AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ VE TÜRK HUKUKUNA ETKİLERİ
THE CONVENTION ON CYBERCRIMES AND ITS IMPACTS ON TURKISH LAW

Ar. Gör. Merve Erdem, LL.M.
Av. Gürkan Özocak, LL.M.

ÖZET

Siber suçlar açısından, yalnızca bu suçların maddi ceza hukuku normlarında tanımlanması değil, aynı zamanda hem ulusal hem uluslararası alanda siber suçlulukla mücadele de büyük önem arzetmektedir. Bu nedenle 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan Avrupa Konseyi Siber Suç Sözleşmesi, Türkiye tarafından da 2010 yılında imzalanmış ve 2014 yılında yürürlüğe girmiştir. Ancak, Türk ceza hukuku ve ceza muhakemesi hukuku yönünden sözleşme hükümlerinin iç hukuk ile uyumlulaştırılması yönünden ciddi sıkıntılar söz konusu olduğu gibi, sözleşmenin bölgesellikten öteye gidememesi ve adli yardımlaşma yönünden zorunluluğu bulunmaması gibi sorunları mevcuttur.

ANAHTAR KELİMELER

Avrupa Siber Suç Sözleşmesi, Bilişim Hukuku, Siber Suçlar, Bilişim Suçları, Adli Yardımlaşma.

ABSTRACT

It is vital that not only describing cybercrimes in norms of criminal law, but also struggling them on the national and international stage. The European Convention on Cybercrimes was opened for signature in Budapest on 23 November 2001 because of this reason. Turkey signed the Convention in 2010 and put it into force in 2014. However, there are some issues about harmonization of domestic legislation with the provisions of the Convention in the field of criminal and criminal procedure law. Also, the Convention has some problems on being regional and not mandatory in terms of judicial cooperation.

KEYWORDS

The European Convention of Cybercrimes, IT law, cybercrimes, judicial cooperation.

1. GİRİŞ

Siber suçlar veya ülkemizdeki daha yaygın kullanımıyla "bilişim suçları", doktrinde üzerinde mutabık kalınan bir tanımı yapılamamakla birlikte, genel olarak, verilerin bilişim temelli olarak ve otomatik bir biçimde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içerisinde işlenen, bir bilgisayara veya bilgisayar ağına yahut bir bilişim sisteminin bir kısmına ya da tamamına yahut bu sistemde bulunan verilere yönelik olarak veya bu sistemlerin araç olarak kullanılması suretiyle gerçekleştirilen haksız eylemler olarak tanımlanmaktadır[1]. Söz konusu tanım salt bilişim alanında işlenen suçlara yönelik

[1] **DÜLGER, Murat Volkan**, Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi, s. 2; **İÇEL, Kayıhan,** "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C: LIX, Sayı: 1-2, 2001, s. 3 (3-10); **KURT, Levent**, Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 49-53; **ÖZEN, Muharrem/BAŞTÜRK, İhsan**, Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011, s. 90-91.

olduğundan ve bilişim sistemlerinin kullanılması ile gerçekleştirilen sahtecilik, dolandırıcılık, çocuk pornografisi, hakaret vb. suçları kapsamadığından, bugün doktrinde bilişim suçları "*bilişim alanındaki suçlar*" ve "*bilişim sistemleri aracılığıyla işlenen suçlar*" olarak ikiye ayrılmaktadır. İlk gruptaki suçlar, yukarıda da tanımlanan, yetkisiz erişim, bilişim sistemine veya burada bulunan verilere müdahale gibi salt bilişim alanında işlenen, bütün sebep ve sonuçlarıyla sanal alanda ortaya çıkıp sonuçlanan suçlardır. İkinci gruptaki suçlar ise, "*geleneksel*" ya da "*klasik*" suçlar olarak tanımlanan, ancak bir bilişim sistemi aracılığıyla işlenen suçlardır. Örneğin; e-posta yoluyla işlenen tehdit veya hakaret suçu, yine bilgisayar veya İnternet siteleri üzerinden işlenen haberleşmenin gizliliğini ihlal, cinsel taciz, halkı kin ve düşmanlığa tahrik etme gibi suçlar bu grupta sayılabilir. Teknolojik imkanların müthiş bir hızla artması ve gelişmesi ile birlikte, artık insan öldürme suçuna kadar her suç bilişim yoluyla işlenebileceği için, bu gruptaki suçların sınırını belirlemek mümkün değildir[2].

Siber suçlar yönünden, bilişim alanında gerçekleşen eylemlerin ceza normu olarak öngörülmesi ve bu suçların kapsamının belirlenmesi kadar, söz konusu suçlarla mücadele edilmesi de son derece önemlidir. Suçta kullanılan bir araç olan internetin doğası gereği, siber suçlar, önlenmesi ve soruşturulmasında en çok işbirliğine ihtiyaç duyulan bir çalışma alanıdır. Zira diğer sınıraşan suç türlerinde en çok işbirliği ihtiyacı duyulan ülkeler komşu ülkeler ya da karşılıklı insan trafiği çok olan ülkeler olduğu halde, söz konusu durumun siber suçlar alanında da aynen geçerli olduğunu söylemek mümkün değildir. Çünkü internet üzerinde tüm ülkeler birbiriyle komşudur. Bu nedenle, siber veya bilişim suçları alanında işbirliğinde büyük internet servis sağlayıcılarının bulunduğu ve en çok suçlunun barındığı ülkeler gibi farklı ölçütler ön plana çıkmaktadır[3].

Ne var ki günümüzde, teknolojinin gelişimi ile birlikte çok farklı yollarla işlenebilen ve çoğu kez uluslararası karakteri haiz olan siber suçlarla mücadele edilmesinde karşımıza çıkan en büyük sorun, devletlerin ulusal mevzuatlarının hem maddi hukuk hem de usul hukuku bakımından farklılık arz etmesi ve siber suçlar bakımından adli yardımlaşmanın yetersiz kalmasıdır.[4]

Bu sorunların çözümü için, devletlerin gerek maddi hukuk gerekse de usul hukuku yönünden yeknesak bir siber suç uygulaması ve etkili bir uluslararası adli yardımlaşma rejimi oluşturabilmeleri amacıyla, Avrupa Konseyi Siber Suç Sözleşmesi meydana getirilmiştir. Sözleşme, genel itibariyle, telif haklarının ihlali, siber suçlar, bilişim yoluyla yapılan sahtecilik, çocuk pornografisi, güvenlik ağlarının ihlali ve uluslararası adli yardımlaşma ile siber suçlarla mücadele konularına odaklanarak, imzacı devletler arasında yeknesak bir siber suçlarla mücadele rejimi oluşturmayı hedeflemektedir.

2. AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

a. Genel Olarak

Avrupa Siber Suç Sözleşmesi, siber suçların giderek yaygınlaşması, sınır aşan boyutu itibariyle devletler arasında yardımlaşmayı zorunlu hale getirmesi ve bazı devletlerin

---

[2] **ÖZDİLEK, Ali Osman**, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006, s. 112.
[3] **ŞEN, Bilal/CENGİZ, Mahmut,** "Bir Sınıraşan Suç Türü Olarak Bilişim Suçları", Sınıraşan Organize Suçlar – Kavramlar, Yöntemler, Eğilimler, Ankara, 2011, s. 67-68.
[4] **WEBER, Amalie**: The Council of Europe's Convention on CyberCrime, Berkeley Technology Law Journal, Vol. 18, 2003, s.425. (424- 446)

mevzuatında söz konusu suçların dahi düzenlenmemiş olması gibi sebeplerle kaleme alınmış bir sözleşmedir.[5] 1997 yılında Avrupa Konseyi bünyesinde kurulan Siber Suç Uzmanlar Komitesi'nin kurulmasıyla başlayan çalışmalar neticesinde Sözleşme, 23 Kasım 2001 tarihinde imzalanmış ve 1 Temmuz 2004 tarihinde yürürlüğe girmiştir.[6] Yine aynı şekilde Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesi'ne Ek Protokol de 28 Ocak 2003 tarihinde imzaya açılıp, 1 Mart 2006 tarihinde yürürlüğe girmiştir.[7]

Siber suçlarla mücadele alanında akdedilen ilk sözleşme olan Avrupa Siber Suç Sözleşmesi, Avrupa Konseyi nezdinde akdedilmiş olsa bile, salt bölgesel bir Sözleşme olma amacı gütmemektedir.[8] Nitekim Sözleşme'nin müzakere aşamasında, Avrupa Konseyi'ne üye olamayan Kanada, Japonya, Güney Afrika ve Amerika Birleşik Devletleri (ABD) de görüşmelere davet edilmiştir.[9] Söz konusu devletler Sözleşmenin nihai metninin imzalamış, hatta ABD Sözleşme'yi onayarak Sözleşme'nin tarafı olmuştur.[10]

Türkiye ise hem Sözleşme'yi imzalamak hem de onaylamak bakımından uzun yıllar beklemiş; 10 Kasım 2010 tarihinde imzalanan Sözleşme için, 22 Nisan 2014 tarihinde uygun bulma kanunu çıkarılmış, Bakanlar Kurulu onay kararnamesinin 9 Ağustos 2014 tarihinde yayımlanması ile birlikte onay işlemi tamamlanmıştır.[11] Sözleşme'de öngörüldüğü üzere, Türkiye 1 Ocak 2015 tarihinden itibaren Sözleşme'nin tarafı olmuştur.[12]

Siber suçlarda, suçun işleniş biçimleri çeşitli olup tek bir/belli başlı şablonlar çıkarmak şimdilik mümkün gözükmemektedir. Çoğu ulusal sistem, söz konusu suçluluk türüne yabancı ya da farklı farklı düzenlemelere sahiptir. Siber suçların sınıraşan boyutları, suçun tespitini, teknik takibini ve yargılamayı oldukça zorlaştırmaktadır.[13] Siber suçlarla mücadelede işbu zorluklar dolayısıyla, Sözleşme hem maddi hukuka, hem usul hukukuna, hem de adli yardımlaşmaya ilişkin ortak hükümler getirerek alanla ilgili iç hukuk mevzuatlarının yeknesaklaşmasını ve böylelikle siber suçlarla mücadeleyi kolaylaştırmayı amaçlamaktadır. Devletlerin konuyla ilgili ortak bir ceza hukuku ve ceza yargılaması politikası oluşturarak devletleri oluşturan toplumları siber suçtan ve etkilerinden etkin bir şekilde korunması da

---

[5] **WEBER**, s. 429.

[6] Avrupa Konseyi Siber Suç Sözleşmesi akdedilmeden önce, Konsey nezdinde bilişim suçları ile ilgili O.E.C.D raporları ve Konsey'in tavsiye kararları, Sözleşme'nin akdedilmesini hazırlayan gelişmelerdir. Ayrıntılı bilgi için bkz. **DÜLGER**, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, 2014, İstanbul,s. 193; **İÇEL,** s. 4- 6; **ÖNOK,** Murat, Avrupa Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Prof. Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt.19, Sayı:2, 2013, s. 1239 (1229- 1269); **VATIS, Michael,** The Council of Europe Convention on Cybercrime, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academy Press, Washington D.C., 2010, s. 207- 210. (207- 223)

[7] Halihazırda 23 Avrupa Konseyi devleti söz konusu Protokol'ün de tarafıdır. Liste için bkz. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=nOtm1q80 et. 26.01.2015.

[8] **HARLEY**, s. 2; **WEBER**, 2003, s. 429.

[9] **MARION**, **Nancy**, "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation", International Journal of Cyber Criminology, Vol. 4, Issue: 1&2, 2010, s. 701. (699- 712).

[10] Sözleşmeyi onaylayan devletlerin listesi için bkz. http://www.coe.int/en/web/conventions/full-list/-/convention s/treaty/185/signatures?p_auth=Sg9IxpBi et. 27.01.2016.

[11] 09.08.2014 T. ve 29083 S. Resmi Gazete. http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/08/20140809.htm&main=http://www.resmigazete.gov.tr/eskiler/2014/08/20140809.htm et: 26.01.2015.

[12] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=iaDgY9vB et: 14.01.2016.

[13] **ÖNOK,** s. 1232 – 1236.

sağlanmış olacaktır.[14]

b. Sözleşme'nin Getirdiği Yenilikler

Siber suçların niteliği ve sınır aşan boyutları, siber suçların hem maddi ceza hukuku hem de usul hukuku bakımından özel olarak düzenlenmesine ve devletler arasında adli yardımlaşmanın geliştirilmesi ihtiyacını doğurmaktadır.[15] Söz konusu ihtiyaçtan hareketle kaleme alınan Sözleşme, siber suçları düzenlerken başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklere saygı, bilişim suçları düzenlemede minimum standarda uyulması, bilişim suçuna vücut veren fiilin hukuka aykırı olması ve kasten işlenmesi gibi temel ilkelere sahiptir.[16]

Maddi hukuk boyutu bakımından, hangi fiillerin "siber suç" teşkil edebileceği ifade özgürlüğü ile ulusların ahlaki değerleri arasındaki ilişkiye verdikleri farklı tepkilere göre farklılık arz etmektedir. Dolayısıyla bir devlet nezdinde siber suç kabul edilebilecek bir fiil başka bir devlet nezdinde ifade özgürlüğünden faydalanabilir.[17] Usul hukuku bakımından başka bir sorun da yargı yetkisi, soruşturma, kavuşturma ve cezalandırmanın oldukça zor olmasıdır.[18] Yine aynı şekilde suçun işlendiği yerle, suçun sonuçlarının sirayet ettiği yerlerin farklılık göstermesi de, suçun sınır aşan boyutunu teşkil etmekte, işbu durum soruşturmayı ve kovuşturmayı zorlaştırmaktadır. Sözleşme, siber suçlarla mücadeleye ilişkin işbu handikapları göz önüne alarak, siber suçlarda hem maddi hukuk, hem usul hukuku hem de adli yardımlaşmaya ilişkin ortak hükümler öngörülmüştür.

