AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESI IŞIĞINDA SİBER SUÇLARLA MÜCADELEDE ULUSLARARASI İŞBİRLİĞİ

(International Co-operation in the Fight against Cybercrimes in the Light of the Council of Europe Convention on Cybercrime)

Murat ÖNOK*

ÖZET

Bu çalışmada, öncelikle siber suç kavramı ele alınmış ve bu yeni suçluluk türüyle mücadele etmekte yaşanan hukuki ve fiili sorunlar açıklanmıştır. Ardından, uluslararası alanda siber suçlarla mücadele bakımından kabul edilen bazı enstrüman veya organlara kısaca değinilmiştir. Çalışmanın esasını ise, Avrupa Konseyi bünyesinde 2001 yılında Budapeşte'de kabul edilen Siber Suç Sözleşmesi'nde yer alan adli yardımlaşmaya dair hükümler teşkil etmektedir. Önce Sözleşme, sonra Türkiye uygulamasında adli yardımlaşma hakkında genel nitelikli bilgiler verildikten sonra, Sözleşme'nin 3. Kısmında yer alan, uluslararası yardımlaşmaya ilişkin ilkeler ve hükümler incelenmiştir. Sonuç kısmında ise, siber suçlarla mücadelede varılan nokta değerlendirilmiştir.

Anahtar kelimeler: Siber suç, Siber Suç Sözleşmesi, Budapeşte Sözleşmesi, Siber suçlarla mücadele, Uluslararası adli yardımlaşma

Abstract

In this study, the concept of "cybercrime" has been studied first, and the legal and factual problems encountered in the fight against this new type of criminality have been then explained. Certain instruments or organs adopted in the international arena in the fight against cybercrimes have been mentioned shortly. The provisions concerning legal cooperation embodied in the 2001 'Convention on Cybercrime' adopted in Budapeste within the framework of the Council of Europe constitute the essential part of the study. After providing general information about the Convention first, and legal cooperation in Turkish practice after, the principles and provisions concerning international cooperation embodied in Chapter III of the Convention have been analyzed. In conclusion, the current situation as to where we stand in the fight against cybercrimes has been evaluated.

Keywords: Cybercrime, Convention on Cybercrime, Budapest Convention, Fighting cybercrimes, International cooperation

* Yrd. Doç. Dr., Koç Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Öğretim Üyesi

Giriş

Her teknolojik gelişmede olduğu gibi, bilişim teknolojilerinin ve bu arada internetin gelişimi bir çok yeni hukukla beraber hem yeni suç tiplerini hem de geleneksel suçların farklı işleniş biçimlerini ortaya çıkarmıştır[1]. Böylece, günlük ve mesleki hayatımızı önemli ölçüde kolaylaştıran teknoloji ve internet, bir yandan da, yeni hukuki düzenlemeleri zorunlu kılan bir sorun hâline gelmiştir[2]. Bu çalışmada, gelişen teknolojinin doğurduğu hukuki sorunlardan sadece siber suçlar üzerinde durulacak; bu kapsamda, yine siber suç olgusunun ortaya çıkardığı sorunlardan birisi olan, uluslararası işbirliği meselesi, esas olarak incelenecektir.

Çalışmamızın ana konusunu oluşturan 2001 tarihli Avrupa Konseyi Sözleşmesi'nin başlığına uygun olarak, "siber suç" (*cybercrime*) terimini makalemizde esas almaktayız[3]. Buna karşılık, Türk literatüründe "bilişim suçu" teriminin yaygın olarak kullanıldığını ifade etmek gerekir[4]. Her halükârda, gerek doğru terimin tespiti gerekse

---

1 Füsun Sokullu-Akıncı, *Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, s. 11; Yee Fen Lim, *Cyberspace Law, Commentaries and Materials*, Oxford University Press, 2002, s. 247; Mahmut Koca, *Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku*, Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, Cilt III, 2003, s. 785.

2 Berrin Bozdoğan Akbulut, *Bilişim Suçları*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Milenyum Armağanı, Cilt 8, Sayı 1-2, 2000, s. 547-548. Hukuksal değerlerin yeni ihlal modellerinin ortaya çıkması durumunda, devletin bu ihlalleri engellemek, konuya dair gerekli düzenlemeleri yapmak ve ihlalin varlığı durumunda ilgili kimseleri kovuşturarak cezalandırmak yükümlülüğü vardır (Yener Ünver, *Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından* Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, s. 62.; bkz. benzer anlamda R. Yılmaz Yazıcıoğlu, *Bilgisayar Suçları – Kriminolojik, Sosyolojik ve Hukukî Boyutlarıyla*, İstanbul, 1997, s. 292. Kıyaslayınız Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara, 2008, s. 41).

3 Uluslararası platformda da genelde "siber suç" kavramı kullanılmaktadır (İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* Ankara, 2008, s. 14; B. Zakir Avşar/Gürsel Öngören, *Bilişim Hukuku*, Türkiye Bankalar Birliği, İstanbul, 2010, s. 47). Türk hukukunda da bu kavramı tercih edenler mevcuttur (Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul, 2001, s. 69; Yazıcıoğlu, Sempozyum, s. 452). Buna karşılık, "bilişim suçları"nın "siber suçlar"ı içeren bir üst kavram olduğu da savunulmaktadır (A. Caner Yenidünya/Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim* Suçları, İstanbul, 2003, s. 33). Öte yandan, ulusal doktrinimizde siber suçları tasnif girişimleri içim bkz. Yazıcıoğlu, Bilgisayar Suçları, s. 143 vd.; Hatice Akıncı/A. Emre Alıç/ Cüneyd Er, *Türk Ceza Kanunu ve Bilişim Suçları*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 174 vd.; Mehmet Özcan, *Siber Terörizm ve Ulusal Güvenlik*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 305-307; Ergün, s. 27 vd.; Avşar/Öngören, s. 123 vd.; Ali Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, 3. Baskı, Ankara, 2011, s. 56 vd.; Muharrem Özen/ İhsan Baştürk, *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku*, Ankara, 2011, s. 90. Yine çeşitli suç tipi örnekleri ve kovuşturulmalarında yaşanan sorunlar için bkz. Lim, s. 281 vd. Türkiye'de bu suçların işleniş biçimleri hk. bkz. Feridun Yenisey, İnternet Suçlarının Yeni İşleniş Biçimleri, Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002, s. 447-450.

