği görülmektedir. İdari tedbir olarak verilen erişim engelleme kararlarına karşı hangi hukuki yola başvurulacağı 5651 sayılı Kanunda açıkça düzenlenmemiştir. Bu nedenle genel hükümler dairesinde bir belirleme yapılmak durumundadır.

İdari tedbir olarak verilen erişim engelleme kararlarının bir idari kurum ya da kuruluş tarafından verilmesi halinde söz konusu işlem bir idari işlem niteliğinde olacağından bu karara karşı İYUK hükümleri çerçevesinde idari başvuru yoluna gidilmesi ya da dava açılması mümkündür. Bu kapsamda erişim engelleme kararının idari işlem olması halinde; ilgili kişi dava yoluna gitmeden idari işlemin kaldırılması, geri alınması, değiştirilmesi veya yeni bir işlem yapılmasını üst makamdan, üst makam yoksa işlemi yapmış olan makamdan, idari dava açma süresi içinde isteyebileceği gibi doğrudan bu karara karşı idari yargı mercilerinde iptal veya tam yargı davası da açılabilecektir.

5602 sayılı Kanunun md.3/1-hükmünde yer alan tanım gereğince istisnai olarak özel hukuk tüzel kişileri tarafından da (örneğin; Türkiye Jokey Kulübü) erişimin engellenmesi kararı verilebilmesi mümkün kılınmıştır. Ancak burada her ne kadar özel hukuk tüzel kişileri ifadesi yer almış olsa da tanımda *"ilgili mevzuat gereğince yetkilendirilmiş idareler tarafından yetkinin devredildiği özel hukuk tüzel kişileri"* şeklinde bir ifadeye yer verilmiştir. Dolayısıyla bu yetkinin asıl sahibi esas itibariyle

mevzuat gereğince yetkili olan idari kurum ya da kuruluştur. Bu çerçevede her ne kadar bir özel hukuk tüzel kişisi tarafından engelleme kararı verilecek olsa da işlemin özü ve niteliği itibariyle bir idari işlem olması nedeniyle bu kararlara karşı da İYUK hükümleri dairesinde idari yargı mercilerinde dava açılması mümkün olacaktır.[56]

6. Anayasa Mahkemesinin E.2014/149 ve K.2014/151 Sayılı Kararının İncelenmesi

5651 sayılı Kanunun 8 inci maddesine 10.09.2014 tarihli ve 6552 sayılı Kanunun 127 nci maddesi ile eklenen on altıncı fıkra hükmü Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli kararı ile iptal edilmiştir. İptal edilen hüküm; *"Millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi nedenlerinden bir veya bir kaçına bağlı olarak gecikmesinde sakınca bulunan hâllerde, erişimin engellenmesi Başkanın talimatı üzerine Başkanlık tarafından yapılır. Erişim sağlayıcıları Başkanlıktan gelen erişimin engellenmesi taleplerini en geç dört saat içinde yerine getirir. Başkan tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar."* şeklindedir.

Anayasa Mahkemesi söz konusu hükmün esas yönünden Anayasaya uygunluğunun incelenmesinde; bu hüküm ile getirilen erişimin engellenmesi müdahalesinin öncelikle Anayasanın 22 nci maddesinde düzenlenen haberleşme hürriyeti ve 26 ncı maddesinde düzenlenene düşünceyi açıklama ve yayma hürriyeti ile doğrudan ilgili olduğu tespitinde bulunmaktadır. Mahkemeye göre; internet modern demokrasilerde başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin kullanılması bakımından önemli bir değere sahip bulunmaktadır. Bu yönüyle internet konusunda yapılacak düzenlemelerde ve uygulamalarda devletlerin ve idari

[56] Çırakoğlu, "5651 sayılı Kanun Çerçevesinde İnternet Erişiminin Engellenmesi ve Erişim Sağlayıcıları Birliği," 53.

makamların çok hassas davranmaları gerekmektedir. Demokratik ülkelerde çocuk pornografisi, çocukların cinsel istismarı ve ırkçılık gibi ağır suçlar için getirilen "erişimin engellenmesi" tedbiri, yargı kararı ile yargılama sürecinin bir parçası olarak uygulanan zorunlu ve istisnai bir tedbir olarak düzenlenmektedir. Dolayısıyla erişimin engellenmesi kararı bir yaptırım niteliğinde olmayıp tedbir mahiyetindedir.

Dava konusu kural ile "milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi" nedenlerinden bir veya birkaçına bağlı olarak gecikmesinde sakınca bulunan hallerde TİB Başkanına erişim engellenmesi yetkisi verilmektedir. Mahkemeye göre; kuralda geçen "milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi" gibi nedenlerin ayrıntılı olarak somutlaştırılması ve önceden tek tek belirlenmesi mümkün değildir. Bu ifadeler uygulama ve yargı kararlarıyla anlam kazanmakta ve içerikleri bu şekilde somutlaştırılmaktadır. Anayasanın 22. maddesinin ikinci fıkrası hükmü gereğince kanunla yetkili kılınmış mercinin yazılı emri ile haberleşmenin engellenebileceği belirtilmektedir. Ancak burada bahsi geçen yetkili merciin belirlenmesinde yasa koyucu sınırsız bir yetkiye sahip değildir. Söz konusu nedenlere dayalı olarak erişimin engellenmesi konusunda yetkilendirilen TİB'in bu nedenler çerçevesinde bir değerlendirmede bulunacak konumda olmadığı açıktır. Dolayısıyla yetki verilen kurumun söz konusu nedenlere dayalı olarak değerlendirme yapma ve karar verme yetkisi gözetilmeksizin yetkilendirilmiş olması Anayasaya aykırılık oluşturmaktadır.

Mahkemeye göre; haberleşme hürriyeti ile düşünceyi açıklama ve yayma özgürlüğüne demokratik toplumlarda zorunlu tedbirler nedeniyle birtakım sınırlamalar ve koşullar getirilmesi mümkündür. Ancak bu sınırlamalar, hakkın özüne dokunamayacağı gibi Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin gereklerine ve ölçülülük ilkesine aykırı olamayacaktır. Bu haklara kamu gücü tarafından bir sınırlama imkânı getirildiği hallerde Kanunda böyle bir yetkinin

kullanılmasına ilişkin kapsam ve usullerin yeterli açıklıkta belirtilmesi gerekmektedir. Getirilen bu sınırlama yetkisinin ölçülülük ilkesine uygun olabilmesi için; "hukuken korunması gereken amaçla" , bu amacı gerçekleştirmek için kanunda tanımlı "aracın" orantılı olması gerekmektedir. Amacın gerçekleştirilmesi için seçilen aracın hak ve özgürlüğü zedeleme tehlikesinin yüksek olduğu hallerde orantılı bir sınırlamanın bulunmadığı sonucuna ulaşılmaktadır. Kuralda yer alan "milli güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi" nedenlerine dayalı olarak erişimin engellenmesi tedbiri, "amaç-araç" dengesi bakımından ifade özgürlüğü, haberleşme hürriyeti, düşünce ve ifadeyi yayma özgürlüğü noktasında bireylere tanınan temel hak ve özgürlükleri ölçüsüzce sınırlandırma tehlikesini taşıyan bir hukuki himaye vasıtasıdır. Ölçülülük ilkesi gereğince amaca ulaşmak için seçilen aracın elverişli ve zorunlu bir araç olması gerekmektedir. Bu kapsamda istenilen amaca ulaşmak için seçilen aracın bireylerin temel hak ve özgürlüklerine en az düzeyde zarar verici nitelikte olması gerekmektedir. Dava konusu kural ile yetkilendirilen TİB, belirtilen nedenlere dayalı olarak zararlı içeriğin bulunduğu internet sitesinin tamamına erişimi engelleme yetkisine sahip kılınmıştır. Kanunda yargı mercileri tarafından kullanılan yetkide dahi kademeli bir erişim engellenme tedbirinin alınması öngörülmüş iken söz konusu düzenlemede bu yönde bir sınırlandırmanın ve kademelendirmenin yapılmaması idareye çok geniş bir müdahale imkânı tanımaktadır.

Bu değerlendirmeler neticesinde Anayasa Mahkemesi söz konusu hükmün Anayasanın 2, 13, 22 ve 26. maddelerine aykırı olduğu sonucuna ulaşarak hükmün iptaline karar vermiştir.

Anayasa Mahkemesinin bu kararında yer alan gerekçelerinden bir kısmı gerek karara katılmayan üyelerin karşı oy yazılarında gerekse de doktrinde eleştirilmiştir. Gerekçeye yönelik getirilen eleştirilerden bir tanesi Anayasa Mahkemesinin TİB'e yönelik yaptığı değerlendirmeler ve tespitlerdir. Anayasa

Mahkemesi gerekçesinde TİB'in kurumsal yapısı ve görevleri itibariyle böyle bir değerlendirmeyi tek başına yapacak konumda olmadığını belirtmektedir. Mahkeme ayrıca TİB'in gerek kuruluş mevzuatı gerekse yürüttüğü görevler bakımından bir regülasyon otoritesi ya da bir adli veya idari kolluk olarak nitelendirilemeyeceği tespitinde de bulunmaktadır. Ancak doktrinde, TİB'in BTK bünyesinde çalışan bir birim olması ve görevleri arasında internetin düzenlenmesine ilişkin hususların yer alması nedeniyle internet alanında faaliyet gösteren özel bir idari kolluk olduğu ifade edilmiştir.[57] Öte yandan karşı oy yazılarında da Anayasanın 22 nci maddesine göre yetkili merciinin belirlenmesi hususunda takdir yetkisinin kanunkoyucuda olduğu, dolayısıyla kanunla yetkilendirilmiş olan kurumun bu konuda karar verebilecek birikime ve uzmanlığa sahip olup olmadığının değerlendirilmesinin Anayasaya uygunluk denetimi kapsamında yapılamayacağı ifade edilmiştir.[58] Kanaatimizce de Anayasa Mahkemesinin TİB'e ilişkin yaptığı değerlendirmeler ve tespitler yasamanın genelliği ilkesine uygun değildir. Anayasanın 22. maddesi kanunla belirlenmiş olan yetkili merci tarafından bu kararın alınabileceğini belirtmekle beraber bu merciin hangi niteliğe sahip olması gerektiği yönünde bir sınırlandırma yoluna gitmemiştir. Bu bakımdan karar verme konusunda yetkili merciinin belirlenmesinde yasa koyucunun takdir yetkisine sahip olduğunu kabul etmek gerekir. Kanunkoyucunun iradesi ile belirlenmiş olan yetkili merciinin niteliğini ve liyakatini değerlendirmek Anayasaya uygunluk denetimi kapsamı içerisinde olmamalıdır.

---

[57] Çırakoğlu, "5651 sayılı Kanun Çerçevesinde İnternet Erişiminin Engellenmesi ve Erişim Sağlayıcıları Birliği," 23.

[58] Bkz. Nuri Necipoğlu ve Muhammed Emin Kuzu'nun karşı oy gerekçesinin sekizinci paragrafı.

C. Kanunun 8/A Maddesine Göre Erişimin Engellenmesi

1. Maddenin İncelenmesi

Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli kararı ile iptal edilen on altıncı fıkra hükmü iptal gerekçeleri de dikkate alınarak yeniden düzenlenmiştir. Söz konusu düzenleme 27.03.2015 tarihli ve 6639 sayılı Kanunun 29 uncu maddesi ile 5651 sayılı Kanuna 8/A maddesi olarak eklenmiştir.

"Gecikmesinde sakınca bulunan hallerde içeriğin çıkarılması ve/veya erişimin engellenmesi" başlıklı madde içerisinde beş fıkra hükmüne yer verilmektedir. Maddenin birinci fıkrasında hangi sebeplere dayalı olarak kimlerin erişim engelleme kararı verebileceği, ikinci fıkrasında bu kararların yargısal denetime tabi tutulacağı, üçüncü fıkrasında bu erişimin engelleme kararının uygulanmasında kullanılacak yöntem, dördüncü fıkrasında suç duyurusunda bulunma yükümlüğü ve son olarak beşinci fıkrasında ise kararın yerine getirilmemesi halinde uygulanacak yaptırım düzenlenmektedir.

Maddenin birinci fıkra hükmünde düzenlenen erişim engellenmesi kararı verilebilecek halleri ikiye ayırarak incelemekte yarar vardır. Hükme göre birinci durumda; *"yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması"* sebeplerinden bir veya bir kaçına bağlı olarak hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhurbaşkanlığı tarafından erişimin engellenmesi kararı verilebilecektir. İkinci durumda ise gecikmesinde sakınca bulunan hallerde *"millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması"* sebeplerine bağlı olarak ise ilgili bakanlıkların talebi üzerine BTK başkanı tarafından erişimin engellenmesi kararı verilebilecektir.

Birinci fıkra hükmünün lafzından hareket edildiğinde erişimin engellenmesi kararı verme konusunda asıl yetkinin hâkimde olduğu görülmektedir. Kanunkoyucu belirtilen

sebeplere bağlı olarak öncelikle hâkim tarafından; ancak gecikmesinde sakınca bulunan hallerde, yani ivedi durumlarda, Cumhurbaşkanlığı ya da ilgili Bakanlıkların talebi üzerine BTK başkanı[59] tarafından erişimin engellenmesine karar verilebileceğini belirtmektedir. Dolayısıyla bu madde kapsamında idari merciler tarafından bu yetkinin kullanılması ancak gecikmesinde sakınca bulunan hallerde söz konusu olabilecektir.

Söz konusu madde kapsamında erişimin engellenmesi kararı vermekle yetkilendirilmiş olan mercilere bakıldığında bunlardan bir kısmının birer idari merci olduğu görülmektedir. Nitekim bu madde kapsamında erişimin engellenmesi kararını verme yetkisinin Cumhurbaşkanlığına ve ilgili Bakanlıkların talebi üzerine BTK başkanına bırakıldığı görülmektedir. Kanaatimizce kanunun sistematiğinden hareketle bu madde kapsamında idari merciler tarafından verilen erişim engelleme kararlarını da idari tedbir olarak verilen erişim engellenmesi kararı olarak nitelendirmek çok da yanlış olmayacaktır.

Hükme göre erişimin engellenmesi kararları; birinci durumda *"yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması"* sebeplerine; ikinci durumda ise *"millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması"* sebeplerine bağlı olarak verilebilecektir. Doktrinde söz konusu engelleme sebepleri soyut nitelikte olmaları ve geniş anlamlar

[59] Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli iptal kararının gerekçesinde TİB'e yönelik yapılan değerlendirmeler göz önüne alınarak BTK Başkanı tek başına bu konuda karar vermekle yetkilendirilmemiştir. BTK Başkanı ancak ilgili Bakanlığın talebi üzerine bu madde kapsamında erişimin engellenmesi kararı verebilecektir. Bu kararı tek başına alması mümkün değildir.

içermeleri nedeniyle eleştirilmektedir.[60] Eleştiriye göre; temel hak ve özgürlüklere yönelik müdahale sonucunu doğuracak bu yetkinin anlamı açık olmayan ve uygulayıcıya geniş bir takdir yetkisi imkânı veren sebeplerle kullanılabilmesi hukuki belirlilik ve ölçülülük ilkesine aykırılık teşkil etmektedir.[61]

Anayasanın 13. maddesine göre temel hak ve özgürlükler özlerine dokunulmaksızın yalnızca Anayasada belirtilen sebeplere bağlı olarak kanunla sınırlanabilmektedir. Bu sınırlamalara; Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve laik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamayacaktır. Ölçülülük ilkesi gereğince bir hak veya özgürlüğe yönelik yapılacak müdahalenin orantılılık ilkesine uygun olarak yapılması gerekmektedir. Kanaatimizce; anlamı son derece geniş ve muğlâk sebeplere dayalı olarak tanınan bu yetkinin temel hak ve özgürlüklerin ölçüsüzce sınırlandırılması sonucunu doğurma tehlikesi bulunmaktadır. Öte yandan Anayasanın 2. maddesinde düzenlenmiş olan hukuk devleti ilkesinin unsurları arasında hukuki belirlilik ve hukuki öngörülebilirlik ilkeleri yer almaktadır[62]. Hukuki belirlilik ilkesi, hukuk kurallarının ve bunların uygulanmasından doğacak sonuçların açık, anlaşılır ve ilgililer üzerindeki hukuki etkilerinin önceden bilinebilir olmasını ifade etmektedir.[63] Hukuki öngörülebilirlik ilkesi ise, bireylerin hukuk kurallarını ve bunların yol açacağı hukuki sonuçları önceden bilerek buna göre yaşamlarını sürdürmelerini

---

60 Taşkın, "İnternete Erişim Yasakları", 272; Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 49-50.

61 Taşkın, "İnternete Erişim Yasakları", 272; Kırış, "Ceza Hukuku Açısından İnternet Yayıncılığı," 49-50.

62 Selda Çağlar, *Hukuk Devletinin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi* (İstanbul: Beta Yayıncılık, 2013), 187.

63 Çağlar, "Hukuk Devletinin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi," 191; İsmail Köküsarı, *Anayasa Hukukunda Hukuki Güvenlik İlkesi* (Ankara: Adalet Yayınevi, 2015), 69.

ifade etmektedir.[64] Söz konusu Kanun hükmü hangi hallerde kişilerin internet ortamında yaptıkları yayınlara erişimin engelleneceğini önceden açık ve objektif bir biçimde ortaya koyamaması nedeniyle bu ilkelerle de uyuşmamaktadır.

Maddenin ikinci fıkra hükmüne göre; erişimin engellenmesi kararının idari mercilerce verilmesi halinde bu karar BTK başkanı tarafından yirmi dört saat içinde sulh ceza hâkiminin onayına sunulmak zorundadır. Hâkim tarafından yapılacak incelemede kararın uygun bulunmaması ya da kırk sekiz saat içerisinde hâkim tarafından kararın açıklanmaması halinde erişim engellenmesi kararı ortadan kalkacaktır.

Madde kapsamında verilen erişimin engellenmesi kararları BTK başkanı tarafından derhal erişim sağlayıcılara ve ilgili içerik ve yer sağlayıcılara bildirilecektir. Kararın gereği ilgili erişim, içerik ve yer sağlayıcısı tarafından derhal ve en geç kararın bildirilmesinden itibaren dört saat içerisinde yerine getirilmek zorundadır. Her durumda bu kararın gereği Kararın gereğini yerine getirmeyen erişim sağlayıcılar ile içerik ve yer sağlayıcıları hakkında BTK Başkanı tarafından elli bin Türk Lirasından beş yüz bin Türk Lirasına kadar idari para cezası verilecektir.

Söz konusu erişimin engellenmesi kararları; kural olarak ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verilecektir. Ancak, teknik olarak ihlale ilişkin içeriğe erişimin engellenmesi yapılamadığı veya ilgili içeriğe erişimin engellenmesi yoluyla ihlalin önlenemediği durumlarda (örneğin; https sisteminin kullanılması gibi) internet sitesinin tümüne yönelik olarak erişimin engellenmesi kararı verilebilecektir.[65]

---

64 Köküsarı, "Anayasa Hukukunda Hukuki Güvenlik İlkesi," 138.

65 Görüldüğü üzere Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli iptal kararının gerekçesinde yer verilen kademeli yöntemin uygulanmasına yeni düzenlemede yer verilmiştir.

Maddenin dördüncü fıkra hükmüne göre, suça konu internet içeriklerini oluşturan ve yayanlar hakkında BTK başkanı tarafından, Cumhuriyet Başsavcılığına suç duyurusunda bulunulacaktır. Kanunun 8 inci maddesinin altıncı fıkrasından farklı olarak burada suç duyurusunda bulunmak için faillerin kimliklerinin belirlenmesi şartının aranmadığı görülmektedir. Hükmün devamında faillere ulaşmak için gerekli olan bilgilerin içerik, yer ve erişim sağlayıcılar tarafından hâkim kararı üzerine adli mercilere verileceği belirtilmektedir. Bu bilgileri adli mercilere vermeyen içerik, yer ve erişim sağlayıcılarının sorumluları, fiil daha ağır bir cezayı gerektiren başka bir suç oluşturmadığı takdirde, üç bin günden on bin güne kadar adli para cezası ile cezalandırılacaktır.

Maddenin birinci ve ikinci fıkra hükümlerinin iptali talebiyle Anayasa Mahkemesinin 2015/61 Esas numarasına kayıtlı bir iptal davası açılmıştır. Anayasa Mahkemesi tarafından yapılan inceleme neticesinde verilen E.2015/61, K.2016/172 sayılı ve 02.11.2016 tarihli kararda; söz konusu kuralların 15.8.2016 tarihli ve 671 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname'nin 21 inci maddesiyle değiştirildiğinden[66] bahisle bu fıkralar hakkında karar verilmesine yer olmadığına hükmedilmiştir.

2. Anayasa Mahkemesinin Yaklaşımı

5651 sayılı Kanun kapsamında verilen erişim engelleme kararları Kanunda öngörülen itiraz yolunun tüketilmesiyle kesinleşmektedir. Söz konusu erişim engelleme kararlarıyla Anayasada düzenlenen bir temel hak ve özgürlüğünün ihlal

[66] 15.8.2016 tarihli ve 671 sayılı KHK'nın 21 inci maddesiyle, bu maddenin birinci ve ikinci fıkralarında yer alan *"Başkanlık"* ibareleri *"Başkan"* şeklinde değiştirilmiş olup, daha sonra bu hüküm 9.11.2016 tarihli ve 6757 sayılı Kanunun 18 inci maddesiyle aynen kabul edilerek kanunlaşmıştır. Yine 2/7/2018 tarihli ve 700 sayılı Kanun Hükmünde Kararnamenin 181 inci maddesiyle bu maddenin birinci ve ikinci fıkralarında yer alan *"Başbakanlık"* ibareleri "*Cumhurbaşkanlığı*" şeklinde değiştirilmiştir

edildiğini iddia eden kişiler kesinleşen bu kararlara karşı Anayasa Mahkemesi nezdinde bireysel başvuruda bulunmaktadır. Bireysel başvuru incelemesinde Anayasa Mahkemesi, erişim engelleme kararlarının Anayasada düzenlenen bir temel hak ve özgürlüğü ihlal edici nitelikte olup olmadığını değerlendirmektedir.