Üç bölümden oluşan Sözleşme'de ilk bölüm tanımları, ikinci bölüm ulusal düzeyde alınacak tedbirleri, üçüncü bölüm ise uluslararası düzeyde alınacak tedbirleri düzenlemektir.

İkinci bölümde ulusal düzeyde alınacak tedbirler başlığı altında hem maddi ceza hukuku hem usul hukuku hem de yargılama yetkisine ilişkin ulusal düzeyde alınacak tedbirler yer almıştır.

İkinci bölüm birinci kısımda düzenlenen maddi ceza hukuku hükümlerinde, ulusal düzeyde düzenlenmesi öngörülen suçlar şunlardır: Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar (yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı); bilgisayarla bağlantılı suçlar (Bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık); içerikle bağlantılı suçlar (çocuk pornografisiyle bağlantılı suçlar), telif hakkı ve bununla bağlantılı hakların ihlaline karşı suçlar.

İkinci bölümün ikinci kısmında düzenlenen usul hukuku hükümleri öncelikle usul hükümlerinin kapsamını ve tedbirleri düzenleyen ortak hükümleri kaleme almıştır. Daha sonra depolanmış bilgisayar verisinin acilen koruma altına alınması ve trafik verilerinin acilen koruma altına alınması ve kısmen açıklanması, üretim emri, depolanmış bilgisayar verilerinin aranması ve bunlara el konulması, Bilgisayar verilerinin gerçek zamanlı

---

[14] **ARCHICK, Kristen**, Cybercrime: The Council of Europe Convention", içinde Cybercirme and cyberterrorism Current Issues (John Blane ed.), Novinka Books, NewYork, 2003, s. 2. (1-6); **HELVACIOĞLU, Aslı Deniz**, Avrupa Konseyi Siber Suç Sözleşmesi, içinde İnternet ve Hukuk, İstanbul (Yeşim ATAMER ed.), Bilgi Üniversitesi Yayınları, 2004, s. 279; **MARION**, s. 701;

[15] **DÜLGER,** s. 184- 185.

[16] **İÇEL**, s. 6- 10.

[17] Marion burada pornoyu örnek olarak göstermekte ve ABD'de pornonun pek çok türünün anayasa bakımından koruma altında olduğunu ifade etmektedir. **MARION,** s. 699- 700.

[18] **MARION**, s. 700.

toplanması (Trafik verilerinin gerçek zamanlı toplanması ve içerik verilerinin takibi).

İkinci bölümün üçüncü kısmında da, önemli tartışma konularından birini teşkil eden yargı yetkisi düzenlenmiştir.

Üçüncü bölümde, Sözleşme'nin önemli akdediliş amaçlarından birini teşkil eden uluslararası işbirliği hükümleri öngörülmüştür. Üçüncü bölüm birinci kısmında uluslararası işbirliğine ilişkin genel ilkeler, suçluların iadesine ilişkin ilkeler, karşılıklı yardımlaşmaya ilişkin genel ilkeler (karşılıklı yardımlaşmaya ilişkin genel ilkeler, kendiliğinden bilgi verme), uluslararası antlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardım taleplerine ilişkin usuller (uluslararası antlaşmaların yürürlükte olmadığı hallerde yapılan karşılıklı yardım taleplerine ilişkin usuller, gizlilik ve kullanımın sınırlandırılması). İkinci kısımda ise uluslararası işbirliğine ilişkin özel hükümler kaleme alınmıştır. Buna göre; geçici tedbirlere ilişkin karşılıklı yardımlaşma (depolanan bilgisayar verilerinin acilen koruma altına alınması, korunan trafik bilgilerinin derhal açıklanması), soruşturma yetkileri konusunda karşılıklı yardımlaşma (depolanan bilgisayar verilerine erişim konusunda karşılıklı yardımlaşma, depolanmış bilgisayar verilerine izinli şekilde veya bu verilerin halka açık olduğu durumlarda sınır ötesi ulaşım, trafik verilerinin gerçek zamanlı toplanması hakkında karşılıklı yardımlaşma, içerik verilerine el konulmaması hususunda karşılıklı yardımlaşma), 7/24 iletişim ağı.

Maddi hukuka ilişkin getirdiği suç tiplerinde öncelikle karşımıza çıkan husus, salt siber suç olarak adlandırılan fiillerin değil; aynı zamanda elektronik ortamda delil toplanmasını gerektiren her bir suçu, ayrıca bilişim sistemlerini kullanmak suretiyle işlenebilecek her bir suç tipini kapsamına almıştır.[19]

Ayrıca maddi hukuk bakımından içerikle bağlantılı suçlar bakımından çocuk pornografisinin düzenlendiği görülmektedir. İşbu 9. madde çocuk pornografiyle mücadele bakımından en önemli madde olma özelliğini taşımaktadır. Çocuk pornosunun da bir siber suç olarak sınır aşan boyutları dolayısıyla, Sözleşme'ye taraf olmadan çocuk pornosu ile mücadele etmenin pek mümkün olamayacağı ifade edilmektedir.[20]

Söz konusu madde uyarınca çocuk pornografisini üretmek, sunmak, dağıtımını yapmak, temin etmek ve depolamak gibi, bilgisayar sisteminin verinin her bir aşamasına ilişkin fiilleri suçun kapsamına almış ve çocuk pornografisi reşit olmayan/reşit olmayan şahıs görüntüsüne sahip şahsın cinsel içerikli eylemde bulunması ya da cinsel içerikli eylemde bulunmasını betimleyen gerçekçi görüntüler olarak tanımlanmıştır. Suçun kapsamının bu kadar geniş olması, çocuk pornografisiyle mücadelede gelinen son nokta olarak ifade edilmektedir.[21]

İçerikle bağlantılı suçlar kapsamında ırkçı içerikli yayınların da internet ortamında dağıtımını öngören bir suç tipi de Sözleşme'nin kapsamında tartışılmışsa da, üzerinde karara varılamadığı için, akdedilen ek protokol ile bilgisayar sistemleri üzerinden ırkçı ve nefret söylemi içeren yayınların dağıtımı ya da başka yollarla kamu oyuna sunulması, ırkçılık ya da

---

[19] **ÖNOK**, s. 1230.

[20] **SOKULLU- AKINCI**, **Füsun**, Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt. 59, Sayı: 1-2, 2001, s. 37. (11- 38).

[21] **DÜLGER, Murat Volkan,** Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler, İstanbul Barosu Dergisi, Sayı: 4, 2004, s. 1491.

nefret söylemiyle tehdit ya da aşağılama fiilleri yasaklamıştır. Bunun yanında, soykırımı ya da insanlığa karşı suçları reddeden, aşırı küçülten, kabul edene ya da meşrulaştıran materyallerin dağıtımı ya da başka yollarla kamu oyuyla paylaşılması da, işbu protokol kapsamından siber suçların kapsamına alınmıştır. Sözleşme ile Protokol arasındaki ilişkiyi düzenleyen 8. maddeyle, Sözleşme'nin tanımlar (m.1), teşebbüs ve yardım veya yataklık (m.11), kurumsal yükümlülük (m.12) ve yaptırımlar ve tedbirler (m.13), federal devletlere ilişkin madde (m. 41), değişiklikler (m. 44), uyuşmazlıkların çözümü (m. 45) ve taraflar arasındaki istişarelere ilişkin (m.46) maddeleri, Protokol'de de uygulama alanı bulacaktır.[22] İçerik bakımından Sözleşme'yi tamamlasa da, Sözleşmeyi onaylayan devletler ile Protokol'ü onaylayan devletle farklı olduğu için, söz konusu suçun ayrıca düzenlenmesi, Sözleşme'nin iç hukukları uyumlulaştırma amacına kanımızca aykırı gözükmektedir.

Bilgisayarla ilgili sahtecilik fiilinin farklı yorumlarının olduğu ifade edilmektedir. Sahteciliğin belgenin yazarına mı yoksa verinin içeriğine göre mi belirleneceğine ilişkin farklı yorumlar olmakla birlikte, genel görüşün, verinin içeriğine ilişkin sahteciliğin göz önüne alınması olduğu ifade edilmektedir.[23]

Sözleşme genel adli yardımlaşma sistemini ilga etme amacında değildir, sadece konuya ilişkin özel bir adli yardımlaşma sistemi getirmektedir.[24] Dolayısıyla siber suçlar bakımından adli yardımlaşma hükümleri, genel adli yardımlaşma hükümleri karşısında, *lex specialis* ilkesi gereği öncelikle uygulanma alanı bulacaktır.

Sözleşme adli yardımlaşma usulleriyle ilgili sınır ötesi depolanmış veriye ulaşmayı öngörmüştür. Ancak Sözleşme'nin akdedilmesi aşamasında, uzaktan ülke dışı araştırmaların yapılabilmesi hususu kabul görmemiş ve depolanmış verilere ulaşmayı sağlayacak kapsamlı ve devletler açısından bağlayıcı bir düzenlemenin gelinen bu aşamada yapılmasının mümkün olmadığı sonucuna ulaşılmıştır.[25]

Suçların soruşturulması ve kovuşturulması, devletlerin egemenlik alanı ile sınırlı olduğu için, sınıraşan suçların devletler tarafından soruşturulması ve kovuşturulması için adli yardımlaşmanın varlığı şarttır. Hele ki siber suçların, işlendiği yer ile suçun meydana geldiği yerin farklı olması itibariyle adli yardımlaşmanın varlığı daha da elzem hale gelmektedir.

Devletler arasında halihazırda uygulanmakta olan mevcut adli yardımlaşma yöntemlerinin özellikle siber suçlarla mücadelede yetersiz kalması Sözleşme'nin akdedilmesindeki önemli etkenlerden birini oluşturmaktadır. Özellikle suçluların iadesi bakımından çifte cezalandırılma ilkesinin varlığının bir önkoşul olması, devletler arasında mevzuat uyumunu gerekli kılmakta ve bu da iade taleplerinin geri çevrilmesi sonucuna vücut vermektedir. Siber suçlar sözleşmesinin adli yardımlaşma bakımından getirdiği en büyük yeniliğin, söz konusu çifte cezalandırılabilirlik ilkesini aşan nitelikte özel düzenleme getirmesi Sözleşme'nin getirdiği önemli yeniliklerden biridir.[26]

---

[22] Protokol İngilizce Orijinal Metni İçin bkz. http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f et. 27.01.2016.

[23] **HELVACIOĞLU**, s. 286.
[24] **WEBER**, s. 433.
[25] Tabi bunun sebebi, Komitenin söz konusu alanda uluslararası bir sözleşme akdetmek konusunda tecrübesiz olması ve söz konusu sistemin düzenlenmesinin siber suçlara ilişkin bir uluslararası sözleşme akdedilmesini önleyeceği düşüncesi olarak gösterilmektedir. **WEBER**, s. 433.
[26] **WEBER**, s. 434.

Sözleşme ile getirilen önemli bir düzenleme de verilerin korunmasıdır. 16. ve 17. madde ile düzenlenen verilerin korunması meselesinin önemi; verilerin kolaylıkla değiştirilebilmesi, bilgisayarla ilişkili suçların büyük çoğunluğunun bilgisayar sistemleri vasıtasıyla yapılan iletişim yayınlarından kaynaklanması, yasadışı içerik veya suça yönelik fiili kanıtlayacak verilerin muhafaza edilmesi, soruşturma bakımından delil niteliğindedir.[27]

c. Sözleşme'ye Getirilen Eleştiriler ve Değerlendirilmesi

Avrupa Konseyi Siber Suç Sözleşmesi'nin akdedilmesi bakımından hem olumlu hem de olumsuz eleştiriler karşımıza çıkmaktadır. Sözleşme'yi destekleyen yaklaşımlar, Sözleşme'nin devletlere iç hukuklarında siber suçu düzenleme ve cezalandırma ödevi yüklemesi bakımından, siber suçlarla mücadelede önemli bir adım teşkil ettiği ifade edilmektedir.[28]

Siber suçlarla mücadele en büyük sorun, devletlerin konuya ilişkin farklı iç hukuk düzenlemeleri olması ve hatta bazı devletlerde düzenleme olmamasıdır. Söz konusu durum da ancak ve ancak iç hukuk kurallarının uyumlulaştırılması ve farklı yargı yerleri arasındaki işbirliğinin sağlanması ile mümkündür.[29] Devletler arasında siber suçlarla mücadelede işbirliği ve uyumluluk olmaması durumu, bir süre sonra devletlerin tek taraflı olarak uzaktan adli bilişim soruşturması yapmasına ve siber suçlar üzerinde ülke dışı yargı yetkisi etmesine neden olacaktır. Söz konusu durum, nitekim Amerika – Rusya olayında olduğu gibi devlet egemenliğini tehdit eden bir hal alacaktır.[30]

Avrupa Konseyi Genel Sekreteri de, Sözleşme'nin siber suçlarla mücadele açık ve kapsamlı çözümler getirdiği, Asya-Pasifik Ekonomik İşbirliği, Avrupa Birliği, Interpol ve Amerika Devletleri Organizasyonu tarafından da oldukça desteklendiğini ifade etmiştir.[31]

Sözleşme'nin varlığına ilişkin olumlu eleştiriler yanında, Sözleşme'ye ilişkin kapsamlı ve ciddi olumsuz yaklaşımlar da söz konusudur. Hemen hemen her yazar Sözleşme'nin varlığının önemini yadsımaz iken, Sözleşme'nin getirdiği düzenlemeleri bazı hususlarda yetersiz, bazı hususlarda baskıcı ve kısıtlayıcı bulmaktadır.