4 Akbulut, s. 549 vd.; Yenidünya/Değirmenci, s. 31; Akıncı/ Alıç/ Er, s. 195 vd.; Murat Volkan

bilişim suçu kavramı üzerinde Türk doktrininde bir uzlaşı olmadığını belirtmek gerekir[5]. Hatta uluslararası alanda da "siber suç" kavramının içeriği konusunda mutabakat bulunmamaktadır[6]. Yine de, basitçe, siber suçları, bilişim sistemleri aleyhine veya bilişim sistemleri aracılığıyla işlenen suçlar, olarak tanımlayabiliriz[7]. Bilindiği üzere, "bilişim alanında suçlar", 5237 sayılı Türk Ceza Kanunu'nun 243.-245. maddeleri arasında düzenlenmiştir[8]. Bununla birlikte, yukarıda anladığımız şekilde siber suç kavramı, hakaret, cinsel taciz, dolandırıcılık gibi klasik bir çok suç tipinin bilişim sistemleri aracılığıyla işlenmesini de kapsamaktadır.

Dülger, *Bilişim Suçları*, Ankara, 2004, s. 66; Avşar/ Öngören, s. 46; Cevat Özel, *Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 341 vd.; Cankat, s. 12; Karagülmez, s. 41 vd.; Ketizmen, s. 32 vd. (fakat yazar, belirli bir tanımı esas almaktan çok, bilişim suçu adı altında incelenen suçların sosyo-ekonomik dönüşümle bağlantısının daha rahat kurulabilmesine olanak sağladığı gerekçesiyle bu kavramı tercih ettiğini açıklamıştır, age, s. 39). Kıyaslayınız Yazıcıoğlu, Bilgisayar Suçları, s. 125 vd. (yazar, eserinin başlığında "bilgisayar suçları" kavramını kullanmaktadır; ancak bunun temel nedenini, bilişim araçlarının en yaygınının bilgisayar olması ve "bilgisayar suçları" kavramının alışkanlık teşkil etmesi ile açıklamaktadır (s. 131). Gerçekten, bu eserin yazıldığı dönemde yurt dışında (ve özellikle ABD'de daha sonraki yıllarda bile, bkz. Dülger, s. 63) "computer crimes" kavramının genellikle kullanıldığını belirtmek gerekir. Hatta, yazar, Türk kanunkoyucusunun ceza kanununda "bilişim" terimini seçmesini "yerinde" bulmakta (s. 129-130), bilişim suçları kavramının, aslında bilgisayar suçlarını da kapsayan bir üst kavram olduğunu da ifade etmektedir (s. 131. Nitekim, daha sonraki tarihli bir eserinde, yazar, "siber suçlar" kavramını tercih etmektedir, bkz. Yazıcıoğlu, Sempozyum, s. 452); Veli Özer Özbek, İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 4, Sayı 1, 2002, s. 106-107 – yazar "internet suçları" ifadesini tercih etmektedir); Ünver, İÜHFM, s. 79 (yazar, siberuzay ortamında siberuzay aracılığıyla işlenen suç veya bilişim sistemi aracılığıyla işlenen suç, terimlerini önermektedir); Özen/Baştürk, s. 12 (yazarlar, bilgisayar suçları ile bilişim suçları kavramlarının doktrinde eşanlamlı olarak kullanıldığını belirttikten sonra, ilk kavramın bugün için tercih edildiğini ifade etmektedirler). Öte yandan, siber suç kavramı ile bilgisayar suçu kavramının aynı olduğu da savunulmaktadır (Koca, Tekinalp'e Armağan, s. 788), fakat "siber suç"u "bilişim suçu" ile eşdeğer anlayacaksak, her iki kavramın, "bilgisayar suçu" kavramını da içeren bir üst kavram olduğunu kabul etmek gerekir.

5 Yazıcıoğlu, Bilgisayar Suçları, s. 129; Akbulut, s. 549; Özel, s. 342; Şaban Cankat Taşkın, *Bilişim Suçları*, İstanbul, 2008, s. 12; Ergün, s. 12; Avşar/Öngören, s. 46. Çeşitli tanımlar için bkz. Yazıcıoğlu, Bilgisayar Suçları, s. 136-143; Karagülmez 42 vd.; Avşar/Öngören, s. 46 vd. Kullanılan çeşitli terimler için bkz. Dülger, s. 64-65.

6 Uluslararası literatürde tanım ve tipoloji tasnifleri denemeleri için bkz. Marco Gercke, *Understanding Cybercrime. A Guide for Developing Countries,* 2nd ed. (Draft March 2011), s. 25 vd.; Susan W. Brenner, "*S.Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 The Journal of Criminal Law & Criminology 379 (2007) s.382 vd.; Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime,* 43 Colum. J. Transnat'l L. 705 (2004-2005), s.711 vd.

7 Karagülmez, s. 44; Taşkın, s. 10 (gerçi, yazar, bilişim suçlarının işleniş şekli olarak bunu belirtmektedir). Benzer bir tanım için bkz. Akbulut, s. 551; Yazıcıoğlu, Sempozyum, s. 459. Kıyaslayınız Koca, Tekinalp'e Armağan, s. 788 ve Avşar/Öngören, s. 47 ("bilgisayar" kavramı üzerinden aynı tanım verilmektedir). Kıyaslayınız Dülger, s. 67: "verilere karşı ve/veya veri işlemle bağlantılı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar".

8 Bununla birlikte, diğer klasik bir çok suç tipinin (hakaret, cinsel taciz, dolandırıcılık gibi) de bilişim sistemleri aracılığıyla işlenebildiği hatırda tutulmalıdır.