Bu kapsamda Kanunun 8/A maddesine dayanılarak verilen erişim engelleme kararlarının da Anayasa Mahkemesi nezdinde bireysel başvuru incelemesine konu edildiği görülmektedir. Temel hak ve özgürlüklerin korunmasının yanı sıra bireysel başvuru incelemesinde Anayasa Mahkemesi tarafından yapılan değerlendirmeler maddenin yorumlanması açısından da önem arz etmektedir. Her ne kadar bunlarla sınırlı olmamakla birlikte Kanunun 8/A maddesine yönelik somut tespit ve değerlendirmelere yer verilmesi nedeniyle çalışmamızda; Anayasa Mahkemesinin 2015/15977 başvuru numaralı ve 12/6/2019 tarihli bireysel başvuru kararı ile 2015/16368 başvuru numaralı ve 11/3/2020 tarihli bireysel başvuru kararı incelenmektedir.

a. Anayasa Mahkemesinin 2015/15977 Başvuru Numaralı ve 12/6/2019 Tarihli Bireysel Başvuru Kararının İncelenmesi

Karar, Kerem ALTIPARMAK ve Yaman AKDENİZ isimli akademisyenler tarafından Anayasa Mahkemesine 2/10/2015 tarihinde yapılan bireysel başvuru neticesinde verilmiştir. Bireysel başvuru, 5651 sayılı Kanunun 8/A maddesine dayanılarak verilen bazı internet sitelerinde ve sosyal medya hesaplarında yer alan içeriklere erişimin engellenmesi kararlarının haber ve fikir alma ile bilgiye erişme haklarını ihlal ettiği iddiasına dayanmaktadır.

Bireysel başvurunun konusunu oluşturan erişim engelleme kararları; Türk Silahlı Kuvvetleri tarafından 24/7/2015 tarihinde düzenlenen terör örgütlerine yönelik operasyon hakkında bazı internet sitelerinde ve sosyal medya hesapları üzerinden yapılan paylaşımlara ilişkindir. Bu kapsamda (dönemin) Başbakanlık

Güvenlik İşleri Genel Müdürlüğü talebi üzerine (kapatılan) TİB tarafından bahsi geçen terör operasyonları hakkında paylaşımda bulunan toplamda 615 internet sitesi ve sosyal medya hesabına erişimin engellenmesine karar verilmiştir. Söz konusu erişim engelleme kararları 5651 sayılı Kanunun 8/A maddesinin ikinci fıkra hükmü gereğince Gölbaşı Sulh Ceza Mahkemesinin onayına sunulmuştur. Gölbaşı Sulh Ceza Mahkemesi tarafından yapılan inceleme neticesinde; "…*Bahse konu internet ortamında yayınlanan içeriklerin yaşam hakkı ile kişilerin can ve mal güvenliğinin ihlaline sebebiyet verildiği bu sebeple TİB Başkanlığı tarafından verilen kararın usul ve yasalara uygun olduğu"* gerekçesiyle (kapatılan) TİB tarafından verilen erişim engelleme kararları onaylanmıştır. Bu kararlardan bir kısmına CMK hükümleri doğrultusunda itiraz yoluna gidilmiş ancak itirazlarının reddedilmesiyle kararlar kesinleşmiştir. Bunun üzerine söz konusu erişim engelleme kararlarına karşı başvurulacak başka bir hukuki yol kalmadığından ilgililer Anayasa Mahkemesine bireysel başvuruda bulunmuştur.

Anayasa Mahkemesi başvuruyu Avrupa İnsan Hakları Sözleşmesinin 10 uncu maddesinin birinci fıkrasında hüküm altına alınan "ifade özgürlüğü" ile ilişkili görmüştür. Bu kapsamda Mahkeme, Avrupa İnsan Hakları Mahkemesinin yerleşik içtihatlarında Sözleşmenin 10 uncu maddesinin yalnızca haber verme hakkını değil aynı zamanda haber alma hakkını da kapsayıcı şekilde yorumlandığını belirtmiştir. Bunun yanında Mahkeme, Sözleşmenin halk davası *(actio popularis)* açma imkânı vermediğini, dolayısıyla yalnızca eylem ya da ihmalden doğrudan mağdur olan kişi tarafından bireysel başvuruda bulunulabileceğini vurgulamıştır. Mahkeme bu hususta Avrupa İnsan Hakları Mahkemesinin 20877/10 başvuru numaralı *Akdeniz/Türkiye*, 40150/98, 40153/98, 40160/98, başvuru numaralı *Tanrıkulu, Çetin, Kaya ve diğerleri/Türkiye* ile 48226/10, 14027/11 başvuru numaralı *Cengiz ve diğerleri/Türkiye* kararlarındaki değerlendirmelere atıfta bulunmuştur.

Başvurucular; Türkiye'nin önde gelen insan hakları araştırmacıları ve aktivistleri olduklarını, farklı bir anlayışla habercilik yapan (erişim engeli getirilen) internet sitelerinden faydalandıklarını, işlerinin gereği olarak farklı görüşlere ulaşma hakları ve ödevleri olduğunu ve bu nedenle de kendileri için önemli olan bu internet sitelerine erişimin sistemli bir şekilde engellenmesinin bilgiye ulaşamamaları nedeniyle ifade özgürlüklerini ihlal ettiğini iddia etmiştir. Öte yandan başvurucular tek bir kararla birden çok sitenin engellendiğini, gerek erişim engelleme kararının verilmesi gerekse sulh ceza mahkemesi tarafından yapılan onaylama süresinin çok kısa olduğunu ve bu kadar kısa sürede inceleme yapılmasının mümkün olamayacağını, erişimi engellenen adreslerin her birinin hangi gerekçeye dayanılarak engellendiğinin kararda belirtilmediğini ve bu nedenle de gerekçeli karar haklarının ihlal edildiğini iddia etmiştir.

Anayasa Mahkemesi, başvurucular tarafından ileri sürülen iddialar çerçevesinde ortaya çıkan hukuki sorunun haber ve fikir alma, bilgiye erişim haklarına müdahale çerçevesinde değerlendirilmesi gerektiğini belirtmiştir. Mahkeme, Anayasanın 26. maddesinde düzenlenen düşünceyi açıklama ve yayma hürriyetinin internet üzerinden yapılan paylaşımları da kapsadığını, internet sitelerine yönelik yapılan kısıtlamaların bilgi alma ve verme özgürlüğüne müdahale niteliğinde olduğunu açıkça ortaya koymuştur. Ancak Mahkemeye göre haber ve fikir alma özgürlüğü, erişim engelleme yoluyla yapılan her müdahaleden herkesin doğrudan etkilendiği anlamına gelecek şekilde geniş yorumlanamayacaktır. Yine Mahkemeye göre, başvurucunun söz konusu müdahaleden dolaylı olarak etkilenmesi mağdur sıfatını alması için yeterli değildir. Mahkeme, önceki içtihatlarına atıfta bulunarak toplumsal menfaatin korunması amacıyla açılan ve halk davası *(actio popularis)* olarak isimlendirilen başvuruları başvuru hakkı kapsamında kabul etmediğini, bireysel başvuruda mağdur sıfatına sahip olunabilmesi için ilgili kişinin başvuruya konu

işlem, eylem ya da ihmal nedeniyle güncel ve kişisel bir hakkının doğrudan etkilenmiş olması gerektiğini belirtmiştir. Bu kapsamda başvurucuların söz konusu işlem, eylem ya da ihmalden doğrudan etkilendiği konusunda Anayasa Mahkemesini ikna etmesi gerektiği vurgulanmıştır.

Mahkeme, bilgi alma ve verme hakkı kapsamında üçüncü kişiler tarafından ifade özgürlüğünün ihlal edildiğine yönelik yapılan başvurularda, başvurucuların mağdur sıfatına sahip olup olmadıklarının tespit edilebilmesi amacıyla birtakım kriterler ortaya koymuştur. Buna göre Mahkeme, somut olayın koşullarını göz önüne alarak belirlediği yedi adet kriter[67] üzerinden bir sonuca ulaşacağını belirtmiştir. Bu kriterler üzerinden somut olayı değerlendiren Mahkeme; ilk olarak başvurucuların engelleme kararı verilen internet sitelerinin aktif kullanıcıları olduklarını ortaya koyamadıklarını, bu sitelere erişim engeli getirilmesinin başvurucuların akademik çalışmalarını hangi ölçüde etkilediğini açıklayamadıklarını ve buna ilişkin kanıt da ileri süremediklerini, engellenen sitelerin hangi yönleriyle alternatifi olmadığının anlaşılamadığını belirterek başvurucuların önemli bir iletişim kaynağından yoksun kaldığı gibi bir sonuca ulaşılamayacağını belirtmiştir. Bu kapsamda Mahkeme, söz konusu engelleme kararlarının

---

[67] *"…Bu, soyut bir değerlendirme değildir. Anayasa Mahkemesi bu değerlendirmeyi yaparken somut olayın koşullarına uyduğu ölçüde; i. Başvurucunun ifade aracını (internet sitesi, sosyal medya platformu, kitap, gazete, dergi vb.) kullanma şekli (içerik sağlayıp sağlamaması: aktif kullanıcı-pasif kullanıcı), ii. İfade açıklamasına yönelik tedbirin bilgi alma hakkına sahip başvurucu üzerinde doğurabileceği sonuçların ağırlığı, iii. Bilgiye başka yollardan erişim sağlama imkânının bulunup bulunmadığı, iv. İfade aracının (somut olayda erişimi engellenen internet sitelerinin ve sosyal medya hesaplarının) özellikleri (kullanıcı/ziyaretçi/takipçi sayısı, işlevi, ulusal/uluslararası platformlarda bilinirliği, alternatifi olup olmaması vb.), v. İfade aracına yapılan müdahale nedeniyle önemli bir iletişim kaynağından yoksun kalınıp kalınmadığı, vi. Alınan tedbirin başvurucunun kamusal tartışmaya katılımına engel olup olmadığı, vii. Alınan tedbir nedeniyle başvurucunun somut olarak belirlenebilir bir menfaatten yoksun kalıp kalmadığı gibi hususları inceleyerek sonuca varacaktır…"*

başvurucular üzerinde ancak dolaylı bir etki doğurabileceği tespitinde bulunmuştur. Sonuç itibariyle Mahkeme, başvurucuların erişim engellenmesi tedbiri ile bilgi ve fikir alma hakları arasında doğrudan ve kişisel bir bağ kuramadıkları, mağdur olduklarını soyut iddiaların ötesine geçen makul ve ikna edici gerekçelerle kanıtlayamadıkları gerekçesiyle bireysel başvurunun kişi bakımından yetkisizlik nedeniyle kabul edilemez olduğuna hükmetmiştir.

Kanaatimizce, internetin bilgiye ulaşmada önemli bir araç olduğu ile internet adreslerine yönelik uygulanan erişim engelleme tedbirlerinin bilgi alma ve verme hakkı çerçevesinde üçüncü kişilerin ifade özgürlüğüne bir müdahale oluşturacağına yönelik Anayasa Mahkemesi tarafından yapılan değerlendirme ve tespitler oldukça yerinde ve önemlidir. Ancak her ne kadar Mahkeme, hüküm itibariyle başvurunun kabul edilemez olduğu sonucuna ulaşmış olsa da bazı iddiaları değerlendirmekten kaçınmıştır. Özellikle başvuruya konu kararların 5651 sayılı Kanunun 8/A maddesine dayanılarak verildiği göz önüne alındığında, başvurucuların iddiaları arasında yer alan erişim engelleme kararlarının Kanunda öngörülen kısa sürelerde onaylanmasının mümkün olamayacağı iddiası ile her bir internet içeriği bakımından hangi gerekçeyle engelleme kararı verildiğinin karar gerekçelerinde yer almadığı iddiası değerlendirilmeye muhtaçtır. Somut olayda erişim engelleme kararı verilen toplamda 615 internet sitesi ve sosyal medya hesabı bulunmaktadır. 5651 sayılı Kanunun 8/A maddesi hükmüne göre bu kararlar talep üzerine derhal ve en geç kararın bildirilmesinden itibaren dört saat içerisinde uygulanmakta; akabinde kararlar sulh ceza mahkemesinin onayına sunulmakta ve mahkeme kırk sekiz saat içerisinde bu hususta kararını vermektedir. Dolayısıyla Kanunda öngörülen inceleme süreleri oldukça kısadır. Somut olay bakımından değerlendirildiğinde onay mercii olan sulh ceza mahkemesi tarafından kırk sekiz saat gibi kısa bir süre içerisinde toplamda 615 adet internet sitesi ve sosyal medya hesabındaki paylaşımların incelenmesi ve her

birisi için tek tek Kanunun 8/A maddesinde öngörülen engelleme sebeplerinin *(yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması)* bulunup bulunmadığı yönünde değerlendirme yapılabilmesi mümkün değildir. Bu incelemenin yapılması yeterli olmayıp her bir engelleme kararı verilen adres bakımından yine Kanunun 8/A maddesinde öngörülen sebeplerden hangisine dayanılarak kararın verildiğinin gerekçede belirtilmesi de bir başka gerekliliktir. Nitekim Anayasanın 141 inci maddesinin üçüncü fıkra hükmüne göre bütün mahkemelerin her türlü kararları gerekçeli olarak yazılmak zorundadır. Bu nedenle somut olay özelinde Kanunda öngörülen süreler içerisinde onay mercii tarafından gerekli inceleme ve değerlendirmelerin yapıldığını kabul etmek çok da mümkün olmayacaktır.

Kanaatimizce söz konusu karar kapsamında değerlendirilmesi gereken bir diğer hukuki sorun başvuruculaların mağdur statüsüne sahip olup olmadığıdır. Gerek Anayasa Mahkemesi nezdinde gerekse Avrupa İnsan Hakları Mahkemesi nezdinde yapılan bireysel başvurularda başvurunun kabul edilebilirliğinin temel şartlarından bir tanesi "mağdur" statüsünün kazanılmasıdır.[68] Nitekim Avrupa İnsan Hakları Sözleşmesinin "Bireysel başvurular" başlıklı 34 üncü maddesinde; Sözleşmede tanınan haklarının ihlal edilmesinden dolayı "mağdur" olduğunu iddia eden kişilerin başvuruda bulunabileceği açıkça belirtilmektedir.[69] Avrupa İnsan Hakları Mahkemesinin yerleşik içtihadına göre; bir kimsenin Sözleşme

---

[68] Mustafa Baysal, "Avrupa İnsan Hakları Mahkemesine Bireysel Başvuruda Mağdur Kavramı," *Uyuşmazlık Mahkemesi Dergisi*, no. 5 (2015): 195.

[69] Bkz. AİHS md. 34; *"Bu Sözleşme veya protokollerinde tanınan haklarının Yüksek Sözleşmeci Taraflar'dan biri tarafından ihlal edilmesinden dolayı mağdur olduğunu öne süren her gerçek kişi, hükümet dışı kuruluş veya kişi grupları Mahkeme'ye başvurabilir. Yüksek Sözleşmeci Taraflar bu hakkın etkin bir şekilde kullanılmasını hiçbir surette engel olmamayı taahhüt ederler."*

ihlali nedeniyle "mağdur" statüsünü kazanabilmesi için iddia edilen eylem ya da ihmal ile başvurucu arasında doğrudan bir bağlantı bulunmalıdır.[70] Dolayısıyla hak ihlali iddiasına konu işlemin, eylemin ya da ihmalin etkilerinin doğrudan başvurucu üzerinde doğması gerekmektedir. Bir başka ifadeyle, başvuruya konu işlem, eylem ya da ihmalin başvurucuyu etkilediğinin makul ve ikna edici gerekçelerle ortaya koyulabilmesi gerekmektedir. Bu kapsamda bizim de katıldığımız görüşe göre bireysel başvuruda mağdur kavramı; *"idari bir işlem ya da eylemden veya ihmalden doğrudan etkilenen kişi ya da kişiler"* şeklinde tanımlanmaktadır.[71] Bu çerçevede somut olay değerlendirildiğinde başvuruculların söz konusu kararların kendileri üzerindeki doğrudan etkilerini açık bir biçimde ortaya koyamadıkları görülmektedir. Zira erişim engelleme kararı verilen internet adresleri ile başvurucular arasındaki somut ilişkinin ne olduğu ve engelleme tedbirinin başvurucular üzerinde oluşturduğu "somut" etkilerin neler olduğu anlaşılamamaktadır. Örneğin; akademisyen olan başvuruculların bir araştırmasında ya da eserinde erişim engeli verilen internet adreslerinden bir tanesini kaynak olarak göstermesi gibi somut bir ilişki başvuru kapsamında mevcut değildir. Bu noktada başvuruculların mağdur olup olmadığına ilişkin Anayasa Mahkemesince, belirlenen kriterler üzerinden, yapılan değerlendirmelere ve başvuruculların mağdur statüsüne sahip olmamaları gerekçesiyle başvurunun kişi bakımından yetkisizlik nedeniyle kabul edilemez olduğu yönündeki hükme katılmaktayız.

b. Anayasa Mahkemesinin 2015/16368 Başvuru Numaralı ve 11/3/2020 Tarihli Bireysel Başvuru Kararının İncelenmesi

---

70 Baysal, "Avrupa İnsan Hakları Mahkemesine Bireysel Başvuruda Mağdur Kavramı," 203.

71 Baysal, "Avrupa İnsan Hakları Mahkemesine Bireysel Başvuruda Mağdur Kavramı," 204.

Karar, *www.sendika.org* isimli internet sitesinin temsilcisi Ali Ergin DEMİRHAN tarafından Anayasa Mahkemesine 9/10/2015 tarihinde yapılan bireysel başvuru neticesinde verilmiştir. Bireysel başvuru, *www.sendika.org* isimli internet sitesinin tamamına yönelik 5651 sayılı Kanunun 8/A maddesine dayanılarak alınan erişim engelleme kararlarının ifade ve basın özgürlüğünü ihlal ettiği iddiasına dayanmaktadır.

Başvuruda, erişim engelleme kararının uygulandığı *www.sendika.org* isimli internet sitesinin *"ırkçı-gerici-cinsiyetçi-gerçek dışı ve hakaret içeren içerikler dışında"* en geniş tartışmalara yer veren bir internet sitesi olduğu ifade edilmiştir. Ayrıca söz konusu internet sitesinin bünyesinde yer alan bilimsel çalışmalar nedeniyle ulusal ve uluslararası alanda çalışan akademisyenler için bir referans olarak kabul edildiği belirtilmiştir. Söz konusu internet sitesinde yer alan yayınlar göz önüne alınarak (dönemin) Başbakanlık Güvenlik İşleri Genel Müdürlüğü talebi üzerine (kapatılan) TİB tarafından sitenin tamamının erişimine engellenmesine karar verilmiştir. Söz konusu erişim engelleme kararı 5651 sayılı Kanunun 8/A maddesinin ikinci fıkra hükmü gereğince Gölbaşı Sulh Ceza Mahkemesinin onayına sunulmuştur. Gölbaşı Sulh Ceza Mahkemesi tarafından yapılan inceleme neticesinde, TİB tarafından ileri sürülen, *"bahse konu içeriklerin yaşam hakkı ile kişilerin can ve mal güvenliğinin ihlaline sebebiyet vermesi"* gerekçesiyle söz konusu erişim engelleme kararı onaylanmıştır. Bu karara başvurucu tarafından Ankara 6. Sulh Ceza Mahkemesi nezdinde yapılan itirazın 14/8/2015 tarihinde reddedilmesiyle söz konusu erişim engelleme kararı kesinleşmiştir. İtirazın reddi kararının başvurucuya tebliğ edilmesinin akabinde başvurucu, gidilecek başka bir hukuki yol kalmadığından, Anayasa Mahkemesine bireysel başvuruda bulunmuştur.

Başvurucu; temsilcisi olduğu internet sitesine erişimin tamamen engellendiğini, gerek idare tarafından gerekse yargı mercii tarafından verilen kararlarda söz konusu engelleme kararının hangi gerekçeyle alındığının belirtilmediğini, internet

sitesinin tamamına yönelik alınan engelleme kararının sansür niteliğinde olduğunu, bu kararın ifade özgürlüğüne yönelik orantısız bir müdahale olması nedeniyle ifade ve basın özgürlüklerini ihlal ettiğini iddia etmiştir. Adalet Bakanlığı görüşünde ise; erişime kapatılan içeriklerin *terörü öven, şiddete ve suça teşvik eden ve kamu düzenini ve millî güvenliği tehdit eden* nitelikte yayınlar olduğu, uygulanan tedbirin demokratik toplumda gerekli olduğu, zorlayıcı toplumsal bir ihtiyacı karşıladığı ve orantılı olduğu belirtilmiştir.

Anayasa Mahkemesince yapılan değerlendirmede; ilk olarak başvuruda yer alan erişim engelleme kararlarına karşı sulh ceza mahkemeleri nezdinde etkili bir itirazda bulunmanın imkânsız olduğu yönündeki şikâyetler Mahkemenin önceki içtihatlarına atıf yapılarak incelemeye değer görülmemiştir. Mahkeme, başvurucunun bu şikâyetleri dışında kalan iddialarını ise "ifade özgürlüğü" ve "basın özgürlüğü" kapsamında incelemiştir. Başvurunun kabul edilebilirlik şartlarını taşıdığını tespit eden Mahkeme başvurunun esas yönünden incelenmesine karar vermiştir. Mahkemeye göre; *www.sendika.org* isimli internet sitesinin tamamına yönelik alınan erişim engelleme kararıyla başvurucunun ifade ve basın özgürlüklerine müdahalede bulunulmuştur. Mahkeme, söz konusu müdahalenin bir ihlal niteliğinde olup olmadığını ise Anayasanın 13. maddesinde yer alan kanunilik, meşru amaç ve demokratik toplumun gereklerine uygunluk ilkeleri üzerinden değerlendirmiştir. Mahkemeye göre; başvuruya konu engelleme kararı, 5651 sayılı Kanunun 8/A maddesine dayanılarak yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması amacıyla verildiğinden Anayasanın 13. maddesinde öngörülen kanunilik ve meşru amaç ilkelerine uygundur. Mahkeme, söz konusu engelleme kararıyla yapılan müdahalenin bir ihlal oluşturup oluşturmadığını esas itibariyle *"demokratik toplum düzeninin gereklerine uygunluk ilkesi"* üzerinden ele almıştır. Bu kapsamda Mahkeme, 5651 sayılı Kanunun 8/A maddesine dayanan erişimin engellenmesi kararı hakkında bazı tespitlere ve bu

maddeye göre verilen erişim engelleme kararlarında idari ve yargısal makamlar tarafından gözetilmesi gereken hususlara yönelik değerlendirmelerde bulunmuştur.