Öncelikle Sözleşme'nin tadili oldukça zordur. Bu durumda hızla değişen ve gelişen teknoloji karşısında, siber suçların da değişim göstermesi, Sözleşme'nin siber suçluluğun gerisinde kalma gibi olasılık doğurmaktadır.[32]

Sözleşme çekinceye izin vermiş ve çekinceler maddesi altında, oldukça geniş bir perspektifte devletlere hareket alanı bırakmıştır.[33] Bunun yanında çekincelere çok geniş bir yelpazede izin verilmiş olması, Sözleşme'ye taraf devletlerin farklı konularda farklı yasama ve tedbirler

---

[27] **HELVACIOĞLU**, s. 290.
[28] **ARCHICK**, s. 3.
[29] **HARLEY, Brian**: "A Global Convention on Cybercrime?", **http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/ et: 05.01.2016.**
[30] ABD, Rusya'nın yardımı olmaksızın, kendi ülke sınırları dışında iki Rus hackerı Rusya serverleri üzerinden takip etmiş, kullanıcı adları ve şifrelerini öğrenerek, yaptıkları hackerlık faaliyetlerle ilgili delil elde etmiştir. Nitekim ABD'nin kendi ülkesel sınırları dışında yürüttüğü işbu faaliyetin hukuka uygunluğu tartışma konusu olmuştur. Ayrıntılı bilgi için bkz. **WEBER**, s. 428.
[31] Contribution of the Secretary General of the Council of Europe to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 16 Februrary 2010, **VATIS,** s. 219, dn. 100'den atfen.
[32] **ÖNOK,** s. 1245; **WEBER**, 2003, s. 442.
[33] **ÖNOK,** s. 1245.

öngörmeleri sonucuna yol açacaktır. Bu durumda Sözleşme'nin temel amaçlarından biri olan iç hukukların uyumlulaştırılması amacı da sekteye uğrayacaktır.[34]

Sözleşme aynı zaman da adli yardımlaşmanın reddedilmesine ilişkin olarak da geniş bir hareket alanı vermektedir. Söz konusu durum da Sözleşme'nin etkililiği açısından sorgulanmaktadır. Ancak adli yardımlaşma yükümü farklı olarak devletlerin egemenliği bakımından da eleştirilmektedir. Yani kimi görüşler adli yardımlaşmadaki işbirliğini yetersiz bulurken kimi görüşler baskıcı bulup, Sözleşme'nin adli yardımlaşmaya ilişkin düzenlemelerinin devlet egemenliği bakımından sorunsallık taşıdığını ifade etmektedir.[35]

Sözleşme metninin hazırlanması aşamasında, Avrupa Konseyi devletleri dışında yukarıda da belirtildiği üzere, sadece ABD, Kanada, Japonya ve Güney Afrika görüşmelere davet edilmiş, bunun dışında gelişmekte olan devletlerin görüşmelerde yeterince temsil edilmemiştir. Sorunun kaynağı siber suçları düzenleyen ve etkin bir şekilde kovuşturan gelişmiş devletler değil, siber suçlular için özgür hareket alanı oluşturan gelişmekte olan devletlerdir. Onların da aktif bir şekilde sisteme dahil olmaları siber suçlarla etkin mücadele açısından önem arz etmektedir.[36]

Sözleşme internet servis sağlayıcılarına verileri depolama ve dağıtma konusunda ödevler yüklemektedir. Söz konusu verilerin depolanması yükümü, verilerin depolanması zorunluluğu sebebiyle ortaya çıkan maliyet, ayrıca verilerin paylaşılması yükümlülüğüne ilişkin düzenlemelerin özel hayatın gizliliği ve kişisel verilerin korunmasına ilişkin sakıncalar doğurması eleştiri konusu edilmektedir.[37] Nitekim sivil toplum örgütleri Sözleşme'nin özel hayatın gizliliğine ilişkin hakları sınırlandırması ve idareye verilerin araştırması ve toplanması bakımından geniş bir hareket alanı vermesine karşı çıkmaktadır.[38] Sözleşme'nin internet servis sağlayıcıları üzerinde öngördüğü yükümlülük bakımından, ilgili maddenin yanlış yorumlandığı ve Sözleşme'nin aslında hazırlık soruşturmasında, yetkili mercilerin suçla ilgili olduğu tespit edilen verilere ulaşabilmek amacıyla, verilerin depolanmasını değil, verilerin korunmasını düzenlediği ifade edilmektedir.[39] Ancak ISS yükümlülükleri bakımından, söz konusu yorum kanımızca bir farklılık arz etmemektedir.

Sözleşme'nin öngördüğü soruşturma usullerinin temel hak ve özgürlüklere aykırı olduğunu savunan görüşler söz konusudur. Ancak Sözleşme'nin 15. Maddesinde, Sözleşme'de öngörülen yetki ve usullerin tanımı, yürürlüğe konulması ve uygulanması taraf devletlere bırakılmış olsa da, insan hak ve özgürlüklerinin gerekli ölçüde korunmasını sağlayacak ve orantılılık ilkesini yerine getirecek şart ve güvencelere tabi olması öngörülmüştür. Yani Sözleşme devletler bakımından belli bir ortak standartların olduğunu ve söz konusu ortak

---

[34] **WEBER**, 2003, s. 444

[35] Nitekim Rusya'nın Sözleşme'ye taraf olmaması ve Sözleşme nezdindeki temel eleştirilerinden birinin, Sözleşme'nin adli yardımlaşma hükümlerinin devlet egemenliğine müdahale teşkil ettiği görüşüdür. **ÖNOK,** 1259; **VATIS,** s. 218.

[36] **ÖNOK,** s. 1245.

[37] **HELVACIOĞLU**, s. 298; **MARION**, s. 705; **ÖNOK**, s. 1246; **SINAR**, Hasan, Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme, Prof. Dr. Çetin Özek Armağanı, Galatasaray Üniversitesi Yayınları, İstanbul, 2004, s. 780.

[38] **WALES,** Elspeth, Draft Council of Europe Cybercrime Convention Upsets Civil Rights Bodies, Computer, Fraud & Security, Vol. 2000, Issue: 12, December 2000, s. 7. Öyle ki Sözleşme'de öngörülen araştırma ve veri toplama serbestinin Amerikan Hukukunda izin verilmeyeceği savunulmaktadır. **ARCHICK**, s. 4; **MARION**, s. 705.

[39] Söz konusu görüş ABD hükümet birimleri tarafından savunulmuştur. Bkz. **SINAR,** s. 780.

standartların devletler tarafından göz önüne alınması yükümlülüğü olduğunu ifade etmiştir.[40] Sözleşme işbu ortak standartlar bakımından, Sözleşme 1950 Avrupa İnsan Hakları Sözleşmesi, 1966 Birleşmiş Milletler Medeni ve Siyasi Haklar Uluslararası Sözleşmesi ve diğer uygulanabilir uluslararası insan hakları belgelerine atıf yapmıştır. İlgili maddede kişisel verilerin korunması, ifade özgürlüğüne ve özel hayatın gizliliğine ayrıca atıf yapılmamıştır. Sözleşme'nin kişisel verilerin korunmasına ilişkin açıkça düzenleme içermemesi de, Sözleşme'nin otoriter yönünü ortaya koymaktadır.[41] Sadece Sözleşme'nin giriş kısmında herkesin müdahale olmaksızın düşünceye sahip olma hakkını, sınırlardan bağımsız olarak her türlü bilgi ve düşünceyi arama, alam ve iletme hakkı da dahil olmak üzere, ifade özgürlüğü, özel hayata saygı gösterme yükümlülüğü ile kanunların uygulanması arasında uygun bir dengenin sağlanması ihtiyacı dile getirilmiştir.[42]

Siber suçların işlenişi ve sonuçları itibariyle global bir sorun olması karşısında, Sözleşmenin bölgesel kalması da eleştirilmektedir.[43] Nitekim siber suçluluğun yoğun olduğu Yemen, Güney Kore gibi devletlerin Sözleşme'ye taraf olmamasının, Sözleşme'nin siber suçlarla mücadelede etkinliğini zedeleyeceği ifade edilmektedir.[44] İşbu durum Sözleşme'nin siber suçluluk bakımından caydırıcılığını da sekteye uğratmaktadır.[45]

Sözleşme'nin pek çok devlet tarafından imzalanmasına rağmen geç onaylanması ve onaylayan devletlerin aslında siber suçluluğa özgürlük sağlayan problematik devletler olmamasıdır. Yani asıl sözleşmeyi uygulaması gereken devletler, söz konusu mücadele sisteminin bir parçası değildir. Aynı şekilde siber suçla mücadele güçlü teknik, maddi ve personel altyapı gerektirmektedir. Adli bilişim araçlarının her devlette aynı seviyede gelişmiş olduğunu söylemek de mümkün değildir.[46]

Sözleşme'nin siber suçlulukla mücadelede önemli bir adım olmakla birlikte, uzun vadede sınırlı bir varlık göstereceği, çünkü Sözleşme'nin sembolik bir politikanın ürünü olduğu ifade edilmektedir.[47] Devletler bakımından; eleştirilerden biri devletlerin siber suçlarla mücadele farklı politikalarının olması, farklı teknik imkanlara sahip olmaları ve çifte cezalandırma ilkesinin kaldırılması bakımından da farklı suç tipleri öngörmüş olmalarıdır.[48]

Bunun yanında, sembolik politikanın ahlaki, diğer devletler nezdinde model olması ve suç işlenmesinde caydırıcılık fonksiyonları da bulunmaktadır. Bu bakımdan Sözleşmenin suçların kendisini bizzat düzenlemeyip düzenleme yükümü öngörmesi de, bu unsurları karşılayıp karşılamama bakımından sorun teşkil eder. Devletler nezdinde özellikle içerik bakımından siber suçları düzenleme yükümü getiren Sözleşme'nin ahlaki boyutu ve her devlet nezdinde siber suçluluğun yeknesak düzenlenmesi amacı model olma boyutunu karşılamaktadır. Ancak sözleşmenin, siber suçları düzenlemeyi yine de devletlere bırakması, Sözleşme'nin özellikle siber suçların maddi hukuk boyutu yününden caydırıcı olma unsurunu sekteye uğratmaktadır.

---

[40] **GÜNAYDIN, Barış**, İnternet Yayıncılığı ve İfade Özgürlüğü, Adalet, Ankara, 2010, s. 53- 54.
[41] **SINAR,** s. 781.
[42] Nitekim söz konusu durumun eleştirilebilir olmakla birlikte, Sözleşme'nin ilgili hakları korumadığını söylemenin doğru olmadığı ifade edilmektedir. **ÖNOK,** s. 1246.
[43] **WEBER**, 2003, s. 443.
[44] **HELVACIOĞLU**, s. 299.
[45] **ARCHICK**, s. 4.
[46] **MARION**, s. 704.
[47] *Marion,* Edelman'ın politikanın sembolik kullanımı teorisine atıf yapmaktadır. Buna göre sembolik politika ele alınan meseleyle ilgili, gerçekte önemli bir değişiklik yapılmamasına rağmen, kamuoyunda problemin gerçekten çözülmüş algısı yaratma politikasını ifade etmektedir. **MARION,** s. 702.
[48] **MARION**, s. 704.

Çünkü devletler, söz konusu sözleşme gereği maddi suçlardan hepsini düzenlemiş/düzenleyecek olabilecekleri gibi bir kısmını es geçebilirler. Nitekim bu durum sözleşmenin yeknesaklık amacına hizmet etmeyecektir.[49]

Bazı yazarlar Sözleşme'nin özellikle terörle mücadele bakımından yetersiz olduğunu ileri sürmektedirler. Nitekim Sözleşme'nin metninde içerikle bağlantılı suçlar bakımından siber terörizme yer verilmediği görülmektedir.[50] Ancak Avrupa Konseyi Terör Uzmanları Komitesi'nin 2008 yılında yayınladığı görüş metninde, internetin terörist faaliyetler için kullanılmasında ya da bizzat internet kanalıyla terör faaliyetinin gerçekleştirilmesiyle mücadele için ayrı bir Sözleşme'nin şimdilik gerekli olmadığı ifade edilmiştir. Bunun yerine, Siber Suç Sözleşmesi'nin ve Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesi'nin etkin bir şekilde uygulanmasının sağlanması ve internet servis sağlayıcılarının sorumluluğunun, özellikle içerik yayını bakımından, yeniden gözden geçirilmesinin gerekliliği vurgulanmıştır.[51]

Nitekim siber terör olarak ifade edilen faaliyetleri ikiye ayıracak olursak, özellikle siber saldırılara vücut veren fiillerin pek tabi Sözleşme ile yasaklanan yasadışı erişim, yasadışı araya girme, verilere müdahale gibi suçların kapsamında bilişim suçu olarak nitelendirilip soruşturulması ve kovuşturulması mümkündür. Ancak içerik bakımında terör faaliyetlerinin ve örgütlerin propagandasını yapan yayınların, bilişim suçu kapsamında değerlendirilmesi, ancak bunların içerik yönünden bilişim suçu kapsamına sokulması ile mümkün gözükmektedir. Sözleşme'nin de bu noktada, işbu hususu eksik bıraktığını söylemek kanımızca yanlış olmayacaktır.[52]

Siber terörizmle mücadelenin hukuken düzenlenmesi yanında teknik, yasal ve operasyonel zorluklar da barındırdığı ifade edilmektedir.[53] Siber terörizm için kullanılan birtakım fiillerin Sözleşme kapsamına sokularak, Sözleşme'nin bilişim suçları ile mücadelede öngördüğü uyumlaştırma ve adli işbirliği hükümlerinin siber terörizmle mücadele etmek bakımından önem arz ettiğini söylemek yanlış olmayacaktır.[54]

---

[49] **MARION**, s. 707.

