Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2022,Cilt:11, Sayı:1, 109-134
doi:10.28956/gbd.1109756

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2022,Volume:11, Issue:1, 109-134
doi:10.28956/gbd.1109756

Makale Türü ve Başlığı / Article Type and Title
Araştırma / Research Article
Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ve Türk Hukuku'nda Karşılığı
Council of Europe Convention on Cybercrime and Its Equivalent in Turkish Law

Yazar(lar) / Writer(s)
Yusuf KARADENİZ, Jandarma ve Sahil Güvenlik Akademisi e-posta: yusuf.karadeniz@hbv.edu.tr. ORCID: https://orcid.org/0000-0002-7709-0580.

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :10.08.2021
Makale Kabul Tarihi / Accepted :11.03.2022

Atıf Bilgisi / Citation:
Karadeniz, Y. (2022). Avrupa Konseyi sanal ortamda işlenen suçlar sözleşmesi ve Türk hukuku'nda karşılığı. *Güvenlik Bilimleri Dergisi, 11(1), ss 109-134, doi:10.28956/gbd.1109756*

AVRUPA KONSEYİ SANAL ORTAMDA İŞLENEN SUÇLAR SÖZLEŞMESİ VE TÜRK HUKUKU'NDA KARŞILIĞI

Öz

Hızla gelişen dijital teknoloji ve ağ sistemleri sonucunda internet, "Vahşi Batı" misali siber suçların odak noktası haline gelmiştir. Mevcut durum, devletlerin egemenlik hakları kapsamında yargı yetkilerini paylaşmama eğilimi ile birlikte ele alındığında, bu suçlarla mücadele kapsamında uluslararası adli iş birliği, gerçekleşmesi zor bir ihtimal haline gelmektedir meğerki siber suçlarla mücadele özelinde bağlayıcı nitelikte uluslararası boyutu olan bir uzlaşı sağlanabilsin.

Çalışmamız; konuya ilişkin literatür taraması, güncel yargı kararlarının incelenmesi ile uluslararası ve yerel mevzuat incelemelerinden edinilen bilgiler bağlamında şekillendirilmiştir. Öncelikle her devletin kendi sosyal, kültürel ve ekonomik değerleri özelinde farklılık gösteren siber suç terimi ile ilgili kavramsal bir incelemede bulunularak metnin devamında olması muhtemel anlam karmaşasının önüne geçilmek istenmiştir. Sonrasında ise Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşme (Council of Europe Convention on Cybercrime, Budapeşte Sözleşmesi) dışında ulusal ve uluslararası alanda siber suçlarla mücadele amacıyla yapılan girişimler değerlendirilecektir.

Sözleşme'nin getirdiği yükümlülükler açısından Türk Hukuku'ndaki etkileri ile Türkiye'de siber suçlarla mücadele amacıyla düzenlenen mevzuatın Sözleşme'yi karşılama durumu incelenecektir. Bu inceleme kapsamında ilk önce maddi ceza hukuku bağlamında siber suç tipleri belirlenecek, müteakiben suçla mücadele kapsamında uygulanacak koruma tedbirleri ve usul hükümleri ifade edilecektir.

Son olarak da siber suçların sınır tanımaz yapısı gereği bu suçlarla mücadele açısından ülkeler arası sağlanacak adli yardımlaşma ilkelerinden bahsedilecektir.

Anahtar Kelimeler: *Siber Suç, Adli Yardımlaşma, Sınır Tanımaz, Budapeşte Sözleşmesi.*

COUNCIL OF EUROPE CONVENTION ON CYBERCRIME AND ITS EQUIVALENT IN TURKISH LAW

Abstract

As a result of rapidly developing digital technology and network systems, the internet has become the focal point of cybercrime, like the "Wild West". When the current situation is considered together with the tendency of states not to share their jurisdiction within the scope of their sovereign rights, international judicial cooperation within the scope of combating these crimes becomes a difficult possibility, unless a binding international agreement with a binding international dimension can be achieved in the fight against cybercrime.

Our study has been shaped in the context of the literature review on the subject, the examination of current judicial decisions and the information obtained from international and local legislation reviews. First of all, it is aimed to avoid possible confusion in the continuation of the text by making a conceptual analysis of the term cybercrime, which differs in each state's own social, cultural and economic values. Afterwards, attempts made to combat cybercrime in the national and international arena will be evaluated, apart from the Council of Europe Convention on Cybercrime (Budapest Convention).

Within the scope of the obligations brought by the Convention, its effects on Turkish Law and the compliance of the legislation in Turkey with the aim of combating cybercrime will be examined. Within the scope of this review, firstly, the types of cybercrime in the context of substantive criminal law will be determined, then the protection measures and procedural provicions to be applied within the scope of combating crime will be expressed.

Finally, due to the borderless nature of cybercrimes, the principles of judicial assistance to be provided between countries in terms of fighting these crimes will be mentioned.

Keywords: *Cybercrime, Legal Aid, Borderless, Budapest Convention.*

GİRİŞ

Dijital teknolojinin ve internetin baş döndüren gelişimine paralel olarak bilişim sistemleri üzerinde ve aracılığıyla işlenen, sınır tanımaz niteliğe sahip, siber suç olarak da tanımlayabileceğimiz, suç tiplerinin yoğunluğunda ve işleniş tekniklerinde ortaya çıkan durdurulamaz artış ile birlikte devletlerin ulusal seviyede yaptıkları mücadelenin yetersizliği topyekûn göz önünde bulundurulduğunda, problemin küresel boyutu daha iyi anlaşılmaktadır.

Sunduğu fırsatlar ve kolaylıklar bakımından gündelik ve mesleki hayatın vazgeçilmez bir parçası hâline gelen bilişim teknolojileri, bu alanda gerek gerçekleşen suçların gerek bu suçların faillerinin takip edilememesi noktasında da aynı oranda imkân sağlamaktadır. Ayrıca bu sistemler aracılığı ile işlenen suçlar yoluyla kişiler veya devletler üzerinde meydana gelen önemli maddi zararlar ile suçla mücadelenin yüksek maliyet ve teknik personel gerektirmesi hâlleri, tüm devletler tarafından ilgilenilmesi zaruri ciddi sorunlar olarak karşımızda durmaktadır.

Söz konusu olumsuz koşulların doğal sonucu olarak ortaya çıkan Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi, bu alanda uluslararası boyutta bağlayıcı niteliğe sahip ilk anlaşmadır. Sözleşme'nin; üyeliği Avrupa Konseyi devletlerle sınırlandırmaması, taraf devletler açısından belli yükümlülükler öngörmesi, diğer devletler açısından uluslararası seviyede başvurulabilecek bir referans sunması ve kapsam olarak sadece bilişim sistemleri üzerinde işlenen suçları değil, bilişim sistemleri aracılığıyla işlenen diğer suçlar ve delillerin toplanmasında bilişim sistemlerine ihtiyaç duyulan tüm suçları da içerecek şekilde düzenlenmesi bu alanda küresel nitelikte atılan ilk adım olduğuna açık bir göstergedir. Ancak Sözleşme'nin taraf devletlere sunduğu geniş çekince hakkının olumsuz etkisi sebebiyle bu nitelik, gerçekleşmesi ve sürdürülmesi zor bir hayal olmaktan öteye geçememektedir.

Hülasa çalışmamızın temel amacı; yukarıda kısaca değindiğimiz Sözleşme'nin küresel boyutta getirdiği yükümlülükler açısından Türk Hukuku'ndaki etkileriyle birlikte ülkemizin siber suçlarla yerel ve uluslararası alanda mücadele sürecindeki hâlihazırda bulunduğu durumu tespit etmektir.

1. SİBER SUÇ

"Siber suç" kavramı üzerinde uluslararası kapsamda görüş birliğine varılmış bir tanım bulunmamaktadır. Bu nedenle çalışmamız açısından olması muhtemel anlam

karmaşasına sebebiyet vermemek adına kavramsal bir incelemeyle başlamanın uygun olacağını değerlendiriyoruz.

1.1. Siber Suç Kavramı

Günümüzde, salt teknik ve teknolojik gelişmelerin dahi, toplumların ve ortak değerlerinin üzerindeki muazzam etkileri yadsınamaz bir kabuldür. Özellikle bilişim teknolojileri ve internetin hızlı gelişimi de düşünüldüğünde, gerek uluslararası alanda gerek de Türk doktrininde, "siber suç" kavramı anlamında 'sanal suç, dijital suç, bilgisayar suçu, elektronik suç, ileri teknoloji suçu, telekomünikasyonla ilgili suç, bilgisayarla ilgili suç, bilgisayar yardımlı suç, internetle ilgili suç, çevrim_içi suç ve e-suç' benzeri birçok adlandırmanın (Smith vd., 2004, p. 5) kullanılıyor olması, olağan karşılanacaktır.

Türk doktrininde her ne kadar "bilişim suçu" kavramı egemen olsa da uluslararası alanda genel kullanıma sahip olması ve çalışmamızın inceleme alanını oluşturan 2001 tarihli Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne de paralellik arz etmesi sebebiyle "siber suç" terimini kullanmayı tercih ettik. Ancak öncelikle belirtmekte fayda var ki, Sözleşme'nin Türkiye üzerinde etkileri ile ilgili yapılacak değerlendirmelerde kullanacak olan "bilişim suçu" kavramının, siber suç ile aynı manada anlaşılması gerekmektedir.