Mahkeme; Kanunun 8/A maddesiyle internet ortamında işlenen suçlarla etkin bir şekilde mücadele edilmesi amacıyla özel ve hızlı sonuç alınabilecek bir idari tedbir usulünün öngörüldüğü, öngörülen bu yolun ancak ivedilikle müdahale edilmesi gereken hallerde uygulanması gereken istisnai bir yol olduğu, yetkili makamların *(somut olayda TİB güncel mevzuatta BTK Başkanı)* bu yolun işletilmesinde istisnai bir yol olduğu bilinciyle hassasiyetle hareket ederek karar vermesi gerektiği tespitlerinde bulunmuştur. Akabinde Mahkeme, internet ortamındaki demokratik toplum düzenini tehlikeye atan yayınların daha ileri bir inceleme yapmaya gerek olmaksızın "görünüşte veya ilk bakışta" anlaşılabildiği hallerde ancak idare tarafından Kanunun 8/A maddesi kapsamında öngörülen tedbire tabi tutulabileceğini belirtmiştir. Mahkemeye göre, internet ortamında yapılan yayınlara erişim engellenmesi kararıyla "idare" tarafından yapılan müdahale ancak gecikmesinde sakınca bulunan bir durumun varlığı ve müdahalenin haklılığının ilk bakışta anlaşılabildiği durumlarda ifade hürriyetinin ihlali sonucunu doğurmayacaktır. Yine Mahkeme, internet ortamındaki yayının demokratik toplum düzenini tehlikeye atıp atmadığının ilk bakışta anlaşılamadığı ve bunun anlaşılmasının daha ileri bir incelemeyi gerektirdiği durumlarda Kanunun 8/A maddesiyle idare için öngörülen istisnai yol yerine yine aynı maddede öngörülen "mahkeme yolunun" işletilmesi gerektiğini ortaya koymuştur. Son olarak Mahkeme, Kanunun 8/A maddesine dayanılarak verilen erişim engelleme kararlarının gerekçeli olması gerektiğini ve kararı onaylayan mahkeme kararında idari kararın gerekçesinin tekrarlanması veya bu gerekçeye atıfta bulunulması halinde idarenin gerekçesinin Mahkemece yapılacak değerlendirmede esas alınacağını belirterek idari ve yargısal makamların

gerekçelerinde bulunması gereken unsurları açıkça ortaya koymuştur.[72]

Anayasa Mahkemesi, ortaya koyduğu ilkeler ve kriterler çerçevesinde; erişim engelleme kararının gerekçesinde söz konusu adreste yer alan içerikle sınırlama sebebi arasındaki ilişkinin ortaya konulamaması, idare tarafından alınan bu kararda gecikmesinde sakınca bulunan halin ne olduğunun

---

[72] *"…i. İnternet içeriğine erişimin engellenmesi kararı verilebilmesi için gecikmesinde sakınca bulunan bir durumun varlığı idari ve yargısal makamlar tarafından ortaya konulmalıdır. ii. Gecikmesinde sakınca bulunan hâllerin yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden bir veya birkaçına bağlı olarak ortaya çıkabileceği dikkate alındığında yayının içeriği ile bu sebepler arasındaki ilişkinin tam olarak gösterilmesi gerekir. iii. Böyle bir analizin yapılabilmesi için eğer söz konusu yayının terör örgütleriyle veya terör faaliyetlerinin meşru gösterilmesiyle bir ilişkisi varsa ifade özgürlüğü ile demokratik toplumun terör örgütlerinin faaliyetlerine karşı kendini korumaya ilişkin meşru hakkı arasında denge kurulmalıdır. iv. Zikredilen dengelemenin yapılabilmesi için; - Bütünüyle ele alındığında müdahaleye konu yayının özel bir kişiyi, kamu görevlilerini, halkın belirli bir kesimini veya devleti hedef gösterip göstermediğinin, onlara karşı şiddete teşvik edip etmediğinin, - Yayınla bireylerin fiziksel şiddet tehlikesine maruz bırakılıp bırakılmadığının, bireylere karşı nefretin alevlendirilip alevlendirilmediğinin, - Yayında iletilen mesajda şiddete başvurmanın gerekli ve haklı bir önlem olduğunun ileri sürülüp sürülmediğinin, - Yayınla şiddetin yüceltilip yüceltilmediğinin, kişilerin nefrete, intikam almaya, silahlı direnişe tahrik edilip edilmediğinin, - Yayının suçlamalara yer vererek veya nefret uyandırarak ülkenin bir kısmında veya tamamında daha fazla şiddete sebebiyet verip vermeyeceğinin, - Yayının kişi veya kuruluşları paniğe yöneltecek yalan ve yanlış bilgileri, tehdit ve hakaret oluşturan ifadeleri içerip içermediğinin, - Yayın tarihinde ülkenin bir kısmında veya tamamında çatışmaların yoğunluk derecesi ile ülkedeki tansiyonun yükseklik derecesinin yayına erişimin engellenmesi kararına etki edip etmediğinin, - Karara konu sınırlayıcı tedbirin demokratik bir toplumda zorlayıcı bir toplumsal ihtiyacın karşılanması amacına yönelik olup olmadığının ve tedbirin başvurulabilecek en son çare niteliğinde bulunup bulunmadığının, - Son olarak sınırlamanın güdülen kamu yararı amacını gerçekleştirmek için ifade özgürlüğüne en az müdahale eden ölçülü bir sınırlama niteliğinde olup olmadığının yayının içeriğiyle birlikte değerlendirilmesi gerekir…"*

belirtilmemesi, söz konusu internet sitesinde yer alan yayınların hangi kısımlarının hangi nedenlerle yaşam hakkı ile kişilerin can ve mal güvenliğinin ihlaline sebebiyet vereceğinin gerekçede belirtilmemesi ve erişim engelleme kararının ihlalin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL vb.) verilememesinin nedeni açıklanmadan doğrudan internet sitesinin tamamına yönelik verilmesi gerekçeleriyle erişim engelleme kararıyla yapılan müdahalenin Anayasanın 26 ncı maddesinde güvence altına alınan ifade özgürlüğü ile Anayasanın 28 inci maddesinde güven altına alınan basın özgürlüğünü ihlal ettiğine hükmetmiştir.

Kanaatimizce söz konusu karar, internet ortamında yapılan yayınlara yönelik verilen erişimin engellenmesi kararlarının hangi ölçüt ve koşullar dâhilinde ifade ve basın özgürlüğünün ihlaline sebebiyet vermeyeceğini açıkça ortaya koyması bakımından oldukça önem arz etmektedir. Öte yandan Mahkemenin 5651 sayılı Kanunun 8/A maddesine göre erişim engelleme kararı verilmesine ilişkin yaptığı tespit ve değerlendirmeler çalışmamızın konusu açısından ayrı bir öneme sahiptir. Söz konusu tespit ve değerlendirmelerde Mahkemenin yalnızca, somut olayın özelliğinden hareketle, idari tedbir olarak verilen erişim engelleme kararlarını ele aldığı görülmektedir. Bu kapsamda Mahkeme, madde kapsamında idari mercilerce verilen erişim engelleme kararları bakımından "ilk bakışta haklılık" doktrinini benimsemiştir. Görünüşte ya da ilk bakışta haklılık, doktrinde *"prima facie"* olarak da adlandırılmaktadır.[73] Bu doktrine göre, kanunda öngörülen erişim engelleme sebebinin *(suç işlenmesinin önlenmesi, kişilik haklarının ihlali vb.)* somut olayda bulunduğunun ilk bakışta, yani daha ileri bir

[73] Kemal Gözler, "Kişilik Haklarını İhlal Eden İnternet Yayınlarının Kaldırılması Usulü ve İfade Hürriyeti: 5651 Sayılı Kanunun 9'uncu Maddesinin İfade Hürriyeti Açısından Değerlendirilmesi," *Legal Hukuk Dergisi*, Rona Aybay'a Armağan Özel Sayı (2014): 10.

incelemeye gerek olmaksızın, anlaşılması halinde ancak yetkili makam tarafından erişim engellemek kararı verebilecektir.[74] Mahkemenin benimsediği ilk bakışta haklılık doktrinine katılmakla birlikte bu kapsamda yapılan tespit ve değerlendirmeleri eksik bulmaktayız. Zira Mahkeme bu hususta açıklamalarını, yalnızca idari tedbir olarak, yani BTK Başkanı tarafından, verilen erişim engelleme kararlarıyla sınırlı tutmuştur. Oysaki madde kapsamında erişim engelleme kararı "hâkim" tarafından da verilebilmektedir. Dolayısıyla Mahkemenin *"5651 Sayılı Kanun'un 8/A Maddesine Dayanan Erişimin Engellenmesi Kararı Hakkında Bazı Tespitler"* başlığı altında yalnızca maddeyi bir yönüyle ele alması kanaatimizce yerinde olmamıştır. Öte yandan Mahkeme, bu tespit ve değerlendirmelerinin sonunda; *"…müdahalenin haklılığı ilk bakışta anlaşılamıyorsa yayınların idare tarafından engellenmesi biçimindeki istisnai usul yerine yine 5651 sayılı Kanun'un 8/A maddesinde öngörülmüş olan mahkeme yolunun işletilmesi gerekir…"* değerlendirmesine yer vermiştir. Kanaatimizce söz konusu değerlendirme anlatımındaki eksiklik nedeniyle maddenin yorumlanmasından ziyade daha çok sorunun akla gelmesine neden olmaktadır. Şöyle ki; Kanunun 8/A maddesinde erişim engellenmesi kararının yargı mercii tarafından verilmesi hususunda *"hâkim tarafından"* ibaresine yer verilmiştir. Mahkemenin yaptığı değerlendirmede ise *"mahkeme yoluyla"* ibaresi kullanılmıştır. Dolayısıyla Anayasa Mahkemesinin buradaki hâkim ibaresini "sulh ceza mahkemesi" olarak mı yoksa "genel mahkemeler" olarak mı yorumladığı tam olarak anlaşılamamaktadır. Bir başka açıdan Anayasa Mahkemesinin ifadesiyle "mahkeme yoluna" gidildiğinde; erişim engelleme kararının verilmesinde mahkemenin nasıl değerlendirme yapacağı, maddenin ikinci fıkrasında öngörülen 48 saatlik onay kararı süresinin mahkeme tarafından yapılan incelemelerde de

---

[74] Gözler, "Kişilik Haklarını İhlal Eden İnternet Yayınlarının Kaldırılması Usulü ve İfade Hürriyeti: 5651 Sayılı Kanunun 9'uncu Maddesinin İfade Hürriyeti Açısından Değerlendirilmesi," 10.

bağlayıcı olup olmayacağı ve mahkemenin incelemesini hangi usul ve şartlar dairesinde yerine getireceği gibi hususlar üzerinde durulmamıştır. Bize göre, Kanundaki "hâkim tarafından" ibaresini Kanunun sistematiğine uygun olacak şekilde "sulh ceza mahkemesi" olarak yorumlamak daha uygun olacaktır.

Kanaatimizce karar kapsamında değerlendirilmesi gereken bir başka hukuki sorun Kanunun 8/A maddesine göre verilen erişim engelleme kararlarının yetkili makamlarca gerektiği gibi gerekçelendirilmemesidir. Madde hükmüne göre; *"yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması"* şeklindeki birbirinden bağımsız sebeplerin bir veya birkaçına bağlı olarak erişim engelleme kararı verilebilmektedir. Bireysel başvuruya konu erişim engelleme kararının gerekçesinde de olduğu gibi karar veren makamlar bu sebeplerin bir veya birkaçını somut olayla ilişki kurmadan katalog biçimde gerekçeye yazmaktadır. Bu açıdan Mahkemenin *"5651 Sayılı Kanun'un 8/A Maddesi Kapsamında Erişimin Engellenmesine Karar Verilmesi Biçimindeki Müdahalelerde İdari ve Yargısal Makamlar Tarafından Gözetilmesi Gereken Hususlar"* başlığı altında erişim engelleme kararlarının gerekçelendirilmesine ilişkin yaptığı değerlendirmeler oldukça önem arz etmektedir. Mahkemenin bu başlık altında yaptığı değerlendirmelerin tamamına ve erişim engelleme kararıyla yapılan müdahalenin ifade ve basın özgürlüklerini ihlal ettiği yönündeki hükme katılmaktayız.

SONUÇ

İnternet günümüz dünyasında en yaygın kullanılan kitle iletişim araçlarından birisidir. Bireylere sağladığı katkıların yanı sıra internet kullanımının ortaya çıkardığı bazı olumsuz durumlar da söz konusudur. Bu olumsuzluklardan bir tanesi de internet aracılığıyla suç işlenmesi ve böylece bireylerin hukuki hak ve menfaatlerinin ihlal edilmesidir. Devletler internet aracılığıyla suç işlenmesinin önlenmesi amacıyla bazı

yöntemlerin kullanılmasını iç mevzuatlarında düzenlemektedir. Ülkemiz açısından bu düzenlemelerin başında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun gelmektedir. Kanun'da internet aracılığıyla suç işlenmesinin önlenmesi amacıyla getirilmiş yöntemlerden bir tanesi de suç konusu içeriğin yayınlandığı internet sitesine erişimin engellenmesidir.

İnternet erişiminin engellenmesi hukuki niteliği itibariyle bir ceza değil, tedbirdir. Bu yönüyle erişimin engellenmesi kararının temelinde yatan amaç konusu suç teşkil eden içeriğin internet ortamında yayınlanmasının durdurulmasıdır. Bir başka ifadeyle; suç teşkil eden içeriğin internet ortamında görülebilirliğinin sonlandırılmasıdır. Erişim engelleme kararı bu amacın gerçekleşmesi için alınan geçici bir tedbirdir. İçeriğin meydana getirdiği zararlı sonuç ortadan kalkana kadar erişim engelleme kararı etki ve sonuçlarını doğurmaya devam edecektir.

Suç işlenmesinin önlenmesi amacıyla internet erişiminin engellenmesi kararı 5651 sayılı Kanunun 8 ve 8/A maddeleri kapsamında yer alan hükümler çerçevesinde verilmektedir. Kanunun 8 inci maddesi kapsamında erişim engelleme kararının verilmesi; koruma tedbiri ve idari tedbir olmak üzere ikili bir ayrım yapılarak düzenlenmiştir. Kanunkoyucu tarafından yapılan bu nitelendirme ya da adlandırmanın kararı veren merciiye göre yapıldığı anlaşılmaktadır. Nitekim madde hükümlerinde; adli merciiler tarafından engelleme kararının verildiği hal koruma tedbiri olarak; idari merciiler tarafından engelleme kararının verildiği hal ise idari tedbir olarak erişimin engellenmesi şeklinde belirtilmektedir. Koruma tedbiri kavramı ceza muhakemesi hukukunda kullanılan teknik bir kavramdır. Ceza muhakemesi hukukuna göre koruma tedbiri, bir ceza yargılamasının sağlıklı bir şekilde yürütülebilmesi ve maddi gerçeğe ulaşabilmek amacıyla alınan tedbirleri ifade etmektedir. Ceza muhakemesi hukukunda ifade ettiği anlam itibariyle

koruma tedbiri, bir suçun işlenmesinin önlenmesi amacını ihtiva etmemektedir. İdari tedbir ise idare hukukunda karşılığı olan teknik bir kavramdır. İdare hukukundaki anlamı itibariyle idari tedbir, kamunun uğrayacağı zararları önlemek amacıyla idare tarafından önceden alınan tedbirlerdir.

Kanaatimizce; ceza yargılamasının yürütülmesi amacıyla alınabilecek haller dışında (örneğin; delillerin yok edilmesi ihtimali gibi) sırf bu kararın adli merciler tarafından verilmesi nedeniyle bu kararların koruma tedbiri olarak nitelendirilmesi hukuken yerinde olmayacaktır. Her bir karar özelinde kararın alınmasının temelinde yatan amaç göz önünde bulundurularak hukuki nitelendirme yapılmasının daha uygun olacağı düşünülmektedir. İdari tedbir kavramının özünde bir önleme amacı olduğu için Kanunda bu kapsamda yapılan nitelendirmenin yerinde olduğu düşünülmektedir.

Koruma tedbiri olarak erişimin engellenmesi kararı Kanunda sayılan katalog suçlara ilişkin yürütülen bir ceza soruşturması ya da kovuşturması kapsamında hâkim veya mahkeme tarafından verilmektedir. Dolayısıyla bu kapsamda yargısal bir süreç içerisinde erişimin engellenmesi kararı verilmektedir. İdari tedbir olarak erişimin engellenmesi kararı ise Kanunda sayılan idari merciler tarafından verilmektedir. Bu kapsamda idari mercilere ve hatta özel hukuk tüzel kişilerine suça ilişkin değerlendirme yapma ve resen engelleme kararı alma yetkisinin tanındığı görülmektedir. Ayrıca maddede bu kararların bir hâkim denetimine tabi kılınmadığı da anlaşılmaktadır. Kanaatimizce; idari merciler ve hatta özel hukuk tüzel kişileri tarafında suç işlendiğine ilişkin değerlendirme yapılarak tek taraflı engelleme kararı verilmesine ve bu kararın hâkim denetimine tabi kılınmamasına ilişkin bu hükümler, başta Anayasanın 22 inci maddesinin ikinci fıkrası olmak üzere, Anayasaya aykırıdır. Anayasaya uygunluğun sağlanması amacıyla idari merciler tarafından engelleme kararı verme yetkisinin ancak gecikmesinde sakınca bulunan hallerle sınırlandırılması ve verilen kararların en geç yirmi dört saat

içerisinde hâkim onayına sunulmasının zorunlu kılınması gerekmektedir.

5651 sayılı Kanunun 8 inci maddesine 10.09.2014 tarihli ve 6552 sayılı Kanunun 127 nci maddesi ile eklenen on altıncı fıkra hükmü Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli kararı ile iptal edilmiştir. Söz konusu iptal kararının gerekçesinde Anayasa Mahkemesi tarafından çeşitli değerlendirmelere yer verilmiştir. Kanaatimizce, Anayasa Mahkemesinin TİB'e ilişkin yaptığı değerlendirmeler ve tespitler yasamanın asliliği ilkesine uygun değildir. Anayasanın 22 nci maddesi kanunla belirlenmiş olan yetkili merci tarafından bu kararın alınabileceğini belirtmekle beraber bu merciin hangi niteliğe sahip olması gerektiği yönünde bir sınırlandırma yoluna gitmemiştir. Bu bakımdan karar verme konusunda yetkili merciinin belirlenmesinde yasa koyucunun takdir yetkisine sahip olduğunu kabul etmek gerekir. Kanunkoyucunun iradesi ile belirlenmiş olan yetkili merciinin niteliğini ve liyakatini değerlendirmek Anayasaya uygunluk denetimi kapsamı içerisinde olmamalıdır. Mahkemenin bunun dışındaki tespit ve değerlendirmelerine ise katılmaktayız.

Anayasa Mahkemesinin E.2014/149, K.2014/151 sayılı ve 2.10.2014 tarihli kararı ile iptal edilen on altıncı fıkra hükmü iptal gerekçeleri de dikkate alınarak yeniden düzenlenmiş ve bu düzenleme 5651 sayılı Kanuna 8/A maddesi olarak eklenmiştir. Kanaatimizce; söz konusu maddeyle iptal edilen hükümdeki Anayasaya aykırılık teşkil eden hususlar giderilmiştir.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.

KAYNAKÇA

Baysal, Mustafa. "Avrupa İnsan Hakları Mahkemesine Bireysel Başvuruda Mağdur Kavramı". *Uyuşmazlık Mahkemesi Dergisi*, no. 5 (2015): 193-233.

Bilgi Teknolojileri ve İletişim Kurumu. "Erişimin Engellenmesi Tedbiri İstatistikleri". Erişim Tarihi: Kasım 10, 2021. https://www.guvenliweb.org.tr/dosya/brEi5.pdf.

Centel, Nur ve Hamide Zafer. *Ceza Muhakemesi Hukuku*. İstanbul: Beta Basım, 2015.

Çırakoğlu, Melikşah. "5651 sayılı Kanun Çerçevesinde İnternet Erişiminin Engellenmesi ve Erişim Sağlayıcıları Birliği". Yayımlanmamış Yüksek Lisans Tezi, Yıldırım Beyazıt Üniversitesi, 2015.

Çağlar, Selda. *Hukuk Devletinin Hukuki Belirlilik İlkesi Üzerinden Değerlendirilmesi*. İstanbul: Beta Yayıncılık, 2013.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yayıncılık, 2018.

Dülger, Murat Volkan ve Yasin Beceni. *Türkiye'de İnternet Sitelerinin Erişiminin Engellenmesi Konusunda Farklı Hukuk Disiplinleri Açısından Değerlendirmeler*. Ankara: TÜSİAD Yayınları, 2011.

Görkemli, Burcu. Yargı Kararları Işığında Türk Hukuku'nda İnternet Erişiminin Engellenmesi. Ankara Adalet Yayınevi, 2015.

Gözler, Kemal. "Erişimi Engellenen Bir Web Sayfasının İçerik Sağlayıcı Tarafından Yayından Çıkarılması Ne İşe Yarar? Erişim Sağlayıcıları Birliğinin 3 Eylül 2019 Tarihli Bir E-Postasının Düşündürdükleri (İçerik Sağlayıcıları İçin Bir Uyarı)". ANAYASA.GEN.TR. Erişim tarihi Kasım 30, 2020. https://www.anayasa.gen.tr/esbnin-epostasi.htm.