[50] **ÖZCAN, Mehmet,** Siber Terörizm ve Ulusal Güvenlik, içinde İnternet ve Hukuk, İstanbul (Yeşim ATAMER ed.), Bilgi Üniversitesi Yayınları, 2004, s. 310.

[51] Committee of Experts on Terrorism (CODEXTER) Opinion of the Committee of Experts on Terrorsim Fort he Attention of the Committee of Ministers on Cyberterrorism and USe of Internet for Terrorist Purposes, 27-28, February 2008, https://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf et: 27.01.2016, s. 3. Bunun yanında Standford Üniversitesi'nin siber terörizmi özel olarak düzenleyen Siber Suç ve Terörizm Hakkın Uluslararası Sözleşme Taslağı da, siber terörizmin düzenlenmesine ilişkin tartışmaların merkezinde yer almaktadır. Metin için bkz. http://cisac.fsi.stanford.edu/publications/proposal_for_an_international_convention_on_cyber_crime_and_terrorism_a et. 27.01.2016.

[52] Nitekim Avrupa Konseyi Terör Uzmanları Komitesi'nin yayınlarıdığı görüşde de benzer durum dile getirilmiştir. Committee of Experts on Terrorism (CODEXTER) Opinion of the Committee of Experts on Terrorsim Fort he Attention of the Committee of Ministers on Cyberterrorism and USe of Internet for Terrorist Purposes, 27-28, February 2008, https://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion_%20E.pdf et: 27.01.2016, s. 1.

[53] **ÖZCAN,** s. 325- 335.

[54] Siber terörizm faaliyetlerinden birini oluşturan siber atak, sadece bilişim suçları bakımından değil, uluslarlararası barış ve güvenliğin korunması bakımından da önem arz etmektedir. Dolayısıyla, ceza hukuku hükümleriyle bireylerin soruşturulması ve kovuşturulması değil, genel olarak faaliyetin kendisinin bir güvenlik meselesi olarak görülüp devletlerin işbirliği ile engellenmesi gündemdedir. İşbu mesele, özellikle 2008 yılından beri NATO'nun gündeminde olup, siber güvenliğin, teşkilatın önemli ortak savunma konularından birini teşkil ettiği ifade edilmiş ve siber saldırıları takip etme ve savunma amacıyla çeşitli merkezler kurulmuştur. Ayrıntılı bilgi için bkz. http://www.nato.int/cps/en/natohq/topics_78170.htm et.26.01.2016.

Sözleşme'nin, taraf devletlerin yükümlülüklerini yerine getirip getirmediğini denetleyen bir yürütme ve yaptırım mekanizması olmaması da eleştiri konusu edilmektedir. Nitekim taraf devletlere Sözleşme'yi uygulamak bakımından mevcut durumlarını raporlama zorunluluğu getirilmesi işbu eksikliği gidermeye yardımcı olabilir.[55]

Sözleşme'nin işbu haliyle uyumlaştırmadan ziyade baskı aracı haline geldiği ifade edilmekte, siber suçları düzenleyen bir uluslararası antlaşma yerine alternatif model bir siber suç kanunun oluşturulup, devletlerin söz konusu modeli göz önüne alarak kendi iç hukuklarını düzenlemelerinin teşvik edilmesinin daha etkili bir çözüm olacağı ifade edilmektedir. Söz konusu modelin yaygınlaşması, amaçlandığı üzere devletler arasında siber suçlarla ilgili iç hukuk düzenlemelerinin uyumlulaştırılmasını kolaylaştıracak ve teknolojik gelişmeler karşısında iç hukuk düzenlemelerinin tadilinin daha kolay olması sebebiyle, model kanunun geride kalma tehlikesi de bertaraf edilebilecektir.[56]

Bunun yanında her bir devletin iç hukuk kanunları çıkarmasının ya da yeni antlaşmalar akdedilmesinin siber suçlulukla mücadelede yeterli olmadığı, yasama faaliyetleri dışında daha kapsamlı politikaların yürütülmesi gerektiği de önerilmektedir. Özellikle siber suçlarla mücadele açısından güvenlik güçleri arasındaki işbirliğinin geliştirilmesi gerektiği ve Interpol gibi kuruluşların, siber suçlulukla mücadelede, bilgi değişimini ve uluslararası işbirliğini sağlamak bakımından daha etkin bir rol oynamaları gerektiği ifade edilmektedir.[57] Bunun yanında Sözleşme'nin sembolik olması dolayısıyla uzun vadede etkililiğinin sorgulanması gerekeceği, Sözleşme'nin daha etkili hale getirilmesi adına, Sözleşme'de açık ve net olmayan düzenlemelerin giderilmesi ve Sözleşme'nin daha geniş çapta onaylanıp uygulanmasının sağlanması gerektiği savunulmaktadır. [58]

Model siber suç kanunu önerisini değerlendirecek olursak, öneri, samimi ve idealist olmakla birlikte, uluslararası toplumun yapısını göz önüne aldığımızda, önerinin gerçekçilikten uzak olduğu söylenebilir. Öncelikle, uluslararası toplumun temel süjesi olan devletler, her ne kadar devlet merkezci eski klasik uluslararası hukuk yaklaşımı etkinliğini azaltmış olsa da, özellikle uluslararası hukuk kurallarının oluşumunda temel irade sahibidirler. Devletleri, bir uluslar arası antlaşma altında toplayıp, o uluslar arası antlaşmaya uygun davranmalarını sağlamak bile güç bir işken, genel- geçer uyumlu bir kanunlaştırma hareketi neredeyse imkansız gibidir. İkinci husus, söz konusu kanunlaştırma hareketinde, hangi modelin örnek alınacağının belirsiz olmasıdır. Söz konusu durum, diğer gelişmiş devletlerin uyumlaştırma hareketine destek vermesini zora sokabilecektir.

İkincisi, söz konusu kanunlaştırma ve uyumlulaştırma hareketinde, iç hukuk kurallarının değiştirilmesi, uluslararası hukuk kurallarının (gerek uluslararası antlaşmaların, gerek uluslararası örf ve adet hukuku kurallarının) değiştirilmesinden daha kolay gerçekleşecektir. Ancak, işbu durum iç hukuklar arasındaki uyumu bozacak sonuçlara yol açabilir. Nitekim devletler istedikleri zaman kendi iç hukuklarında birbirleriyle uyumlu olmayan değişiklikler yapabilir ve devletlerin siber suç kanunları bir süre sonra farklılık arz edebilecektir.

---

[55] **VATIS**, s. 217.

[56] *Weber* burada, genel geçer bir siber suç kanunun bütün problemleri bitirecek nitelikte olmadığını ve böyle ortak bir kanunlaşma hareketinin uzun zaman alabileceğinin farkında olduğunu ifade etmektedir. **WEBER**, s. 445.

[57] **MARION**, s. 708.

[58] **MARION**, s. 709.

Siber Suç Sözleşmesi'nin uzun vadede özellikle de bölgesel kalması nedeniyle etkinliğinin sorgulanması gerektiği eleştirisine biz de katılmaktayız. Ancak bölgesel bir örgüt tarafından akdedilen Sözleşme'nin nasıl global bir boyut kazanacağı da sorgulanması gereken bir husustur. Kanımızca Siber suç Sözleşmesi'nin düzenlemelerini ve eleştirileri ışığında, yapılması gereken husus, bölgesel değil evrensel bir uluslararası sözleşme akdedilmesi olmalıdır. Söz konusu sözleşme pek ala Birleşmiş Milletler nezdinde akdedilebilir.[59] Avrupa Konseyi'nin işbu sözleşmenin akdedilmesi ve yürürlüğe girmesinden bu yana edinilen tecrübeden de faydalanılarak yeni bir sözleşme akdedilebilir.[60]

d. Sözleşmenin İç Hukuk Yönünden Etkileri ve Türkiye

Siber Suç Sözleşmesi yukarıda da bahsettiğimiz üzere, devletlere ilgili konularla ulusal mevzuatlarını düzenleme ve gerekli tedbirleri alma yükümü getirmiştir. Yani Sözleşme, farklı bir sistematik izleyerek, kuralın kendisini bizzat koymayıp, devletlere ulusal mevzuatlarını nasıl düzenlemeleri gerektiğine ilişkin bir çerçeve sunmuştur.

Yukarıda da belirttiğimiz üzere Sözleşme'nin en çok eleştirilen hususlarından biri olan çekinceler meselesi bakımından da Türkiye'nin Sözleşme'nin uygulanması bakımından koyduğu beyan ve çekincelerden bahsetmek mümkündür. Buna göre Türkiye;

- 40. madde ve 2. maddeye istinaden, suçun bilgisayara verilerini elde etmek veya başka bir sahtekar niyetler veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koştuğunu beyan etmiştir.

Söz konusu beyan maddede öngörüldüğü gibi özel nitelikli bir fiile ilişkin olup, yasadışı erişim için kişinin özel olarak güvenlik tedbirlerini aşmasını suçun maddi unsuru bakımından gerekli gören bir düzenleme getirmek gerekecektir.

- 40. madde ve 7. maddeye istinaden; bilgisayarla bağlantılı sahteciliğe ilişkin Madde 7'deki suç tanımının Türk kanunlarına göre dolandırma veya benzeri hileli davranış kastını gerektirdiğini beyan etmiştir.

Söz konusu beyanla birlikte, bilgisayarla bağlantılı sahtecilik için genel kast yanında özel kast getirilmiş olmaktadır.

- 42. madde ve 14. maddenin 3(b) paragrafına istinaden, Türkiye Cumhuriyeti Devleti herhangi bir hizmet sağlayıcının bilgisayar sistemi üzerinden iletişime ilişkin olarak, söz konusu sistemin belirli bir kullanıcı grubunun menfaatine işletiliyor olması; halka açık iletişim şebekelerini kullanmıyor olması ve halka açık ya da özel nitelikli başka bir bilgisayar sistemine bağlı olmaması halinde, söz konusu aktarıma ilişkin olarak 20. ve 21. maddelerde belirtilen önlemleri uygulamama hakkını saklı tutar.

---

[59] Benzer görüş için bkz. **MARION,** s. 708.

[60] Nitekim Birleşmiş Milletler Uyuşturucu ve Suç Ofisi tarafından hazırlanan raporda, siber suçlulukla mücadelede uluslararası bir sözleşme akdedilmesinin göz önüne alınması gerektiği ifade edilmiştir. Bkz. Working Paper on Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime, 12- 19 April, 2010. http://www.unodc.org/documents/crime-congress/ 12th-CrimeCongress/Documents/A_CONF.213_9/V1050382e.pdf et: 27.01.2016.

Türkiye işbu çekince beyanıyla, trafik verilerinin gerçek zamanlı toplanması ve içerik verilerinin takibi gibi, siber suçlulukla mücadelede servis sağlayıcıları nezdinde öngörülen yükümlülüklerin bazı sistemler bakımından vareste tutulmasını sağlayacaktır. Dolayısıyla, siber suç işlense dahi, işbu suçun takibi, servisin belli bir kullanıcı grubunun menfaati gibi muğlak bir gerekçe nedeniyle mümkün olmayacaktır.

- 42. madde ve 22. maddeye istinaden, TC devleti, Türk vatandaşının yurt dışında işlemiş olduğu suçlardan dolayı TCK'nın 11. ve 13. maddeleri çerçevesinde yargı yetkisini kullanma hakkını saklı tutar.

Bu durumda Türkiye siber suçlar üzerindeki kişi bakımından yargı yetkisini, diğer devletlerin yarı-ülkesel yargı yetkisine üstün tutacak şekilde kullanacaktır.

- 42. ve 29. maddenin 4 paragrafına istinaden, Türkiye Cumhuriyeti devleti, çifte suçluluk şartının verilerin açıklandığı tarihte yerine getirilemiyor olduğuna ilişkin gerekçeler bulunması halinde, işbu madde çerçevesinde verilerin korunması talebini reddetme hakkını saklı tutar.

Söz konusu çekince ile birlikte, Türkiye'de siber suç olarak düzenlenmeyen bir suça ilişkin olarak Türkiye'ye iletilen adli yardım talepleri, Türkiye tarafından geri çevrilebilecektir. Bu bakımdan, siber suçlulukla mücadelede karşılaşılan zorluklardan biri olarak adlandırılan çifte suçluluk şartı işbu çekince ile korumuş olmaktadır.

Bunun yanında, Sözleşme'nin Türkiye'de onaylanması esnasında oluşan çeviri farklılığına dikkat çekmek gerekmektedir. Buna göre Sözleşme'nin orijinal metninin 5. maddesinde, sistemlere müdahale suçunda bahsedilen engellemenin "ciddi" olması gerekmektedir ve söz konusu ciddiyet tanımının da taraf devletlerce yapılması kararlaştırılmıştır.[61] Burada problematik olan iki husus olduğunu düşünmekteyiz.