Siber suç olgusuyla mücadele etmek bakımından en önemli husus, aşağıda detaylı olarak izah edileceği üzere, uluslararası adli yardımlaşmadır. Bunun bilincinde olan devletler, uluslararası örgütler ve sivil toplum kuruluşları, yeknesak bir mücadeleyi mümkün kılmayı amaçlayan sayısız girişimlerde bulunmuşlardır. Bu sayede ortaya çıkan hukuki enstrümanlardan en önemlisi, Avrupa Konseyi bünyesinde kabul edilen 2001 tarihli Siber Suç Budapeşte Sözleşmesi'dir.

Çalışmamızın ilk kısmında, siber suçlarla mücadelenin arz ettiği güçlükler izah edilecektir. İkinci kısımda, özetle, yukarıda bahsettiğimiz uluslararası girişimlerden bazılarına, ana hatlarıyla, değinilecektir. Üçüncü kısımda, çalışmamızın üzerinde yoğunlaştığı Budapeşte Sözleşmesi hakkında genel bilgi verilecektir. Çalışmanın ana kısmı ise, uluslararası adli yardımlaşmanın ele alındığı dördüncü kısımdır. Burada, adli yardımlaşma konusunda Türk uygulamasına dair temel bazı bilgilere yer verildikten sonra, Budapeşte Sözleşmesi ile getirilen uluslararası işbirliği rejimi, iki alt başlık altında, izah edilecektir.

§ 1. Siber Suçlarla Mücadelenin Zorluğu

Siber suçlarla baş etmenin ne denli zor olduğu, son yıllarda tecrübe ile sabit olmuş, herkesçe malum bir husustur. Bu mücadelenin hukuk sistemini bu kadar zorlaması ise şu faktörlere bağlanabilir[9]:

1) Siber suçluluk oldukça yeni bir fenomen olduğundan, suçun işleniş biçimleri hakkında şablonlar çıkarmak mümkün olmamaktadır[10]; bu da, bu olguyla mücadelede kaynakların ne şekilde dağıtılması gerektiğini gösteren "suç haritaları" geliştirilmesine engeldir[11]. Sorunun gerçek boyutu hakkında elimizdeki bilgiler sınırlı olmakla birlikte[12], hızla artan bir suçluluk türü olduğu kesindir[13].

2) Yeni bir suçluluk türü söz konusu olduğundan, ceza adaleti sisteminin bir çok aktörü konuya henüz aşina değildir[14]. Polisin daha hızlı adapte olduğu söylenebilse de, savcı ve hakimlerin bilişim suçları meselelerinde henüz yeterli teknik bilgi-

---

9 Bu konuda kapsamlı bilgi için bkz. Gercke, *Understanding Cybercrime*, s. 123 vd.

10 Benzer yönde Akbulut, s. 555. Bununla birlikte, bilişim sistemlerinden istifade eden organize suç gruplarının tasnifi hk. bir çalışma için bkz. Kim-Kwang Raymond Choo, *Organised crime groups in cyberspace: a typology,* 11 Trends Organ Crim 270 (2008).

11 Susan W. Brenner, *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 Rutgers Computer & Tech. L.J. 1 (2004), s. 33.

12 Karagülmez, s. 33. "Siyah rakamlar"ın bu suçlarda son derece yüksek olduğuna dair bkz. Yazıcıoğlu, Bilgisayar Suçları, s. 83. Bu konuda önemli bir kaynak için bkz. Gercke, *Understanding Cybercrime,* s. 35 vd.

13 R.E. Bell, *The Prosecution of Computer Crime,* 9 Journal of Financial Crime 308 (2002), s. 308; Laviero Buono, *Investigating and prosecuting crimes in cyberspace: European training schemes for judges and prosecutors,* 11 ERA Forum 207 (2010), s. 209; Karagülmez, s. 47.

14 Soumyo D. Moitra, *Developing Policies for Cybercrime*, 13 Eur. J. Crime Crim. L. & Crim. Just. 435 (2005), s. 446; Francesco Calderoni, *The European legal framework on cybercrime: striving for an effective implementation*, 54 Crime Law Soc Change 339 (2010), s. 341.

ye sahip olduklarını söylemek güçtür; bu konuda ciddi bir eğitime ihtiyaç vardır[15]. Kaldı ki, büyük hızla yeni suç işleme yöntemleri ortaya çıktığından, bu yetkililerin bilgilerini sürekli güncellemeleri de şarttır[16]. Ayrıca, bu çalışmada ele alacağımız uluslararası işbirliği yanında, bilişim suçları bakımından, her suçta olduğundan daha fazla, ulusal düzeydeki işbirliği çok önemlidir[17].

3) Siber suçların mukayeseli hukuktaki tanımı yeknesak olmadığı gibi, mevcut tanımlar da her zaman çok net değildir[18]. Oysa, maddi ceza hukuku bakımından gözlemlenen farklılıklar, etkili bir adli yardımlaşmayı da engellemektedir. Bu nedenle, siber suçlara dair maddi ceza kurallarının yeknesaklaştırılması önemlidir[19]. Mevzuat güncellenmeyip, klasik suç tipleri, bilişim teknolojisinin ortaya çıkardığı suçluluk türlerine uygulanmak istendiğinde, faili cezalandırmak her zaman mümkün olmamaktadır[20]. Kaldı ki, hızla gelişen teknoloji, siber suçların yeni görünüm şekillerini ortaya çıkarmakta, bu da, yeni düzenlemeler yapan devletler açısından dâhi, mevcut yasal çerçevenin aynı hızla değiştirilmesini ve geliştirilmesini gerektirmektedir[21].