1.2. Siber Suçun Tanımı

Türk Dil Kurumu tarafından bilişim terimi; 'İnsanoğlunun teknik, ekonomik ve toplumsal alanlarda iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik' olarak ifade edilmiş, ayrıca bilişim suçu ile ilgili herhangi bir açıklamada bulunulmamıştır (Türk Dil Kurumu [TDK], 2019). Mukayeseli hukuk bakımından ise; Amerika Birleşik Devletleri'nde yaygın olarak kullanılan Black's Law hukuk sözlüğünde bilgisayar suçu terimi ile elektronik olarak depolanan verilerin çalınması ve sabote edilmesi gibi bilgisayar kullanımını gerektiren suçlar (Akpek, 2015, s. 4), Avustralya hukuk sözlüğünde internet suçu terimi ile 'internet, telefon ve kablosuz teknolojiler gibi iletişim teknolojilerinin etkinlik alanında kullanılan veya oluşan suç faaliyetleri' (Mann ve Blunden, 2021), Oxford Hukuk Sözlüğünde ise siber suçlar terimi ile 'internet aracılığı ile işlenen suçlar' (Law ve Martin, 2021) şeklinde tanımlamalara yer verildiği görülmektedir.

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu ise "bilişim suçları" kavramını seçerek 1983 yılında Paris Konferansında yaptığı ve birçok devlet

tarafından referans alınan tanımlamasında; 'bilgileri otomatik işleme tabii tutan veya dataların taşınmasına yarayan bir sisteme karşı veya sistem ile gayri-kanuni, ahlak dışı ve yetkisiz icra edilen her türlü davranış' ifadelerine yer vermiştir (Altunok ve Vural, 2011, s. 75).

Son olarak Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde yapılan tanımlamada; siber suç terimi tercih edilerek bilgisayar veri ve sistemlerinin gizlilik, bütünlük ve erişilebilirliğine yönelik suçları (yasadışı erişim, yasadışı araya girme, verilere müdahale, cihazların kötüye kullanılması); bilgisayarla bağlantılı suçları (sahtecilik, dolandırıcılık); içerikle bağlantılı suçları (çocuk pornografisi ile bağlantılı suçlar); telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçları gerçekleştirmeye yönelik kötü niyetli eylemler, olarak kapsamı belirlenmiştir (Aliusta ve Benzer, 2018, s. 38).

1.3. Siber Suçun Özellikleri

Geleneksel hukuk sistemleri; uyum sağlama konusunda telefon, televizyon, radyo ve arabaların keşfinde gösterdiği başarıyı sanal uzayda ivme kazanarak devam eden bu büyük gelişim sürecinde gösterememektedir. Siber suçlarla mücadelede görevli gerek yargı makamlarının gerek de kolluk kuvvetlerinin yeterli teknik bilgi ve uzmanlığa sahip olmaması gerçeği de, suçun icrası hakkında oluşturulacak şablonlar ile mücadelede kullanılacak gücün planlamasını gösteren suç haritalarının geliştirilmesinde; aşılması personel, zaman ve maliyet gerektiren bir sorun teşkil etmektedir (Önok, 2003, s. 1232).

Ayrıca yukarıda ifade ettiğimiz birçok farklı tanımdan da anlaşılacağı üzere uluslararası veya ulusal alanda yeknesaklığın sağlanamaması ile teknolojinin hızla gelişimiyle eş zamanlı olarak siber suçun yeni görünümlerinin ortaya çıkmasının doğal sonucu olarak devletlerin maddi ceza hukuklarında farklı düzenlemelere gidilebilmektedir. Pek tabii ki bu farklılıkların, adli yardımlaşma özelinde uluslararası alanda suçla mücadeleye olumsuz etkilerinin olacağı, izahtan varestedir (Sınar, 2004, s. 766).

Siber suçları geleneksel suçların dışında tutan en karakteristik ve mücadele kapsamında en büyük zorluk çıkaran özelliği, Wall (2009, p. 105) 'ın 'eski şarap yeni şişede, yeni şarap yeni şişede, yeni şarap şişe yok' deyiminde ifade ettiği üzere kaba sığmayan ve sınır tanımayan yapısıdır. Devletlerin yargı yetkisinin belirlenmesinde genel kural olan mülkilik ilkesi kapsamında az önce ifade ettiğimiz niteliklere sahip bulunan siber suçlarla mücadele, neredeyse imkânsız bir hâl almaktadır. Ayrıca bu durumun diğer bir sonucu olarak şüpheli ile zarar gören

arasında bulunan mekânsal uzaklık, gerek şüphelinin tespiti ve yakalanması gerek de delillerin zarar görmeden muhafaza altına alınmasında, ciddi bir sorun olarak karşımıza çıkmaktadır. Bu sorunların çözümü bağlamında "uluslararası iş birliğinin", tüm devletler açısından kaçınılmaz bir yöntem olarak kabulü gerekmektedir (Akpek, 2015, ss. 6 – 8).

Son olarak, siber suç yoluyla asgari masraf ve emek ile ciddi seviyede zararlara sebebiyet verilebilmesine karşın bu suçlarla mücadele; ciddi ekonomik güç, teknik uzmanlık ve gayret gerektirmektedir. (Önok, 2003, s. 1236).

2. SİBER SUÇLA MÜCADELE KAPSAMINDA YAPILAN GİRİŞİMLER

Yerel düzenlemelerin genel olarak uluslararası sözleşmelerden kaynaklanan yükümlülükler kapsamında ele alındığı kabulü gereği öncelikle uluslararası alanda yapılan girişimler, bilahare ulusal girişimler hakkında kısaca bilgi verilecektir.

2.1. Uluslararası Alanda Yapılan Girişimler

Siber suç ile mücadelede, uluslararası adli iş birliğinin ve bu iş birliğinin tesisi için ulusal seviyede dünya devletlerinin mevzuat bağlamında uyumlarının gerekliliğinden önceki bölümlerde kısaca bahsetmiştik. Bu kapsamda her ne kadar bağlayıcı olmasa da uluslararası alanda referans bir ölçüt sunması açısından Ekonomik Kalkınma ve İşbirliği Örgütü (OECD)'nün çalışmaları, belirttiğimiz uyumlaştırma alanında ilk olması hasebiyle önem arz etmektedir. İlgili Örgüt'ün 1983 yılından itibaren süregelen çalışmaları neticesinde 1992 yılında bilgi sistemleri güvenliği için standart ve prensipleri belirleme amacıyla aldığı tavsiye kararının, 1997 ve 2002 yıllarında tekrar gözden geçirilmesi sonrası 2002 yılında OECD Konseyi tarafından kabul edilen "Bilgi Sistemleri ve Ağlarının Güvenliği İçin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru" tavsiyesi kararı, siber suçla mücadele kapsamında ihtiyaçları karşılayacak yeni bir çerçeve sunmaktadır (Önok, 2003, s. 1240).

OECD'den farklı olarak bağlayıcı karar alabilme yetkisine ve kapsam olarak da uluslararası alanda en büyük örgüt özelliğine sahip olan Birleşmiş Milletler de 1980'li yılların ortalarından itibaren aldığı tavsiye kararlar ile siber suçlarla mücadele amacıyla ülkelerin maddi ceza hukukları, usul hukuklarının uyumlaştırılması ve adli işbirliğinin sağlanması alanlarında katkı sağlamaya çalışmıştır (Aliusta ve Benzer, 2018, s. 37). 2005 yılı sonrasında ise tavsiye kararlardan ziyade ülkelere teknik destek ve yardım sağlanmasının mücadele

açısından daha faydalı olacağı değerlendirmesi sebebiyle çalışmalarını bu doğrultuda devam ettirmiştir (Favanski, 2009, p. 230).

Dünyanın en büyük 8 ekonomisini oluşturan devletlerin bir araya gelmesi ile oluşan G-8, 1997 yılında oluşturduğu "Yüksek Teknolojili Suçlara Dair Alt Komite" ile aldığı ilke kararları ve 10 prensipten oluşan eylem planı doğrultusunda siber suçla mücadele çalışmalarına başlamıştır (Rusya'nın 1998 yılında üye olması sebebiyle Komite'nin kurulduğu dönemde Örgütün adı G – 7 idi). G – 8 tarafından ortaya çıkarılan ve uluslararası adli iş birliği bağlamında ana kaynak oluşturan "Contact Points Network" düşüncesine, çalışmamızın ana konusunu teşkil eden Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 35'inci maddesi ile de atıf yapılmıştır. Ancak Sözleşme hakkında açıklama yapılacak kısımda konuya ilişkin ayrıntılı incelemede bulunulacağından, bu kısımda sadece mevcudiyetinden bahsedilmesiyle yetinilecektir. G-8, devam eden süreçte de siber suçla mücadele amacıyla faillerin kullanabileceği kurtarılmış bölgelerin engellenmesi, mücadelede kullanılabilecek usul hükümleri, internetin suç işlenmesinde -özellikle terörist faaliyetlerde- kullanılmasını önleme amaçlı alınması gereken tedbirler kapsamında çalışmalarını devam ettirmektedir (Gercke, 2014, pp. 123 – 124).

Avrupa Birliği özelinde ise Konsey tarafından 2005 yılında kabul edilen "Bilişim Sistemleri Aleyhinde Saldırılara Dair Avrupa Birliği Çerçeve Kararı" önem taşımakta, bunun dışında ana konumuz ile paralellik gösteren 2009 tarihli "Lizbon Antlaşması" ile de AB, siber suç ve cezası ile ilgili tanımlamalarda en alt standardı sağlayacak şekilde devletlerin maddi ve usul ceza hükümlerinin uyumlaştırılması görevini üstlenmiş bulunmaktadır (Gercke, 2014, pp. 128 – 129). Siber suçla mücadele amacıyla EUROPOL bünyesinde "İleri Teknoloji Suçlar Merkezi" ile Avrupa Komisyonu, Eurojust ve AB'ye üye devletlerin ilgili suçla mücadele birimlerinin amirlerinden meydana gelen "Avrupa Siber Suç Timi" adıyla iki yapı kurulmuştur. Bu yapıların oluşturulmasındaki genel gaye, sınır tanımayan yapısı gereği siber suçla mücadele de zaruri bir gereklilik arz eden ülkeler arası iş birliğini sağlamak ve hızla gelişen teknolojinin sebep olacağı aksaklıkları gidermektir (AB'ye üye ülkeler kapsamında) (Aliusta ve Benzer, 2018, s. 37).

Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ile ilgili çalışmamızın devamında detaylı incelemede bulunulacağından, bu kısımda sadece Sözleşme'nin Avrupa genelinde siber suçla mücadele konusunda uluslararası boyutta bağlayıcı etkiye sahip ilk sözleşme olması niteliğine vurgu yapılması yeterli görülmüştür (Kutlu vd., 2019, s. 4).

2.2. Yerel Girişimler

Dünya genelinde İnternet'in ilk kullanımına (Dülger, 2020, s. 91)[1], (Ergüney, 2020, s. 99)[2] paralel olarak bilgisayar sistemleri ile ilgili ilk düzenleme 1977 yılında ABD'de hazırlanan "Federal Bilgisayar Sistemlerinin Korunması" kanun taslağı ile ortaya çıkmıştır. Siber suçlar özelinde düzenlemeler ise 1970 ve 1980'li yıllarda bilgisayarın araç olarak kullanıldığı ekonomik suçlar ile bilgisayarda bilgilerin depolanması ve iletilmesi konularıyla kısıtlı kalmıştır. Yine bu dönemde bilgisayar teknolojilerinin gelişimi ile meydana çıkan fikri mülkiyet hakları kapsamında güvence sağlayacak düzenlemeler oluşturulmuştur.

1990'ların ortalarına kadar devam eden süreçte ise internet üzerinden hakaret, tehdit, pornografi, çocuk pornografisi ve nefret suçlarına sebebiyet veren illegal içeriklerin engellenmesine ilişkin tedbirlere ağırlık verilmiştir (Sieber, 1998, pp. 28-30). ABD'de 1996 Şubat'ında yürürlüğe giren "İletişim Ahlak Yasası" ile 1934 tarihli "Telekomünikasyon Yasası'na eklenen yeni maddelere göre İnternet aracılığı ile pornografik ve şiddet içeren yayınların yasaklanması ve ihlale neden olan kişiler için de 2 yıla kadar hapis cezası ile 250.000 dolara kadar adli para cezası öngörülmüştür. Her ne kadar bu hüküm; yaklaşık bir yıl sonra Yüksek Mahkemenin 'Demokratik bir toplumda serbest toplumsal fikir alışverişinin

[1] *'İkinci Dünya Savaşı sonrası süreçte Sovyetler Birliği'nin 1957 yılında Sputnik isimli uzay aracını yörüngeye göndermesi sonucunda ABD, karşısında ne boyutta bir teknolojik güce sahip bir devlet olduğunun farkına vardı. Bu farkındalık sonrasında olgunlaşan, 'thinking – tank' olarak da bilinen RAND Corporotion isimli bir Amerikan kuruluşunun, sosyal karışıklıklar veya olması muhtemel bir nükleer savaş sonrası gerek yönetim kademesinin gerek de askerî birliklerin silah imalatçılarıyla kesintisiz ve emniyetli bir şekilde iletişim kurmasını sağlamak amacıyla tek bir merkez servis sağlayıcıdan ziyade tüm bilgisayarların birbirleriyle iletişim kurabileceği ağ sistemlerinin kurulması fikriyle, internetin ortaya çıkış süreci başlamıştır'*

[2] *Tarihte Ekim Füzeleri Bunalımı olarak bilinen ABD'nin Türkiye'ye nükleer başlıklı füze yerleştirmesine misilleme olarak SSCB'nin Küba'da nükleer başlıklarını konuşlandırması hadisesi üzerine ABD, iletişim ağı üzerindeki çalışmalarını yoğunlaştırmaya başladı (Erümit, 2022, s. 7). Bu kapsamda ilk etapta ABD'nin üniversite ve laboratuvarlarında başlanan İnternet üzerindeki çalışmalar; 1970'li yıllarda ARPANET (Advanced Research Projects Agency of the Department of Defence) bilgisayar ağının kurulması ile sonuçlanmıştır. Kurulan bu ağ sayesinde elektronik posta ve ağ haberleri benzeri hizmetler olumlu yönde gelişme göstermiştir. Bilahare, 1980 yılında askerî amaçla MILNET'in (Military Network) kurulmasıyla birlikte ARPANET, tamamen sivil alanın kontrolüne bırakılmıştır. Devam eden süreçte internet ağlarının, İngiltere ve Japonya'da kurulması ile özel sektör ve kamu yönetimi alanında yaygınlaşması neticesinde, 1993 yılında World Wide Web(www) temelinde ağlar kurulmuştur'*

sağlayacağı toplumsal yarar, internette sansürün sağlayacağı toplumsal yararla karşılaştırılamayacak kadar çok daha önemlidir' gerekçesi ile anayasaya aykırı bulunarak iptal edilmiş olsa da gelecekte yapılacak düzenlemeler ile ilgili ifade özgürlüğü kapsamında göz önünde bulundurulması gereken kriterleri göstermesi açısından önem arz etmektedir (Ergüney, 2020, s. 100).

Nihayetinde tüm devletler kendi güvenlikleri ve iç hukukları kapsamında yaptıkları düzenlemeler ile kendi bağlamında siber suçlarla mücadele etmeye çalışmıştır (Sieber, 1998, p. 31).

3. AVRUPA KONSEYİ SANAL ORTAMDA İŞLENEN SUÇLAR SÖZLEŞMESİ

Genel olarak Budapeşte Sözleşmesi olarak bilinen Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi; 4 ana bölüm ile bu bölümleri oluşturan 48 madde ve sonrasında dâhil edilen Ek Protokol'den müteşekkildir. Sözleşme; Avrupa siber suç politikasının modern suç politikasına uygun olarak temel ilkelerini belirlemek, geleceğe ilişkin taşıdığı nitelik, düzenlenen siber suç tiplerinin münhasıran kasten icra edilebileceğinin ön plana çıkarılması ve mezkûr suç tipleri açısından hukuka aykırılık unsurunun ortaya konması olacak şekilde dört temel ilke doğrultusunda düzenlenmiştir (Dülger, 2020, s. 201). Çalışmamızın bu bölümünde öncelikle Sözleşme hakkında genel bilgilere yer verilecek, sonrasında ise karşılaştırmalı olarak fayda ve eksiklikleri ifade edilecektir.

3.1. Sözleşme'nin Kuruluş Süreci ve Amacı

Avrupa Suç Sorunları Komitesi (European Committee on Crime Problems)'nin özetle 'bilgi teknolojilerinin hızlı gelişimi sonucu telekomünikasyon sistemleri ile sağladığı bütünleşme ve internetin ortaya çıkışı neticesinde 'siber uzay' adı ile kurulan sistemde; herkes tarafından, mesafeden bağımsız olarak, istediği her yerde bilgisayar sistemlerinin ve telekomünikasyon ağlarının bütünlüğüne, erişilebilirliğine ve gizliliğine karşı suç işlenebileceği gibi bilgisayar sistemleri aracılığı ile de her ülkenin kendi iç mevzuatında düzenleme altına aldığı diğer suçlarında işlenebileceği, suçun sınır tanımaz özelliğinin devletlerin mülkilik ilkesi kapsamında çelişkili durumlara neden olduğu, siber suçla mücadele kapsamında ulusal kavramların uyumlaştırılması ve uluslararası düzeyde ortak çalışmanın mecburiyeti vurgulanarak bu konuları içeren bağlayıcı uluslararası araçların geliştirilmesi gerektiği' gerekçesi (İçel, 2001, s. 5) ile 1996 yılında Avrupa Konseyi'ne siber suçlarla mücadele hakkında çalışma yapmak üzere bir uzman

komite kurulmasına yönelik sunulan tavsiye kararı, Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'ne giden sürecin ilk adımını oluşturmaktadır.

Avrupa Konseyi Bakanlar Kurulu; yaklaşık bir yıl sonra öneriye uygun olarak "Siber-Uzay Suçları Uzman Komitesi"ni kurmuştur. Bu Komite tarafından, öngörülen bitirme zamanı olan 31 Aralık 2000 tarihini de aşan yaklaşık dört yıllık bir çalışma neticesinde siber suçlara karşı mücadele hakkında hazırlanan Sözleşme taslağı, Haziran 2001'de gönderildiği Avrupa Suç Sorunları Komitesinin genel kurulunca onaylanmış, müteakiben de Avrupa Konseyi Bakanlar Komitesine sunularak 8 Kasım 2001 tarihinde kabul kararı alınmıştır (Özbek, 2015, s. 77). Bilahare Sözleşme, 23 Kasım 2001 tarihinde Macaristan'ın başkenti Budapeşte'de tüm devletlere imzaya açılmıştır. Yürürlüğe girişi ise 01.07.2004 tarihinde olmuştur. İlk imzalandığı yer olması sebebiyle "Budapeşte Sözleşmesi" olarak da bilinen Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi; Avrupa Konseyi'ne üyelik şartı öngörmemesi sebebiyle 21'i üyesi olmayan toplam 68 devlet tarafından imzalanmış, imzalayan 65 devlet tarafından da hukuki süreç başlatılmıştır (Counsil of Europe, 2020).

Sözleşme'nin kabul edilme sürecinde ifade özgürlüğünün engellenmesi açısından bazı devletler tarafından ileri sürülen eleştiriler sebebiyle üstünde uzlaşıya varılamayan bilgisayar sistemleri aracılığı ile işlenen ırkçı ve yabancı düşmanlığı içerikli suçların cezalandırılmasına yönelik "Bilişim Sistemleri Aracılığı ile İşlenen Irkçı ve Yabancı Düşmanı Eylemleri Suç Hâline Getirilmesi için Avrupa Siber Suç Sözleşmesine Ek Protokol" ise 28.01.2003 tarihinde Strazburg'da kabul edilerek 01.03.2006 tarihinde yürürlüğe girmiştir (Gercke, 2014, p. 417).