1. Öncelikle ciddi engellemedeki ciddiyet unsurunun değerlendirilmesinin taraf devletlere bırakılması kanımızca Sözleşme'yle *reason d'etre*'sini oluşturan mevzuat yeknesaklaştırmasına tezat oluşturmaktadır.
2. İkinci önemli husus da Sözleşme'nin Türkçe çevirisi ile İngilizce orijinal metnindeki farklılıktır. Şöyle ki, İngilizce orijinal metinde yukarıda da yer verdiğimiz üzere ciddi engellemeden bahsedilmektedir.

Türkçe metinde; *"taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişini haksız yere engellenmesinin, kasten gerçekleştirildiği zaman kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir."*

İngilizce metinde ise; *"each party shall adopt such legislative and other measure as may be necessary to establish as criminal offences under its domestiv law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or supressing computer*

[61] **HELVACIOĞLU**, s. 285.

data."

Söz konusu iki metindeki farklılık sorun arz etmektedir. çünkü Türk sistemi Sözleşme'de suçun bir unsuru yer alan bir kritere hiç yer vermeyerek, suçu oluşturan fiilin kapsamını değiştirmiş olmaktadır. Bu bilinçli bir tercih midir yoksa bir çeviri hatası mıdır bilinmez, ama ilgili maddenin uygulanması bakımından hangi metnin baz alınacağı tartışma teşkil edecektir. Kanımızca, Sözleşme'nin orijinal metninin İngilizce olması dolayısıyla, Türk yasa koyucusunun Sözleşme uyarınca sisteme müdahale suçunu iç hukukta düzenlerken, orijinal metni baz alarak veriyi bilgisayara sisteminin işleyişinin kasten, haksız ve ciddi engellenmesi olarak düzenlenmesi gerektiği kanaatindeyiz.

3. AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİNİN İÇ HUKUK YÖNÜNDEN ETKİLERİ

a. Genel Olarak

Avrupa Konseyi Siber Suç Sözleşmesi, taraf devletler arasında ortak bir "bilişim suçları" dili oluşturmayı, buna göre ulusal bazda yapılacak düzenlemeleri yeknesak hale getirmeyi ve bu devletler arasında ortak bir adli işbirliği rejimi oluşturabilmeyi hedeflemektedir. Bu itibarla, Sözleşmenin uluslararası hukuk yönünden önemi kadar, iç hukuk yönünden doğurduğu etkilerin incelenmesi de önemlidir.

Sözleşmede metnin amacı dört ana başlık altında düzenlenmiş olup, Sözleşme hükümlerinin iç hukuk yönünden etkilerini de bu minvalde değerlendirmek gerekecektir:

i. Siber alanda işlenen suçlarla ilgili ortak tanımlar yapmak,
ii. Devletler arasında maddi ceza hukuku normlarını uyumlulaştırmak,
iii. Suçların soruşturulması ve kovuşturulması için yerel usul hukuku yetkileri sağlamak,
iv. Uluslararası adli işbirliği rejimi oluşturmak.

b. Sözleşmede Öngörülen Maddi Ceza Hukuku Kuralları ve Bunların Türk Ceza Hukuku Yönünden Etkileri

Sözleşmenin 2. Bölümünde, 2 ilâ 10. maddeler arasında, esas itibariyle dört grup suçun düzenlendiği görülmektedir. Bunlar; bilişim sistemlerine yasadışı erişim (m. 2), sisteme veya veriye müdahale (m. 4-5), yasadışı araya girme (m. 3), bu suçların işlenmesi için cihaz (donanım) üretimi ve bunların kötüye kullanılması (m. 6) gibi bilişim suçları; bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen sahtecilik (m. 7) ve dolandırıcılık (m. 8) suçları; çocuk pornografisiyle bağlantılı suçlar (m. 9); telif hakkı ve bununla bağlantılı fikri mülkiyet haklarının ihlaline ilişkin suçlar (m. 10) olarak sayılabilir. Sözleşmenin 11. maddesinde ise, "suça etki eden nedenler" olarak teşebbüs ve iştirak düzenlenmiş olup, bu madde ile de taraf devletlerin yukarıda sözü edilen suçlara teşebbüs edilmesinin ve iştirak halinde bu suçların işlenmesinin de ceza yaptırımına bağlanması için gerekli tedbirlerin alınması şart koşulmuştur. Ancak bu kurumlar zaten TCK'nun genel hükümler kısmında, bütün suçlar yönünden düzenlendiğinden, çalışmamızda ayrıca tartışma konusu yapılmayacaktır.

Sözleşme, taraf devletleri, burada düzenlenen fiilleri ulusal mevzuatlarında suç olarak düzenlemekle yükümlü kılmaktadır. Burada bahsi geçen yükümlülük söz konusu düzenlemelerin birebir olarak ulusal mevzuata aktarılması değildir. Ulusal ceza hukuku

mevzuatlarında, içerik olarak, burada öngörülen fiillerin suç olarak düzenlenmesi yeterli görülmektedir. Ancak Portekiz gibi bazı ülkeler, Sözleşmedeki hükümleri kelimesi kelimesine iç mevzuatlarına aktararak, 'Siber Suç Kanunu' çıkarmayı tercih etmişlerdir[62].

Sözleşmede yer alan fiiller genel olarak Türk Ceza Kanunu'nda düzenlenmiş olmakla birlikte, ulusal mevzuatımızdaki düzenlemelerin Sözleşme hükümlerini doğrudan karşıladığını söylemek güçtür. Sözleşme'nin 2. maddesinde yer alan yasadışı erişim, TCK'nun 243. maddesinde yer alan 'Bilişim Sistemine Girme' suçunun karşılığıdır. Ne var ki, Sözleşme hükmü, bir kimsenin bilişim sistemlerine yasadışı, yani hukuka aykırı olarak 'girme'yi suç olarak sayarken, TCK m. 243'deki suçun maddi unsuru *"bir bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme"* olarak öngörülmüştür. TCK m. 243'ün bu düzenlemesi, şüphesiz ki, suçun niteliğini de değiştirmiştir. Zira, madde, bilişim sistemine girme ve orada kalmaya devam etmeyi suç olarak öngördüğü için, suç bir *'mütemadi (kesintisiz) suç'* halini almış ve suçun tamamlanabilmesi için sisteme girmek yeterli sayılmayarak, dolayısıyla suçun tanımının kapsamı daraltılarak, sisteme girme sonrasında belirli bir süre orada kalma şartı aranmıştır[63]. Bu itibarla, TCK'ndaki düzenleme bilişim sistemine yasadışı veya yetkisiz erişimin kapsamını Sözleşme'nin 2. maddesindeki düzenleye göre daha sınırlı tuttuğu için, bu düzenleme ile Sözleşmenin Türkiye'ye yüklediği yükümlülük iç hukukta yerine getirilmemiştir. Yükümlülüğün yerine getirilmesi için, TCK m. 243'teki düzenlemenin, TCK m. 116'daki konut dokunulmazlığının ihlali suçundaki lafza benzer bir biçimde, *"bir bilişim sistemine hukuka aykırı olarak giren veya sisteme hukuka uygun olarak girdikten sonra hukuka aykırı olarak orada kalmaya devam eden"* şeklinde değiştirilmesi gerektiği kanaatindeyiz.[64]

Sözleşmenin 3, 4 ve 5. maddelerinde düzenlenen, online yasadışı müdahale ve bilişim sistemlerine veya verilere müdahale eylemleri, TCK'nun 244. maddesinde yer alan suç ile büyük oranda örtüşmektedir. TCK m. 244'ün birinci fıkrasında bilişim sistemine müdahale, ikinci fıkrasında ise sistemin içerisinde yer alan verilere müdahale eylemleri suç olarak düzenlenmiştir. Sözleşmenin ilgili maddelerinde de genel olarak bu eylemler suç olarak düzenlenmekte ise de, özellikle Sözleşmenin 3. maddesinde, bilişim sistemleri aracılığıyla olmasının dışında, elektromanyetik dalgalar ve benzeri online yöntemlerle araya girme, bir başka deyişle bilişim sistemine erişim sağlama fiili de ayrıca düzenlenmişken, TCK m. 244'te bu eylem doğrudan düzenleme alanı bulmamıştır. Kanaatimizce TCK m. 243 veya 244'e bu yönde bir fıkra eklenmesi Sözleşme ile yüklenen yükümlülüğün yerine getirilmesi için gerekli ise de, TCK'nun mevcut hali de, online yöntemlerle araya girme durumunda, verilere müdahale olup olmamasına göre, TCK m. 243 veya 244/2 uyarınca failin cezalandırılmasında yeterli olacaktır.

Sözleşmenin 6. maddesinde, yukarıda düzenlenen suçların icrasında kullanılacak cihazların üretimi, satışı, tedariki, ithali, dağıtımı veya başka bir şekilde erişilebilir hale getirilmesi de suç olarak düzenlenerek, ulusal mevzuatlarda buna uygun düzenlemeler yapılması öngörülmüştür. Sözleşme, bu hükmün kapsamını, 2 ilâ 5. maddedeki suçların işlenmesinde kullanılacak donanımın yanı sıra, bir bilgisayar sisteminin tamamına veya bir kısmına erişimi mümkün kılan bilgisayar şifresi, erişim kodu veya benzeri her türlü veriyi almıştır.

---

[62] **ÖZBEK, Mücahid**, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", s. 79, (http://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf), 24.01.2016.

[63] **KETİZMEN, Muammer**, Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008, s. 107; **KARAGÜLMEZ, Ali**, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara, 2005, s. 170.

[64] Burada Türkiye'nin 2. maddeye getirdiği beyanı da göz önüne almamız gerekiyor.

Dolayısıyla, bilgisayarlara uzaktan erişimi mümkün kılan *remote viewer* yazılımları ve buna benzer, yukarıdaki suçların işlenmesine yarayacak veya bunları kolaylaştıracak donanım ve yazılımların bulundurulması da suç olarak düzenlenmiştir. Ancak bu hüküm, ceza hukuku mevzuatımızda suç olarak düzenlenmemiş ve bu husus doktrinde ciddi bir eksiklik olarak değerlendirilmiştir[65].

Türk Ceza Hukukunda, hazırlık hareketleri, suç olarak değerlendirilmemekte ve ceza sorumluluğunun dışında tutulmaktadır. Zira, hazırlık hareketleri esnasında ortada ceza hukuku anlamında, kanunun öngördüğü suç tipini ihlal eden bir fiil mevcut olmadığından, cezalandırılabilir bir davranıştan söz etmek de mümkün değildir[66]. Sözleşmenin 6. maddesinde yer alan eylemlerin de, henüz ortada işlenen bir suç olmadığından ve bu suçların işlenmesinde kullanılacak araçların temini veya bulundurulması düzenleme konusu yapıldığından, hazırlık hareketleri olduğu şüphesizdir. Bu nedenle, kanun koyucunun bu eylemleri suç olarak düzenlememesinin, hazırlık hareketlerinin ceza yaptırımı dışında olacağı yönündeki temel cezalandırılma ilkesine uygun olduğu söylenebilir.

Ancak kanun koyucu, kimi istisnai durumlarda hazırlık hareketlerini bağımsız bir suç olarak düzenlemekte ve cezai yaptırım kapsamına almaktadır. Bu tür durumlarda kanun koyucuya göre, hareketin özelliği veya failin tehlikeliliğini ortaya koyma biçimi, hazırlık hareketlerinin bağımsız bir suç olarak yasada tanımlanması gerekliliğini doğurmaktadır[67]. Örneğin, TCK madde 227/1'de düzenlenen "fuhuş yapmaya teşvik" suçunda yahut TCK madde 314/1'de düzenlenen "suç işlemek için silahlı örgüt kurma" suçunda cezalandırılması öngörülen hareketler, esasen bir başka suç için gerekli olan (fuhuş yapma suçu veya örgüt bünyesinde işlenen silahlı suçlar) hazırlık hareketleridir. Buna karşın kanun koyucu, söz konusu fiillerin başlı başına tehlikeliliğini öngörerek, toplumun korunması adına bunların cezalandırılmasını gerekli görmüştür[68]. Bu bağlamda, özellikle siber suçlarla mücadelede suçluların tespit edilip cezalandırılması kadar ve belki ondan daha çok, suçların önlenmesi de büyük önem arzettiğinden, kanun koyucunun Sözleşmeye uygun bir biçimde, fakat sınırlarını iyi çizmek suretiyle, Sözleşmenin 6. maddesi uyarınca bir ceza normu düzenlemesi ve belirli koşullarda bahsi geçen cihazların temini ve kullanmak için bulundurulması eylemlerini de suç olarak düzenlemesi gerektiği kanaatindeyiz.

Sözleşmenin 7. ve 8. maddelerinde düzenlenen bilişim sistemleri araç olarak kullanılmak suretiyle işlenen sahtecilik ve dolandırıcılık suçları ise, çalışmamızın giriş bahsettiğimiz iki kategori halinde değerlendirilen bilişim suçlarından, "*bilişim aracılığıyla işlenen suçlar*" kategorisine girmektedir. Zira, bilişim alanında işlenen suçlar salt bilişim suçu olup kanunda özel olarak öngörülen fiillerken, bu ikinci kategori suçlar sınırlı sayıda olmayan, bilişim sistemlerinin araç olarak kullanılabileceği her suçu kapsamına alan suçlardır. Bu bağlamda, Sözleşmenin 7. maddesinde düzenlenen sahtecilik suçları, TCK'nun 204 ilâ 212. maddeleri arasında düzenlenen resmi ve özel belgede sahtecilik suçlarının, bilişim sistemleri aracılığıyla, verilere müdahale edilmek suretiyle işlenen hallerinden ibaret olup, bu yönüyle TCK hükümlerinin Sözleşmedeki düzenlemeyi büyük ölçüde karşıladığı söylenebilir. Ancak yine

---

[65] **DÜLGER, Murat Volkan**; "Avrupa Siber Suç Sözleşmesi ile Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nun Karşılaştırılması", s. 13.