4) Siber suçluluğun karakteristik bir özelliği, fail ile mağdur arasında mekansal mesafe bulunmasıdır[22]. Ayrıca, bilişim teknolojisinin işleyiş tarzı sebebiyle, suç çoğu zaman bir çok ülkeyi ilgilendirebilmektedir[23]; gerçekten, siber suçların temel özelliği, sınır tanımamalarıdır[24]. Her iki husus da, adli işbirliğini zorunlu kılmak-

---

[15] Calderoni s. 341. Yine bkz. Özcan, s. 337; Dülger, s. 322-323; Taşkın, s. 178. Hakim ve savcıların eğitimi hk. bkz. Buono s. 215 *vd.*

[16] Özgür Uçkan/Yasin Beceni, *Bilişim-İletişim Teknolojileri ve Ceza Hukuku*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 423; Taşkın, s. 179.

[17] İşbirliğinin türleri için bkz. Karagülmez, s. 366 vd.

[18] Moitra s.446.

[19] Hasan Sınar, *Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme*, Prof. Dr. Çetin Özek Armağanı, İstanbul, 2004, s. 766; Dülger, s. 103.

[20] Gregor Urbas, *Criminalising Computer Misconduct: Some Legal and Philosophical Problems,* 14 Asia Pac. L. Rev. 95 (2006), s. 99.

[21] Sınar, İnternet ve Ceza Hukuku, s. 48; Yenidünya/Değirmenci, s.111; Marco Gercke, *Europe's Legal Approaches to Cybercrime*, 10 ERA Forum 409 (2009), s.410; Özcan, s. 330-331.

[22] Brenner in Rutgers Computer & Tech. L.J. s.23; Gercke, *Understanding Cybercrime,* s.134; Karagülmez, s. 380.

[23] Gercke, *Understanding Cybercrime,* s.133; Özcan, s. 326-327.

[24] Sokullu-Akıncı, İÜHFM, s. 12; Fatih S. Mahmutoğlu, *Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu,* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, s. 39; Brenner in Rutgers Computer & Tech. L.J., s.25; Ergün, s. 44; Raluca Simion, *Cybercrime and its challenges between reality and fiction. Where do we actually stand?,* Rivista di Criminologia, Vittimologia e Sicurezza, Vol. III- N. 3, Vol. IV, N. 1- Settembre 2009-Aprile 2010, s. 310; Karagülmez, s. 67.

tadır[25]. Ayrıca, suçun nerede işlenmiş sayılacağı sorunu da ortaya çıkmaktadır[26]. Suçun çoğu zaman birden çok ülkeyi kapsaması, devletlerin egemen eşitliği ilkesi karşısında zorluklar çıkarmaktadır. Zira, ceza muhakemesi hukukunda geçerli olan klasik anlayış, devletlerin ulusal yargı yetkisinin coğrafi sınırlarla belirlenmesidir[27]. Bu da, uluslararası hukukun temel ilkelerinden biri olan, ulusal düzenlemeleri uygulama yetkisinin (*jurisdiction to enforce*), ilgili devletin açık izni olmadıkça, ülke dışında yerine getirilemeyeceği şeklindeki kural ile bağlantılıdır[28]. Bunun sonucunda, ilgili devletin rızası olmadıkça, diğer bir devlet onun ülkesi üzerinde soruşturma işlemleri sürdüremez. Bu ise, siber suçlulukla mücadele konusundaki temel engellerden birini doğurmaktadır: devletlerin yetkileri kendi sınırları dışına uzanamadığından, sınır tanımayan siber suçlulukla mücadelede klasik yargı yetkisi anlayışı yetersiz kalmaktadır[29]. Zira, siber suçluluk tüm suçlar arasında en sınıraşan nitelikte olanı ise de, devletlerin uygulama yetkisi ülkesel olmak zorundadır[30]. Klasik egemenlik fikrine dayalı bu yetki anlayışı, teknolojinin söz konusu olmadığı, gerçek, yani fiziksel dünyada işlenen suçlar açısından tasarlanmıştır[31]. Oysa, siber suçlarda, fail belirli bir devletin yargı yetkisi dahilinde bulunmakta, eylemleri ise, diğer bir çok ülkedeki bilişim sistemlerini ve mağdurları etkileyebilmektedir. Her ne kadar başka suçluluk türlerinde de bu özelliğe rastlanabilse de, bu mekansal uzaklık ve sınır aşan boyut, siber suçluluğun yapısında mündemiç bir özelliktir[32]. Neticede, bu suçlarla mücadelede, uluslararası adli yardımlaşma elzem hale gelmekte; bunun

---

[25] Gercke, *Understanding Cybercrime,* s.173; Sınar, İnternet ve Ceza Hukuku, s. 49; Uçkan/Beceni, s. 380-381; Özcan, s. 328; Dülger, s. 327; Karagülmez, s. 68.

[26] Fikret İlkiz, İnternet Ortamında Yayınlar, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 457; Taşkın, s. 176. Siber suçlarda suçun işlendiği yer sorunu hk. bkz. Özbek, DEÜHFD, s. 113 vd.; Sınar, İnternet ve Ceza Hukuku, s. 127 vd.; Karagülmez, s. 464 vd.

[27] Peter Csonka, *The Council of Europe's Convention on Cyber-Crime and Other European Initiatives, Revue internationale de droit pénal*, 2006/3 Vol. 77, p. 473-501. DOI : 10.3917/ridp.773.0473, s. 477; Gregor Allan, *Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative*, 2005 N.Z. L. Rev. 149 (2005), s.153.

[28] James Crawford. *Brownlie's Principles of Public International Law* (8th ed., Oxford: Oxford University Press, 2012), s.479; Malcolm N. Shaw. *International Law* (6th ed., New York: Cambridge University Press, 2008) s.645-6; Martin Dixon. *Textbook on International Law* (6th ed., Oxford: Oxford University Press, 2007), s.113; Ray August, *International Cyber-Jurisdiction: A Comparative Analysis,* 39 American Business Law Journal 531 (2002), s.561.

[29] Brenner in Rutgers Computer & Tech. L.J. s.3; David R. Johnson & David G. Post, *Law and Borders – The Rise of Law in Cyberspace,* 48 STAN.L.REV. 1367 (1996). Ayrıca bkz. Simion s.296.