Sözleşmenin oluşturulma sürecinden de anlaşılacağı şekilde ana amacını kısaca ifade edecek olursak; sözleşmeye taraf olan devletlere yükümlülükler getirmek ve taraf olmayan devletlere referans noktası olmak yoluyla genel olarak adli yardım ve iş birliğini geliştirmek adına siber suçlarla ilgili iç hukuk düzenlemelerinde asgari seviyede uyum sağlamak ile siber suçların ve elektronik delillerin toplanmasını gerektiren diğer suçların muhakeme usullerinde uygulama birliğini sağlamaktır, diyebiliriz (Özbek, 2015, s. 77).

3.2. Sözleşme'nin Fayda ve Mahzurları

Sözleşme, siber suçla mücadele kapsamında farklı siyasal, kültürel, ekonomik ve sosyal yapılara sahip devletleri sınırlı da olsa uzlaşabilecekleri ortak noktalarda birleştirmeyi hedeflese de sağladığı kolay çekince koyma hakkı, hedefin nihayete

ulaşmasının önünde ciddi bir engel teşkil etmektedir (Aliusta ve Benzer, 2018, s. 38). Özelikle Rusya, Çin, Hindistan, Brezilya gibi siber suçların yoğun olarak işlendiği ülkelerin Sözleşme'ye taraf olmaması hâli ile birlikte değerlendirildiğinde küresellik iddiası uzak bir hayal olmaktan öteye gidememektedir. Tabii onay ve taraf olma süreçlerinin de uzun zaman alması sebebiyle Sözleşme'nin uluslararası etkinliği olumsuz yönde etkilenmektedir (Gercke, 2014, p. 417). Örnek olması açısından Türkiye bağlamında bu süreç, 2010 yılında imzalanması sonrası 2014 yılında gerçekleşen Cumhurbaşkanı onayı ile aşağı yukarı 4 yıl devam etmiştir.

Taraf devletlere Sözleşme'nin 25'inci maddesinde düzenlenen karşılıklı yardımlaşmaya ilişkin genel ilkeler kapsamında birbirlerine karşı en geniş ölçüde yardım etme yükümlülüğü getirilmiştir. Bu bağlamda 7/24 çalışma düzeninde kurulan irtibat noktaları aracılığı ile bilgisayar sistemlerine karşı veya diğer suçlarla ilgili elektronik delillerin toplanmasında sadece çok acele ve istisnai durumlarda kolaylık sağlamış olsa da Sözleşme'nin uygulanabilirliği açısından önem teşkil etmektedir (Akpek, 2018, s. 27). Ancak talebe konu olayın karşılıklı iki devlet açısından da suç sayılması olarak ifade edebileceğimiz "çifte suçluluk" ilkesi açısından düzenleme, olumsuz tepkilere maruz kalmıştır.

Diğer bir kritik konu ise özellikle Rusya tarafından devletlerin egemenlik haklarının ihlaline sebep olacağı gerekçesi ile karşı çıkılan Sözleşme'nin 32/b maddesi gereği bilgisayar verilerinin açıklanması hususunda yetkili kişinin "yasal ve gönüllü rızası" olması hâlinde taraf devletlerin birbirlerine bilgi vermeden ilgili verilere ulaşabilme ve bu verileri temin edebilme haklarına ilişkin hükümdür (Markoff ve Kramer, 2019).

Ayrıca taraf devletlerin Sözleşme'nin kabul sürecinde eşit ve yeterli şekilde temsil edilmemiş olması da vurgulanması geren önemli diğer bir eksikliktir. Ancak yine de ortaya koyduğu şablon bakımından küresel anlamda devletlerin iç hukuklarında etkili olacak şekilde bir standart oluşturduğu, güncel örnekler ışığında, yadsınamaz bir gerçektir (Önok, 2003, s. 1235).

Son olarak, Sözleşme'nin bireylerin temel hak ve özgürlüklerini sınırlandıracak boyutta devletlere yetki veren otoriter bir yapıda olduğu iddiasında olan birçok düşünür tarafından, hâlihazırdaki şekliyle imzalanmaması gerektiğinin ileri sürüldüğünü ifade edebiliriz (Dülgen, 2020, s. 203).

3.3. Sözleşme Hakkında Genel Bilgiler

Sözleşme 4 ana kısım ve sonradan ilave edilen Ek Protokolden ibarettir.

İlk bölümde siber suçlar ve bilişim teknolojileri ile ilgili terimler ifade edilmiştir. İkinci bölümde ülkeler arası mevzuat uyumunun sağlanması amacıyla ulusal düzeyde alınacak önlemler düzenlenmiştir. Bu kapsamda öncelikle maddi ceza hukuku alanında bilgisayar sistemlerine yönelik ve bu sistemler aracılığı ile işlenen suç tipleri tanımlanmış, devamında da ceza muhakemesi alanında bazı usule ilişkin yetkilere yer verilmiş, ayrıca yargı yetkisi hususu ile ilgili birtakım genel ilkeler ortaya konulmuştur. Üçüncü bölümde bir önceki bölümde düzenlenen yetkilerin kullanımı açısından uluslararası adli yardımlaşmanın sınırları belirlenmiş, son bölümde ise Sözleşme'nin uygulamasına yönelik bazı usul ve teknik düzenlemelere yer verilmiştir (Aliusta ve Benzer, 2018, s. 38).

Çalışmamızın devamında Sözleşme'nin siber suçların önlenmesi kapsamında Türkiye'nin konuya ilişkin düzenlemelerine etkisi incelenecek, müteakiben bu düzenlemelerin Sözleşme ile belirlenen yükümlülükleri karşılama durumu ele alınacaktır.

4. SÖZLEŞME'NİN SİBER SUÇLAR BAĞLAMINDA TÜRK HUKUKU'NA ETKİLERİ

Siber suçlar açısından Türk Ceza Mevzuatı'nda ilk düzenleme; 765 Sayılı Türk Ceza Kanunu'nun (TCK) 1991 yılında 3765 Sayılı Kanun ile "Bilişim Alanındaki Suçlar" başlığı altına eklenen suç tipleri ile olmuştur. Belirlenen suç tiplerinin temeli ise öncesinde siber suç tiplerinin mal varlığına karşı suçlar kapsamında düzenlendiği 01.03.1994 tarihli Yeni Fransız Ceza Kanunu'nun (YFCK) da "verileri otomatik olarak işleme tabi tutan sistemlere yönelik saldırılar" başlığı altında 7 farklı siber suça esas teşkil eden 05.01.1988 tarihli 88 – 19 Sayılı Yasa'dır (Yazıcıoğlu, 2005, s. 394).

765 Sayılı TCK'nın 525/a, b, c, d fıkralarında bilgisayar sistemlerinde verileri ele geçirme; bu verileri üçüncü kişilere zarar vermek amacıyla kullanma, nakletme veya çoğaltma; bilgisayar sitemlerine, sisteme kayıtlı verilere veya diğer unsurlara kısmen veya tamamen zarar verme, değiştirme, silme, işlemesini engelleme, yanlış işlemesine neden olma, sistem aracılığı ile kendine veya başkasına yarar sağlama; delil niteliğinde sahte belge oluşturmak maksadıyla bilgisayar sistemlerine veri yerleştirme, var olan verilere zarar verme, zarar verilmiş verileri bilerek kullanma suçları ve bazı ek yaptırımlar düzenlenmiştir.

Devam eden süreçte yürütülen TCK Kanun Tasarı çalışmaları neticesinde oluşturulan 26.09.2004 tarih ve 5237 Sayılı Yeni TCK ile siber suçlar son şeklini almıştır. Belirtmek gerekir ki Yasa'ya esas teşkil eden Tasarı çalışmalarının siber

suçlar ile ilgili hükümleri, yukarıda ifade ettiğimiz YFCK'de yer alan ilgili suç çeşitlerinden esinlenilerek hazırlanmıştır.

Fransa'nın Sözleşme'yi 2001 yılında onayladığı ve 2006 yılında imzaladığı bilgisi kapsamında nihai bir değerlendirme yapacak olursak görüleceği üzere Fransa'nın Sözleşme'ye daha taraf olmadan neredeyse siber suçlarla mücadeleye ilişkin tüm düzenlemelere sahip olduğu, 765 Sayılı TCK'nin ve siber suçlar kapsamında yapılan yasa değişikliklerinin yürürlük tarihlerinin 23.10.2001 tarihinde Macaristan'ın başkenti Budapeşte'de imzaya açılan Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi ile kıyaslandığında etkisi olmasının fiilen mümkün olmadığı, 5237 Sayılı Yeni TCK'nin siber suçlar ile ilgili hükümlerinin esin kaynağının Sözleşme öncesi yürürlüğe giren Fransız mevzuatı olması sebebiyle de Sözleşme'nin Türkiye'nin siber suçlarla ilgili iç hukuk düzenlemeleri kapsamında etkisinin olduğunu söylemenin mümkün olmadığını ifade edebiliriz.

Ayrıca siber suçların yoğun olarak düzenlendiği 5237 Sayılı TCK, bazı usule ilişkin yetki ilkelerinin düzenlendiği 5271 Sayılı Ceza Muhakemesi Kanunu ve 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nun hazırlanma süreçleri ve gerekçelerinde Sözleşme'ye atıfta dahi bulunulmamıştır (Akpek, 2015, s. 54). Elektronik imzaya ilişkin araçların ve hizmet sağlayıcılarının düzenlendiği, 15.01.2004 tarihinde TBMM'ce kabul edilerek geçici madde gereği 15.07.2004 tarihinde yürürlüğe giren (Demirdöğen, 2019, s. 33) 5070 Sayılı Elektronik İmza Kanunu'nun[3] yasalaşma sürecinde de 13 Aralık 1999 tarihli Avrupa Parlamentosu ve Konseyi Elektronik İmza Direktifi (Directive 1999/93/EC of the European Parliament and of the Council), BM'nin 14 Haziran 1996 tarihli Elektronik Ticarete İlişkin Model Kanunu, Amerika Birleşik Devletleri, Fransa gibi ülkelerin aynı konuya ilişkin düzenlemelerine atıfta bulunulmasına rağmen Sözleşme'den bahsedilmemiştir (Türkiye Büyük Milet Meclisi [TBMM], 2021). Benzer şekilde 2010 yılında Anayasa'nın 20. maddesinde yapılan değişiklik gereği[4] ve polis birimleri arasında etkin bir iş birliğini sağlayan EUROPOL ile stratejik iş birliğinin ötesinde operasyonel iş birliği anlaşmasının imzalanabilmesi amacıyla 24.03.2016

[3] 'E-devlet' uygulamasının temel unsurunu oluşturan ve ilerleyen süreçte elektronik ticarete yönelik yapılacak düzenlemelere yol açacak niteliğe sahip elektronik imza uygulaması ve siber suçlar bakımından 16'ncı maddesiyle 'imza oluşturma suçlarının verilerinin izinsiz kullanımı' ile 17'nci maddesiyle 'elektronik sertifikalarda sahtekârlık' suçu bu Kanun kapsamında düzenlenmiştir.