Gözler, Kemal. "Kişilik Haklarını İhlal Eden İnternet Yayınlarının Kaldırılması Usulü ve İfade Hürriyeti: 5651 Sayılı Kanunun 9'uncu Maddesinin İfade Hürriyeti Açısından Değerlendirilmesi". *Legal Hukuk Dergisi*, Rona Aybay'a Armağan Özel Sayı (2014): 1059-1120.

Gültekin, Özkan. *Öğreti ve Uygulamada İddianame ve İddianamenin İadesi*. Ankara: Seçkin Yayıncılık, 2011.

Kalender, Ahmet Buğra. "İfade Özgürlüğü Bağlamında İnternet Erişiminin Engellenmesi". Yayımlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi, 2017.

Karabulut, Mustafa. *İdari Yaptırımların Hukuki Rejimi*. Ankara: Turhan Kitabevi, 2008.

Kaya, Mehmet Bedii. "İnsan Hakları Ekseninde İnternetin Kontrolü ve Hukuki Sorumluluk rejimi". *Anayasa Yargısı Dergisi*, no.2 (2020): 159-203.

Kent, Bülent. *Türkiye'de İnternet Sitelerine Erişimin Engellenmesi*. Ankara: Adalet Yayınevi, 2019.

Kırış, Ferhat Tuna. "Ceza Hukuku Açısından İnternet Yayıncılığı". Yayımlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi, 2019.

Köküsarı, İsmail. *"Anayasa Hukukunda Hukuki Güvenlik İlkesi"*. Ankara: Adalet Yayınevi, 2015.

Memiş, Tekin. "Erişimin Engellenmesi, Hukuki Sorunlar ve Çözüm Önerileri". *Erzincan Üniversitesi Hukuk Fakültesi Dergisi*, no. 3-4 (2009): 161-176.

Oğurlu, Yücel. *İdari Yaptırımlar Karşısında Yargısal Korunma*. Ankara: Seçkin Yayıncılık, 2001.

Öztürk, Bahri. *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, 2012.

Özdilek, Ali Osman. *İnternet ve Hukuk*. İstanbul: Papatya Yayıncılık, 2002.

Söyler, Yasin. *Kamu Hukuku Açısından Devletin İnterneti Düzenleme Yetkisi*. Ankara: Savaş Yayınevi, 2014.

Taşkın, Ş. Cankat. *İnternete Erişim Yasakları.* Ankara: Seçkin Yayıncılık, 2016.

Toroslu, Nevzat ve Metin Feyzioğlu. *Ceza Muhakemesi Hukuku*. Ankara: Savaş Yayınevi, 2020.

Türkiye İstatistik Kurumu. "Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2021". Erişim Tarihi: Kasım 19, 2021. https://data.tuik.gov.tr/Bulten/Index?p=Survey-on-

Information-and-Communication-Technology-(ICT)-Usage-in-Households-and-by-Individuals-2021-37437.

Türkmen, Sevgi. "5651 sayılı Kanuna Göre Erişimin Engellenmesi". REHBERHUKUK.NET, erişim tarihi Kasım 30,2020 https://rehberhukuk.net/uploads/files/SEVGİ%20TÜRKMEN%205651%20sayılı%20kanuna%20göre%20erişimin%20engellenmesi%20.pdf.

Ulusoy, Ali. *İdari Yaptırımlar*. İstanbul: On İki Levha Yayıncılık, 2013.

Ünver, Yener ve Hakan Hakeri. *Ceza Muhakemesi Hukuku*. Ankara: Yetkin Yayınları, 2020.

Araştırma Makalesi/Research Article **Doi: 10.55009/bilisimhukukudergisi.1119881**

SİBER SUÇ, SİBER TERÖR VE SİBER SAVAŞ ÜÇGENİNDE SİBER DÜNYA

Cyber World in the Cyber Crime, Cyber Terror and Cyber War Triangle

Nurullah SANDİLAÇ*

Öz

Bu makale ile siber suç, siber terör ve siber savaş kavramları arasında bir ayrım gözeterek daha geniş bir perspektif üzerinden bu olgu ve kavramların ele alınması amaçlanmıştır. Konu ile ilgili temel araştırma sorusu: Siber suç, siber terörizm ve siber savaş kavramları farklı mıdır? Farklı ise, farklı kılan etmenler nelerdir? sorularına cevap aranmıştır. Bu çalışmada, nitel araştırma yöntemi benimsenmiş olup, araştırma desenine uygun olarak belgelere dayalı gözlem tekniği kullanılmıştır.

Anahtar kelimeler: Siber Suç, Bilişim Suçları, Siber Terör, Siber Savaş, Siber Dünya.

Abstract

With this article, it is aimed to discuss these phenomena and concepts from a wider perspective by making a distinction

* Zabıt Kâtibi, Sakarya Adliyesi, nurullah.sandilac@adalet.gov.tr, ORCID: 0000-0002-7673-2289.

Bu makale, 2021 Yılında Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Sosyoloji EABD tarafından kabul edilen "Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları" adlı yüksek lisans tez çalışmasından üretilmiştir.

Makale Gönderim Tarihi/Received: 23.05.2022.

Makale Kabul Tarihi/Accepted: 27.06.2022.

Atıf/Citation: Sandilaç, Nurullah. "Siber Suç, Siber Savaş ve Siber Terör Üçgeninde Siber Dünya." *Bilişim Hukuku Dergisi* 4, no. 1 (2022): 141-190.

between the concepts of cyber crime, cyber war and cyber terror. Basic research question with the subject: Are the concepts of cyber crime, cyber terrorism and cyber warfare different? If different, what are the factors that make it different? answers to the questions were sought. In this study, qualitative research method was adopted and document-based observation technique was used in accordance with the research design.

Keywords: Cyber Crime, IT Crimes, Cyber War, Cyber Terrorism, Cyber World.

GİRİŞ

Bilgisayar ve internetin ortaya çıkmasından sonra suçun sanal dünyada da işlenebilme kolaylığı görülmektedir. Tek bir tıklama ile dünyanın bir ucundan diğer bir ucuna siber saldırı yapılabilecek teknolojiye kavuşulmuştur. Dolayısıyla siber suçun, elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bilginin elde edilmesi için hazırlık yapılması olarak tanımlandığı görülmektedir.[1]

Siber alanda gerçekleştirilen suçlar ve saldırılar hızlı değişim gösteren konular arasındadır. Bu anlamda devletlerin mevcut yasalarında düzenleme yapması gerekmektedir. Aksi takdirde yasadaki boşluklar, sosyal hayatta önemli problemlerin meydana gelmesine neden olacaktır. Düzenleme yapılmadan önce siber alanda yaşanan değişimlerin takip edilerek, bunlara yönelik kavramların doğru şekilde tanımlanması zorunluluğu mevcuttur. Ancak bu alanda yaşanan gelişmeleri takip etmek ve uygun tanımları ortaya koymak hukukçuların karşılaştığı zorluklar arasındadır. Çünkü bu alanda bir hukukçu kimliğinin yanında internete, bilişim sistemlerine ve buna bağlı teknolojik ürünlere ilişkin kapsamlı bilgilere sahip olunması

---

[1] Emin Doğan Aydın, *Bilişim Suçları ve Hukukuna Giriş* (İstanbul: Doruk Yayınları, 1992), 27-28.

gerekmektedir. Günümüzde bilim ve teknoloji alanında yaşanan gelişmelerden ötürü bilim ve hukuk birlikte çalışmalı ve birlikte ilişki kurmalıdır.[2]

Hukukta kavramların ne anlama geldiği önem taşımaktadır. Bu nedenle çalışmamızda, siber dünyada işlenen bilişim suçlarının tek başına sadece bir suç olarak mı değerlendirilmesinin yerinde olduğu yoksa yöntem ve kullandıkları araçlar bakımından siber suç, siber terörizm ve siber savaş kavramlarının birbirlerinden farklı olarak mı değerlendirilmesi gerektiği, farklı ise farklı kılan etmenlerin neler olduğu şeklindeki sorulara cevap aranarak, siber alanda yaşanan teknolojik gelişmelere bağlı olarak kavramların doğru bir şekilde tanımlanmasına katkı sunulması amaçlanmıştır.

Bu çalışmamızla bilişim sistemi, siber suç, siber terörizm ve siber savaş konuları etrafında birinci bölümde, bilişim sisteminin ne olduğu hangi unsurlardan oluştuğu açıklanmıştır. Bilişim sistemlerinin temelde bilgisayar ve internetten oluştuğu kabul edilmekte olduğundan bilgisayar ve internet tarihinden bahsedilmiştir. Ardından suç kavramı açıklanmış, bilişim ile suç arasındaki ilişki açıklanmaya çalışılmıştır. İkinci bölümde siber ve siber saldırı kavramları açıklanmış, siber suçun saldırı aşamaları, türleri ve kullandıkları siber silahların nelerden ibaret olduğu izah edilmiştir. Üçüncü bölümde siber tehditlerin biçimleri olan siber suç, siber terörizm ve siber savaş kavramları açıklanmıştır. Sonuç bölümünde siber tehdit biçimlerinin ve eylemlerin birbirleriyle olan ilişkisi irdelenmiş ve farkları ortaya çıkarılmıştır.

Bu çalışmada, nitel araştırma yöntemine uygun olarak, belgelere dayalı gözlem tekniği uygulanmıştır. Bu nedenle alan yazında literatür taraması yapılmış olup kitap, dergi, makale, internet belgeleri, tez vb. dokümanlar incelenmiştir.

---

[2] Mehmet Yayla, "Hukuki Bir Terim Olarak 'Siber Savaş'," *Türkiye Barolar Birliği Dergisi,* no. 104 (2013): 178-179.

I. BİLİŞİM ALANINDA KULLANILAN KAVRAMLAR

A. Bilişim

Türk Dil Kurumu Türkçe güncel sözlüğünde bilişim "*insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi"* şeklinde ifade edilmiştir.[3] Ayrıca bu kavram enformasyon kelimesiyle de ifade edilmiştir. Enformasyon kavramı ise Fransızca dilinde *informatique* kelimesinden doğmaktadır. Fakat daha sonra bu yabancı kökenli olan enformasyon kavramı bırakılarak Türkçe karşılığı olan bilişim kelimesinin kullanılması yaygınlık kazanmıştır.[4]

Yazıcıoğlu'na göre bilişim "*bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır*."[5] Yenidünya ve Değirmenci'ye göre bilişim, "*teknik ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır*."[6]

Dülger'e göre "*İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türlü düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda*

---

3 Türk Dil Kurumu Sözlükleri, erişim tarihi: Haziran 21, 2022, http://www.sozluk.gov.tr.

4 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin Yayınları, 2014), 65.

5 Recep Yılmaz Yazıcıoğlu, Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle (İstanbul: Alfa Yayınevi, 1997), 131.

6 Ahmet Caner Yenidünya ve Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları* (İstanbul: Legal Yayıncılık, 2003), 27.

depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."[7]

Dülger bilişim kelimesi yerine bilgisayar kelimesinin kullanılmasının yanlış olduğunu belirtmiştir. Bilişim bir bilim dalıdır. Bilgisayar ise makineyi ifade etmektedir. Dülger, bu sebeple bilişim kelimesinin bilgisayara göre daha geniş ve kapsayıcı bir kelime olduğu görüşünü doğru bulmamakta olsa olsa bilişim sistemi ile bilgisayar kelimelerinin karşılaştırılmasında bu açıklamanın doğru olduğunu ifade etmektedir.[8]

B. Bilişim Sistemi

Öncelikle sistemi açıklamaya çalışırsak; ortak bir hedef için bir arada çalışan, birbirine bağlı ve birlikte hareket etme kabiliyetine sahip parçacıklardan oluştuğu bir bütündür. Örnek olarak eğitim sistemi, ulaşım sistemi vb. sayabiliriz. Bilgisayarlar kullanılmak suretiyle oluşturulan bilgi sistemleri için de *Bilişim Sistemleri* veya *Bilgisayar Tabanlı Bilgi Sistemleri* kavramı kullanılmaktadır.[9]

Bilişim sistemi, veri ya da bilgileri alan, bu bilgileri işleme tabi kılan, sonuçları veya verileri çıktı şeklinde verebilen elektronik sistemler olarak tanımlanabilir.[10] Bilişim sistemi veya bilişim alanı, verileri toparladıktan sonra bunları otomatik işlemlere tabi kılma olanağı veren sistemlerdir.[11]

Avrupa Konseyi Siber Suç Sözleşmesi'nde, bilgisayar sistemi kavramının, bir ya da birden fazlası belirli bir yazılım

---

7 Dülger, Bilişim Suçları, 67.

8 Dülger, Bilişim Suçları, 68.

9 Davut Özkul, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi," *Sayıştay Dergisi* 13, no. 44-45 (2002): 14.

10 Hüseyin Akarslan, *Bilişim Suçları* (Ankara: Seçkin Yayıncılık, 2012), 27.

11 İsmail Malkoç, *Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu-2. Cilt* (Ankara: Malkoç Kitapevi, 2007), 1665.

etrafında otomatik olarak veri işleyebilen bir aygıtıyla da birbirine bağlı ya da birbiriyle ilişkili bir dizi aygıtı olarak tanımlandığı görülmüştür.[12]

Türk ceza hukuku sisteminde bilişim sistemi ilk kez 20.09.2011 tarihinde Resmî Gazete'de yayınlanan Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik'in tanımlar ve kısaltmalar başlıklı 3'üncü maddenin ilk fıkrasının b bendinde "*Bilişim sistemi: Bilgisayar, Çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifa eder"* şeklinde belirtilmiştir. Yönetmelikte bilişim sisteminin bilgisayardan ibaret görülmesi olarak tanımlanmasının hatalı olduğu belirtilmiştir.[13]

C. Bilişim Sisteminin Unsurları

1. Bilgisayar

Bilgisayarı icat edenler bu aygıta İngilizce olarak *computer* adını vermişlerdir. Günümüzde İngilizce dilinin dünyada yaygın olması nedeniyle *computer* kelimesi yerleşik hale gelmiştir. Ülkemizde ise, bilgi işlemek anlamından türetilerek "*bilgi saymak, bilgi vermek*" anlamlarını taşıyan bilgisayar kelimesi, *computer* kelimesinin yerine kullanılmaktadır.[14]

Bilgisayarın birçok tanımı yapılmakla birlikte hızla gelişen bilim ve yeni yeni üretilen teknolojik ürünlerin insan hayatına sokulması sonucunda bilgisayar hakkında yapılmış olan tanımlar eksik kalmış, bilgisayarın ne olduğunu tanımlamak zorlaşmıştır. Çünkü klasik bilgisayarı oluşturan unsurların dışında (fare, kasa, monitör) günümüzde bilgisayarın işlevini gören dizüstü bilgisayar, tablet, akıllı saat gibi yeni bilgisayar

---

[12] İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum* (Ankara: Adalet Yayınevi, 2008), 11.

[13] Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları (*İstanbul: Legal Yayıncılık, 2013), 16.

[14] Dülger, Bilişim Suçları, 55.

türleri çıkmıştır. Yine de genel anlamda bilgisayarın tanımına yer verecek olursak; bilgisayarın yaptığı işler ve işlevlerine göre ve bilgisayarın fiziksel özellikleriyle yaptığı işler ve işlevlerine göre, iki ayrı yöntem izlenerek tanımı yapılmıştır.[15] İlk tanımlamaya göre bilgisayar; "*yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıttır. Bilgisayarı elektronik hesap makineleri ile programlanabilir aygıtlardan ayıran özelliği bilgisayarın bilişim özelliğine sahip olması yani bilgisayarın genel amaçlı kullanılabilmesidir*."[16] İkinci tanımlamaya göre bilgisayar; dış ortamdan farklı yöntemlerle aldığı verileri, içeriğinde barındırdığı yazılımları depo edip, işleyen, bu verilerden yeni sonuçlar çıkaran, çıkardığı sonuçları kullanan kişiye gösteren, bu itibarla veri iletişimi sağlayan makinedir.[17]

a. Bilgisayarın Unsurları

Bilişim sisteminin ilk unsuru olan bilgisayar çeşitli kısımlardan meydana gelir. Bilgisayar somut ve soyut parçalardan oluşur. Somut anlamda, bilgisayarın tüm fiziki parçalarına donanım, soyut anlamda ise, bu donanımların nasıl çalışacağını tespit eden fiziki olmayan kısmına ise yazılım denmektedir.

Donanım; mikro- işlemci, ROM, RAM, çevre/giriş-çıkış birimleri (yazıcı, fare, monitör, klavye, disket sürücüsü, tarayıcı, cd sürücüsü vs.) dir.

Yazılım ise verilerin elektronik biçimde toplanabildiği, depolanabildiği, işlenebildiği, belli bir komutu yerine getirebilmek için bilgisayara yüklenen ya da önceden bünyesine yerleştirilen bilgisayara işlerlik kazandıran komutlar bütününe denilmektedir. Doktrinde genelde kabul edilen ayrım; işletim

---

15 Dülger, Bilişim Suçları, 55.

16 Dülger, Bilişim Suçları, 56.

17 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 19.

yazılımı ve uygulama yazılımı şeklinde tasnif edilmektedir.[18] İşletim yazılımı, bilgisayarın işletilebilmesi için yerine getirmesi gereken yazılımdır. Uygulama yazılımı ise, mevcut olan işletim sistemine yüklenen ve belli bir amaç için kullanılan programlardır.[19]

2. İnternet

Türkçe'de ağların ağı ya da ağlar arası olarak ifade edilebilen internet, birden fazla bilgisayarın birbirlerine bağlanarak, dünyada yaygınlaşan ve sürekli gelişen bir iletişim teknolojisidir. İnternet, insanların sürekli üretilmekte olan bilgiyi, saklayabilme, paylaşabilme ve ona kolayca ulaşabilme isteklerinden dolayı meydana gelmiş bir teknoloji ürünüdür. İnsanlar bu teknoloji sayesinde birçok alandaki bilgilere kolaylıkla, hızlı bir şekilde, güvenli ve ucuz olarak ulaşabilmektedir.[20]

İnsan, internet ile herhangi bir yerden bağlanarak elde ettiği bilgiyi bilgisayarına aktarabilmektedir. Ayrıca bilimsel bilgilere, devlet belgelerine, eğlence amaçlı oluşturulmuş listelere, iş ve kişisel ilanlara ve veri tabanlarındaki her türlü alandaki bilgiye erişmeyi ve bu bilgileri kullanmayı mümkün kılabilmektedir.[21]

a. İnternetin Ortaya Çıkışı ve Gelişimi

İnternetin kökenleri 1960 yılında Amerikan Federal Hükümeti Savunma Bakanlığı'na bağlı araştırma ve geliştirme

---

[18] Levent Kurt, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması (Ankara: Seçkin Yayınevi, 2005), 31-36.

[19] Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 23-24.

[20] Aslan İnan, *İnternet El Kitabı* (İstanbul: Sistem Yayıncılık, 2000), 7-9.

[21] Tülay Bektaş Şeker, *İnternet ve Bilgi Açığı* (Konya: Çizgi Kitapevi Yayınları, 2005), 67.

birimi olan The Defense Advanced Research Projects Agency'e (DARPA)[22] dayandırılmaktadır.[23]

İlk önce ABD Savunma Bakanlığı, 1950 yıllarında SSCB'nin ilk yapay uydusu Sputnik'i uzaya göndermesine karşılık, ARPA isminde bir birim kurmuştur. ABD ve SSCB arasındaki soğuk savaş sırasında Amerikan ordusu, askeri verilerin ana bilgisayar kontrolünde diğer bilgisayarlarda da görünmesi ve tüm birimlerin aralarında kesintisiz iletişim sağlanabilmesi için bir ağ yapısı geliştirmeye karar vermiştir.[24]

ABD Savunma Bakanlığı 1969 yılında askeri araştırma projelerini ve çeşitli bilgisayar bilimlerini desteklemek için paket anahtarlamalı ağı yani ARPANET'i oluşturmuştur. Bu ağ daha sonra ABD'deki araştırma kuruluşlarında ve üniversitelerde kullanılarak büyümüştür. Bu ağ için 1973 yılında ise Stanford Üniversitesi,[25]Üniversite Koleji, BBN[26] ve Londra ile farklı bilgisayarların birbirlerini anlamak için protokol seti geliştirmek amacıyla internet working projesi başlatmıştır. 1978 yılına kadar farklı bilgisayarın birbirlerini anlayabileceği "*İletim Kontrol Protokolü*" (TCP) geliştirilmiştir. 1980 yılında bu protokol sabitleştirilmiştir ve ARPANET'e bağlı bilgisayarlar arasındaki iletişim kolaylaştırılmıştır. 1983 yılında ise tüm ARPANET kullanıcıları yeni bir protokol olan İletim Kontrol Protokolü/İnternet Protokolü'ne (TCP/IP) geçiş yapmıştır. Daha sonra ARPANET 1990 yılında kullanımdan kaldırılmıştır. Ancak

---

22 Savunma İleri Düzey Araştırma Projeleri Kurumu

23 Kürşat Çağıltay, *İnternet* (Ankara: METU PRESS, 1997), 5.

24 Ömer Sıddık Budak, "Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği" (Yüksek lisans tezi, Atatürk Üniversitesi, 2015), 4.

25 Stanford Üniversitesi, ABD'nin Kaliforniya eyaletinde San Francisco'nun 40 km güneydoğusunda bulunan özel bir üniversitedir. Üniversite, şu anda dünyadaki en büyük bütçeye sahip 3. Üniversitedir.

26 Raytheon BBN Technologies, başlangıçta Bolt Beranek ve Newman isimli Amerikalı araştırma ve geliştirme şirketi

TCP/IP protokolünün kullanımı ve geliştirilme süreci devam etmiştir.[27] Daha sonra ARPANET askeri kolu MILNET sivil kolu NSFNET olarak ikiye ayrılmış ve kendisi INTERNET adını almıştır.