[30] Yılmaz Yazıcıoğlu, *TCK 2000 Tasarısında Bilişim Şebekeleri Vasıtasıyla İşlenen Suçlar,* Uluslararası İnternet Hukuku Sempozyumu, DEÜ Yayını, İzmir, 2002, s. 456; Pedro Verdelho, *The effectiveness of international co-operation against cybercrime: examples of good practice*, Discussion paper (draft) prepared within the framework of the Project on Cybercrime of the Council of Europe, 2008, s. 4.

[31] Brenner in Rutgers Computer & Tech. L.J., s.3.

[32] Pedro Verdelho, Discussion paper (draft), s. 4.

etkin olarak işleyebilmesi ise, ilgili devletlerin siber suçluluk mevzuatları arasında uyum bulunmasına bağlı olmaktadır[33].

5) Siber suçları tespit etme ihtimali geleneksel suçlara göre çok daha düşüktür[34]. Gerçekten, bu suçların işlendiği araç ve sistem çok teknik ve sürekli değişkendir; interneti anonim olarak kullanma fırsatı nedeniyle failleri tespit etme olanağı bazen çok sınırlıdır[35]. Ayrıca, mağdurlar, özellikle de prestij kaybından çekinen ticari şirketler, bu suçları ihbar konusunda isteksiz olabildikleri gibi[36], özellikle bilişim sistemleri hakkındaki bilgisi iyi olmayan kişiler, bir çok kez durumun farkına bile varamamış olabilirler[37].

6) Siber suçu ortaya çıkarmaya yarayacak delillerin türü ve formatı[38] , bir de bunları elde etme yöntemleri geleneksel suçlara nazaran farklıdır[39]. Delilleri elde etmek zor olduğu gibi[40], bunları mahkemeler nezdinde kabul görecek şekilde, mevcut usuli kurallara uygun olarak toplamak ayrıca bir meseledir[41]. Bu da, "adli bilişim" adı verilen, "potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan" uygulamaları[42] ele alan disiplinin önemini ortaya koymaktadır. Bu bakımdan, bu suçları soruşturacak personelin çok ciddi bir uzmanlığa sahip olması şarttır[43]. Öte yandan, dijital delillerin her an kaybolabilme ihtimali karşısında[44], yardımlaşma sürecinin hızlı işlemesi de şarttır; bu ise, hele ikiden fazla ülke aracılığıyla suçun işlendiği durumlarda, klasik adli yardımlaşmada

---

33 Csonka, s.477; Mike Keyser, *The Council of Europe Convention on Cybercrime,* 12 J. Transnational Law & Policy 287 (2003), s.326.

34 Moitra, s.446; Karagülmez, s. 51.

35 Gercke, *Understanding Cybercrime,* s.142; Allan, s.151-2; Ergün, s. 43. Yine bkz. Özcan, s. 326-327.

36 Yazıcıoğlu, Bilgisayar Suçları, s. 110; Özcan, s. 335; Brenner in Rutgers Computer & Tech. L.J., s.48-9; Lorenzo Picotti & İvan Salvadori, *National legislation implementing the Convention on Cybercrime – Comparative Analysis and good practices*, Discussion paper, Version 28 August 2008, s.78; Taşkın, s. 177; Bell, s.321; Karagülmez, s. 51.

37 Roderic Broadhurst, *Developments in the global law enforcement of cyber-crime*, 29 Policing: An International Journal of Police Strategies & Management (2006), s. 410; Karagülmez, s. 63.

38 Bu konuda bkz. Peter Grabosky, *Requirements of Prosecution Services to Deal with Cyber Crime,* 47 Crime Law Soc Change 201 (2007), s.213.

39 Aynı yönde Özen/Baştürk, s. 91.

40 Bunun net bir örneği, internet üzerinden, Voice over Internet Protocols (VoIP) teknolojisi ile yapılan canlı sesli görüşmelerin denetlenmesidir (Buono, s.211).

41 Bell, s.311. Bu konuda bkz. Choo, s.286 vd.

42 Bu tanım için bkz. Leyla Keser Berber, *Adli Bilişim (Computer Forensic)*, Ankara, 2004, s. 39. Konu hk. bilgi için bkz. söz konusu eser, s. 1 vd.; Karagülmez, s. 373 vd.

43 Bell s.313; Uçkan/Beceni, s. 423. Bu bakımdan, "ya bir polisi alıp bilgisayar uzmanı yapacaksınız, ya da bir bilgisayar uzmanını polis yapacaksınız" lafının haklılığı vardır (Yenidünya/Değirmenci, s. 111).

44 Serap Keskin, *Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, s. 155.

mümkün değildir. Bu nedenle, yeni ve hızlı adli yardımlaşma yöntemleri de gerekli olmaktadır[45]. O hâlde, meşakkatli resmi prosedürlere bağlı olduğu için yavaş işleyebilen klasik adli işbirliği opsiyonları[46], siber suçlulukla mücadele bakımından etkisiz kalabilmektedir[47].

7) Siber suçlarda, çok az masraf ve gayretle, çok büyük zarar vermek mümkün olabilmektedir[48]. Oysa, bu suçla mücadele ve de adli işbirliği, büyük zahmet ve masraf gerektirebilmektedir.

8) Siber suçlulukla ceza hukuku yoluyla mücadelede en büyük sorun, bu alanda, çok az sayıda ülkenin bile mevzuatında gerekli düzenlemeleri yapmamasının, "kurtarılmış bölge/sığınak" arayan siber suçlular için yeterli olmasıdır. Gerçekten de, daha önce belirtildiği gibi, siber fail, herhangi bir ülkeden faaliyet göstererek, istediği ülke veya ülkelerdeki kişileri hedef alma imkanına sahiptir[49]. Bu bakımdan, doktrinde belirtildiği gibi, "siber suçlara karşı mücadele ya global olacaktır ya da hiç anlamı yoktur"[50]. Zira, bir kaç devlet dâhi bu mücadeleye katılmazsa, 'jurisdiction shopping' denilen olgu gerçekleşecek ve siber suçlular, bu suçlar için mevzuatında en az cezayı öngören veya diğer devletlerle adli yardımlaşma antlaşması mevcut bulunmayan devletleri tespit ederek, faaliyetlerini oradan sürdüreceklerdir[51]. Hele, iade antlaşmalarında yer alan "çifte cezalandırılabilirlik" (*double criminality*) koşulu, yani, iadenin gerçekleşebilmesi için, fiilin hem kendisinden iade talep edilen hem de iadeyi talep eden devlette suç teşkil etmesi gerekliliği, devletlerin mevzuatları arasındaki uyumu daha da önemli kılmaktadır[52].