[4] Kişisel verilen korunması hakkının temel insan hak ve özgürlükler arasında kabul edilmesinden dolayı ne şekilde güvence altına alınacağına ilişkin detayların kanun yoluyla düzenleneceği öngörülmüştür.

tarihinde kabul edilen, 07.04.2016 tarihinde yürürlüğe giren 6698 Sayılı Kişisel Verilerin Korunması Kanunu bakımından atıf yapılan birçok uluslararası belge[5] arasında Sözleşme bulunmamaktadır (Türkiye Büyük Milet Meclisi [TBMM], 2021). Bu kanunların dışında 5187 Sayılı Basın Kanunu, 5411 Sayılı Bankacılık Kanunu, 5809 Sayılı Elektronik Haberleşme Kanunu gibi birçok düzenlemede siber suçlara yer verilmiş olmasına (Demirdöğen, 2019, s. 34) rağmen kanunlaşma süreçlerinde Sözleşme dikkate alınmamıştır. Sadece idari nitelikte tedbirlerin düzenlendiği 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a temel teşkil eden Adalet Komisyonu raporunda bahsedildiğini, yine aynı Kanun'un 4'üncü maddesindeki içerik sağlayıcının sorumluluğu ve 5'inci maddesindeki yer sağlayıcının yükümlülüklerine ilişkin hükümlerin oluşturulması aşamasında Sözleşme maddelerinin göz önünde bulundurulduğunu ifade edebiliriz (Akpek, 2015, s. 54).

5. SÖZLEŞMESİ'NİN İÇ HUKUK BAĞLAMINDA İNCELENMESİ

Avrupa Konseyi'nin kurucu üyeleri arasında yer alan Türkiye; Sözleşme'yi 10.11.2010 tarihinde imzalamıştır. 22.04.2014 tarih ve 6533 Sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun ile Meclis'te bulunan tüm partiler tarafından mutabakata varılarak kabul edilmesine müteakip 02.05.2014 tarihinde Cumhurbaşkanı'nın onayı ile de iç hukukta geçerli hâle getirilmiştir (Özbek, 2015, s. 77).

6533 Sayılı Kanun; TBMM tarafından Sözleşme'ye konulan 3 çekince ve 5 beyan koşulu ile 3 maddeden oluşacak şekilde kabul edilmiştir. Genel olarak bu çekince ve beyanlardan bahsedecek olursak, yasadışı erişim suçunun güvenlik tedbirlerinin ihlal edilmesi şartı ile işlenebileceği; bilgisayarla bağlantılı sahteciliğe ilişkin suç tipinin Türk Kanunlarına göre dolandırma ve benzeri hileli davranış kastını da içermesi gerektiği; hizmet sağlayıcılara yükümlülük getirilmesi kapsamında suça konu bilgisayar sisteminin halka açık veya özel nitelikli başka bir bilgisayar sistemine bağlı olmaması hâlinde trafik bilgilerinin gerçek zamanlı toplanması ve içerikle ilgili bilgilere müdahale edilmesi tedbirlerini uygulamama

[5] OECD tarafından kabul edilen 23.09.1980 tarihli *'Kişisel Alanın ve Sınır Aşan Kişisel Bilgi Trafiğinin Korunmasına İlişkin Rehber İlkeler'*; Avrupa Konseyi tarafından kabul edilen 108 sayılı *'Kişisel Verilerin Otomatik İşleme Tabii Tutulması Karşısında Bireylerin Korunması Sözleşmesi'*; Avrupa Birliği tarafından 24.10.1995 tarihinde kabul edilen 95/46/EC sayılı *'Kişisel Verilerin İşlenmesi Sırasında Gerçek Kişilerin Korunması ve Serbest Veri Trafiği Direktifi'*.

hakkının saklı olduğu, şahsilik ilkesi bağlamında Türk vatandaşlarının yurt dışında işledikleri suçlardan dolayı yargı yetkisinin kendisine ait olduğu, çifte suçluluk şartının sağlanamıyor olması hâlinde verilerin korunması talebinin reddi hakkının bulunduğu, suçluların iadesi ve geçici tutuklama talepleri ile karşılıklı yardım konusunda koordinenin sağlanması bağlamında Adalet Bakanlığı'nın yetkili kılındığı, 7/24 esasına göre Sözleşme kapsamında görev yapacak irtibat noktasının Emniyet Genel Müdürlüğü Bilişim Suçlarıyla Mücadele Daire Başkanlığı olduğu, şeklinde ifade edebiliriz. Yine kabul sürecinde Komisyonlar tarafından düzenlenen raporlarda Sözleşme'ye taraf olmak için üyelik şartının olmadığı vurgulanarak Sözleşme, küresel bağlamda geçerli bir referans belgesi olarak nitelendirilmiştir (Türkiye Büyük Millet Meclisi, [TBMM], 2013).

5.1. Maddi Ceza Hukuku Bağlamında Düzenlemeler

Bilişim alanında meydana gelen hızlı gelişime paralel olarak ortaya çıkan yeni terimler ile ilgili Sözleşme'nin ilk kısmı bağlamında getirilen tanımların, yüklenen anlam bakımından, iç hukukumuzda karşılık gelen kavramlar ile tutarlılık içinde olduğu görülmektedir (Yazıcıoğlu, 2005, s. 404). Mesela Sözleşme kapsamında "bilgisayar sistemi" terimi, verileri otomatik olarak işleyerek çalışan bir cihaz veya birbiri ile bağlantılı cihazlar olarak ifade edilirken; iç hukukumuz kapsamında seçilen "bilişim sistemi" terimi ise veri işleme özelliğine sahip tüm cihazlar şeklinde birbirini karşılayacak içerikte tanımlanmıştır. Sözleşme'nin de hâlihazırda kendi getirdiği terimlerin üye devletler tarafından tıpatıp kopyalanması gibi bir yükümlülük getirmediğini, ifade edebiliriz (Akpek, 2015, s. 57).

Sözleşmenin ikinci bölümünde "Bilgisayar veri ve sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar" başlığı altında bulunan suç tiplerinin karşılığı olarak 5237 Sayılı TCK'nın 243'üncü maddesinde "bilişim sistemlerine girme", 244'üncü maddesinde "sistemi engelleme, bozma, verileri yok etme veya değiştirme", 245/A maddesinde "yasak cihaz ve programların kullanılması" suç tipleri düzenlenmiştir. 5237 Sayılı Kanun'un 243'üncü maddesindeki suçun ilk hâlinde Sözleşme'den farklı olarak suç teşkil eden fiilin tipikliği oluşturabilmesi için sadece sisteme girme değil, orada kalmaya devam edilmesi de aranmaktaydı. 24.03.2016 tarih ve 6698 Sayılı Kanun'un 30'uncu maddesinin getirdiği değişiklik ile "ve" ifadesi "veya" olarak değiştirilerek Sözleşme ile uyum sağlanmış oldu. Yani suçun kanuni tanımındaki tipikliğin oluşabilmesi için sadece sisteme girilmesi yeterli olacaktır. Yine Sözleşme'nin 3'üncü maddesinde bulunan "yasadışı müdahale" suçunun 5237 Sayılı Kanun'un 243'üncü maddesinin ilk hâlinde olmadığını, aynı Kanun değişikliği ile maddenin

4'üncü fıkrasında sisteme girmeksizin teknik araçlarla veri transferinin izlenilmesi şeklinde düzenlendiğini, ifade edebiliriz (Aliusta ve Benzer, 2018, s. 39).

Sözleşme'nin 6'ncı maddesinde düzenleme altına alınan "cihazların kötüye kullanılması" suç tipinde bilgisayar sistemlerine karşı veya bu sistemler aracılığı ile işlenecek suçlarda kullanılmak üzere bir cihazın üretimi, ithali, sevki, nakli, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması yasaklanmıştır. Hazırlık hareketlerinin cezalandırılmaması ilkesi kapsamında 5237 Sayılı Kanun'un ilk hâlinde bulunmayan bu düzenleme yine mezkûr Kanun değişikliği bağlamında ilgili yasanın 245/A maddesi ile mevzuata dâhil edilmiştir. Ayrıca sahte banka veya kredi kartının cihaz olarak kabulü hâlinde 5237 Sayılı Kanun'un 245/2'nci maddesinin sınırlı da olsa Sözleşme'nin 6'ncı maddesine karşılık gelebileceği söylenebilir.