1970-1981 yılları arasında çeşitli ağlar oluşturulmaya başlanmıştır. Bunlar arasında UUCP (Unix-to-Unix Copy), bilgisayar bilimleri alanında çalışan 100'e yakın araştırmacının elektronik posta ile iletişim kurabilmesi amacıyla Wisconsin Üniversitesi'nde Larry Landweber adlı kişi tarafından THEORYNET, üniversitelerin bilgisayar bölümleri arasında araştırma gayeli bir bilgisayar ağı oluşturulması amacıyla 1979 yılında Wisconsin Üniversitesi, NSF ve DARPA arasında bir görüşme yaparak UUCP kullanılarak CSNET, BITNET, USENET kurulmuştur. 1986 yılında omurga hızı 56Kbps olan NSFNET kurulmasına müteakip NSF, ABD dahilindeki internetin belkemiği NSFNET'in ticari anlamda çalıştırılması amacıyla Michigan Üniversitesi, MCI ve IBM'nin oluşturduğu ve Merit Network Inc. ismi verilen konsorsiyum ile sözleşme imzalanmıştır. Bu şekilde bilgisayarların bir diğer bilgisayara bağlanmasına yarayan bir sistem kurulmuştur.[28]

1989 yılında internetin sivilleşme süreci başlamıştır. İsviçre'de Tim Bernard Lee adında bir araştırmacı Nükleer Araştırmalar Merkezi'nde çalışmıştır. 1992 yılında bu araştırmacı World Wide Web (WWW) adlı teknolojisini meydana getirerek interneti sivil kullanıma açmıştır. "WWW" teknolojisi ile her tür görsel/grafik unsuru barındıran sayfalar oluşturabilmeyi ve tıklamalar aracılığı ile bu sayfaların birbirlerine bağlanabilmesini sağlamıştır.[29] Daha sonra dünya genelinde kullanılan milyonlarca ağın da NSFNET'e bağlanması ile 1990 yıllarının başlangıcından günümüzde kullanılan haliyle internetin temeli kurulmuştur.

---

27 Çağıltay, *İnternet*, 5.

28 Çağıltay, *İnternet*, 7-10.

29 Bektaş Şeker, İnternet ve Bilgi Açığı, 68.

b. Türkiye'de İnternetin Gelişimi

Türkiye'de genel amaçlı kullanılan bilgisayar ağları, 1980 yılında üniversitelerin önderliğinde EARN'ın Türkiye'deki uzantısı olan, Türkiye Araştırma Kurumları Ağı (TÜVAKA) ile kurulmuştur.[30]

Türkiye'de internet hazırlıkları 1991 yılında ODTÜ ve TÜBİTAK tarafından oluşturulan TR-NET (Türkiye Internet Proje Grubu) adı altındaki proje grubu ile başlatılmıştır. İlk bağlantı Nisan 1993 yılında ODTÜ-Washington (Türkiye-ABD) arasında gerçekleştirilmiştir.[31] Sonraki bağlantı ise 1994 yılında Ege Üniversitesi'nde TUVAKA kapsamında BITNET bağlantısı amacı ile kullanılan uluslararası hat 64Kbps hız ile Bonn üzerinden internet servisi sunmaya başlanmıştır.[32] Ardından sonraki bağlantılar ise sırasıyla Bilkent Üniversitesi (1995 Eylül), Boğaziçi Üniversitesi (1995 Kasım) ve İstanbul Teknik Üniversitesi (1996 Şubat) bağlantılarını gerçekleştirmiş ve 1996 yılı ağustos ayında TURNET çalışmaya başlamıştır.[33]

TR-NET'in teknik ve idari yönetimi 1996 yılından sonra ODTÜ BİDB[34] tarafından üstlenilmiştir. İlk internet servis sağlayıcı olan TURNET servisinin devreye girmesi ile TR-NET'in de konumu değişmiş ve TR-NET akademi dışı kuruluşlara hizmet sağlayan bir internet servis sunucusu (ISS) olarak çalışmaya başlamıştır.[35]

Türkiye'de kendi omurgaları olan iki kuruluştan biri ULAKBİLİM, diğer ise TURNET'tir. Bunlardan ilki, akademik amaçlı bağlantılar amacıyla çalışmaya başlamıştır. Diğer ise ticari amaçlı faaliyetlerini sürdürmüştür. Daha sonra 1 Haziran

---

30 Çağıltay, *İnternet*, 24.

31 İnan, İnternet El Kitabı, 7

32 Çağıltay, *İnternet*, 24.

33 İnan, İnternet El Kitabı, 66

34 ODTÜ Bilgi İşlem Daire Başkanlığı

35 Çağıltay, *İnternet*, 25-26.

1996 yılında TUBİTAK çatısında Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBIM) ismiyle Yüksek Öğretim Kurulu'nun da yardımıyla yeni merkez kurulmuştur. TÜBİTAK, ULAKBİM'in yeni teknolojileri kullanarak ülke çapında bütün araştırma ve eğitim kurumlarını birbirine bağlayacak Ulusal Akademik Ağ (ULAK-NET) adıyla bir veri iletişim ağı kurmuş ve bilgi hizmetleri vermiştir. TUR-NET ise 1995 yılı içinde açtığı bir ihale ile, ilk ODTÜ-ABD bağlantısını sağlayan grubun da başlangıçta içinde olduğu bir konsorsiyum tarafından oluşturulmuştur.[36]

D. Suç Kavramı

Suç olgusu topluma, mekâna ve zamana göre farklı anlamlar barındırmaktadır. Herhangi bir zamanda veya herhangi bir yerdeki toplum tarafından suç olarak görülmeyen bir eylem farklı zamanda veya başka yerdeki toplum tarafından suç olarak kabul edilebilmektedir. Bu nedenle suç olgusunu tanımlamak kolay değildir.[37] Suç kavramının her toplumda oldukça farklı anlamları mevcut ise de bu kavramı hukuki boyutta ele almak gerekmektedir. Sözlük anlamında suç; "*toplum düzenini bozan, kanunlarca yasaklanan, hukuka aykırı davranışlardır*."[38] Başka bir tanımlamaya göre ise; "*hukuk düzeninin cezai müeyyide altına aldığı insan davranışlarıdır*."[39]

Suç dinamik ve sosyal bir olgudur. Dinamik olgudur çünkü toplumsal değişimler içerisinde farklılık göstermektedir. Sosyal olgudur çünkü birden fazla insanın olduğu yerde birine göre suç

---

36 İnan, İnternet El Kitabı, 68.

37 Senem Burkay, "Teorik Çerçevede Suç," *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar* 2, no. 4 (2008): 2.

38 Fadime Dilber, "Kitle İletisim Araçları ve Suç Olgusu," *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomık Arastırmalar Dergısi* 16, no. Özel Sayı 1 (2014): 64.

39 Wilhelm Gallas, "Cezalandırılabilirliğin Temelleri ve Sınırları (Suç Kavramı Üzerine Düşünceler)," çev. İzzet Özgenç, *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 4, no. 1-2 (1994): 306.

olarak kabul gören bir davranış başka birine göre suç olarak kabul görülmeyen bir davranış ortaya çıkmaktadır. Örnek vermek gerekirse teknolojinin gelişmesiyle birlikte bilgisayar kullanımının yaygınlaşmasıyla bilgisayar aracılığıyla suçun işlenebilmesi mümkün hale gelmiş, bu şekilde bilgisayar suçları veya bilişim suçları ismi altında yeni bir suç tipi ortaya çıkmıştır. İlk olarak ABD'de işlenen bu suç tipi 1970'li tarihlerden itibaren tüm ülkelerde görülmüştür.[40]

Kanunların suç kabul ettiği cezai yaptırımlara bağladığı, hukuka aykırı eylem olarak nitelendirilen suç kavramı ve yaptırımları ancak kanunlar tarafından konulur ya da kaldırılır bu nedenden ötürü bir davranış kanunlarca suç olarak kabul edilmemiş ise hukuka aykırı bir davranış olsa dahi suç olarak kabul edilmemektedir.[41] Yani hukuki anlamda suçu ceza kuralı belirler. Eğer kural yoksa suç da yoktur. Ceza hukukunun temel ilkelerinden biri suç ve cezanın, yasada tanımlanmış olmasıdır. Özetle suç kavramını tanımlayacak olursak, ceza tehdidi altında yasaların yapılmasını yasakladığı olumlu ve olumsuz eylemler olarak ifade edebiliriz.

E. Bilişim ve Suçun Kesişimi

Bilişim ve iletişim; teknolojinin büyük hızla gelişmesine paralel olarak hayatımızın önemli bir parçası olmuştur. Gelişen teknolojinin kötüye kullanılmasıyla yeni suç alanları, araçları ve tipleri ortaya çıkmış; diğer bir ifadeyle bilişim teknolojisi, fiil ve fail tipolojisini temelden değiştirmiştir.[42]

Bilişim suçlarının hızlı evrimi ile hukukun ağır işleyen yapısı, problemlerin ortaya çıktığı noktada çatışmakta, hukukun nefesi bilişim suçlarına yetmemektedir.[43] Nitekim yasal

---

40 Burkay, "Teorik Çerçevede," 2.

41 Burkay, "Teorik Çerçevede," 3.

42 Erdoğan, Türk Ceza Kanunu'nda, 42.

43 Erdoğan, Türk Ceza Kanunu'nda, 43.

düzenlemelere ihtiyaç duyulması karşısında; mevzuat hazırlık süreci, yürürlük safhası, uygulamanın kamu ve özel sektörde sağlıklı şekilde yerleşmesi, olası eksiklik ve sorunların giderilmesi gibi süreçlerin eşzamanlı olarak etkin şekilde uygulanabilmesi her zaman mümkün olamamaktadır.[44]

Siber alanda sorumluluk bilinciyle hareket edilmemesi sonucunda bilgisayar sistemini kullanmanın etik ilkelerine aykırılık oluşturacağı gibi, bazı durumlarda hukuk kurallarını ihlale de sebebiyet verebilmektedir. Siber suçlar konusunda yapılan ve yapılacak hukuki düzenlemelerde suç politikasının evrensel nitelikteki temel ilkelerine uygun davranılması mecburiyeti vardır. Suç politikası, ceza hukukunun toplumu koruma görevini en iyi şekilde yürütmesi için hangi esaslar dahilinde düzenlenmesi gerektiği sorunuyla ilgilenmektedir. Bu sorunun çözümüyle ilgili olarak, suçun sebepleri üzerine odaklanır, ceza hukukunda uygulanan müeyyidelerin etkinliklerini araştırır, hukuku ihlal eden eylemlerin etkili biçimde önlenmesi için kanun koyucunun, ceza hukukunun kapsama alanını nereye kadar genişletebileceğini düşünür ve suç olayını en iyi belirleyen yasal unsurların neler olabileceğini inceler. Suç politikasında izlenen bu amaca ulaşmak için uyulması gereken temel ilkeler, kusur ilkesi, hukuk devleti ilkesi ve hümanizm ilkesi olarak tüm demokratik sistemlerde kabul edilmiştir. Suç politikasının evrensel nitelik kazanmış bu temel ilkelerine uyulmadan siber suçlar alanında yapılacak her normatif düzenlemede önemli yapısal problemlerin olacağı açıktır.[45] Bu nedenle bu çalışmamız ile bilişim suçları ile muhatap olan uygulayıcıların teknik terimler nezdinde; suçun oluşması ve işleniş şekillerinin anlaşılması açısından bu

---

[44] Burak Cesur Aköz, "Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri" (Bilişim uzmanlığı tezi, Bilgi Teknolojileri ve İletişim Kurumu, 2018), 21.

[45] Kayıhan İçel, "Avrupa Konseyi Siber Suçlar Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri'," *İstanbul Üniversitesi Hukuk Mecmuası* 59, no. 1-2 (2011): 3-4.

kavramların sağlıklı bir şekilde anlaşılması ehemmiyet arz etmektedir.

II. SİBER SALDIRI

A. Siber ve Siber Saldırı Kavramı

"Sibernetik" (*cybernetics*) sözcüğünün bir ön takısı olan "siber" kelimesinin, aynı zamanda sözcüğü kısaltmak amacıyla kullanıldığı görülmüştür.[46] Cyber sözcüğünden dilimize siber olarak tercüme edilmiştir. Bunun en önemli sebebi, siber kelimesinin gelişim süreci içerisinde yüklenmiş olduğu dönemsel anlam ve kültürel bütünlüğüdür. Merriam-Webster sözlüğünde "*cyber*" kavramının köken bilimsel olarak kökeninin "*cybernetic*"ten geldiği söz edilmektedir. "*Cybernetic*," otomatik hakimiyet sistemleri (sinir sistemi gibi) etrafında kontrol ve iletişim kuramının yer aldığı bilim dalı olarak tanımlanmıştır.[47] 1948 yılında sibernetik ilk defa, Norbert Weiner adlı Amerikalı bir bilim insanı tarafından "*makinelerde ve hayvanlarda iletişim ve hâkimiyet bilimi*" manasında kullanılmıştır.[48] Cyber ise, cybernetic'ten türemiş ve bilgisayar ağları için kullanıldığı belirtilmiştir. 1980 yıllarında, bilgisayar ağlarının online dünyası siber alan (*cyberspace*) olarak adlandırılmıştır. Bu dönemde "cyberpunk" akımının etkisiyle, rave/techno alt kültürü bünyesinde, teknolojiyi öğrenmeye ve etkin bir biçimde kullanmaya karşı arzulu, bağımsız kişiler "*hacker*" olarak anılmaya başlanmıştır.[49]

---

[46] Haydar Çakmak ve Cenker Korhan Demir, "Siber Dünyadaki Tehditler ve Kavramlar," iç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok (Ankara: Barış Platin Kitabevi, 2009), 25.

[47] Aslı Deniz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi- Temel Hükümlerin İncelenmesi," iç. *İnternet ve Hukuk*, ed. Yeşim M. Atamer (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004), 277.

[48] Çakmak ve Demir, "Siber Dünyadaki," 25.

[49] Helvacıoğlu, "Siber Suç Sözleşmesi," 278.

Tekrardan bahsedecek olursak bilişim kelimesi, siber sözcüğünün ilerisinde bir manayı hedef göstermektedir. Bilişim ve siber kelimeleri ara sıra birbirinin yerlerine kullanılmış olsa da siber, elektronik sistemlerin bulunduğu alan, bilişim ise bu alandan aktif bir şekilde yararlanma ve bu ortam aracılığıyla bilgi işlenmesi/üretilmesi anlamlarını taşımaktadır.[50] Çalışmamızın ilerleyen bölümlerinde siber suç ve bilişim suçu kavramlarının durumu tartışılmıştır.

Siber saldırılar, devletler, kuruluşlar, teröristler, işletmeler veya kişilerin belli bir amaç doğrultusunda siber alanda gerçekleştirmiş oldukları saldırı faaliyetlerini ifade etmektedir. Siber saldırılar, altyapıyı, yazılımı ve donanımı hedef almaktadır.[51]

B. Siber Saldırı Aşamaları

Siber saldırıların genellikle 6 aşamada gerçekleştiği ifade edilmektedir. Bu anlamda sistemle ilgili bilgi toplama; sisteme sızma; sıradan kullanıcı girişi; ayrıcalıklı kullanıcı girişi; sistem kaynaklarının ele geçirilmesi; sistem kaynaklarının etkilenmesi aşamalarından oluşur. Birinci aşamada, bir sisteme saldırıda bulunmadan önce, o sistemle ilgili maksimum düzeyde bilgi toplamak gerekir. Bu bilgiler, internet üzerinden toplanabileceği gibi, istihbarat örgütleri aracılığıyla ya da sosyal mühendislik metotlarıyla da toplanabilmektedir. İkinci aşamada, toplanan temel bilgilerden sonra otomatik yazılım araçları (NMap, Nessus gibi) kullanılarak sistemin zafiyetleri araştırılır. Yani bilişim sistemine kolay şifre testi, önceki bilgileri kullanarak daha karmaşık şekilde tahmin yürütme ya da daha önce tespit edilen şifreler aracılığıyla girilmeye çalışılır. Üçüncü aşamada öncelikle sıradan kullanıcı yetkileriyle giriş sağlanarak sistemin kaynakları keşfedilmeye çalışılır (kullanıcı adları, servisler, ağ yapısı gibi). Bu aşamada ele geçirilen bilgiler ve sistemdeki

---

50 Çakmak ve Demir, "Siber Dünyadaki," 26.

51 Hasan Çiftçi, *Her Yönüyle Siber Savaş (*Ankara: TÜBİTAK Popüler Bilim Kitapları, 2013), 133.

güvenlik zaafları sayesinde, ayrıcalıklı kullanıcı yetkileri alınır. Dördüncü aşamada, sisteme ayrıcalıklı yetkileri elde ettikten sonra (*root*, *superuser*, *administrator*) kötü niyetli eylemleri gerçekleştireceği yetkilere sahip olunur. Beşinci aşamada ise saldırgan, sistemdeki bilgileri ileride birtakım bir bileşene (dosya sunucusu, web sunucusu, etki alanı sunucusu, veri tabanı sunucusu, güvenlik sunucusu vb.) saldırmak için kullanır. Ele geçirilen veriler de FTP (File Transfer Protocol) kullanılarak sistem dışına aktarılabilir ya da gelecek bir zamanda aktarılmak üzere saklanabilir. Son aşamada ise saldırgan, sistemdeki bilgi veya işlemleri, değiştirmek, bozmak veya yok etmek için zararlı programlar yükleyebilir ya da bu eylemleri bizzat kendisi yapabilir.[52]

C. Siber Saldırı Türleri

a. Kabloya Saplama Yapma (Wire Tapping)

Emniyete alınmamış iletişim ağ kablolarına, özel teçhizat kullanılarak fiziki anlamda saplama yapılması ve iletişim kurulmasıdır. Bu yöntem ile tüm trafiğin ele geçirilmesi mümkündür. Telefon trafiği de bu yöntemle dinlenebilmektedir.[53]

b. Tuzak Kapı (Backdoor)

İşletim sistemleri normal şartlar altında yetkisiz şekilde girişe veya herhangi bir program ya da kod çalıştırmasına ve değiştirilmesine izin vermeyecek şekilde tasarlanmaktadır. İşletim sistemlerini ve programları hazırlayan programcılar, ilerde ortaya çıkabilecek durumlara karşı hatta bulma amacıyla kod ekleyebilmek veya ara program çıktısı alabilmek amacıyla programa istediğinde "trap doors" adı verilen durma mekanizmaları eklerler. Bu gizli kapıların program ve işletim sistemi tamamlandığında temizlenmesi gerekir. Ancak bazı

---

52 Çiftçi, Her Yönüyle Siber Savaş, 135-138.

53 Çiftçi, Her Yönüyle Siber Savaş, 139.

durumlarda hata sonucu olarak ya da ileride kullanılmak amacıyla gizli kapılar kapatılmaz. Bu durumlarda gizli kötü niyetli kişiler tarafından kullanılabilmektedir.[54]

c. Hizmet Dışı Bırakma (Denial of Service, Dos)

Bilgisayarı veya bilgisayar sistemlerini hedef kullanıcı topluluğunun taleplerine cevap veremez hale getirmektir.[55] Hizmet dışı bırakmak için kullanılan yöntemler şunlardır:

- İletişim ağı bant genişliği, işlemci zamanı ya da disk alanı gibi kaynakların tüketilmesi,
- Konfigürasyon verilerinin bozulması,
- Sistem durum bilgilerinin bozulması,
- Sistem bileşenlerinin fiziksel olarak bozulması,
- Kullanıcı ve sistem arasındaki iletişimin kanalının kesilmesi[56]

d. Kriptografik Saldırılar

Şifrelenmiş mesaj veya verilerin şifresinin çözülmesi maksadıyla uygulanan saldırılardır. Temel prensibi güçlü bir algoritmanın güvenliği bütünüyle anahtarın içindedir; algoritmanın tasarım detaylarında değildir.[57]

e. Zamanlama Saldırıları

Kriptografik saldırıların özel bir türüdür. Kriptografi de kripto algoritmasının çalışması için geçen sürenin analiz edilerek kripto sisteme nüfuz edilmesi amacıyla yan kanal saldırısı yapılmasına "zamanlama saldırısı" adı verilmektedir. Bilgisayarda yapılan her işlem bir süre gerektirmektedir. Bu süre sisteme verilen girdiye bağlı olarak değişir. Hassas süre ölçümü

---

54 Ebru Altunok ve Ali Fatih Vural, "Bilişim Suçları," *Denetişim*, no. 8 (2011): 79.

55 Alper Başaran, *Siber Savaş Cephesinden Notlar (*İstanbul: Arion Yayınevi, 2016), 29.

56 Çiftçi, Her Yönüyle Siber Savaş, 140.

57 Çiftçi, Her Yönüyle Siber Savaş, 141.

yapılmak suretiyle kripto sistemin özelliklerine ve girdiye ulaşılması çalışılır.[58]

f. İnternet Servis Saldırıları

Bilgisayarlar birbirleriyle iletişim ağı aracılığıyla, internet protokol ve servisleriyle bağlanmakla ve iletişim kurmaktadır. İnternette kullanılan protokollerin (TCP/IP, FTP, Telnet, POP3, HTTP, SMTP, DNS, DHCP BGP gibi) zayıf noktaları veya bu protokolleri gerçekleştiren yazılımlardaki açıklıklar kullanılarak bilgisayarlara saldırı yapılabilmektedir.[59]

g. Trafik Analizi

İletişimin yakalanıp analiz edilerek iletişim örüntülerinden (*pattern*) bilgi çıkarma eylemidir. Burada, giden ve gelen verinin içeriğinden ziyade, verinin örüntüsü veya üst bilgisine bakarak sonuca varılır. Trafik analizi, mesajlar şifreli veya çok fazla miktarda olduğunda da uygulanabildiği için etkilidir. Mesajların deşifre edilmesine gerek duyulmaz. Özellikle askeri istihbarat birimleri tarafından uygulanarak düşmanın eylemleri ile ilgili veri toplanması amaçlanır. Örneğin çok fazla trafik, planlama yapıldığında, trafik olmayışı, planın sonuçlandırıldığına veya bir şeylerin beklendiğine, belirli noktalar arası trafiğin fazla olması, o noktalar arası organizasyonel bir ilişkinin olması anlamına gelebilir.[60]

h. IP Aldatmacası

Kullanılan bilgisayarın gerçek IP adresinin farklıymış gibi gösterilerek gerçek IP adresini gizlemek ya da başkasının yerine geçmek amacıyla kullanılan saldırı yöntemidir. IP aldatmacası, saldırganın kimliğini gizlemek için kullandığı yöntemlerden biri olduğundan, çok önemli bir yöntemdir. Hizmet dışı bırakma saldırılarında sıklıkla kullanılır.[61]

---

58 Çiftçi, Her Yönüyle Siber Savaş, 143.