Bütün bu tehlikeler ve zorluklar, siber suçlulukla mücadelede yasakoyucunun devreye girmesini zorunlu kılmaktadır. Öte yandan, siber suçlarla mücadele amacıyla birtakım düzenlemeleri - özellikle kamu hukuku alanında - yaparken, doğası gereği açık ve özgür olması gereken internet üzerinde temel hak ve özgürlükleri sınırlamada titiz ve hassas olunması gerektiği de unutulmamalıdır[53]. Keza, siber suçlar konusundaki düzenlemelerin suç politikasının evrensel nitelikteki temel ilkelerine uygun olması gereği de, haklı olarak, vurgulanmaktadır[54]. Özellikle ceza

---

45 Csonka s.480.

46 Bunlar için bkz. Durmuş Tezcan/Mustafa Ruhan Erdem/R. Murat Önok, *Uluslararası Ceza Hukuku*, Ankara, 2009, s. 173 vd.

47 Grabosky s.215; Bell s.316.

48 Broadhurst s.410, Özcan, s. 329. Geleneksel suçluluğa nazaran bu özelliğin yarattığı neticeler açısından bkz. Brenner in Rutgers Computer & Tech. L.J., s. 27 vd.

49 Gercke, *Understanding Cybercrime,* s.238.

50 Esposito, G. (2004), "The Council of Europe Convention on cyber-crime: a revolutionary instrument?", in Broadhurst, R. (Ed.), Proceedings of the 2nd Asia Cyber Crime Summit, Centre for Criminology: University of Hong Kong, Hong Kong, s. 54'ten naklen Broadhurst s.412.

51 Choo s.290; Gercke, *Understanding Cybercrime,* s.134.

52 Allan s.154. Yine bkz. Karagülmez, s. 373; Sınar, Özek Armağanı, s. 784.

53 Sınar, İnternet ve Ceza Hukuku, s. 46; Yenidünya/Değirmenci, s.111; Taşkın, s. 184; Özen/Baştürk, s. 94. Yine bkz. Ünver, İÜHFM, s. 83-84; Akıncı/Alıç/Er, s. 275; Uçkan/Beceni, s. 365-366.

54 Kayıhan İçel, *Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri,* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001, s. 3.

hukuku müdahalesi bakımından; "özgürlükçü demokratik yaşamın vazgeçilmez bir parçası haline gelmiş olan internet"in düzenlenmesinde bu yola başvurulmasının son çare olduğunun akılda tutulması gerektiği yönündeki görüşe[55] katılıyoruz[56].

Avrupa İnsan Hakları Mahkemesi'nin 18.12.2012 tarihli Ahmet Yıldırım/Türkiye kararında, oybirliğiyle, ifade özgürlüğüne ilişkin AİHS m. 10'un ihlal edildiğinin tespiti, Türk yasakoyucusunun interneti kullanma hakkını sınırlama konusunda gerekli özeni göstermediğini ortaya koymaktadır[57]. AİHM'in bu içtihadı,

[55] Özbek, s. 105. Yine bkz. Koca, Tekinalp'e Armağan, s. 786-787.

[56] İnternet süjelerinin karşılaştırmalı hukukta sorumluluğu için bkz. Sınar, İnternet ve Ceza Hukuku, s. 86 vd.; Mahmutoğlu, İÜHFM, s. 41 vd.; Ünver, İÜHFM, s. 67 vd.; Özen/Baştürk, s. 256 vd. İnternetin yönetimi ve düzenlenmesi konusunda özellikle bkz. Yaman Akdeniz/Clive Walker/David Wall (ed.), *The Internet, Law and Society*, Longman, Dorchester, 2000, s. 27 vd. ve 47. vd.'nda yer alan iki makale. Bilişim suçlarının düzenlenme yöntemleri için bkz. Dülger, s. 83 vd.