[66] Buna ilişkin tartışmalar için bkz. **ARTUK, Mehmet Emin / GÖKÇEN, Ahmet / YENİDÜNYA, Caner**, Ceza Hukuku Genel Hükümler I, Ankara, 2002, s. 760; **TANER, Tahir**, Ceza Hukuku Umumi Kısım, İstanbul, 1953, s. 264-265.

[67] **CENTEL, Nur / ZAFER, Hamide / ÇAKMUT, Özlem**, Türk Ceza Hukukuna Giriş, İstanbul, 2006, s. 450; **ÖNDER, Ayhan**, Ceza Hukuku Dersleri, İstanbul, 1992, s. 391; **TANER**, s. 265.

[68] **CENTEL / ZAFER / ÇAKMUT**, Türk Ceza Hukuku, s. 450.

de, özellikle işbirliği hükümleri yönünden mevzuatın uyumlulaştırılması ve uygulamada yeknesaklık sağlanabilmesi adına, bu suçların bilişim sistemleri vasıtasıyla işlenmesine yönelik TCK'nda düzenleme yapılmasının doğru olacağı kanaatindeyiz.

Dolandırıcılık suçu yönünden ise, TCK'nun 158/1. maddesinin (g) bendinde, dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi, suçun nitelikli hali olarak düzenlenmiştir. Bu bağlamda, TCK'nun bu hükmünün, Sözleşmenin 8. maddesi ile öngörülen yükümlülüğü yerine getirdiğini söylemek mümkündür.

Sözleşmede düzenlenen bir diğer suç ise, 9. maddedeki çocuk pornografisiyle bağlantılı suçlardır. İlgili hüküm, beş bent halinde, bir bilgisayar sistemi üzerinden dağıtımını yapmak üzere çocuk pornografisi üretme, bunları sunma veya erişilebilir hale getirme, bunların dağıtım ve iletimlerini yapma, kendisi veya başkası için bilgisayar üzerinden çocuk pornografisi temin etme ve bilgisayar sistemi ve bunların depolama aygıtlarında çocuk pornografisi bulundurma eylemlerini kapsama almış ve taraf devletlere bu fiilleri ulusal mevzuatlarında düzenleme yükümlülüğü getirmiştir. Ayrıca, maddenin ikinci fıkrasında, çocuk pornografisinin tanımı da yapılmış, buna göre, bir görselde gerçekten reşit olmayanların cinsel içerikli eylemlerde bulunmaları veya reşit olmayan şahıs görüntüsüne sahip kişilerin cinsel içerikli eylemlerde bulunmaları yahut reşit olmayan şahsın cinsel içerikli eylemlerde bulunmasını betimleyen gerçekçi görüntüler, çocuk pornografisi olarak tanımlanmıştır. Üçüncü fıkrada ise, "reşit olmayan" ibaresinin onsekiz yaşının altındakileri kapsadığını, ancak taraf devletlerin bu sınırı, onaltıdan az olmamak üzere daha aşağı çekebilecekleri kabul edilmiştir. Çocuk pornografisi suçu, uluslararası alanda adli makamların suçlulukla mücadelede en önem verdikleri ve bu nedenle de hızla aksiyon alınabilmesini gerektiren bir suç tipidir. Bu nedenle, taraf devletlerin mevzuatlarında bu eylemlerin ve buna ilişkin alınacak tedbirlerin düzenlenmesi büyük önem taşımaktadır.

Çocuk pornografisi, TCK'nun 226. maddesinde '*Müstehcenlik'* ana başlığı altında düzenlenmiştir. Esasen hükmün içeriği doğrudan pornografi ile ilgili olmasına rağmen, kanun koyucu ucu son derece açık bir biçimde '*müstehcenlik'* tabirini kullanmayı tercih etmiştir. Oysa, müstehcenlik kavramının içeriği ve anlamı, devirden devire, ülkeden ülkeye, kültürden kültüre, hatta aynı ülke içindeki bölgeden bölgeye değişebilmektedir[69]. Dolayısıyla, TCK m. 226'nın başlığının '*Müstehcenlik'* yerine '*Pornografi'* olarak değiştirilmesinin, suçun kapsamı ve niteliğinin belirlenmesi açısından daha doğru olacağı kanaatindeyiz[70].

Her ne kadar çocuk pornografisi ile ilgili eylemler TCK m. 226'da düzenlenmekteyse de, çocuk pornografisinin, özellikle Siber Suç Sözleşmesi'nin 9. maddesi örnek alınarak ayrı bir suç tipi olarak düzenlenmemesi Sözleşme ile Türkiye'ye yüklenen yükümlülüğün tam olarak yerine getirilmemesi anlamını taşımasının yanı sıra, TCK bakımından da önemli bir eksiklik oluşturmaktadır[71]. Ayrıca gelişen bilişim teknolojisiyle, çocuk pornografisi içeren görüntüler hızla yayılmakta, kolluk kuvvetleri suç teşkil eden görüntüye ulaşsalar da, görüntü hızla yayılabildiğinden kaynağına ulaşamamaktadır. Bunun yanı sıra, İnternet, çocuk istismarcısı ve pedofil kişilerin birbirini kolayca bulmalarına ve suç alanının genişlemesine de olanak sağlamaktadır[72]. Bunun yanı sıra, TCK m. 226'da çocuk pornografisinin kapsamını veya

---

[69] **YARSUVAT, Duygun**; "*Müstehcenliğin Neresindeyiz?",* Güncel Hukuk Dergisi, S. 9, İstanbul, Eylül 2004, s. 49.
[70] **DÜLGER,** Bilişim Suçları, s. 641.
[71] **DÜLGER**, Bilişim Suçları, s. 641.
[72] **SOKULLU-AKINCI, Füsun**, *"Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi",* İÜHFM, C. 59, S. 1-2, İstanbul, 2001, s. 38.

tanımını öngören bir düzenleme de bulunmamaktadır. Ayrıca, çocuk pornografisinin ayrı bir suç tipi olarak düzenlenmemiş olmasının Türkiye'nin diplomatik ilişkilerinde de kimi sorunlara yol açtığı söylenmektedir[73].

Bütün bu nedenlerle, bilişim sistemleri üzerinden işlenen çocuk pornografisi eylemlerinin, Sözleşmenin 9. maddesi düzenlemesine paralel bir biçimde, ayrı bir suç tipi olarak düzenlenmesi gerektiği kanaatindeyiz.

Son olarak Sözleşmenin 10. maddesinde, taraf devletlerin, telif hakları ihlalinin kasıtlı olarak, ticari ölçekte ve bir bilgisayar sistemi aracılığıyla işlenmesinin ulusal mevzuatlarında suç olarak düzenlenmesi gerektiğini öngörmektedir. Telif haklarının ihlaline ilişkin suçlar, bunlara ilişkin hukuki koruma hükümleri ve cezai yaptırımlar 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 71 ilâ 75. maddeleri arasında ayrıntısıyla düzenlenmiş olup[74], buna göre Sözleşmenin 10. madde hükmünün Türk mevzuatı yönünden FSEK'ndaki düzenlemelerle karşılandığını söylememiz mümkündür.

c. Sözleşmede Öngörülen Ceza Usul Hukuku Kuralları ve Bunların Türk Ceza Usul Hukuku Yönünden Etkileri

Sözleşmenin 14 ilâ 21. maddeleri arasında, ceza usul hukuku kuralları düzenlenmiş ve taraf devletlere, ulusal mevzuatlarında buna paralel düzenlemeler yapma yükümlülüğü getirilmiştir. Öncelikle 14. maddede, Sözleşmede öngörülen koruma tedbirlerinin kapsamı belirtilmiş ve sadece bilişim alanındaki suçlar yönünden değil, herhangi bir suçun delillerinin elektronik ortamda bulunması durumunda da bu tedbirlerin uygulanacağı öngörülmüştür. Zira bilişim suçlarının soruşturulmasında ve elektronik aygıtlar üzerinde bulunan verilerin herhangi bir bilinmezi aydınlatmasının umulduğu durumlarda, faillerin veya eylemlerinin sunucular (*serverlar*) üzerinde bıraktığı iz, delil ve işaretler (*log kayıtları*) son derece hayati önem taşırlar. Bu kayıtların bir çoğu uçucu (*volitale*) veya kısa zamanda silinmesi muhtemel delillerdir. Sadece bilişim suçlarını değil, herhangi bir suçu, sunucular veya tekil bilgisayarlar üzerinde bulunan verilerle aydınlatma veya önleme ihtiyacı oluştuğunda, dünyanın neresinde olunursa olunsun bu verilerin öncelikle muhafaza altına alınması gerekir[75].

Buna göre, Sözleşmenin bu bölümünde; bilgisayar sistemi aracılığıyla depolanan verilerin hızlı bir şekilde korunması (m. 16); haberleşmenin iletiminde trafik verilerinin hızlı bir şekilde korunması (m. 17); 'Üretim emri' başlığı altında depolanan verilerin ve ayrıca hizmet sağlayıcıları yönünden mülkiyeti veya kontrolünde bulunan hizmetlere ilişkin abone bilgilerinin teslimi (m. 18); depolanmış bilgisayar verilerinin aranması ve bunlara el konulması (m. 19); bir bilgisayar sistemi aracılığıyla iletilmiş gerçek zamanlı trafik verilerinin toplanması ve kaydedilmesi (m. 20) ve bir bilgisayar sistemi aracılığıyla iletilmiş gerçek zamanlı, belirlenmiş iletişim kayıtlarına yönelik içerik verilerinin toplanması ve kaydedilmesi (m. 21) düzenlemeleri yapılmış ve taraf devletlere iç hukuklarında buna ilişkin düzenlemeler yapma yükümlülüğü öngörülmüştür.

Görüldüğü üzere, Sözleşmenin usul hukuku ile ilgili kuralları düzenlediği bölümünde, siber suçlara ilişkin bir arama ve el koyma tedbiri rejimi düzenlenmiş, ancak teknolojinin hızlı gelişimi ve buna paralel olarak suç işleme yöntemlerinin de devamlı olarak değişmesi ve

---

[73] **ÖZBEK**, s. 83.
[74] Ayrıca detaylı bilgi için bkz. **YAZICIOĞLU, Yılmaz**, Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar, İstanbul, 2009, s. 81 vd.
[75] **ŞEN/CENGİZ**, s. 81-82.

gelişmesi nedeniyle, ihtiyacı karşılamak amacıyla, bu tedbirlere dair kurallar detaylı bir biçime ele alınmaya çalışılmıştır.

Sözleşmenin bu bölümünde öngörülen tedbirler esasen adli bilişimin konusunu oluşturmaktadır[76]. Nitekim, bu bağlamda adli bilişimi, disketlerden, sabit disklerden ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma işlemi olan ve elektronik delillerin muhteva ettiği bilgileri, delil inceleme süreçlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak, delilin bütünlüğünü koruyarak ve maddi gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgeleme süreçlerinin bütünü şeklinde tanımlamak mümkündür[77]. Buna göre, Sözleşmede öngörülen adli bilişim süreçlerinin söz konusu olabilmesi için, ortada bir suç şüphesi ile başlamış bir ceza soruşturması, daha doğrusu genel anlamıyla bir muhakeme sürecinin bulunması ve bu minvalde söz konusu tedbirlere başvurma zorunluluğunun bulunması gerekir. Bunun dışında, taraf devletler söz konusu düzenlemeleri kendi ulusal mevzuatlarında yaparlarken, diğer kriterleri kendi iç hukuklarına ve hukukun genel ilkelerine göre yapacaklardır. Ancak, söz konusu tedbirler aynı zamanda kişilerin özel hayatının gizliliği yahut haberleşmenin gizliliği gibi temel haklarına müdahale anlamı taşıdığından[78], bu düzenlemeler yapılırken Siber Suç Sözleşmesi yanında Avrupa İnsan Hakları Sözleşmesi başta olmak üzere uluslararası sözleşme hükümlerinin muhakkak dikkate alınması gerektiği kanaatindeyiz.

Ülkemizde ceza usul hukukunda uygulanan ana kanun olan Ceza Muhakemesi Kanunu'nda bilişim suçları yönünden uygulanan koruma tedbirlerine ilişkin, esas olarak bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbiri (CMK m. 134) ile bazı hallerde iletişimin tespiti, dinlenmesi ve kayda alınması (CMK m. 135) tedbiri uygulama alanı bulmaktadır.

Mevzuatımızdaki bilgisayarlarda yapılacak arama ve el koyma işlemleri için uygulanan esas koruma tedbiri olan CMK m. 134'ün, Sözleşmenin 18. ve 19. maddesinde yer alan üretim emri ile bilgisayar verilerinin aranması ve el konulması tedbirlerini karşıladığını ve genel olarak bu hükümle Sözleşmenin ilgili iki hükmüne dair yükümlülüğün yerine getirildiğini söyleyebiliriz. Her ne kadar CMK m. 134, yalnızca bilgisayarlarda ve bilişim sistemlerinde yapılacak yerinden arama, kopyalama ve el koyma işlemlerinden bahsetmekteyse de[79], hükmün lafzı yönünden, özellikle Sözleşmenin 18. maddesinde öngörülen depolanan ve soruşturulan suça ilişkin verilerin ve ayrıca hizmet yahut servis sağlayıcıların elinde bulunan abone bilgilerinin alınması veya bunlara el konulmasını da mümkün kıldığından, söz konusu tedbirin Sözleşmenin 18. ve 19. maddesini genel olarak karşıladığını söylemek mümkündür. Fakat, özellikle 18. madde yönünden hizmet sağlayıcılar yönünden getirilmesi öngörülen abone bilgilerini saklama vb. yükümlülüklere ilişkin hukukumuzda bir düzenleme yapılmadığından, Sözleşmede bu hükümle öngörülen amacın CMK m. 134'teki tedbirin

---

[76] **ROHRMANN, Carlos Alberto / NETO, Jason S. Albergaria,** *"Digital Evidence and Electronic Law Suit: How far do we go?"*, Ankara, 2007, s. 602.