59 Çiftçi, Her Yönüyle Siber Savaş, 144.

60 Çiftçi, Her Yönüyle Siber Savaş, 145.

61 Çiftçi, Her Yönüyle Siber Savaş, 145.

i. Zararlı Yazılım Kullanımı

Bilgisayar virüsleri işletim sisteminin ve makine dilinin verdiği olanaklar kullanılarak yazılan, kendi kendisini çoğaltabilen, kopyalarını çeşitli yöntemlerle başka bilişim sistemlerine ulaştırarak bu sistemleri de etkileyebilen zararlı yazılım (virüs, solucan, Truva atı vb.) yüklemek veya yüklenmesini sağlamaktır.[62]

j. Oturum Çalma

İki bilgisayar arasındaki oturumun çeşitli yöntemlerle ele geçirilerek karşıdaki bilgisayara yetkisiz giriş yapma hakkının kazanılmasıdır. Bu saldırıda saldırgan mağdur ve sunucu arasına da girip ikisi arasındaki tüm trafiği dinleyebilir.[63]

k. Yığın E-Posta (Spam) Gönderme

Yığın e-posta, benzer içerikli e-postaların çok sayıda kullanıcılara gönderilmesidir. Yığın e-posta göndericiler, internet sitelerinden, haber gruplarından, müşteri listelerinden, sosyal medya sitelerinden vb. e-posta adresi toplar. Adresler, genellikle reklam mesajları göndermek için kullanılır. Çeşitli kaynaklarda farklı sayılar olsa da yığın e-posta miktarının toplam e-postalarının %75 ile %86'sını oluşturduğu görülmektedir.[64]

l. Açık Mikrofon Dinleme

Açık mikrofon dinleme, casus bir yazılım aracılığıyla, bilgisayara sahibinin haberi olmadan, bilgisayarın mikrofonunu açarak ortam dinlenmesinin yapılmasıdır. Ayrıca benzer şekilde bilgisayarın kamerası da açılabilmekte ve görüntü alınabilmektedir.[65]

---

62 Altunok ve Vural, "Bilişim Suçları," 79.

63 Çiftçi, Her Yönüyle Siber Savaş, 146.

64 Çiftçi, Her Yönüyle Siber Savaş, 147.

65 Çiftçi, Her Yönüyle Siber Savaş, 147.

m. Sosyal Mühendislik

İnsanlar arasındaki iletişimdeki ve insan hareketlerindeki modelleri zaaflıklar olarak tanıyıp, bunlardan yarar sağlamak suretiyle güvenlik aşamalarını atlatma yöntemine dayanan müdahaleleri içermektedir. En fazla kullanılan sosyal mühendislik metotları şunlardır:

- Karşı taraftakini güvenilir bir kaynak olduğuna inandırmak,
- Hedef sistemin atıklarını karıştırmak,
- Ortak tanıdıklar üzerinden yakınlık kurmak,
- Başkasını taklit etmek,
- Gizlice zor bir durum meydana getirerek yardım ediyormuş görünümü vermek[66]

n. Ağ Tarama (Network Scanning)

İletişim ağından akan verilerin gözlenmesi veya iletişim ağına bağlı donanımların zafiyetlerinin araştırılması eylemidir. Saldırı maksatlı olarak yapılabileceği gibi sistemin güvenlik ve performansını test etmek için de yapılabilir.[67]

o. Yerine Geçme (Masquerading)

Bilişim sistemleri erişim imkanları bakımından sınıflara ayrılmaktadır. Bazı bilişim sistemleri erişim yetkisi bakımından geniş yetkilere sahipken, bazıları da sınırlı yetkiye sahiptirler. Sistem işleyişinde bu yetkiyi tanımlayabilmek için parola veya erişim kodu ister. Ancak bazı durumlarda ufak hileler sonucunda sınırlı erişim yetkisi olan kişilere erişim hakkı tanınabilmektedir. Yetkisi olmayan veya sınırlı erişim yetkisi olan bir kişinin, parola veya erişim kodunun yazılması veya ona özgü niteliklerin taklit edilmesi şeklinde yapılıyor ise yerine geçme olarak isimlendirilir.[68]

---

66 Çiftçi, Her Yönüyle Siber Savaş, 147.

67 Çiftçi, Her Yönüyle Siber Savaş, 148.

68 Olgun Değirmenci, "Bilişim Suçları" (Yüksek lisans tezi, Marmara Üniversitesi, 2002), 65.

p. Yemleme (Phishing)

İnternette bulunan web sayfalarının tıpatıp benzerini yaparak yani onun yerine geçerek kişilerin burada gizli bilgilerini ve şifre bilgilerini girmek suretiyle bu özel bilgileri elde etme eylemidir. Bu yolla kullanıcıları kandırmak için popüler sosyal web siteleri, açık artırma siteleri, çevrim içi alışveriş siteleri, bankacılık siteleri vb. taklit edilmekte ve kullanıcılar dolandırılmaktadır. Genelde kullanıcıların e-postalarına sanki bankadan veya kullanılan başka bir siteden geliyormuş gibi mesajlar yazılmakta, kullanıcının e–postada verilen bağlantıyı yani linke tıklaması sağlanmaktadır. Açılan internet sayfası da aynen taklit edilen siteninkine benzemektedir. Ancak gerçekte bağlanılan, erişilen yer farklıdır. Kullanıcının gözünden kaçması ihtimali çok yüksektir. Örneğin "www.Facebook.com" adresi yerine www.facebooki.com adresine bağlanılmaktadır. Kullanıcı burada kullanıcı adı ve şifresini girmekte hata mesajı almakta ve gerçek facebook sitesine yönlendirilmektedir. Bu şekilde kişilerin kullanıcı adı ve parolaları toplanmaktadır.[69]

D. Siber Silahlar

Siber tehditler amacıyla kullanılan araçlara siber silahlar denilmektedir. En çok kullanılan siber silahlar şunlardır:[70]

- **Adware:** Kullanıcıların istekleri dışında reklam amaçlı açılan internet sitelerine tıklandığında ana sayfayı değiştiren programlardır.
- **DoS (Denial Of Service):** Bir sistemin ya da bir yazılımın geçici olarak durdurulması veya tümüyle kilitlenmesini amaçlayan bir exploiterdir (sömürücü).
- **Fake Mail:** Kamu kuruluşların, alışveriş sitelerinin, şirketlerin, bankaların sayfalarına benzer sahte bir sayfa

---

69 Çiftçi, Her Yönüyle Siber Savaş, 149.

70 Çetin Gümüş, "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi" (Doktora tezi, Fırat Üniversitesi, 2008), 16-19.

üretilerek kullanıcıların şifre ve bilgilerini elde etmeye yönelik bir formdur.

- **Keylogger:** Kullanıcıların şifrelerini takip etmek için klavye üzerinde basılan tuşların izlerini süren programlardır.
- **Sniffer**: Koklayıcı anlamında olup yerel ağdan şifrelenmemiş paketlerin kopyalanmasında ve bilgilerin elde edilmesinde kullanılır.
- **Spam Tool:** Bilgisayar kullanıcısının isteği dışında gönderilen reklam ya da e-postaların gönderildiği program çeşididir.
- **Spoofer:** Bilgisayar korsanlarının bilişim sistemlerine yetkili biriymiş gibi kendilerini göstermelerini sağlayan bir programdır.
- **Telnet:** Uzaktaki bilgisayara erişim sağlanırken yerel sunucuya bağlanıyormuş gibi kontak kuran terminal yazılımıdır.
- **Truva Atları (Trojan):** İlk bakışta zararsız gibi gözüken ancak içinde barındırdığı zararlı kodlarla bilişim sisteminin bozulmasına neden olan programlardır.
- **Virüs:** Bilgisayar verilerinin bozulmasına, silinmesine, çalışmasının engellenmesine, yavaşlatılmasına ya da başka problemlere sebep olacak şekilde oluşturulan programlardır.
- **Worm:** Worm aslında bir solucandır ve virüslere benzer. Bilgisayar korsanının açık bulduğunda bu zaafa odaklanıp kodları yayar ve makinelere kendi kendine kopyalar. Bunlar da verileri silebilir, şifreleri wormu yazana ulaştırabilir.

III. SİBER TEHDİTLER

Siber tehditler, siber suç, siber terörizm ve siber savaş terimlerinden oluşmaktadır. Şimdi bu kavramları açıklamaya çalışıp, farklarını ortaya koymaya çalışacağız.

A. Siber Suç veya Bilişim Suçu

1960 tarihinden itibaren Amerika'da siber suç eylemlerinin ortaya çıkmasının neticesi olarak Amerikan öğretisinde yaygın bir şekilde "bilgisayar suçları" (*computer crimes*) terimi kullanılmıştır. Diğer devletlerin hukukçularınca da benimsenmiş olup, Amerika'da bilişim suçları yerine bilgisayara karşı suçlar, bilgisayar suçu, bilgisayar ilişkili suç ya da bilgisayar yardımlı suç kavramlarının kullanıldığı görülmektedir.[71]

Siber suçlar, devletlerin mevzuatlarında tanımlanmış bir suç şekli değildir.[72] Bilişim teknolojilerinin kullanımı, yaygınlığı ve gelişmişliği ülkeden ülkeye değiştiğinden ve bilişim teknolojileri alanında sınır çizmek zor olduğundan bilişim suçu ile ilgili ortak tanımlama yapılamadığı görülmüştür.[73]

Ülkemizde de bu konuda bir kavram kargaşası mevcuttur. Bilgisayar suçu, internet suçu, siber suç, bilişim sistemi aracılığıyla işlenen suç, bilgisayar ile ilgili suç, bilgisayarlara karşı işlenen suç, bilişim suçu ve bilgisayarlar aracılığı ile işlenen suç vb. şeklindeki kavramların, bu alanı tanımlamak için kullanıldığı görülmektedir.[74]

Yukarıda bahsettiğimiz kavramların bazılarına yönelik söz konusu alanda eleştiriler mevcuttur. Örneğin ilk olarak internet suçu kavramından bahsetmek gerekirse; internetin bilişim suçları için zemin hazırlayan bir ağ olduğu, her ne kadar kullanımı kapsamlı olan bir ağ olsa da internet haricinde başka ağlardan da (intranet ve eksranet gibi) bilişim suçlarının işlenmesinin mümkün olduğu belirtilmiştir. Bu nedenle bilişim suçlarının işlenme ortamına göre farklı şekillerde isimlendirilmelerinin doğru olmadığı; örneğin kasten öldürme

---

71 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 30.

72 Ergün, Siber Suçların Cezalandırılması, 12.

73 Akarslan, *Bilişim Suçları*, 33.

74 Dülger, *Bilişim Suçları*, 69-70.

suçunu işlendiği ortama göre adam öldürme, bina içinde işlenirse bina suçu, otobanda işlenirse otoban suçu, açık alanda işlenirse açık alan suçu gibi adlandıramıyorsak, bilişim suçlarının da işlendikleri ağa göre isimlendirmenin doğru olmadığı, olsa olsa internet aracılığı ile işlenen suçlar kavramının kullanılmasının daha uygun olduğu yönünde eleştiriler getirilmiştir.[75]

Siber suç kavramından bahsedildiğinde aslında bilişim suçundan söz edildiği anlaşılmaktadır. Bilişim suçları, aslında sadece bir bilişim sisteminde işlendiği anlamı taşımamaktadır. Ayrıca bu suçun, bilişim sistemi ağları aracılığıyla da (özellikle internet) işlenebildiği anlaşılması gerekmektedir. Bilişim suçu kavramının, siber suç kavramına göre bir üst kelime olduğu ve siber suçu da ihtiva ettiği eleştirisi mevcuttur.[76]

Ancak her ne kadar bilişim suçunun, siber suç kavramına göre bir üst kavram olsa da Avrupa Birliği ile müzakere sürecinde AB müktesebatına uyum adı altında yedi paket halinde yüzlerce yasada değişiklik yapılmıştır. Türk Ceza Kanunu, Ceza Muhakemeleri Usulü Kanunu, Medeni Kanun, Hukuk Usulü Muhakemeleri Kanunu gibi 80 yıllık temel kanunlar değiştirilmiştir. En önemlisi Avrupa Birliği'ne uyum sağlamak için Anayasa'nın değiştirildiği, 1949 yılından beri Türkiye'nin kurucu üyesi sayılmakta olduğu Avrupa Konseyi'nin "Siber Suç" kavramını kullanması ve özellikle son zamanlarda yapılan çalışmalarda siber suç kavramının tercih edildiği görülmektedir.[77]

Biz de bu görüşe katılmaktayız. Bu nedenle çalışmamızda dünyadaki gelişmeleri de kapsayan ve ifade eden "siber suç" kavramı kullanılmıştır. Ancak bilişim suçu kavramına yüklenen kültürel ve dönemsel anlam bütünlüğü de göz önüne alındığında geçmiş ve mevcut yasal düzenlemeler ışında Türk

---

75 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 31-32.

76 Yenidünya ve Değirmenci, *Mukayeseli Hukukta*, 32-33.

77 Ergün, Siber Suçların Cezalandırılması, 14.

Ceza Kanunu'nda "bilişim alanında suçlar" kavramı hem öğreti de hem uygulamada görüş birliği halinde yerleşmiş olduğu ve tercih edildiği görülmektedir. Bu itibarla ülkemizdeki gelişmeleri ifade ederken siber suç kavramı yerine bilişim suçu kavramının kullanılması daha uygun olduğu görülmüştür.

Literatürde bilişim suçu kavramının tanımı incelendiğinde birçok tanım mevcuttur. Bilişim suçları izah edilmeye gayret edilmiş ise de üzerinde uzlaşılmış ortak bir tanım mevcut değildir.[78] Çünkü bir tanımlama yapılırken ne tür bir eylemin bilişim suçu olarak değerlendirilip hangilerinin bu eylem dışında bırakılacağı açıklığa kavuşmuş görünmemektedir.[79] Bilişim suçları altı farklı ölçüt dikkate alınarak tanımlanmaktadır. Bunlar: bilgisayarın amaç veya araç olmasını arayan tanım, bilişim suçlarını malvarlığı ihlalleriyle sınırlayan tanım, bilişim sistemleriyle herhangi bir şekilde ilişkili olan suçları esas alan tanım, bilgisayar kullanımını esas alan tanım, suçu işleyen faili esas alan tanım ve sınıflandırmaya tabi tutulamayan tanımlardır.[80] Yine de hukuk doktrinindeki tanımlardan birkaçına değinecek olursak; Aydın, *"elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi hırsızlığı için hazırlık yapılmasıdır."*[81] Ergün; *Bilişim "sistemleri ve bilişim teknolojileri kullanılarak bu sistemlerde ve bilişim ağlarında işlenen suçlardır"* şeklinde tanımlama yapmıştır.[82] Dülger; "*verilere ve/veya veri işlemle bağlantısı olan sistemlere veya sistemin düzgün ve işlevsel işleyişine karşı, bilişim sistemleri aracılığı ile işlenen suçlar"* şeklinde tarif yapmıştır.[83]

---

78 Berrin Bozdoğan Akbulut, "Bilişim Suçları," *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 549.

79 Dülger, *Bilişim Suçları*, 72.

80 Dülger, *Bilişim Suçları*, 72.

81 Aydın, *Bilişim Suçları*, 27-28.

82 Ergün, Siber Suçların Cezalandırılması, 16.

83 Dülger, *Bilişim Suçları*, 73.

Bu tanımlamalardan hareketle sonuç olarak bilişim suçu; veri işleyebilen, depolayan tüm elektronik cihazlara, yine bu sistemlerin aracı kılınması suretiyle doğrudan veya dolaylı biçimde yasa dışı yollarla erişilerek sistemi bozma, içindeki kayıtları silme veya bu kayıtları elde etme eylemi olarak görülmektedir.

1. Bilişim Suçlarının Yapısı ve Özellikleri

Bilişim suçunun işlenebilmesi için gerekli olan bilişim ortamının temel unsurları üçe ayrılmaktadır. Bilişim suçunun unsurlarından birincisi, bilgisayar ve bilgisayar benzeri akıllı cihazlardır. İkincisi, bilgisayar ve bilgisayar benzeri akıllı cihazlar arasında veri iletişimin sağlanabilmesi için gerekli bir iletişim ortamıdır. Üçüncüsü ise, bu bilgisayar ve benzeri cihazların çalışması için gerekli olan enerjinin (elektrik) sağlanmasıdır.[84] Bilişim suçunun en temel özelliklerinden bahsetmek gerekirse bu suçun işlenmesi oldukça kolay bir o kadar da tespit edilmesi ve cezalandırılması açısından zor olmasıdır.

2. Uluslararası Alanda Siber Suçların Sınıflandırılması

Siber suçların sınıflandırılmasında ortak bir ayırım yapılamamıştır. Birçok tasnifi mevcuttur. Strasbourg'daki 21 Kasım 2000 tarihinde Avrupa Topluluğu'nun 24 sayılı proje çalışmalarında siber suçların dört bölüm olarak tasnif edildiği görülmektedir. Bunlar; verilerin ve bilişim sistemlerinin kullanımına, bütünlüğüne ve güvenliğine ilişkin suçlar, manevi varlığa ve bununla alakalı haklara ait suçlar, bilişim suçları, muhteviyatı itibariyle suçlardır.[85]

---

[84] Akarslan, *Bilişim Suçları*, 37.

[85] Tezcan Özkan,"Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi" (Yüksek lisans tezi, Anadolu Üniversitesi, 2006), 69.

Avrupa Komisyonu'nun 2007 yılındaki tebliğinde; elektronik ağlara ilişkin suçlar, elektronik basın üzerinde yayınlanan yasa dışı muhteviyata ilişkin suçlar ve elektronik ağlar aracılığı ile işlenen klasik suçlar biçiminde de sınıflandırma yapılmıştır.[86]

Özcan'a göre bilişim suçları üç ana başlık altında toplanmaktadır. Bunun yanında teknolojiye paralel olarak sürekli artmaktadır. Birincisi, saldırı bir bilgisayarın kendisi hedefi olabilir. Bu şekilde bir bilgisayarın sunmuş olduğu hizmetler, bilgisayarın bütünlüğü ve gizliliği tehdit altındadır. Bu durumda bir saldırı gerçekleşirse bilgisayar maddi zarar görmektedir. İkincisi, suç işlemek amacıyla bilgisayar aracı kılınabilir. Üçüncüsü ise bilgisayarın hardiskinde depolanmaması gereken bilgilerin saklanması ile suça karışılabilir (pornografik videolar, resimler vb.).[87] Bir başka tasnife göre ise; kişilere karşı işlenen bilgisayar suçları, malvarlığına karşı işlenen bilgisayar suçları ve devlete karşı işlenen bilgisayar suçları şeklindedir.[88]

3. Siber Suç Türleri

Özcan siber suç türlerini belirtirken İnterpol'ün hazırladığı "İnterpol Bilgisayar Suçları Kılavuzu", Birleşmiş Milletler'in "Bilgisayar Bağlantılı Suçların Önlenmesi ve Kontrolüne İlişkin Birleşmiş Milletler El Kitabı" ve Avustralya Polis Teşkilatı'nın "Bilgisayar Temelli Suçların Soruşturulması için Asgari

---

86 Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları," *Uluslararası Güvenlik ve Terörizm Dergisi* 4, no. 2 (2013): 137.

87 Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenlik," iç. *İnternet ve Hukuk*, ed. Yeşim M. Atamer (İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004), 305-307.

88 İbrahim Balcıoğlu, "İnternet Kullanımı ve Getirip Götürdükleri," *Somuncubaba Dergisi*, (2014): 66-67.

Hükümler" kitapçıklarından yararlanarak suç tiplerini belirtmiştir:[89]

a) Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim

i. *Yetkisiz Erişim:* Bilgisayarın sisteminin bütününe ya da bir bölümüne, programlara, içerdiği bilgilere izinsiz ve yetkisiz olarak erişilen suçlardır.

ii. *Yetkisiz Dinleme:* Yetkisiz olarak bir ağ sisteminin ya da bilgisayarın teknik anlamda dinlenilmesidir. Teknik dinleme, iletişimin izlenerek verilerin dolaylı olarak ya da doğrudan elde edilmesi ile bağlantılıdır.

iii. *Hesap İhlali:* Başkasının hesabını kullanarak bilişim sistemlerine yetkisiz erişim sağlanarak yararlanmaktır.

b) Bilgisayar Sabotajı

i. *Mantıksal:* Bilgisayar veya iletişim sisteminin, işlevinin çalışmasını engellemek için bilgisayar verileri ya da programlarının bir kısım zararlı yazılımlar kullanılarak çalışamaz hale getirilmesi, ele geçirilmesi veya değiştirilmesidir.

ii. *Fiziksel:* Bilgisayar sisteminin çalışmaması için bilgisayarı oluşturan unsurlardan birine veya tamamına fiziki müdahalede bulunarak zarar verilmesini kapsamaktadır.

c) Bilgisayar Yoluyla Dolandırıcılık: İşlenen klasik suçların siber ortamda bilgisayar ve iletişim teknolojileri kullanılarak işlenme biçimidir. Bu durum kullanıcıya maddi ve manevi zarara uğratacak şekilde zarar vermektedir.

i. *Banka Kartlarını Kullanma:* ATM cihazlarına yönelik hırsızlık ve dolandırıcılık suçlarını kapsamaktadır. ATM'ye koyulan kopyalama cihazları, kamera gibi araçlar ile banka kartları çoğaltılır veya şifresi ele geçirilir.

ii. *Girdi/Çıktı/Program Hileleri Yapma:* Bilişim sistemindeki mevcut olan verilerin kasıtlı değiştirilmesi ya da sistemden sahte çıktı alınması veya mevcut programların değiştirilmesiyle yapılan hırsızlık ve dolandırıcılıktır.