[57] Zaten TİB'e tanınan bazı yetkilerin "olağan dışı ve hukuka aykırı" olduğu doktrinde ifade edilmekteydi (Özen/Baştürk, s. 318).
Önemi ve güncelliği itibariyle, çalışma konumuzla doğrudan ilgili olmamasına rağmen, söz konusu kararı özetlemek isteriz. Karar, Atatürk'ün hatırasına hakaretten ötürü sahibi yargılanan bir internet sitesine yer sağlayan ("host" eden) Google Sites'a erişimin mahkeme kararıyla kısıtlanmasına ilişkindir. AİHM, yasağın kapsamını düzenleyip olası kötüye kullanmaları önlemeye dönük adli denetim güvencesi sağlayan, katı bir yasal çerçeve olmaksızın internet erişiminin kısıtlanmasını, Sözleşme'ye aykırı bulmuştur. Mahkeme'ye göre, ifade özgürlüğüne yönelik bir kısıtlama kanunda öngörülmüş olmalıdır; bunun içinse kısıtlamaya olanak sağlayan kural "öngörülebilir" olmalıdır. 5651 sayılı Kanun m. 8'e göre, internet ortamında yapılan ve içeriği bu maddede sayılan suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir. Karara konu olayda, yerel mahkeme, Atatürk'e hakaret içerdiği düşünülen siteye erişimi engelleme kararı vermişti. Ancak bunu gerçekleştirmenin tek yolu, Google Sites'a erişimi bütünüyle engellemek olduğu için, Telekomünikasyon İletişim Başkanlığı, buna yönelik olarak tedbir alınmasını istemiş, mahkeme de, bu sefer, Google Sites'a erişimi tümüyle engelleme kararı almıştı. Her iki kararın alınmasında da, ne Google Sites ne de başvurucunun sitesi, mahkeme nezdindeki yargılamanın süjesi değildi. Yerel mahkeme kararında, Google Sites, yer sağladığı site bakımından sorumlu görülse de, 5651 sayılı Kanunda, mahkemenin öngördüğü şekilde bütüncül bir erişim yasaklama tedbiri öngörülmüş değildir. Kanun, Google Sites gibi bir internet alanına bir bütün olarak erişimin engellenmesine de izin vermemektedir.Ayrıca, Google Sites'ın gayrimeşru olarak görülen içeriğe yer sağladığına dair bilgilendirildiğine ya da devam etmekte olan ceza yargılamasının öznesi olan bir siteye ilişkin ihtiyadi tedbir kararına uymayı reddettiğine dair bir delil de yoktur.
AİHM, Kanunun, idari bir organ olan TİB'e, belirli bir siteye ilişkin olarak verilen bir erişim engelleme kararının uygulanmasına dair geniş kapsamlı yetkiler verdiğini gözlemlemiştir. Davadaki vakıalara bakıldığında, TİB, başta sınırlı kapsamlı olan bir erişim engelleme emrinin genişletilmesini rahatlıkla talep edebilmiştir.
AİHM, bir bilgi kaynağına erişimin sınırlandırılmasının, ancak, yasağın kapsamını düzenleyen ve olası kötüye kullanmaları önlemeye dönük adli denetim güvencesi sağlayan, katı bir yasal çerçeve olması durumunda Sözleşme'ye uygun olduğunu teyit etmiştir. Ne var ki, yerel mahkeme, Google Sites'a tüm erişimi kısıtlamaya karar verirken, salt Atatürk'e hakaret içeren spesifik siteye erişimi engelleyen daha dar kapsamlı bir tedbirin alınıp alınamayacağını belirlemeksizin, TİB'in belirttiği görüşü zikretmekle yetinmiştir. AİHM, ayrıca, yerel ceza mahkemesinin, özellikle Google Sites'a bütün erişimin engellenmesinin gerekli olup olmadığını değerlendirmek suretiyle, olayda söz konusu olan çeşitli yararları tartmak açısından herhangi bir teşebbüste bulunduğuna dair bir belirti

Türk yasakoyucusunun 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da değişiklik yapması gerektiğini ortaya koymaktadır.

§ 2. Siber Suçlarla Mücadele Konusundaki Bazı Girişimler

Aslında, bilgisayar ve bilişim sistemleri aracılığıyla ya da bunlara karşı işlenen suçlar bakımından devletlerin hassasiyeti konusunda büyük farklılıklar vardır: bu, her bir ülkenin ekonomi ve altyapısının ne ölçüde dijitalleştiğiyle doğrudan alakalı, teknik bir meseledir[58]. Keza, suç faaliyetlerinin hedefi olmak bakımından da her bir devletin maruz kaldığı tehdit derecesi farklıdır. Bu bakımdan, her iki faktör, devletlerin siber suçluluğa gösterdikleri tepki düzeylerini önemli ölçüde etkiler[59]. Bununla birlikte, siber suçluluk sadece gelişmiş Batılı Devletlerin bir sorunu değildir ve diğer devletleri de etkilemektedir[60].

Bu sorunlu tablo karşısında, siber suçluluk, daha önce hiç olmadığı kadar uluslararası işbirliğini gerektirmekte ve aynı zamanda etkin bir adli yardımlaşmanın önüne emsalsiz engeller çıkarmaktadır[61]. Bu bakımdan, yukarıda açıklandığı üzere, klasik adli yardımlaşma yöntemlerinin siber suçlarla mücadelede yetersiz kaldığında şüphe yoktur[62].

İşte, Avrupa Konseyi bünyesindeki dört yıllık yoğun bir çalışmanın ürünü olan[63] ve çalışmamızda bazı hükümlerini ele alacağımız, 2001 tarihli Siber Suç Söz-

---

de olmadığını gözlemlemiştir. AİHM'e göre, bu eksiklik, Google Sites'a erişimin bir bütün olarak engellenmesinin haklı olup olmadığının incelenmesine dair herhangi bir yükümlülük öngörmeyen ulusal mevzuatın neticesidir. Mahkemeler, böyle bir tedbirin büyük miktarda bilgileri erişilemez kılarak, internet kullanıcılarının haklarını doğrudan etkilediği ve kayda değer bir yan etki doğurduğunu dikkate almış olmalıydılar.

Bu çerçevede, 5651 sayılı Kanunun 8. maddesinin uygulanmasından doğan müdahalenin, Sözleşme'ye göre öngörülebilirlik kıstasını karşılamadığı ve başvurucuya, demokratik bir toplumda hukuk devleti ilkesi gereği sahip olması gereken korunma derecesini sağlamadığı, AİHM tarafından tespit edilmiştir. Mahkeme, ayrıca, AİHS m. 10/1'e göre, ifade özgürlüğünün "ülke sınırları gözetilmeksizin" mevcut olduğuna işaret etmiştir. Söz konusu engelleme tedbirinin etkileri keyfi olmuş, erişime engelleme kararının adli denetimi de, kötüye kullanmaları önlemek açısından yetersiz kalmıştır. Bu nedenle, oybirliğiyle, AİHS m. 10'ün ihlal edildiğine karar verilmiştir.

58 Tonya L. Putnam & David D. Elliott, "International Responses to Cyber Crime", in Abraham Sofaer and Seymour Goodman (eds.), *Transnational Dimension of Cyber Crime and Terrorism,* 2001, s. 50.