Sözleşme'nin ikinci başlığı altında düzenlenen "bilgisayarlarla ilişkili sahtecilik ve dolandırıcılık" suçlarına karşılık olarak ise Türk Hukuku'nda 5237 Sayılı Kanun'un verilere müdahaleye ilişkin 244'üncü maddesi, bilişim sistemleri aracılığı ile gerçekleştirilen dolandırıcılığa ilişkin 158/1 – f maddesi ile belgede sahteciliğe ilişkin 204 – 212 maddeleri arasındaki hükümler sayılabilir (Özbek, 2015, ss. 81 – 82). Yine aynı Kanun'un 142/2 – e maddesinde düzenlenen hırsızlık suçunun nitelikli hâli olarak bilgisayar sistemleri aracılığı ile işlenmesi durumunu da bu kapsamda belirtebiliriz. Bu suç tipi kapsamında "verinin" hırsızlık suçunun konusu olup olamayacağı hususundaki tartışmaya açıklık getirmenin faydalı olacağını değerlendiriyoruz. Genel kanı olarak hırsızlık suçuna konu olabilecek verinin temsil ettiği parasal özelliği gereği taşınır bir mal olmasının kabulü gerekmektedir[6]. Bu bağlamda bilgisayar programları vasıtası ile hesap numaralarının ve şifrelerin ele geçirilerek kendisine veya başkasına para transferi yapılması, kişilerin internet bankacılığına girilerek para transferi yapılması gibi suçlarla ilgili Yargıtay tarafından verilen kararlarda bilişim sistemlerinin araç olarak kullanılması yoluyla hırsızlık yapıldığı yönünde değerlendirmede bulunulmaktadır (Akpek, 2015, ss. 80 – 81). Dijital paralardan farklı bir niteliğe sahip olan bitcoin ve türevleri gibi kripto varlıklar hakkında ise merkezi para ve bankacılık sistemlerine bağlı olmaması ve devlet kontrolünde bulunmaması noktasında 6413 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamında bir menkul

[6] Yargıtay Ceza Genel Kurulu, 17.11.2009, E. 2009/11, K. 2009/268.

kıymet olarak kabullerine imkân olmadığı için bu varlıklara yönelik bilişim sistemleri yoluyla yapılacak bir müdahale neticesinde haksız bir menfaat elde edilmesi hâlinde TCK madde 244/4 hükümlerinin söz konusu olacağını ifade edebiliriz (Geçmez, 2020, s. 146). Bunun dışında Knight Online, LoL, Metin 2 gibi sanal oyun karakterlerinin ciddi bir ekonomik değer teşkil etmelerine rağmen 6413 Sayılı Kanun kapsamında menkul bir kıymet olarak kabullerine imkân olmadığı için bu verilere ilişkin TCK madde 244/1 veya 2 kapsamında yapılacak bir müdahaleyle bağlantılı olarak bir menfaat sağlanması hâlinde TCK madde 142/2 – e değil, TCK madde 244/4 hükümleri uygulama alanı bulacaktır[7].

İçeriğe bağlı suçlar kapsamında Sözleşme'nin 9'uncu maddesi ile düzenleme altına alınan bilgisayar sistemleri aracılığı ile çocuk pornografisiyle ilgili verileri üretmek, kullanıma sunmak, erişim sağlamak, dağıtmak, yaymak veya kendisi ya da üçüncü kişiler için temin etmek suçuna karşılık olarak 5237 Sayılı Kanun'un 226'ncı maddesinde tanımlanan "Müstehcenlik" suçu gösterilebilir. Sözleşme'de suç olarak düzenlenmesine rağmen iç hukukumuz bağlamında çocuk pornografisi ile ilgili verilerin depolanmaksızın sadece kasten erişim sağlanması hâlinin suç kapsamına alınmamasının önemli bir eksiklik olduğu vurgulanmalıdır. Sözleşme'nin kapsamını genişletecek şekilde her türlü ırkçı ve yabancı düşmanlık içerikli bilgilerin bilgisayar sistemleri aracılığı ile yayımlanmasına ilişkin 2003 yılında dâhil edilen ve 01.03.2006 tarihinde yürürlüğe giren Ek Protokol'ün de Türkiye tarafından 19.04.2016 tarihinde imzalanmasına rağmen çalışmamızı yaptığımız an itibari ile hâlen daha onaylanmadığını belirtelim (Aliusta ve Benzer, 2018, s. 39).

Nihai olarak Sözleşme'nin 4'üncü başlığında fikri mülkiyet haklarının ihlali ve uluslararası düzeyde dağıtımı düzenleme altına alınmıştır. Türk Hukukumuzda ise 5846 Sayılı Fikri ve Sanat Eserleri Kanunu ile telif ve benzeri haklar korumaya alınmıştır (Özbek, 2015, s. 83). Belirtmek gerekir ki 5846 Sayılı Kanun ile getirilen düzenlemede ihlalin bilgisayar sistemleri aracılığı ile işlenmesinin suçun gerçekleşmesi bağlamında bir önemi bulunmamaktadır. Yani Kanun'un 71'nci maddesinde düzenlenen manevi, mali ve bağlantılı suçlara tecavüz ile 72'nci maddesinde düzenlenen koruyucu programları etkisiz hâle getirme suçlarının serbest hareketle işlenmesi yeterli kabul edilecektir.

[7] Yargıtay 13. Ceza Dairesi, 06.04.2016, E. 2015/1926, K. 2016/6115, *"…sanal oyun karakterlerinin her ne kadar maddi bir karşılığı olduğu bilinse de veri niteliğinde olmasından dolayı hırsızlık suçunun konusunu oluşturamayacağı kabulünün sonucu olarak somut olayda TCK madde 244/4 hükmünün uygulanması gerektiğine…"*

5.2. Ceza Muhakemesi Hukuku Bağlamında Düzenlemeler

Bilişim teknolojilerinin baş döndüren hızda gelişimi ve siber suçların kendine has sınır tanımaz yapısı karşısında geleneksel ceza muhakemesi koruma tedbirlerinin yetersiz kalacağını söylemek, yanlış olmayacaktır. Özellikle dijital ortamda muhafaza edilen delil niteliğindeki verilere yönelik anlık olabilecek tahrip, değiştirilme, yok etme gibi zarar verici fiilleri engellemek maksadıyla özel koruma tedbirleri alınması önem arz etmektedir. Bu bağlamda Sözleşme'nin 14-21'inci maddeleri arasında ceza muhakeme hukuku kapsamında belirlenen koruma tedbirleri düzenlenmiştir.

Çalışmamızın devamında öncelikle koruma tedbirlerinin kapsamı, sonrasında ise Sözleşme'de düzenlenen koruma tedbirleri incelenecektir.

5.2.1. Siber Suçlara Karşı Koruma Tedbirlerinin Kapsamı

Sözleşme kapsamında koruma tedbirlerine konu olan veriden anlaşılması gereken dijital ortamda depolanmış veya devam eden iletişim sürecinde ortaya çıkan trafik verileri, içerik verileri ve abone verilerinin de dâhil olduğu her çeşit bilgisayar verisidir (Aliusta ve Benzer, 2018, s. 40).

Sözleşme'nin 20'nci ve 21'inci maddelerinde düzenlenen koruma tedbirlerini istisna tutarsak diğer koruma tedbirlerinden sadece Sözleşme'de öngörülen suç tipleri değil, bilgisayar sistemleri aracılığı ile işlenen tüm suçlar ve her türlü suçun dijital ortamdaki delillerinin toplanması amacıyla da faydalanılabilecektir. Niteliği gereği iletişim özgürlüğü ve özel hayatın dokunulmazlığı hakları üzerinde ciddi müdahaleye sebep olunabileceğinden 20'nci ve 21'inci maddelerde düzenlenen koruma tedbirlerinden Sözleşme'ye taraf devletlerin takdirinde sadece ağır suç tipleri kapsamında yararlanılabilecektir (Keskin, 2001, ss. 157 – 158).

Nihayetinde Sözleşme kapsamındaki tüm koruma tedbirlerinden yararlanılabilmesi amacıyla somut bir adli soruşturmanın şart olduğu, önleyici kolluk hizmetleri açısından ise bu tedbirlerin uygulanamayacağını ifade edebiliriz (Özbek, 2015, s. 84).

5.2.2. Sözleşme Kapsamında Düzenlenen Koruma Tedbirleri

Sözleşme'nin 16'ncı maddesi ile bilgisayar verileri, 17'nci maddesi ile de trafik verileri üzerinde geleneksel Ceza Muhakemesinde yer alan arama ve el koyma tedbirleri öncesinde bu tedbirlerin uygulanabileceği şartları oluşturmak amacıyla ön koruyucu nitelikte alınması gereken önlemler düzenlenmiştir. Bu önlemler

kapsamında verilerin; silinmeden, değiştirilmeden, tahrip edilmeden, özgün hâli ile muhafaza edilmesi amaçlanmaktadır.

Bilgisayar verisi kavramına ilişkin çalışmamızın önceki başlıklarında tanımlamada bulunmuştuk. Trafik verisi kavramını ise bilgisayar verisi türü olarak iletişimin başından son varış noktasına kadar olan süreçte üretilen başlangıç/varış noktaları, izlediği yol, saat, tarih, boyutlar, süre ve kullanılan iletişim tipi olarak ifade edebiliriz. Koruma tedbirlerinin konusunu, Sözleşme'nin hizmet sağlayıcı/veri depolayıcılara getirdiği yükümlülük gereği yerel düzenlemeler kapsamında azami 90 gün ile sınırlı olacak şekilde toplanmış ve depolanmış geçmiş zamanlı veriler oluşturmaktadır. Ayrıca şüphelinin soruşturmadan haberdar olmaması ve kişilerin gizlilik ihtiyacını karşılamak amacıyla ilgililere sır saklama yükümlülüğü de getirilmiştir (Keskin, 2001, s. 162).