---

[89] Özkan, "Siber Terörizm," 71-75.

iii. *İletişim Servislerini Haksız ve Yetkisiz Kullanma:* Kişinin kendisine maddi çıkar sağlamak için iletişim protokol servislerine ya da bilgisayar sistemlerine izinsiz şekilde girmektir.

d) Bilgisayar Yoluyla Sahtecilik: Bilişim sistemleri aracılığıyla sahte kâğıt para, senet, kredi kartı vb. materyaller üreterek ya da dijital belgeler üzerinde değişiklik yapılmasıdır.

e) Yasalar ile Korunmuş Bir Programın/Yazılımın İzinsiz Kullanımı: Yasalar ile hakları korunmuş olan programların izinsiz olarak kopyalanması, çoğaltılması ve dağıtılması ve kullanılmasını içerir.

i. Lisanssız Sözleşme İhlali

1) *Lisans Sözleşmesine Aykırı Kullanım:* Normalde bir bilgisayar için kurulması gereken programın birden çok bilgisayara yüklenmesi ve kullanılmasıdır.

2) *Lisans Haklarına Aykırı Çoğaltma:* Yazılımın lisans haklarına aykırı davranarak kopyalanmasıdır.

3) *Lisans Haklarına Aykırı Kiralama:* Yazılımların, oyunların ya da filmlerin lisans sözleşmesine aykırı bir şekilde kiralanmasıdır.

ii. *Taklitçilik:* Lisanslı yazılımın, yasalmış izlenimi verilerek kopyalanması ve satılmasıdır.

iii. *İzinsiz İthalat:* Lisanslı bir yazılımın ilgili kişilerden izin alınmadan ticaretinin yapılmasıdır.

f) Yasadışı Yayınlar: Kanunlar tarafından yasaklanan ve suç teşkil eden her türlü yayın, internet siteleri, e-postalar, haber grupları, dijital kayıtların muhafaza edilmesi, yayınlanması ve dağıtılmasıdır.

g) Diğerleri

i. *Ticari Sırların Çalınması:* Ekonomik menfaat sağlamak veya zarar vermek kastıyla yetkisi veya yasal izni olmadan yasa dışı yollarla bir ticari sırrın kullanılması, açıklanması veya elde edilmesidir.

ii. *Verilerin Suistimal Edilmesi:* Gizli bilgilerin, sırların kişilerin rızası alınmadan çıkar temin etmek veya zarar vermek kastıyla kullanılması, dağıtılması ve satılmasıdır.

iii. *Sahte Kişilik Oluşturma ve Kişilik Taklit Etme:* Kendisine menfaat sağlamak veya karşısındakine zarar vermek kastıyla hayali bir kişilik oluşturmak ya da başkasının bilgilerini kullanarak taklit etmektir.

4. Siber Suçları Geleneksel Suçlardan Ayıran Özellikler

Siber suçların, geleneksel suçlardan ayrıştığı noktalardan biri, işlenen suçların bilişim teknolojilerinin araç olarak kullanılmasıdır. Bilişim suçlarının, geleneksel suçlar ile benzerlik gösterdiği gibi ayrılıkları da mevcuttur:[90]

a. Siber suç olarak nitelendirilen eylemin sonuçları, başka bir devletin sınırları içerisinde görülebilmektedir. Uluslararası alanda suç işlendiğinde ise delil toplama çalışması zorlaşmaktadır.

b. Siber alanda işlenen suçlarda risk geleneksel suçlardaki gibi fazla değildir. Ayrıca birtakım devletlerde kanunda mevcut boşluklar nedeniyle suçun daha kolay işlenmesinde zemin oluşturmaktadır.

c. Siber alanda gizli kalma unsuru, suç işlemeye özgün bir ortam hazırlamaktadır.

d. Siber suçları işleyen kişiler incelendiğinde, bu kişilerin önceden birbirlerini tanımadıkları görülmektedir. Farklı ülkelerde yaşasalar dahi ortak iş yaparak siber suç eylemine iştirak etmektedirler. Hatta siber suçları iş birliği içerisinde yapanların aynı dili dahi kullanmadıkları anlaşılmaktadır.

e. Siber suç eylemine karşı alınan önlemler neticesinde, daha gelişmiş yöntemlerin ortaya çıktığı görülmektedir. Bu yöntemlerin sürekli gelişmesi ve çeşitlenmesinin temel nedeni ise teknolojinin hızlı bir biçimde gelişmesinden kaynaklanmaktadır.

---

[90] Ufuk Taşçı ve Ali Can, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2016): 231.

f. Siber suçların niteliği itibariyle suçlunun yakalanması için genellikle ortak bir çalışmayı, iş birliğini gerektirmektedir.

g. Siber suçları belli bir alanda sınırlandırmak ya da ortadan kaldırmak mümkün görünmemekte aksine yöntemler çoğaldıkça siber suçlar da çoğalmaktadır.

h. Çok az bir bilgi ile ciddi siber suçlar işlenebilmektedir.

i. Siber suçunu işleyenler arasındaki bağlantı, genellikle ekonomik ya da geçici özellikte olup, klasik bir organize suç örgütünün hiyerarşisi ve yapısı bu örgütlerde görülmemektedir. Ancak her siber suç eyleminde örgütlenmeden söz edemeyiz.

j. Siber suçlular, saldırılarını yapmak amacıyla anonimlik, güvenlik, esneklik ve kolluk birimlerinin engellemesine karşı mukavemet göstermesini sağlayan bir altyapıya gereksinim duymaktadırlar.

k. Siber suçlular, her ne kadar çok büyük tahrifat yapsalar da suçu siber alanda işlediklerinden dolayı herhangi bir sorumluluk duymamaktadırlar.[91] Yani gerçek yaşamda aynı mekânda bulunularak sözlü tacizin yapılması, çok ahlaki olmazken ve toplumda büyük bir çoğunluk bu eylemi yapmaya cesaret gösteremezken, internet ortamında yapılan sohbetlerde bireyler, sözlü tacizi kimliğini gizleyerek çok rahatlıkla yapabilmektedir.

B. Siber Terörizm

Siber terör, teröristlerin siber saldırı düzenleyerek, barajın kapaklarını açabilecekleri, askeri ordunun iletişim sistemlerine sızıp yanlış ve yanıltıcı bilgiler bırakabilecekleri, şehrin tüm trafik ışıklarını çalışamaz hale getirebilecekleri, bilişim sistemlerini bozabilecekleri, yolları bozabilecekleri, finans ve bankacılık alanını çökertebilecekleri, kamu kurumlarının

---

91 Nurullah Sandilaç, "Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları" (Yüksek lisans tezi, Sakarya Üniversitesi, 2021), 51.

faaliyetlerini (kolluk, acil yardım, hastane ve itfaiye çalışmaları vb.) engelleyebilecekleri ve nihayet hükümet kurumlarını alt üst edebilecekleri bunun sonucunda da sistemin durdurulabileceği bir siber tehdit unsurudur.[92]

Siber terörü iyi anlamamız için öncelikle terör ve terörizm kavramını açıklamamız gerekmektedir. Ancak her devlet, terör kavramının tanımını kendi politikalarına göre yorumlamaktadır. Bu sebeple, her devlet, uluslararası terör saldırılarını tanımlarken, kendisini hedef alan saldırıları kapsayacak biçimde ve gelmekte olan ya da gelme ihtimali olan dahili ve harici düşmanlarının olası saldırılarını, uluslararası kanuna göre yasa dışı görmek istemektedir. Bununla birlikte her devlet, herhangi bir şekilde otoritelerini kötü biçimde etkiyebilecek ifadelerden uzak durmaktadır. Neticesinde, bir ülke tarafından terörist olarak yaftalanan kişi ya da kişiler, diğer bir ülke tarafında da "özgürlük savaşçısı" olarak görülmektedir.[93] Bu nedenle terörün tanımında uzlaşma tam olarak sağlanamamaktadır.

Terör, sosyolojik açıdan, siyasi yapıda yer alan faaliyettir. Temelde hedef olarak tespit ettiği bireyin, grubun veya toplumun ardındaki yönetim felsefesine, yani legal veya illegal kabul edilmiş olan egemenlik ilişkisine saldırır. Bu faaliyetlerin, otoriter bir yönetime yönelik yapılıyorsa haklı bir tepki, demokratik bir yönetime yönelik yapılıyorsa haksız bir tepki olarak algılanmaktadır. Demokratik yönetimlerde bu faaliyetlerin kabul edilmeyişinin nedeni ise, demokratik yönetimlerdeki egemenlik ilişkisinin, yani yönetim felsefesinin toplumun isteğine ve kabulüne bağlı olmasından kaynaklanmaktadır. Bu egemenlik ilişkisine yapılan saldırılar,

---

92 Sedat Sertoğlu, "Büyük tehlike," Sabah Online, son değiştirilme Aralık 6, 1999, http://arsiv.sabah.com.tr/1999/12/06/y11.html.

93 Mehmet Yayla, "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı," *Hacettepe Hukuk Fakültesi Dergisi* 4, no. 2 (2014): 195.

doğrudan egemenlik ilişkisini dönüştürmeye ve bu ilişkiye hakim olmaya yönelik olduklarından ve insanların da ölümüne neden olduklarından, tanım gereği bu eylemi yapan kişi veya kişiler, terörist olarak nitelendirilmektedir.[94]

Yine de terörün tanımını yapmak gerekirse "*şiddet kullanma ya da şiddet tehididi barındıran anormal yollarla siyasal davranışları etkilemek üzere tasarlanmış sembolik bir fiildir.*"[95] Ayrıca terör, 3713 saylı Teörörle Mücadele Kanunu'nun 1. maddesinde "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasi, hukuki, sosyal, laik , ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir"* şeklinde tanımlanmıştır. Terörizm ise şiddetin sistematik olarak kullanıldığı bir yöntem biçimidir ve aşağıda belirtilen özelliklere sahiptir:

- Önceden planlanmıştır ve korku iklimi yaratmak amacıyla tasarlanmıştır,
- İlk (yakın) mağdurlardan çok daha geniş bir hedefe yönlenmiştir,
- Sivilleri de içine alan rastgele ve sembolik saldırıları içerir,
- Toplum tarafından anormal olarak nitelendirilir,
- Görünürde ayrımcı olmasa da aslında gerçek anlamda ayrımcı bir yapıya sahiptir,

---

94 Emre Kongar, *Küresel Terör ve Türkiye (*İstanbul: Remzi Kitapevi, 2002), 73-74.

95 Çakmak ve Demir, "Siber Dünyadaki," 36.

- Öncelikle, hükümetlerin ve toplulukların siyasi davranışlarını etkilemek için kullanılır.[96]

Yukarıda ifade edilenlere göre; terör örgütünün herhangi bir devlet kurumuna yöneltilecek saldırının temel amacı o kurumun hizmetlerini tamamen sona erdirmek değil, kitlelerin gözünde devleti küçük düşürmek ve toplumda korku duygusunun hâkim olmasını sağlamaktır. Nereye ve kimlere güvenileceğini bilemeyen toplumun paralize (toplumsal felç) edilmesi kolaylaşır ve terörizm de böylelikle nihai amacına ulaşır.[97]

Terör örgütleri siber ortamda sıklıkla internetin sağladığı kolaylıklardan faydalanır. İnternet, teröristler için eşi bulunmaz avantajlar sunmaktadır. Bu avantajlardan bazıları; merkezi bir kontrolden uzaklığı, herhangi bir sınırlamaya uğramaması, isteyen herkesin ulaşımına açık olması, hızlı bilgi akışı, diğer iletişim metotlarına göre ucuz ve kolay olması, multimedya ortamı sağlaması, anonimlik halinin elverişli olması şeklindedir. Bunların dışında internet özellikle hayli küçük grupların kendilerini duyurabilmesi için de önemli fonksiyon görür.[98] Bir kısım terör eylemleri siyasi olmakla birlikte, her siyasi eylem de terör niteliği taşımamaktadır. Bir saldırının terör olarak tanımlanabilmesi için "eylem, örgüt ve ideoloji" unsurlarının bir arada bulunması elzemdir. Belirtilen unsurlardan birinin eksik olduğu takdirde, o eylemin terörizm eylemi dışında bir sınıflamaya tabi tutulduğu görülmektedir. Örneğin bir politik nitelik taşımayan şiddet hareketleri (ırk-mezhep kavgaları) örgütlü görünseler dahi, bu gruplar organize suç faaliyetleri olarak değerlendirilmemesi gerekmektedir.[99] Çünkü toplumda korku duygusunu oluşturma, devletin egemenliğe saldırı gibi ideolojik unsuru ve buna yönelik doğrudan bir eylemi

---

96 Çakmak ve Demir, "Siber Dünyadaki," 36.

97 Çakmak ve Demir, "Siber Dünyadaki," 37.

98 Çakmak ve Demir, "Siber Dünyadaki," 38.

99 Özkan, "Siber Terörizm," 6.

bulunmamaktadır. Bu tür küçük gruplar arasında eylem, örgüt ve ideoloji unsurları birbirleriyle uyumlu bir şekilde bulunmamaktadır.

Siber terörizm ise, terörizmde belirtilen özellikleri taşımak suretiyle siyasal içerikli olup siber alanda, bilgisayar sistemlerine karşı sızma, ihlal etme veya bozma eylemlerinin gerçekleşmesi ya da gerçekleştirme tehdidi gibi bir eylemin sebep olduğu engellenme sonucu, milyonlarca insanın davranışını etkileyerek günlük yaşamını bozmaktır.[100] Stanford Üniversitesi, Uluslararası Güvenlik ve İşbirliği Merkezi (CISAC), Hoover Kurumu ve Bilgi Güvenliği ve Politikaları Alanında Araştırma Konsorsiyumu başkanlığında 9 kişilik bir gruba yaptırdığı siber suçlar ile ilgili bir çalışmada siber terörizmi "*Hukuken yetkili kılınmış görevlilerin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü veya yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara veya mallara karşı önemli zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması veya yapılacağı tehdidi* şeklinde tanımlamıştır."[101]

Başka tanımlara göre ise siber terörizm, siyasi ya da sosyal amaçların gerçekleştirilmesi için bir ülkeyi ya da halklarını aşağılamak ya da korkutmak için bilgisayarlara, ağlara ya da verilerin saklandığı bölümlere gerçekleştirilen yasadışı saldırı ya da saldırı tehditleridir. Siber terörizm, bilgisayar ve iletişim teknolojisi yeteneklerinin siyasi olarak motive olmuş ulus-altı gruplar ya da ajanlarca şiddet, bir toplumu etkilemek ya da bir hükümetin politikalarını değiştirtmek gayesiyle silah ya da hedef olarak kullanılması biçiminde de tanımlanabilir.[102]

Siber terörizm, sadece bilgisayar ve ilgili teknolojilerin bir araç olarak kullanılmasını değil, bir hedef olarak belirlenmesini

---

[100] Çakmak ve Demir, "Siber Dünyadaki," 39.

[101] Özcan, "Siber Terörizm," 309.

[102] Yayla, "Siber Savaş," 195.

işaret etmektedir. Ancak sınır aşan organize suç örgütleri ile terörist örgütlerin eylem alanlarının ve yöntemlerinin yakınlaştığı günümüzde bilgisayarın araç olarak kullanıldığı bazı örnekler konunun karmaşıklaşmasına sebep olmaktadır. Örneğin mali alt yapısının kredi kartı sahteciliğine dayandığı bir terör örgütünün, temel eylemi kredi kartının sahtesini üretmek olduğundan bilgisayarların bu amaçla kullanılması sadece fiilin niteliğini değiştirmektedir. Bu nedenle salt bu gibi eylemler siber terörizm olarak değerlendirilemez. Ancak terör örgütünün kamuya açık bir alanda güvenlik kuvvetlerinin elektronik sistemlerine girilmesi suretiyle gerçekleştireceği eylemlerde ve bunun sonucunda insanlarda yaralanmalara, ölümlere yol açarak toplumda korku, kaygı ve panik duygusunu yaratması siber terörizm kapsamı içinde değerlendirilebilir.[103] Görüldüğü üzere siber suçlarla siber terörizmi birbirinden ayıran temel etken, eylemin siyasal bir sebeple işlenmesi, bilişim teknolojilerinin, araç veya hedef olarak kullanılması ve bunun sonucunda toplumda panik duygusunu yaratması gerçeği yani suçun terörden ayrıldığı noktada ortaya çıkmaktadır.

Bu açıklamalar doğrultusunda siber terörün, klasik terörden farkını Özcan altı maddede açıklamıştır:

- Öncelikle terör örgütleri geleneksel anlamda faaliyetlerini bir nebze de canlarını da gerektiğinde ortaya koymadırlar. Eline silah ya da bomba alan bir terörist ihtimaldir ki bir polis ya da asker tarafından etkisiz hale getirilsin. Fakat dünyanın herhangi bir yerinde internete bağlanan bir siber terörist canını tehlikeye atmadan ülkenin toplumsal yaşamına ciddi zarar vererek eylemini gerçekleştirebilir. Ayrıca siber terörizm kamu binaları gibi terörist eylemlerin hedefi olan yerlerin fiziki güvenliklerinin artırılmalarının yanında daha cazibeli hale gelmektedir. Çünkü, siber terörist kendine çok daha güvenli bir ortamda eylemlerini hazırlayabilmektedir.

[103] Çakmak ve Demir, "Siber Dünyadaki," 39-40.

- İkincisi ise terörün asıl gayesinden yola çıkarak ulaşılan farklı sonuçlardır. Terörün asıl gayesi, yapacağı terör eylemleri ile topluma ve hükümete mesaj vermektir. Ancak siber terörde şiddet araç olmaktan farklı olarak amaç haline dönüşebilmektedir. Bilgisayar aracılığı ile bir siber terörist finans kurumlarının, büyük bankaların ve borsa bilgilerini ve iletişimini mahvedebilir. Bu şekilde toplumun ekonomik yaşamı sekteye uğrayabilir. Ya da bir ilaç firmasının sistemine girerek ilaç içeriğine dair bilgilerde en ufak bir değişiklik yapıldığında dahi binlerce insanın hayatına mal olabilmektedir.
- Üçüncüsü ise klasik terör faaliyetleri ile yapılmak istenen propaganda geniş kitlelere her ne kadar ulaşabilse de aslında eylem itibariyle lokaldir. Yani bir terör eyleminde hedef alınan bir kamu binasına yapılan bombalı saldırı sonucu çökebilir ve sadece orda bulunan insanlar hayatını kaybedebilir. Ancak siber terörde ise eylemin etki alanı klasik terörden çok daha fazladır. Bir terörist, oturduğu yerden, hedef aldığı sisteme sızarak, sistemi çökertebilir. Bu zararın etki alanı ise ülkenin geneline yayılmaktadır. Böylelikle insanların gündelik hayatına daha fazla etki edebilmektedir. Örnek vermek gerekirse operatör şirketlerinden herhangi birine yapılacak saldırı sonucu sızılan bilişim sisteminde bir siber terörist tüm telefon faturalarını artırabileceği gibi azaltabilir. Bu durumda şirketin uğrayacağı zarar ile toplumsal huzursuzluk, devlet kurumuna yapılacak terör faaliyetinden daha fazla olabilmektedir.
- Dördüncüsü, siber terörizmin psikolojik yanı, bilgi teknolojilerini kullanan birey, grup, toplum ve devletlere kadar uzanabilmektedir. Hedefler gerçek ancak sembolik olmadığından, klasik terörizm kadar yaygın dalga içermemektedir. Ayrıca siber terörde bugüne kadar ölüm ve yaralanma gerçekleşmediğinden kamuoyundan duygusal bir tepki daha az doğmaktadır.
- Beşincisi, klasik terör eylemlerinde seçilecek elemanın genelde belirli bir yaşın üzerinden seçilmektedir. Ancak siber terörde böyle bir sınırlama bulunmamaktadır. Çünkü bilgisayar kullanımı çocuk yaştaki birisinin bile kolaylıkla öğrenebileceği,

kullanabileceği bir teknolojidir. Bu nedenle siber terörde çocuklar araç olarak kullanılabilmektedir. Ortaokul ve liseli gençler, devlet kurumlarına macera arayışı ile bir hevesle saldırmaktadırlar.

- Son olarak klasik terörde, teröristler eylemlerini silah ya da bomba gibi araçlarla gerçekleştirmekte iken siber terörde ise bilgisayar ve internet gibi araçları kullanarak eylemlerini gerçekleştirmektedirler.[104]

Siber terörizm ile ilgili karşıt görüşler de mevcuttur. Örneğin Joshua Green, "The Myth of Cyberterroism" başlığını taşıyan makalesinde bilgisayarlar tarafından öldürülen insanların olmadığını, devletlerin çok gizli ve güvenlik gerektiren bölgelerinde internet bağlantılarının bulunmadığını ifade ederek siber terörizm kavramının abartıldığı belirtmektedir.[105]

Akman'a göre, siber terörizm kavramı; 2002 yılında yazılan "The Next War Zone" (Geleceğin Savaş Bölgesi) adlı kitapta ortaya atıldığını ifade etmiştir. Bu kitap, Amerika Birleşik Devletleri Hükümetinin görüşlerini dile getiren bir çalışma olduğunu, bu çalışmada Irak, Kuzey Kore ve Çin'in de ellerinde "Kimyasal Başlıklı Füzeler", "Zehirli Gaz Bombası Atan Uzun Menzilli Silahlar" olduğu; bu ülkelerin, sahip oldukları bu silahları "Sibernetik Sistemler"e yönlendirerek başka ülkelere fırlatma gücüne sahip bulundukları için yakın bir gelecekte, bir "siber terörizm" yaratacakları şeklindeki iddiaları içermektedir.