[77] **BARRY, Sean**; "*Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted",* http://www.dataforensics.com/articles/smoking_microchip_tells_it_all.pdf, (20.01.2016); **KESER BERBER, Leyla**; Adli Bilişim, Ankara, 2004, s. 39.

[78] **ŞEN, Ersan / ÖZDEMİR, Bilgehan**, Tutuklama – Uygulamada Şüpheli ve Sanık Haklarının Korunması, Ankara, 2011, s. 50; **DEĞİRMENCİ, Olgun**, Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara, 2014, s. 97.

[79] **ÖZEN, Muharrem / ÖZOCAK, Gürkan,** *"Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)",* Ankara Barosu Dergisi, S. 2015/1, s. 62. Ayrıca ilgili tedbir hakkında ayrıntılı bilgi için a.g.e. Bkz. s. 41-77.

uygulanmasıyla her zaman gerçekleşeceğini söylemek de zordur. Bunun yanı sıra, CMK m. 134'teki düzenlemenin, genel itibariyle yetersiz, tedbirin amacı ve ihtiyacını karşılamaktan uzak, teknolojik ilerlemenin hızına cevap vermekten yoksun ve bu nedenle ciddi anlamda revizyona ihtiyaç duyan bir düzenleme olduğu da tartışmasızdır[80].

Sözleşmenin 20. ve 21. maddelerinde ise, trafik verilerinin gerçek zamanlı olarak toplanması ve iletişim kayıtlarına yönelik içerik verilerinin hem zamanlı bir biçimde, yani iletişim anında kesilerek toplanması ve kaydedilmesi tedbirleri öngörülmüştür. Her ne kadar bununla ilgili ceza muhakemesi mevzuatımızda doğrudan bir düzenleme olmasa da, CMK'nun 135. maddesinde düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri mevcuttur. Ancak, hükmün Sözleşmede öngörülen tedbirleri karşılamadığını söylememiz gerekir. Zira, CMK m. 135 en az iki kişi arasındaki bir iletişimin bulunması halinde uygulama alanı bulabilen bir tedbir olup sadece bu hallerde uygulanabilirken, Sözleşmenin 20 ve 21. maddelerindeki tedbirler bilişim sistemleri arasındaki her türlü veri aktarımı ve iletişimini kapsamaktadır[81]. Bunun yanı sıra, CMK m. 135 yalnızca 8. fıkrasında sayılan sınırlı sayıdaki (katalog) suç için başvurulabilecek bir tedbirdir ve bu suçların arasında Sözleşmede sayılan suçların hiçbiri yer almamaktadır. Oysa, Sözleşmenin 14. maddesinde her ne kadar bu usul kuralları sadece bilişim suçları ile ilgili olarak öngörülmediyse de, bu suçların da tedbirlerin uygulama kapsamında değerlendirilmesini amaçladığı ortadadır. O halde, CMK m. 135, Sözleşmenin 20. ve 21. maddelerindeki tedbirleri karşılamamaktadır. Bu durumda, CMK'nda, çok sıkı şartlara bağlı kılınmak kaydıyla ve Sözleşmedeki suçlarla sınırlı kalmak üzere, Sözleşmedeki 20. ve 21. maddede öngörülen tedbirlerin düzenlenmesinin düşünülebileceği kanaatindeyiz.

Sözleşmenin 16. ve 17. maddesinde öngörülen bilgisayar sistemi aracılığıyla depolanan verilerin hızlı bir şekilde korunması ve haberleşmenin iletiminde trafik verilerinin hızlı bir şekilde korunması yönündeki tedbirler ile ilgili ise ne CMK'nda, ne de bir başka kanunda, herhangi bir düzenleme bulunmamaktadır. Dolayısıyla, ulusal mevzuatımızda, bu iki hükmün karşılığı olabilecek herhangi bir tedbir söz konusu değildir.

Sonuç olarak, hukukumuzda, Sözleşmenin maddi ceza hukuku hükümleri belli bir karşılık bulmakta ve önemli eksiklikler bulunmakla beraber Sözleşmede suç olarak öngörülen fiiller genel itibariyle iç hukukumuzda da suç olarak düzenlenmekteyse de, aynı şeyi ulusal ceza usul hukukumuz yönünden söylemek imkansızdır. Mevzuatımızda Sözleşmedeki usul kurallarının çok azını karşılayacak şekilde CMK m. 134'ten başka bir ceza usul hukuku normu bulunmadığı göz önüne alındığında, Sözleşmenin taraf devletlere ceza usul hukuku normlarının uyumlulaştırılması hususunda yüklediği ödevin hemen hemen hiç karşılanmadığı ortadadır.

d. Sözleşme ve Türk Hukuku Yönünden Uluslararası Adli İşbirliği Kurumu

Sözleşmenin en önemli başlıklarından biri, siber suçlarla mücadele ile ilgili olarak devletlerin birbirleriyle yardımlaşmaları yönünden bir esaslar bütünü oluşturmaktır. Zira, yukarıda da kısaca söz ettiğimiz üzere, teknolojik gelişimle birlikte siber suçlulukta suçun işleniş yöntemleri hızla çeşitlenmekte, bu da suçla mücadele eden birimler yönünden bir suç haritası çıkarmayı zorlaştırmakta, bunun yanı sıra, suçun teknik boyutu ve failinin teknik uzmanlığı karşısında kolluk kuvvetleri suçlulukla baş etmekte yetersiz kalabilmektedir. Ayrıca çoğu kez

[80] Buna ilişkin sorunlar ve çözüm önerileri hakkında bkz. **ÖZEN/ÖZOCAK**, s. 67-74.
[81] **ÖZBEK**, s. 86.

fail ile mağdur arasında mesafe bulunması gibi nedenlerle siber suçlarla mücadele oldukça zordur[82]. Özellikle fail ile suçun işlendiği yerin farklı ülkeler olması ve devletlerin yargı yetkisinin ulusallığının ceza muhakemesinin önemli ilkelerinden biri olması, uygulamada çoğu kez sorun yaratabilmekte, devletlerin yetkileri kendi sınırları dışına uzanamadığından, sınıraşan siber suçlulukla mücadelede klasik yargı yetkisi ilkeleri yetersiz kalabilmektedir[83]. İşte, devletler arasında adli yardımlaşma ilkeleri belirlenmesi ve bu hususta ortak bir işbirliği rejimi oluşturulabilmesi bu nedenle önem taşımaktadır.

Bu itibarla, Sözleşmenin 23. maddesi itibariyle uluslararası adli işbirliği ya da yardımlaşmaya ilişkin ilkeler getirilerek, sınıraşan siber suçlulukla mücadelede yeknesak bir düzenleme yapma yoluna gidilmeye çalışılmıştır. Sözleşmede, adli yardımlaşmaya ilişkin öngörülen genel ilkeler şunlardır:

- Taraf devletler mümkün olan en geniş biçimde işbirliği yapacaklardır. Bu çerçevede, bilgi akışı ve delil temini önündeki engeller en aza indirgenecektir.
- Bu işbirliği ilkeleri yalnız siber suçlarda değil, klasik suçların elektronik ortamlarda bulunan delilleri yönünden de geçerli olacak, en geniş tabirle "elektronik şekilde" (*in electronic form*) delil toplanması gereken tüm suçlar bu kapsamda sayılacaktır.
- Sözleşmenin adli işbirliğine ilişkin hükümleri, ceza işlerinde adli yardımlaşmaya ilişkin çok taraflı veya iki taraflı uluslararası antlaşmalara göre üstün konumda değildir. Sözleşme ile bu antlaşmaların yerine yeni bir rejim yaratılmamıştır.
- Sözleşme hükümleri iç hukukun da üzerinde değildir. Bazı istisnalar dışında iç hukuktaki usul kuralları uygulanacaktır[84].

Görüldüğü üzere Sözleşmenin adli yardımlaşmaya ilişkin hükümleri ile belirli bir çerçeve çizilmeye çalışılmış, ancak devletlerin yargı yetkilerine ve iç hukuklarındaki delil toplama ve tedbir rejimlerine dokunulmamıştır.

Bu ilkeler ışığında, Sözleşmede öngörülen genel adli işbirliği usulleri şunlardır: Suçluların iadesi yükümlülüğü (m. 24); elektronik ortamda delil toplanması yönünden karşılıklı yardımlaşma (m. 25); bir tarafın kendi ülkesinde yürüttüğü soruşturma ile ilgili önceden talep olmaksızın, kendiliğinden diğer tarafa bilgi verme (m. 26); uluslararası antlaşmanın yürürlükte olmadığı hallerde Sözleşmenin karşılıklı yardımlaşma kurallarının uygulanması ve bu hallerde uygulanacak usuller (m. 27); karşılıklı hukuki yardım talebine ilişkin bilginin gizli tutulması ve başka bir soruşturma veya kovuşturma için kullanılmaması (m. 28). Sözleşmede öngörülen özel, yani ulusal bazda alınması gereken koruma tedbirlerinin uluslararası yansıması niteliğindeki tedbirler ise şunlardır: Bir tarafın diğer taraftan bilgisayar verilerini gecikmeksizin koruma ve güvence altına alma talebinde bulunması (m. 29); bir tarafın diğer tarafa kendince talep üzerine korunan trafik verilerini gecikmeksizin açıklaması (m. 30); bir tarafın diğer taraftan bilgisayar verilerinde arama ve el koyma, bu verilere erişme ve el konan verileri koruma talebinde bulunması (m. 31); diğer tarafın onayı halinde veya verilerin halka açık kaynaktan gelmesi halinde, coğrafi konumlarına bakmaksızın bu verilere erişebilme (m. 32); trafik verilerinin gerçek zamanlı olarak toplanması bakımından karşılıklı yardımlaşma (m. 33); bilgisayar sistemi üzerinden aktarılan haberleşme içeriklerinin verilerine el konulması konusunda karşılıklı yardımlaşma (m. 34);

[82] **GERCKE, Marco,** Understanding Cybercrime: Phenomena, Challenges and Legal Response, Geneva, 2012, s. 123-134; **KARAGÜLMEZ**, s. 380; **UÇKAN, Özgür / BECENİ, Yasin,** *"Bilişim-İletişim Teknolojileri ve Ceza Hukuku"*, İnternet ve Hukuk, İstanbul, 2004, s. 423-424.
[83] **ÖNOK**, s. 1234.
[84] **GERCKE**, s. 463; **ÖNOK**, s. 1249.

bir tarafın diğer taraf için, talep edilen delillere anında el konabilmesi için 7 gün 24 saat erişilebilecek irtibat noktası kurma yükümlülüğü (m. 35)[85].

Özellikle 35. maddedeki, taraf devletlerden her birinde, diğer taraf devletlerin her birine 7 gün 24 saat hizmet verecek irtibat noktalarının kurulması yükümlülüğü getirilmesinin, delillere o anda ulaşabilme ve an be an siber suçlulukla mücadele edebilme imkanı bakımından oldukça elzem olduğu söylenmiştir. Bu irtibat noktasının idari yapı dahilinde nerede konumlandırılacağı ilgili devletin takdirine bırakılmıştır. Türkiye'de 35. maddedeki yükümlülüğe uygun olarak, *Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı* 7 gün 24 saat irtibat noktası olarak belirlenmiş, ancak adli yardımlaşma hükümlerini yürüten merkez olan Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün de 35. madde uyarınca irtibat noktası olarak düşünülebileceği söylenmiştir[86]. Ancak buradaki "irtibat noktası" adli yardımlaşma işlemlerini uygulayan bürokratik bir kurumdan çok, dinamik ve suçlulukla mücadelede teknik olarak etkili çalışan bir organ olarak öngörüldüğünden, bu organın Adalet Bakanlığı'nda konumlandırılmasının gerekli olmadığı kanaatindeyiz. Nitekim, Avrupa Konseyi de suçla mücadelede ülkeler arasında işbirliğinin önemine ek olarak, dinamik yapılar olması gereken kolluk ile servis sağlayıcılar arasındaki işbirliğinin önemine vurgu yapmış ve bu iki kurumsal yapı arasındaki işbirliğini geliştirmek için rehber ilkeler hazırlamıştır[87].

Belirttiğimiz gibi, Sözleşmede adli işbirliğine yönelik öngörülmüş olan hükümler daha çok uluslararası adli yardımlaşma ile ilgili bir çerçeve oluşturmayı, bir "ana ilkeler demeti" meydana getirmeyi amaçlamaktadır. Bunun dışında, Sözleşme ile devletlerin adli yardımlaşma, istinabe, delil temini vb. hususlarda iç hukuklarına yönelik bir müdahale söz konusu olmayıp, aynı zamanda ikili veya çok taraflı uluslararası antlaşmalar da aynı şekilde, Sözleşmenin ilgili hükümlerine göre üstün konumdadır. Nitekim, Sözleşmenin adli yardımlaşmaya ilişkin hükümlerinin birçoğunda *"taraflar arasında yürürlükte olan yeknesak veya karşılıklı mevzuatı temel alan herhangi bir karşılıklı yardım anlaşması veya düzenlemesinin olmadığı durumlarda"* Siber Suç Sözleşmesi adli işbirliği hükmünün uygulanacağı kaydı düşülmüştür.