Türk Ceza Muhakeme Hukuku kapsamında yukarıda ifade ettiğimiz koruma tedbirlerine karşılık gelecek bir hüküm bulunmamaktadır. Ancak internet kullanımı kapsamında idari tedbirlerin öngörüldüğü 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile Bilgi Teknolojileri ve İletişim Kurumu'nca talep hâlinde içerik sağlayıcılarına gerekli bilgileri sağlama ve tedbirleri alma, yer/erişim sağlayıcılarına trafik bilgilerini depolama ve doğruluğunu, bütünlüğünü ve gizliliğini sağlama yükümlülükleri getirilerek boşluk doldurulmaya çalışılmıştır. Ancak trafik verilerinin iletişimin bir parçası olduğu kabulü gereği 5651 Sayılı Kanun kapsamında Hâkim kararına ihtiyaç duymaksızın sadece Cumhuriyet Savcısının talebi ile bu verilerin içerik/yer/erişim sağlayıcılardan alınabilmesinin yerinde olmadığını, 5271 Sayılı Kanun'un 135/6'ncı fıkrasında düzenlenen telekomünikasyon yolu ile iletişimin tespiti uygulamasına aykırılık teşkil ettiğini belirtelim (Akpek, 2015, ss. 80 – 95).

Sözleşme'nin 18'inci maddesi ile taraf devletlerin ulusal sınırları içerindeki kişilerin depolama ve doğrulama yükümlülüğü getirmeden sahip olduğu veya kontrolü altında bulunan geçmiş zaman verilerinin ve hizmet sağlayıcıların sundukları hizmet bağlamında edindikleri aboneleri hakkındaki her tür bilginin (kimlik, adres, iletişim numarası, posta, hizmet sözleşmesi…) teslimi ile ilgili adli soruşturma makamları tarafından zorlanabilecekleri düzenlenmiştir (Keskin, 2001, ss. 167 – 168). Türk Hukuku açısından ise 5271 Sayılı Kanun'un 134'üncü maddesi ile genel arama ve el koymaya konu olacak eşyanın bilgisayar verisi olması özelinde bir düzenlemeye gidilmiştir. Tabii buradaki diğer bir farklılık olarak ise madde 134 kapsamında karar vermeye tek yetkili merciin hâkim

olduğunu vurgulayalım. Hizmet sağlayıcılara talep hâlinde verileri teslim yükümlülüğü getiren 5651 Sayılı Kanun ile ilgili yukarıda bilgi verildiğinden tekrar açıklamada bulunulmayacaktır (Aliusta ve Benzer, 2018, s. 40).

Sözleşme'nin 19'uncu maddesi ile bilgisayar sistemi, bu sistem ile bağlantılı/bağlantısız veri depolama parçaları veya depolanmış bilgisayar verilerinin kopyalanması, eğer mümkün değilse el konulması koruma tedbirine karşılık olarak bir önceki paragrafta ifade ettiğimiz 5271 Sayılı Kanun'un 134'üncü maddesi gösterilebilir (Özbek, 2015, s. 85). Tabii burada tedbirin konusunun geçmiş zamanda depolanmış veriler olacağını belirtelim.

Sözleşme'nin 20'nci maddesi ile iletişim özgürlüğü ve özel yaşamın gizliliğini ihlal edecek nitelikte trafik verilerinin gerçek zamanlı toplanması koruma tedbiri düzenleme altına alınmıştır. Bu tedbir kapsamına konu verileri, bilgisayar sistemleri arasında iletişimin şimdiki zamanda gerçekleştirilen işlemlere ait olan trafik verileri olarak ifade edebiliriz. Bahse konu tedbirin yukarıda bahsettiğimiz temel hak ve özgürlüklere etki edebilme niteliğinin doğal sonucu olarak Sözleşme'nin 14'üncü maddesiyle taraf ülkelerin sadece belli suçlarda kullanılabileceği yönünde sınırlama getirme hakkı saklı tutulmuştur (Keskin, 2001, ss. 172 – 173).

Sözleşme'nin 21'inci maddesiyle de trafik verisi dışında iletişimin anlamı ve amacını ortaya çıkaran, bilgisayar teknolojileri yoluyla aktarılan bilgi veya mesaj olarak tanımlayabileceğimiz içerik verilerinin yolunun kesilip ele geçirilmesi koruma tedbiri düzenlenerek iletişim bilgileri anlık olarak toplanabilecektir (Akpek, 2015, s. 106). Bir önceki koruma tedbirine benzer şekilde temel hak ve özgürlükleri ihlal edebilme niteliği gereği bu tedbirin uygulanabilmesi açısından taraf devletlerin yerel mevzuatlarında belirleyecekleri ağır suçlar ile sınırlayabilme hakkı saklı tutulmuştur (Keskin, 2001, s. 176).

Türk Hukuku bağlamında Sözleşme'nin 20'nci ve 21'inci maddelerinde düzenlenen koruma tedbirlerine karşılık olarak 5271 Sayılı Kanun'un 135'inci maddesi gösterilebilir (Aliusta ve Benzer, 2018, s. 40). Gerek trafik verilerinin gerçek zamanlı toplanması gerek gerçek zamanlı olarak içerik verilerine müdahale edilmesi bakımından bir ayrım gözetmeyen bu Kanun maddesiyle bu iki tedbir birlikte düzenleme altına alınmıştır. Son olarak Sözleşme'de tedbirin uygulanması noktasında görev yüklenen kurumlara belirli bir süre sır saklama yükümlülüğü getirilebileceğinin düzenlendiğini ifade edelim.

5.3. Adli Yardımlaşma

Sözleşme'nin 23'üncü maddesi ile taraf devletlere, adli iş birliğinin mümkün olan en geniş biçimde sağlanması gerektiği yönünde yükümlülük getirilmiştir. Gerek bilgisayar sistemleri ve aracılığı ile işlenen suçlar gerek de diğer sıradan suçların delillerinin dijital sistemler aracılığı ile toplanmasını kapsayacak şekilde iş birliğinin uygulama alanı oldukça geniş tutulmuştur.

Sözleşme'nin uluslararası iş birliğine dair hükümlerinin cezai işlerde adli yardımlaşma ve iadeye ilişkin uluslararası çok taraflı ve iki taraflı anlaşmalar ile ulusal seviyedeki hükümler karşısında üstün olmadığı, bu kapsamda ülkeler arasındaki çok veya iki taraflı anlaşmalar ile yerel mevzuatların muhafaza edilmeye devam edildiği söylenebilir (Önok, 2003, s. 1249). Diğer bir deyişle Sözleşme, aralarında özel bir antlaşma bulunmayan taraf devletlerin karşılıklı adli yardımlaşma anlaşması işlevini yerine getirecektir. Ancak belirtmek gerekir ki aralarında adli yardımlaşmaya ilişkin ikili bir anlaşma olmayan devletlerin dahi açıkça kabul etmeleri hâlinde Sözleşme'nin 27'nci maddesinde düzenlenen usul hükümleri uygulama alanı bulacaktır (Dülger, 2020, s. 208)[8].

Sözleşme'nin öncelikle 24'üncü maddesi ile yine 2-11'inci maddeleri arasında düzenlenen üst sınırı bir yıl veya daha fazla hapis cezasını gerektiren suçlar bakımından sınırlama getirilerek iade yükümlülüğüne konu olabilecek suç tipleri belirlemiştir. Sözleşme'nin taraf ülkelere tanıdığı geniş çekince hakkı gereği iade müessesi de "çifte suçluluk" şartına bağlanmıştır (Önok, 2003, s. 1250). Aynı zamanda adli yardımlaşmanın işlerliğini artırmak maksadıyla Sözleşme tarafından genel ilkeler dışında özel usul hükümleri de düzenlenmiştir. Bu bağlamda Sözleşme'nin 29'uncu maddesinde depolanmış bilgisayar verilerinin ivedi korunması, 30'uncu maddesinde muhafaza edilen trafik verilerinin ivedi korunması ve 31'inci maddesinde ise depolanmış bilgisayar verilerine erişim hususunda karşılıklı yardımlaşma usulleri belirlenmiştir.

Yine Sözleşme'nin 35'inci maddesi ile taraf ülkelere 7/24 esasına göre çalışacak olan irtibat noktaları belirleme yükümlülüğü getirilmiştir. Bu sistemlerin işlevselliği ile ilgili 14 irtibat noktası bağlamında 2007 ve 2008 yıllarının ilk 10 ayını kapsayan bir çalışmada, genel olarak uygulamanın çok acil ve istisnai

[8] Misal olarak Türkiye'nin Sözleşme'ye taraf olması öncesinde ABD ile arasında ikili bir anlaşma olmasına rağmen iki tarafında sahih bir şekilde kabul etmesi hâlinde bu ikili anlaşmanın hükümleri yerine Sözleşme'nin 27'nci maddesinde öngörülen usul hükümleri uygulanacaktır.

durumlar dışında kullanılmamasına rağmen iki yılda ortalama 540 talebin gönderildiği ve bu taleplere karşılık yaklaşık olarak 480 talebin alındığı görülmüştür (Akpek, 2015, s. 27). Türkiye için belirlenen irtibat noktası; Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığıdır (Özbek, 2015, s. 87). Türkiye'de uluslararası adli yardımlaşmadan sorumlu kurum ise 2992 Sayılı Adalet Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname'nin Değiştirilerek Kabul Edilmesine Dair Kanun'un 13'üncü maddesi bağlamında Adalet Bakanlığı'na bağlı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğüdür (Akpek, 2015, s. 111).

SONUÇ

Bilişim teknolojilerinin muazzam gelişiminin günlük hayatta sağladığı artan oranda kolaylıklara paralel olarak ortaya çıkardığı yeni suç alanı, sebep olduğu ciddi zararlar ve ulusal sınırları aşan yapısı bağlamında küresel seviyede ciddi bir problem olarak karşımızda durmaktadır. Devletlerin ulusal güvenlik endişeleri ve farklı kültürel, sosyal, siyasi, ekonomik yapılarına bağlı olarak birbirlerine uyumsuz mevzuat düzenlemelerine sahip olmaları sebebiyle siber suçla uluslararası alanda geleneksel yöntemler ile mücadele, eşyanın tabiatına aykırı bir hâle gelmiştir.