Siber terör uzmanları şu an için çalıntı araçların, bomba yüklü kamyonların ve biyolojik silahların siber terörizmden daha büyük bir tehlike yarattığından bahsetmektedirler. Siber

---

104 Özcan, "Siber Terörizm," 311-313.

105 Çakmak ve Demir, "Siber Dünyadaki," 35.

terör tehdidi abartılmış olarak gözlemlense de ne yok sayılabilir ne de göremezlikten gelinebilir.[106]

Siber terörizmin gerçekleştirilebilirliği tartışma konusudur. Çünkü bugüne kadar devletlerin güvenlik sistemlerine oldukça zarar veren herhangi bir siber terörizm saldırısı meydana gelmemiştir. Bunun nedeni ise devletlerin önemli yerel ağ sistemlerini, genel ağ sistemlerinden ayırmalarından kaynaklanmaktadır. Ancak bu durum gelecekte böyle bir saldırı olmayacağı anlamına da gelmemektedir.[107]

C. Siber Savaş

Savaş kavramı, ulus ya da devlet içerisindeki düşmanlar arasında meydana gelen, açıkça ilan edilmiş silahlı çatışmaları tanımlamak için kullanılmaktadır. Siber savaş ise, rakip devletlerin siber ortamdaki siber saldırılarını ifade etmektedir. Ancak hangi siber saldırıların, siber savaş kapsamında değerlendirilmesi gerektiği konusunda görüş birliği bulunmamaktadır. Bunun nedeni olarak kimileri; siber savaşa gerektiğinden çok ehemmiyet verildiğini, meydana gelecek bir siber saldırının, savaş nedeni olarak kabul edilemeyeceğini, ülke kaynaklı siyasi bir siber saldırının, savaş kadar eski olan casusluk, sabotaj veya tahrip maksatlı bir saldırı ile aynı neticeyi doğuracağını ve konvansiyonel anlamda silahlı kuvvet kullanılmayacağını savunmaktadırlar. Bunun yanında İran,[108]

---

106 Taner Altınok ve Zeynep Kaya, "Siber Tehditlerle Mücadele," iç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok (Ankara: Barış Platin Kitabevi, 2009), 160.

107 Çakmak ve Demir, "Siber Dünyadaki," 43.

108 2010 yılında ABD ve İsrail'in, İran'ın nükleer çalışmalarını sekteye uğratmak için kullandığı Stuxnet adlı solucan yazılımı ile gerçekleştirdiği siber saldırı olayı.

Gürcistan[109] ve Estonya'ya[110] yönelik yapılan siber saldırılar, siber savaşın ehemmiyetini gözler önüne sermekte, savaş hukuku ve uluslararası çerçevesinden konu değerlendirilmektedir. Rakip ülke ya da devlet destekli alt grupça yapılacak bir siber eylemde, siber saldırıya uğrayan devlet tarafından Birleşmiş Milletler Antlaşması'nın 51. maddesindeki "meşru müdafaa hakkı"nın kullanılabileceği düşünülmek ve savunulmaktadır.[111]

Görüş birliğinin olmamasının bir başka neden ise, gelişen teknoloji karşısında bilgi çağı öncesi düzenlenen Birleşmiş Milletler Antlaşması'nın, siber ortamdaki gelişmeleri ve potansiyel tehditleri öngörememesidir. Örneğin silahlı çatışma olarak ifade edilen konvansiyonel savaştan farklı olarak siber ortamda gerçekleşen siber saldırılarda silah kavramının ne olduğu, siber saldırıda kullanılan araçların silah kapsamında değerlendirilmesi gerekip gerekmediği tartışma konusu olmuştur.

ABD Başkanı George W. Bush'un siber güvenlik danışmanı olarak çalışmış olan Richard Clark'e göre siber savaş, bir ülkenin, başka bir ülkenin bilgisayar sistemlerine ya da ağlarına zarar vermek veya kesinti yapmak üzere gerçekleştirilen sızma faaliyetleridir.[112] Yine ABD Genelkurmay Başkanlığı siber savaşa yakın bir anlam içeren tanım yapmış olup, "bilgi savaşı" kavramını kullanmış ve "*düşmanın insan ve araç kaynaklı karar alma sistemlerini etkilemek, etkinliğini azaltmak, bozmak veya ele geçirmek buna karşın kendi sistemlerini korumak*" olarak tanımlamıştır. Birleşmiş Milletler Terimler Sözlüğü'nde, siber

---

[109] 2008 yılında Rusya Federasyonu'nun Gürcistan'a yönelik konvansiyonel saldırısını gerçekleştirmeden önce bu saldırıyı desteklecek şekilde planlama yaptığı ve gerçekleştirdiği siber saldırı olayı.

[110] 2007 yılında Estonya Parlementosu'nun Tallinn Meydanı'ndaki Bronz Asker anıtını kaldırma kararından sonra Rusya Federasyonu tarafından gerçekleştirdiği iddia edilen siber saldırı olayı.

[111] Yayla, "Siber Savaş," 183-184.

[112] Çiftçi, Her Yönüyle Siber Savaş, 5.

savaş (*cyberwar*) bilgi savaşı (*information warfare*) ile aynı anlamda, "*bilgisayar sistemlerinin düşman sistemlerine zarar vermek veya yok etmek maksadıyla kullanıldığı savaş tipidir*" şeklinde tanımlanmaktadır. Siber savaşın, İngilizce karşılığı olan "*cyberwar*", bazı sözlüklerde de bilgi savaşının yani "*information war*" teriminin eş anlamlısı olarak kullanılmakta ve "*elektronik iletişim ve internetin bir ülkenin iletişim sistemi, güç kaynakları, ulaşım sistemi ve benzeri sitemlerini bozması veya çökertmesi*" olarak tanımlanmaktadır. Şangay İş birliği Örgütü ise bilgi savaşını, "*toplum ve devlet düzenini bozmak için toplu psikolojik beyin yıkama faaliyetlerinin yanında devleti, düşman devlet isteklerine göre karar almaya zorlamak*" olarak tanımlamaktadır.[113] Bu tanımlardan dikkat edilecek birinci husus, siber savaşın devletler arasında cereyan etmesi; diğeri ise, karşı tarafın sistemlerine hasar vermeye veya sistemlerde kesinti yapmaya yönelik eylemlerin siber savaş olarak nitelendirilmesidir.[114]

Siber savaşın iki önemi mevcuttur. Birinci önemi, siber savaş yönteminin nasıl uygulanacağı ve gerginliğin artırılmasından nasıl kaçınılacağını içermektedir. İkinci önemi ise, siber savaşın asıl gayesidir. Rakip gördüğü tarafa boyun eğdirmeyi, verilerini çalmayı, sistemlerine sızarak belirli bir süre etkisiz bırakmayı veya komple bozmayı içermektedir.[115]

Siber savaşın silahları sentaktik saldırılar, semantik saldırılar ve karışık saldırılar olmak üzere üç kategoriye ayrılmıştır. Sentaktik saldırıların hedefi, bilgisayar sistemleri olup, zararlı programlar, hizmet engelleme eylemleri ve sisteme girmektir. Semantik saldırılar, bilgisayar sistemini hedeflemez, sadece bilgisayar kullanıcısının ulaşmış olduğu verinin doğru olup olmadığını hedef almaktadır. Sistem problemsiz bir biçimde çalışmasına rağmen içerdiği veriler doğru olmaktan uzaktır. Bu saldırılar, özellikle resmi internet sitelerinin veya

---

113 Yayla, "Siber Savaş," 190-191.

114 Çiftçi, Her Yönüyle Siber Savaş, 5.

115 Çiftçi, Her Yönüyle Siber Savaş, 7.

kritik altyapı tesislerinin sistemleri hedeflendiğinde ciddi neticeler oluşabilir. Karışık saldırılar, semantik ve sentaktik saldırıların bir arada yapılmasıdır. Kritik işletim sistemlerinin yanlış bilgi ile belgelerden beslenerek etkisizleştirilmesi karışık saldırıya örnek teşkil etmektedir.[116]

Siber savaş, genelde parasal kazanç hedeflenen suçtan ve politik amaçlı sembolik saldırılar içeren terörizimden temelde farklılık göstermektedir. Siber savaşın, suç ve teröre nazaran daha belirgin farklılıkları vardır. Her ne kadar bazı ülkeler siber suç veya terör eylemlerinin işlenmesini doğrudan ya da dolaylı olarak desteklese de savaşın örgütlenmiş ve hükümet oluşturmaya niyetli meşru gruplar tarafından uygulandığı, diğer ikisi için genelde böyle bir durumun olmadığı dikkatlerden kaçmamalıdır. Siber savaş, siber suçların ve siber terörün aynı sanal sistemi kullanmaları bir benzerlik gibi görünse de amaçlarda ve motivasyonda farklılık mevcuttur. Ayrıca siber savaş, suç ve terörizmden daha düzenli ve yoğun saldırıları içermektedir. Bunun yanında siber terörizm ve siber suçlar, bireyler veya gruplar tarafından işlenirken siber savaş devlet veya örgütlenmiş bir otorite tarafından işlenmektedir. Bu nedenle kişisel boyutta yapılan eylemler siber savaş içerisinde değerlendirilmemektedir.[117]

SONUÇ VE ÖNERİLER

Bilgisayar ve internetin ortaya çıkmasından sonra suçun sanal dünyada da işlenebilme kolaylığı görülmektedir. Tek bir tıklama ile dünyanın bir ucundan diğer bir ucuna siber saldırı yapılabilecek teknolojiye kavuşulmuştur. Dolayısıyla suç örgütleri devletlere ve toplumun yıkıcı mantığına karşı eski klasik yöntemlerle savaşmamakta, gelişen teknolojik gelişmeler neticesindeki araç ve gereçlerden yararlanmaktadırlar.

---

116 Yayla, "Siber Savaş," 187-188.

117 Çakmak ve Demir, "Siber Dünyadaki," 44-45.

Bunun sonucunda yeni bir dünya; siber dünya ortaya çıkmasının yanında küreselleşme ile birlikte internetin yaygınlaşması, küreselleşmenin negatif etkileri, devletlerin sınırsız müdahaleleri ile yerel milliyetçiliklerin yükselmesi, siber dünyanın boşluklarından faydalanan kötü niyetli, suça meyilli veya suçlu, birey ve grupların ve teröristlerin bu alana yönelmeleri nedeniyle yeni suç türlerinin, suçluların, suç örgütlerinin doğmasına neden olmuş ayrıca siber suç, siber savaş ve siber terörizmi kavramlarını ortaya çıkarmıştır. Ancak hukuk ve güvenlik politikaları bakımından siber dünyada işlenen suçların karmaşıklığından dolayı kavram karışıklığına neden olmuştur. Bu nedenle çalışmamız, bilişim sistemi, siber suç, siber terörizm ve siber savaş konuları etrafında şekillenmiş, siber dünyadaki diğer kavramların, aktörlerin ve eylemlerin de tanımlanması yapılmıştır.

Araştırmanın sonucuna göre, siber dünyada işlenen suçlar; bilgisayar suçu, internet suçu, siber suç, bilişim sistemi aracılığıyla işlenen suç, bilgisayar ile ilgili suç, bilgisayarlara karşı işlenen suç, bilişim suçu ve bilgisayarlar aracılığı ile işlenen suç, bu alanı tanımlamak için kullanıldığı görülmüştür. Yine bu alanı tanımlamak için kullanılan kıstaslar; bilgisayarın amaç veya araç olmasını arayan tanım, bilişim suçlarını malvarlığı ihlalleriyle sınırlayan tanım, bilişim sistemleriyle herhangi bir şekilde ilişkili olan suçları esas alan tanım, bilgisayar kullanımını esas alan tanım, suçu işleyen faili esas alan tanım ve sınıflandırmaya tabi tutulamayan olarak sıralandığı görülmektedir.

Çalışmamızın neticesinde, siber suç, siber terörizm ve siber savaşın saldırı yöntemleri her ne kadar benzerlik gösterse de motivasyon ve amaçları bakımından ayrıldıkları görülmüştür. Buna göre siber suç, bilişim sistemlerinin kullanılması suretiyle kişiden kişiye işlenen suçlar olduğu değerlendirilmektedir. Burada herhangi bir örgütsel eylemin olmadığı anlaşılmaktadır. Bireysel eylem söz konusu olmaktadır. Siber suç, bilişim sistemlerine geçici veya kalıcı zarar vermek, verileri elde etmek

veya yok etmek şeklinde ifade edilmektedir. Ancak bu saldırılar örgütlü bir şekilde ideolojik unsuru barındırıyorsa, devlete karşı bir eylem ise ve toplumları paniğe sokmak, korkutmak ve karışıklık meydana getirmeyi amaçlıyorsa, bu saldırı biçimini, devlet yetkilileri tarafından siber terörizm kapsamında değerlendirdiği anlaşılmıştır. Yine siber saldırılar, doğrudan veya dolaylı yoldan bizatihi devletlerarası gerçekleştiriliyorsa bu saldırı biçimi ise siber savaş kapsamında değerlendirildiği görülmüştür.

Bilişim suçları kapsamında değerlendirilen siber saldırılar, vatandaşların hayatlarını etkilemekte, ekonomi alanında şirketlere büyük kayıplara uğratmakta ve devletlerin güvenliğini tehdit etmektedir. Bu nedenle bu tedirginlikler karşısında herkesin önlemler almasına gerek duyulmaktadır.

Öncelikle vatandaşların bilgisayar kullanımı ve güvenliği konusunda sürekli bilinçlendirilmeleri gerekmektedir. Bu konuda gerekli önlemlerin nasıl alınacağını bilmeyen vatandaşların en azından hükümetlerin internet güvenliği ve antivirüs yazılımlarının kullanımının yaygınlaştırılması, maddi anlamda ulaşılabilir olması bu konuda farkındalık yaratılması gerekmektedir.

Siber terör eylemleri ile siber savaşların etkisi düşünüldüğünde, devletlerin gerek ulusal boyutta gerekse uluslararası boyutta siber tehditlere karşı stratejiler oluşturması gerekmektedir. Teknolojik alt yapılarını ve ağ güvenliklerini gözden geçirmeleri gerekmektedir. Siber saldırıların dünyanın bir ucundan diğer bir ucuna yapılabilir olduğu düşünüldüğünde bu anlamda uluslararası sözleşmeler ön plana çıkmaktadır. Bu nedenle uluslararası kuruluşların öncülüğünde bu alandaki gelişmelerin takip edilmesi, buna göre yasal zeminin güncellenmesi ve suçluların yakalanmasına dair ortak anlaşma ve çalışmalar yürütülmesi elzemdir.

Bunun yanında devletin güvenlik güçlerinin siber suçları engelleme veya kontrol altına alma çabalarının yanında birtakım

problemler ortaya çıktığı görülmektedir. Buradaki temel problem güvenlik güçlerinin siber suçları önlemek için vatandaşların internet gezintilerini gözetleme ve izleme faaliyetlerinde bulunmak zorunda olduğu kadar internet kullanıcıların mahremiyet ve gizliliklerinin de aynı kişiler tarafından korunmak zorunda olduğu gerçeğidir. Bu dengeyi iyi bir şekilde kurması gerekmektedir.

Devletin güvenlik güçleri tarafından, siber suç ve suçlarla mücadele etmek için izleme ve gözetlemenin sınırlarını genişletmeye çabalamaları karşısında internet kullanıcıların özgürlük, mahremiyet ve gizliliğin ihlal edilmemesi için devleti yönetenler ve kanun koyucular tarafından her iki tarafında bunu sağlayan güçlendirici araçların düzenlenmesi gerekmektedir.

Hakem Değerlendirmesi: Çift kör hakem.

Finansal Destek: Yazar bu çalışma için finansal destek alıp almadığını belirtmemiştir.

Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.

Etik Kurul Onayı: Yazar etik kurul onayının gerekmediğini belirtmiştir.

Peer Review: Double peer-reviewed.

Financial Support: The author has not declared whether this work has received any financial support.

Conflict of Interest: The author has no conflict of interest to declare.

Ethics Committee Approval: The author stated that ethics committee approval is not required.

KAYNAKÇA

Akarslan, Hüseyin. *Bilişim Suçları.* Ankara: Seçkin Yayıncılık, 2012.

Aköz, Burak Cesur. "Türk Ceza Kanunu Kapsamında Bilişim Suç ve Cezaları ile Örnek Yargısal Kararların Analizi ve Mevzuat Önerileri." Bilişim uzmanlığı tezi, Bilgi ve İletişim Teknolojileri Kurumu, 2018.

Altınok, Taner, ve Zeynep Kaya. "Siber Tehditlerle Mücadele." İç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok, 137-162. Ankara: Barış Platin Kitabevi, 2009.

Altunok, Ebru, ve Ali Fatih Vural. "Bilişim Suçları." *Denetişim*, no. 8 (2011): 74-84.

Aydın, Emin Doğan. *Bilişim Suçları ve Hukukuna Giriş.* İstanbul: Doruk Yayınları, 1992.

Balcıoğlu, İbrahim. "İnternet Kullanımı ve Getirip Götürdükleri." *Somuncubaba Dergisi*, (2014): 64-67.

Başaran, Alper. *Siber Savaş Cephesinden Notlar.* İstanbul: Arion Yayınevi, 2016.

Bektaş Şeker, Tülay. *İnternet ve Bilgi Açığı.* Konya: Çizgi Kitapevi Yayınları, 2005.

Bozdoğan Akbulut, Berrin. "Bilişim Suçları." *Selçuk Ünüversitesi Hukuk Fakültesi Dergisi* 8, no. 1-2 (2000): 545-555.

Budak, Ömer Sıddık. "Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği." Yüksek lisans tezi, Atatürk Üniversitesi, 2015.

Burkay, Senem. "Teorik Çerçevede Suç." *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar* 2, no. 4 (2008): 1-15

Çağıltay, Kürşat. *İnternet.* Ankara: METU PRESS, 1997.

Çakmak, Haydar, ve Cenker Korhan Demir. "Siber Dünyadaki Tehditler ve Kavramlar." İç. *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, ed. Haydar Çakmak ve Taner Altunok, 23-55. Ankara: Barış Platin Kitabevi, 2009.

Çiftçi, Hasan. *Her Yönüyle Siber Savaş.* Ankara: TÜBİTAK Popüler Bilim Kitapları, 2013.

Değirmenci, Olgun. "Bilişim Suçları." Yüksek lisans tezi, Marmara Üniversitesi, 2002.

Dilber, Fadime. "Kitle İletisim Araçları ve Suç Olgusu." *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomık Arastırmalar Dergısi* 16, no. Özel Sayı 1 (2014): 60-66.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Yayınları, 2014.

Erdoğan, Yavuz. *Türk Ceza Kanunu'nda Bilişim Suçları.* İstanbul: Legal Yayıncılık, 2013.

Ergün, İsmail. Siber Suçların Cezalandırılması ve Türkiye'de Durum. Ankara: Adalet Yayınevi, 2008.

Gallas, Wilhelm. "Cezalandırılabilirliğin Temelleri ve Sınırları (Suç Kavramı Üzerine Düşünceler)." çeviren İzzet Özgenç. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi* 4, no. 1-2 (1994): 305-327.

Gümüş, Çetin. "Bilişim Suçlarıyla Mücadelede Polisin Eğitimi." Doktora tezi, Fırat Üniversitesi, 2008.

Hekim, Hakan, ve Oğuzhan Başıbüyük. "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları." *Uluslararası Güvenlik ve Terörizm Dergis* 4, no. 2 (2013): 135-158.

Helvacıoğlu, Aslı Deniz. "Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi." İç. *İnternet ve Hukuk*. ed. Yeşim M. Atamer, 277-300. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

İçel, Kayıhan. "Avrupa Konseyi Siber Suçlar Sözlşemesi Bağlamında 'Avrupa Siber Suç Polistikasının Ana İlkeleri'." *İstanbul Üniversitesi Hukuk Mecmuası* 59, no. 1-2 (2011): 3-10.

İnan, Aslan. *İnternet El Kitabı.* İstanbul: Sistem Yayıncılık, 2000.

Kongar, Emre. *Küresel Terör ve Türkiye.* İstanbul: Remzi Kitapevi, 2002.

Kurt, Levent. Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. Ankara: Seçkin Yayınevi, 2005.

Malkoç, İsmail. Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu - 2. Cilt. Ankara: Malkoç Kitapevi, 2007.

Özcan, Mehmet. "Siber Terörizm ve Ulusal Güvenlik." İç. *İnternet ve Hukuk*. ed. Yeşim M. Atamer, 301-340. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2004.

Özkan, Tezcan. "Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi." Yüksek lisans tezi, Anadolu Üniversitesi, 2006.

Özkul, Davut. "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi." *Sayıştay Dergisi* 13, no. 44-45 (2002): 11-34.

Sandilaç, Nurullah. "Siber Dünyada Hacker Kültürü, Hacktivizm ve Bilişim Suçları." Yüksek lisans tezi. Sakarya Üniversitesi, 2021.

Sertoğlu, Sedat. "Büyük tehlike." Sabah Online. Son değiştirilme Aralık 6, 1999. http://arsiv.sabah.com.tr/1999/12/06/y11.html.

Taşçı, Ufuk, ve Ali Can. "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014." *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2016): 229-248.

Türk Dil Kurumu Sözlükleri. "Güncel Türkçe Sözlük." Haziran 21, 2022. https://sozluk.gov.tr/.

Yayla, Mehmet. "Hukuki Bir Terim Olarak "Siber Savaş"." *Türkiye Barolar Birliği Dergisi*, no. 104 (2013): 177-202.

Yayla, Mehmet. "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı." *Hacettepe Hukuk Fakültesi Dergisi* 4, no. 2 (2014): 181-200.

Yazıcıoğlu, Recep Yılmaz. Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle. İstanbul: Alfa Yayınevi, 1997.

Yenidünya, A. Caner, ve Olgun Değirmenci. *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.* İstanbul: Legal Yayıncılık, 2003.