Türk uygulamasına bakıldığında da, adli yardımlaşma ve istinabe kurumlarının Adalet Bakanlığı tarafından yürütüldüğü ve buna ilişkin –suçluların geri verilmesi dışında[88]- bir mevzuatın bulunmadığı, işbirliği usulünün Türkiye'nin tarafı olduğu çok taraflı veya ikili uluslararası adli yardımlaşma antlaşmaları ile belirlendiği görülmektedir. Adalet Bakanlığı, karşılıklı işbirliği antlaşmasının tarafı olan devletin talebi halinde bilgi veya delil temini, tanık dinlenmesi yahut başkaca istinabe taleplerini yerine getirmektedir. Bu talepler genel olarak 1959 tarihli *Ceza İşlerinde Karşılıklı Adli Yardımlaşmaya Dair Avrupa Sözleşmesi* çerçevesinde yerine getirilmekte olup, yabancı bir devletten bir istinabe talebinin nasıl yapılacağı yahut yabancı bir devletten istinabe talebi geldiğinde sürecin nasıl işletileceği hususları, Adalet Bakanlığı'nın 1.3.2008 tarihli ve 69/1 sayılı Genelgesinde detaylıca anlatılmaktadır. Buna göre, bir devletin diğer devletle bu bağlamda bir işbirliği yapabilmesi için bulunması gereken iki esas koşul; iki devlet arasında veya iki devletin de taraf olduğu çoklu bir karşılıklı adli yardımlaşma antlaşmasının varlığı ve somut olayda *karşılıklılık*

[85] Detaylı bilgi için bkz. **ÖNOK**, s. 1250-1261.
[86] **ÖNOK**, s. 1261.
[87] Avrupa Konseyi'nin "Siber Suçlara Karşı Kolluk ve İnternet Servis Sağlayıcıları İşbirliği Rehberi"nin önemli maddeleri için bkz. **ŞEN/CENGİZ**, s. 82-85.
[88] Suçluların geri verilmesi usulü TCK'nun 18. maddesinde öngörülmüş olup, iade koşulları ve usulü burada ayrıntısıyla düzenlenmektedir.

*ilkesi*nin bulunması, yani işbirliği talebine konu eylemin, yardım talep edilen devletin iç hukukunda da suç olarak öngörülmüş olmasıdır[89]. Nitekim, ülkemizde yapılan soruşturma ve yargılamalarda yurtdışı, özellikle de ABD menşeli firmalardan veya bu ülkelerdeki hizmet sağlayıcılarından IP adresi ve benzeri soruşturulan suç yönünden delil teşkil eden bilgiler istendiğinde, birçok kez hakaret vb. eylemler yardım talep edilen devletin iç hukukunda suç olarak sayılmadığı ve ifade özgürlüğü kapsamında kabul gördüğü için, yardım taleplerine olumsuz dönüş yapılmaktadır.

SONUÇ OLARAK: SÖZLEŞME VE İÇ HUKUK ARASINDAKİ UYUMLULUK KONUSUNDA GENEL DEĞERLENDİRME

Sözleşme'nin siber suçlarla ilgili ortak cezai ilkeler çerçevesinde belli maddi ve usul hukuku düzenlemeleri öngörmesi iç hukukları uyumlaştırma ve adli işbirliğinin arttırılması çabasının bir yansımasıdır. Ancak yukarıda da ayrıntılı yer verdiğimiz üzere, Sözleşme'nin bölgesellikten öteye gidememesi, siber suçlarla mücadelede iç hukuklar arasındaki yatay uyumluluğu zedeleyen bir faktördür. Sözleşme'nin globalleşmesi de, Sözleşme'nin onay ve eleştiri profiline baktığımızda mümkün gözükmemektedir.

Sözleşme'nin siber suçluluğu düzenlemek ve adli yardımlaşma hususlarında çekinceler ve beyanlar bakımından, devletlere geniş bir serbesti bırakması da, Sözleşme ile elde edilen yatay uyumluluğu zedeleyen diğer bir husus olarak karşımıza çıkmaktadır.

Sözleşme ile Türk Hukuku arasında incelediğimiz dikey uyumluluğa bakıldığında da, Sözleşmenin ulusal ölçekte uygulanabilirliği hususunda sorunlar olduğu görülmektedir. Zira, her ne kadar Sözleşmede öngörülen maddi ceza hukuku ve ceza usul hukuku düzenlemelerinin imzacı devletlerin iç hukuklarında normatif düzenlemelerin konusu olması beklenmekteyse de, Sözleşme 2010 yılında imzalanmış olmasına rağmen, bunun hayata geçirildiğini söylemek zordur. Maddi ceza hukuku normları yönünden belli oranda bir uyumluluğun yakalandığı söylenebilirse de, özellikle çocuk pornografisi ile ilgili ayrı ve detaylı bir yasal düzenlemenin yapılmaması, düzenleme yapılan alanlarda da Sözleşmeye uygun bir şekilde suçların sınırlarının belirgin halde olmaması sorun yaratmaktadır. Ceza usul hukuku kuralları yönünden ise durum daha vahim olup, CMK m. 134 dışında başkaca bir düzenlemenin bulunmadığı ceza usul hukuku düzenimizde, Sözleşme hükümlerinin hiçbir şekilde dikkate alınmadığını söylememiz gerekir.

Sözleşmenin ortaya çıkmasının en önemli sebeplerinden birisi olan uluslararası adli yardımlaşma rejimi oluşturulması hedefi yönünden ise, buna ilişkin Sözleşmede öngörülen ilkelerin devletler nezdinde bir zorunluluğu ve bağlayıcılığı bulunmadığından, bu hedeften baştan vazgeçilmiş görünmektedir. Bu nedenle, adli yardımlaşmaya ilişkin süreçler yine devletler arasındaki ikili antlaşmalara veya beraber taraf olunan çoklu antlaşmalara bağlı yürütülmektedir. Bu noktada altını çizmemiz gereken husus, özellikle yurtdışındaki servis sağlayıcılardan IP bilgisi, log kaydı gibi veriler istendiğinde, ülkemizde halen yasal bir kişisel verilerin korunması düzenlemesi ve altyapısı olmadığından, bu talepler çoğu kez olumsuz sonuçlanmakta ve etkin bir işbirliği yürütülememektedir. Bu nedenle, özellikle devletler arası bilgi ve belge temini yönünden adli yardımlaşmanın daha etkili yapılabilmesi için, öncelikli hedeflerden biri, AB müktesebatına ve uluslararası hukuk metinlerine uygun bir kişisel verilerin korunması kanunu hazırlanması olmalıdır.

---

[89] Uluslararası adli istinabeye ilişkin sürecin ve uygulanacak usulün detayı hakkında bkz. **RUHİ, Ahmet Cemal**, "*Yurt Dışı Tebligat ve İstinabe İstemlerinde Masraf Gerektiren Durumlar",* AÜEHFD, C. IX, S. 3-4, 2005, s. 418 vd.

KAYNAKÇA

ARCHICK, Kristen: Cybercrime: The Council of Europe Convention", içinde Cybercirme and cyberterrorism Current Issues (John Blane ed.), Novinka Books, NewYork, 2003, (s. 1-6).

ARTUK, Mehmet Emin / GÖKÇEN, Ahmet / YENİDÜNYA, Caner, Ceza Hukuku Genel Hükümler I, Ankara, 2002.

BARRY, Sean; "*Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted",* *http://www.dataforensics.com/articles/smoking_microchip_tells_it_all.pdf,* (20.01.2016).

CENTEL, Nur / ZAFER, Hamide / ÇAKMUT, Özlem, Türk Ceza Hukukuna Giriş, İstanbul, 2006.

DEĞİRMENCİ, Olgun, Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara, 2014.

DÜLGER, Murat Volkan, Avrupa Konseyi ve Avrupa Birliği Düzenlemelerinde Çocuk Pornografisinin İnternet Aracılığıyla Yayılmasına Karşı Yapılan Düzenlemeler, İstanbul Barosu Dergisi, Sayı: 4, 2004.

DÜLGER, Murat Volkan, "Avrupa Siber Suç Sözleşmesi ile Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nun Karşılaştırılması".

DÜLGER, **Murat Volkan,** Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayıncılık, 2014, İstanbul.

DÜLGER, Murat Volkan, Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi, http://www.dulger.av.tr/pdf/ytkbilisimsucelestrisi.pdf, (15.01.2016).

GERCKE, Marco, Understanding Cybercrime: Phenomena, Challenges and Legal Response, Geneva, 2012.

GÜNAYDIN, Barış, İnternet Yayıncılığı ve İfade Özgürlüğü, Adalet, Ankara, 2010.

HARLEY, Brian: "A Global Convention on Cybercrime?", **http://stlr.org/2010/03/23/a-global-convention-on-cybercrime/** (05.01.2016).

HELVACIOĞLU, Aslı Deniz, Avrupa Konseyi Siber Suç Sözleşmesi, içinde İnternet ve Hukuk, İstanbul (Yeşim ATAMER ed.), Bilgi Üniversitesi Yayınları, 2004.

İÇEL, Kayıhan: "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında 'Avrupa Siber Suç Politikasının Ana İlkeleri', İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C: LIX, Sayı: 1-2, 2001, (s. 3-10).

KARAGÜLMEZ, Ali; Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Ankara, 2005.

KESER BERBER, Leyla; Adli Bilişim, Ankara, 2004.

KETİZMEN, Muammer; Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.

KURT, Levent; Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

MARION, **Nancy**: "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation", International Journal of Cyber Criminology, Vol. 4, Issue: 1&2, 2010, (s. 699-712).

ÖNDER, Ayhan, Ceza Hukuku Dersleri, İstanbul, 1992.

ÖNOK, Murat, Avrupa Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği, Prof. Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt.19, Sayı:2, 2013, (s. 1229- 1269).

ÖZBEK, Mücahid; "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", (http://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf), 24.01.2016.

ÖZCAN, Mehmet, Siber Terörizm ve Ulusal Güvenlik, içinde İnternet ve Hukuk, İstanbul (Yeşim ATAMER ed.), Bilgi Üniversitesi Yayınları, 2004.

ÖZDİLEK, Ali Osman, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, İstanbul, 2006.

ÖZEN, Muharrem/BAŞTÜRK, İhsan; Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011.

ÖZEN, Muharrem / ÖZOCAK, Gürkan, *"Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK m. 134)",* Ankara Barosu Dergisi, S. 2015/1.

ROHRMANN, Carlos Alberto / NETO, Jason S. Albergaria, *"Digital Evidence and Electronic Law Suit: How far do we go?"*, Ankara, 2007.

RUHİ, Ahmet Cemal, "*Yurt Dışı Tebligat ve İstinabe İstemlerinde Masraf Gerektiren Durumlar",* AÜEHFD, C. IX, S. 3-4, 2005.

SINAR, Hasan, Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme, Prof. Dr. Çetin Özek Armağanı, Galatasaray Üniversitesi Yayınları, İstanbul, 2004.

SOKULLU- AKINCI, Füsun, Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt. 59, Sayı: 1-2, 2001, s. 37. (11- 38)

ŞEN, Bilal/CENGİZ, Mahmut, "Bir Sınıraşan Suç Türü Olarak Bilişim Suçları", Sınıraşan Organize Suçlar – Kavramlar, Yöntemler, Eğilimler, Ankara, 2011, (s. 63-92)

ŞEN, Ersan / ÖZDEMİR, Bilgehan, Tutuklama – Uygulamada Şüpheli ve Sanık Haklarının Korunması, Ankara, 2011.

TANER, Tahir, Ceza Hukuku Umumi Kısım, İstanbul, 1953.

UÇKAN, Özgür / BECENİ, Yasin, *"Bilişim-İletişim Teknolojileri ve Ceza Hukuku"*, İnternet ve Hukuk, İstanbul, 2004, s. 423-424.

VATIS, Michael, The Council of Europe Convention on Cybercrime, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, The National Academy Press, Washington D.C., 2010, (s. 207- 223).

WALES, Elspeth, Draft Council of Europe Cybercrime Convention Upsets Civil Rights Bodies, Computer, Fraud & Security, Vol. 2000, Issue: 12, December 2000.

WEBER, Amalie: The Council of Europe's Convention on CyberCrime, Berkeley Technology Law Journal, Vol. 18, 2003, (s. 424- 446)

YARSUVAT, Duygun; "*Müstehcenliğin Neresindeyiz?",* Güncel Hukuk Dergisi, S. 9, İstanbul, Eylül 2004,

YAZICIOĞLU, Yılmaz, Fikri Mülkiyet Hukukundan Kaynaklanan Suçlar, İstanbul, 2009,

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=iaDgY9vB et: 14.01.2016.

Committee of Experts on Terrorism (CODEXTER) Opinion of the Committee of Experts on Terrorsim Fort he Attention of the Committee of Ministers on Cyberterrorism and USe of Internet for Terrorist Purposes, 27-28, February 2008, https://www.coe.int/t/dlapil/codexter/Source/Cyberterrorism%20opinion%20E.pdf et: 27.01.2016

http://www.nato.int/cps/en/natohq/topics_78170.htm et.26.01.2016.

Working Paper on Recent Developments in the Use of Science and Technology by Offenders and by Competent Authorities in Fighting Crime, Including the Case of Cybercrime, 12- 19 April, 2010. http://www.unodc.org/documents/crime-congress/ 12th-CrimeCongress/Documents/A_CONF.213_9/V1050382 e.pdf et: 27.01.2016.