Suçun sürekli değişime ve gelişime açık yapısı gereği suçla mücadele kapsamında teknik ve uzman personele ihtiyaç duyulması, yer fark etmeksizin ucuz ve az emek gücü ile işlenebilmesinin aksine mücadelenin büyük bütçe ve emek gerektirmesi, siber suçların önlenmesi sürecinde çözülmesi gereken diğer problemlerdir.

Gerek ulusal gerek uluslararası alanda siber suçla mücadele kapsamında birçok girişim bulunmaktadır. Yukarıda ifade ettiğimiz genel gerekçeler göz önünde bulundurulduğunda diğer devletlerden bağımsız olarak ulusal kapsamda alınacak tedbirlerin yetersiz olacağı izahtan varestedir. Uluslararası girişimler de genel olarak istişari nitelikte kalmıştır. Siber suç faillerine gizlenebilecekleri hiçbir "sığınak/korunak alanı" bırakmamak amacıyla tüm devletler tarafından bağlayıcı nitelikte, uluslararası mevzuata uyumu sağlayacak şekilde yükümlülükler getiren bir uzlaşı metnine ihtiyaç duyulmuştur.

Bu şartlar altında ortaya çıkan Budapeşte Sözleşmesi olarak da bilinen Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi; üyelik şartı öngörmemesi, taraf devletler açısından iç mevzuatlarında düzenleme yapma yükümlülüğü getirmesi, taraf olmayan devletler açısından başvurulabilecek uluslararası düzeyde bir şablon

sunması, nihayetinde bağlayıcı nitelikte maddi ceza hukuku, usul hukuku ve adli yardımlaşma bağlamında ilkeler belirleyerek ülkeler arasındaki düzenleme farklılıklarını azaltması sebebiyle siber suçla mücadele kapsamında önemli bir küresel adım olarak kabul edilmektedir. Ancak Sözleşme'nin taraf devletlere sunduğu geniş çekince sunma hakkı; küresellik iddiasını ciddi ölçüde zayıflatmaktadır.

Türkiye tarafında Sözleşme, 10.11.2010 tarihinde imzalanmış, konulan 3 çekince ve 5 beyan koşulu ile 3 maddeden oluşacak şekilde 22.04.2014 tarihinde kabul edilen 6553 Sayılı Kanun'la Türk Hukuku'nda geçerli hâle getirilmiştir. Ancak gerek 765 Sayılı TCK'nin gerek de 5237 Sayılı YTCK'nin siber suçlara ilişkin düzenlemelerinin esin kaynağının Fransız mevzuatı olması, bu bağlamda Fransa'nın Sözleşme'yi onaylama/imzalama ile iç hukuk düzenlemelerinin yürürlüğe giriş tarihi kıyaslandığında Sözleşme'nin Türk Ceza Hukuku kapsamındaki düzenlemeler üzerinde etkisinin olmadığı gerçeğinin kabulü gerekecektir. Ancak yine de yukarıda ifade ettiğimiz üzere Sözleşme'nin ilk kısmında getirilen tanımlara yüklenen anlam, düzenlenen suç tipleri, suçla mücadelede öngörülen koruma tedbirleri ile adli yardımlaşma ve iş birliğine ilişkin uygulamalarına karşılık gelen iç hukukumuzdaki düzenlemeler bakımından genel bir uyum hâlinin olduğu görülmektedir. Diğer taraftan önemle belirtmekte fayda var ki Sözleşme'de suç olarak düzenlenmesine rağmen iç hukukumuz bağlamında çocuk pornografisi ile ilgili verilere depolanmaksızın sadece kasten erişim sağlanması hâlinin suç kapsamına alınmaması, hâlen daha ciddi bir eksiklik olarak karşımızda durmaktadır.

Sonuç olarak siber suçla ulusal veya uluslararası alanda mücadele kapsamında Sözleşme'nin mevcut etkinliği yadsınamaz bir gerçektir. Devam eden süreçte Sözleşme'ye katılımın artırılarak taraf olan veya olmayan devletlerin iç hukuklarında gerekli düzenlemeleri yapması hâlinde sağlanacak iş birliği ile siber suçların engellenmesi, faillerinin sığınabilecekleri korunaklı bölgelerin yok edilmesi, müteakibinde tespiti ve yakalanması sağlanacaktır. Son olarak belirtmekte fayda var ki, bu mücadele sürecinde yapılacak düzenlemelerde kişilerin ifade özgürlüğü ve kişisel verilerin korunması konularında hassasiyet gösterilmesi gerekmektedir. Unutulmamalıdır ki siber suçla mücadele ile mezkûr temel haklar kapsamındaki mevcut düzenlemelerin koruduğu hukuki yarar açısından bir tercih hâli söz konusu değildir. İki hukuki yararın da birbirine feda edilmeden dengeli bir şekilde muhafazası gerekmektedir.

KAYNAKÇA

Akpek, N. O. (2015). *Siber suçlar sözleşmesinin getirdikleri ve iç hukuk açısından konuya ilişkin yaklaşım* (Yayımlanmamış Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi Lisansüstü Eğitim Fakültesi, İstanbul.

Aliusta, C. ve Benzer, R. (2018). Avrupa siber suçları sözleşmesi ve türkiye'nin dâhil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), 35 – 42.

Altunok, E. ve Vural, A. F. (2011). Bilişim suçları. *Denetişim.* 8, 74 – 84.

Council of Europe. (2020). Erişim Tarihi: 27.10.2020, https://www.coe.int/en /web/conventions/full-list/conventions/treaty/185 /signatures?pauth=ecp1 stsJ.

Demirdöğen, M. Y. (2019). Avrupa konseyi sanal ortamda işlenen suçlar sözleşmesinde telif hakkı ve türkiye'nin entegrasyonu, *Yüksek Lisans Tezi (Yayımlanmamış).* Sakarya Üniversitesi Sosyal Bilimler Enstitüsü.

Dülger, M. V. (2020). *Bilişim suçları ve internet iletişim hukuku*. (8. Basım). Ankara: Seçkin Yayınları.

Ergüney, M. (2020). RTÜK'ün internet denetimi: ilgili mevzuat üzerine bir değerlendirme. *Bilişim Teknolojileri Online Dergisi*, 11(41), 2 – 34.

Erümit, S. F. (2020). İnternetin gelişimi: dünü, bugünü ve yarını. *İnternet ve Ağ Toplumu*, (3. Basım), 96 – 122.

Favanski, S. (2009). *Computer misuse: response, regulation and the law.* (1. Edition). United Kingdom: Willan Publishing.

Geçmez, İ. (2020). *Bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçları.* (1. Basım). Ankara: Seçkin Yayınları.

Gercke, M. (2014). *Understanding cybercrime: phenomena, challenges and legal response.*(3. Edition). ITU Telecommunication Development Bureau Press.

İçel, K. (2001). Avrupa konseyi siber suç sözleşmesi bağlamında "avrupa siber suç politikasının ana ilkeleri". *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.* 59(1 – 2), 3 – 10.

Keskin, S. (2001). Avrupa konseyi siber suç sözleşmesinde ceza muhakemesine ilişkin hükümlerin değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.* 59(1 – 2), 155 – 180.

Kutlu, Ö. Kahraman, S. ve Dinçer, S. (2019). Avrupa birliği'ne uyum sürecinde türkiye'nin siber güvenlik politikalarının analizi. *Assam Uluslararası Hakemli Dergi 13. Uluslararası Kamu Yönetimi Sempozyumu Bildirileri Özel Sayısı*. 1 – 14.

Law, J. Martin, E. A. (2021). Oxford dictionary of law. *Cybercrime*. Erişim Tarihi: 25.10.2020, https://www.oxfordreference.com/view/10.1093/acref/9780199551248.001.0001/acref-9780199551248-e-1000?rskey=HuyGij&result=1061.

Mann, T. Blunden, A. (2021). Australian law dictionary. *Cybercrime*. Erişim Tarihi: 25.10.2020, https://www.oxfordreference.com/view/10.1093/acref/9780195557558.001.0001/acref-9780195557558-e-0921?rskey=3mbcxx&result=901.

Markoff, J. Kramer, A. E. (2019). In shift, u.s. talks to russia on ınternet security. *The New York Times*. Erişim Tarihi: 28.10.2020, https://www.nytimes.com/2009/12/13/science/13cyber.html.

Önok, M. (2003). Avrupa konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*. 19(2), 1229 – 1270.

Özbek, M. (2015). Avrupa siber suç sözleşmesinin türk ceza hukukuna etkileri, *GSI Articletter Summer Issue*. 73 – 88.

Sınar, H. (2004). *Avrupa konseyi siber suç sözleşmesi üzerine bir deneme*. (1. Basım). İstanbul: Prof. Dr. Çetin Özek Armağanı.

Sieber, U. (1998). *Legal aspects of computer – related crime in the information society: concrime study*. (1. Version). Europe Eu.

Smith, R. G. Grabosky, P. Urbas, G. (2004). *Cyber criminal on trial*. (1. Edition). Cambridge: Cambridge University Press.

TBMM. (2019). *TBMM mevzuat bilgi sistemi,* Erişim Tarihi: 13.10.2021, https://mevzuat.tbmm.gov.tr/mevzuat/faces/kanunmaddeleri?pkanunlarno=24562&pkanunnumarasi=5070.

TBMM. (2013). *Sanal ortamda işlenen suçların onaylanmasının uygun bulunduğuna dair kanun tasarısı ve dışişleri komisyonu raporu*, yasama dönemi. 24, Yasama Yılı. 3, Sıra Sayısı. 380. Erişim Tarihi: 29.10.2020, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf.

TDK. (2019). *Bilişim*. Erişim Tarihi: 25.10.2020, https://sozluk.gov.tr/.

Wall, D. (2009). *Cybercrimes: new wine, no bottles.* (1. Edition). London: Invisible Crimes, Palgrave Macmillan.

Yazıcıoğlu, Y. (2005). Yeni türk ceza kanunundaki bileşim suçlarının genel değerlendirilmesi, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi.* 2(2). 393 – 412.