59 Putnam & Elliott, s. 50-51.

60 Gercke, *Understanding Cybercrime,* s.124.

61 Broadhurst, s. 422.

62 Bu hususta detaylı bilgi için bkz. Brenner in Rutgers Computer & Tech. L.J., s. 3 vd.

63 1997-2000 yılları arasında çalışan "Committee of Experts on Crime in Cyberspace (Committee "PC-CY")" bu Sözleşme'yi hazırlamıştır (Csonka s.482, dn. 14). Öte yandan, ABD'nin de Sözleşme'nin içeriğinin belirlenmesinde önemli bir rolü olduğu vurgulanmalıdır (Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, s. 207 (http://cs.brown.

leşmesi, işbirliği yoluyla devletlerin müdahale edebileceği alanı genişletmeye çalışmaktadır[64].

Siber suçlulukla mücadele konusunda, Avrupa Birliği, Avrupa Konseyi, Birleşmiş Milletler, OECD (Ekonomik İşbirliği ve Kalkınma Örgütü), Amerikan Devletleri Örgütü (OAS)[65] gibi uluslararası örgüt ve kuruluşlar nezdinde ya da onların desteği veya katılımıyla sürdürülen sayısız girişim olduğu gibi[66], hükümet-dışı uluslararası örgütlerin[67], yani STK'ların yürüttüğü çok sayıda teşebbüs de mevcuttur[68].

Birleşmiş Milletler Örgütü bağlamında; daha 1980'li yılların ortalarından itibaren Birleşmiş Milletler'in Suçların Önlenmesi ve Suçluların Tretmanı Kongrelerinde siber suçla mücadelede çözüm arayışları gündeme gelmiştir[69]. BM Genel Kurulu'nun 45/121 (1990) sayılı Kararı[70], bilgisayar suçları mevzuatına ilişkindir. Bu Karara dayanarak BM tarafından 1994 yılında bilgisayarlarla alakalı suçların önlenmesi ve denetimine dair bir elkitabı hazıranmıştır[71]. 2000 yılında, BM Genel Kurulu'nun 55/63 (2000) sayılı Kararı[72] ile, bilişim teknolojilerinin suç işlemek amacıyla kötüye kullanılmasına karşı mücadele konusu ele alınmıştır. 2002 yılında da aynı konuda bir Genel Kurul kararı (56/121 (2002)) alınmıştır[73]. Sonraki iki yılda da, siber güvenlikle ilgili birer karar daha çıkmış (57/239 (2003) ve 58/199 (2004 sayılı) ve uluslararası işbirliğinin önemi vurgulanmıştır. Daha sonraki yıllarda da, çeşitli Genel Kurul kararları siber suçlar meselesine değinmiştir (60/177 (2006) sayılı Karar, 64/211 (2010) sayılı Karar).[74] Ayrıca, BM nezdinde, Siber suçlara dair Hükümetlerarası Uzmanlar Grubu da kurulmuş ve ilk toplantısını 2011'de yapmıştır[75].

Avrupa Birliği içinde, Konsey'in 2005 tarihli "Bilişim sistemleri aleyhinde

---

edu/courses/csci1950-p/sources/lec16/Vatis.pdf) [son erişim 02.12.2012]. Bunun nedenleri için bkz. Sınar, Özek Armağanı, s. 774-775.

64 Amalie M. Weber, *The Council of Europe's Convention on Cybercrime,* 18 Berkeley Technology Law Journal 425 (2003), s. 425.

65 Çalışmaları için bkz. Marco Gercke, *Understanding cybercrime: phenomena, challenges and legal response*, September 2012, ITU 2012, s. 141 vd. (www.itu.int/ITU-D/cyb/cybersecurity/legislation.html) [son erişim 30.12.2012].

66 Avrupa çapındaki çabaların genel görünümü için bkz. Gercke, ERA Forum, s.411 vd.

67 Örneğin, Uluslararası Telekomünikasyon Birliği'nin çalışmaları için bkz. Gercke, *Phenomena,challenges and legal response*, s. 121 vd.

68 Bölgesel ve evrensel uluslararası kuruluşların girişimleri hk. geniş bilgi için bkz. Gercke, *Understanding Cybercrime,* s. 175 vd.

69 Sınar, Özek Armağanı, s. 767.

70 A/RES/45/121 (14.12.1990).

71 Gercke, *Phenomena,challenges and legal response*, s. 116.

72 A/RES/55/63.

73 A/RES/56/121. Detayı için bkz. Gercke, *Phenomena,challenges and legal response*, s. 117.

74 Detayı için bkz. Gercke, *Phenomena,challenges and legal response*, s. 118 vd.

75 Gercke, *Phenomena,challenges and legal response*, s. 120. BM bünyesindeki, siber suçlarla bağlantılı diğer girişimler için bkz. age, s. 120-121.

saldırılara dair Avrupa Birliği Çerçeve Kararı" önem taşımaktadır[76]. Ayrıca, 2007 yılında, AB'nin siber suçlulukla mücadele politikasını ortaya koyduğu bir belge daha kabul edilmiştir[77]. Aralık 2009'da Lizbon Antlaşması'nın yürürlüğe girmesi önemli bir değişiklik yaratmıştır. Antlaşma'nın m. 82-86 hükümleriyle AB'ye, üye devletlerin maddi ve usuli ceza hukuku hükümlerini uyumlulaştırma görevi açıkça verilmiştir; m. 83 hükmüyle, aralarında bilgisayar suçlarının da açıkça sayıldığı, sınıraşan unsur taşıyan ciddi suçlar bakımından suç tanımlarının ve yaptırımlarının belirlenmesi bakımından asgari standartları tespit eden kurallar öngörme yetkisi tanınmıştır[78]. Bu bakımdan, artık bilgisayar suçlarına ilişkin mevzuatın geliştirilmesi AB ile üye Devletler arasında "paylaşılmış yetki" kapsamına girmekte ve AB'nin konuya ilişkin hukuken bağlayıcı tasarruflarda bulunma yetkisi doğmaktadır[79]. 30 Eylül 2010 tarihli "Bilişim sistemleri aleyhinde saldırılara dair Direktif" Tasarısı ise, 1 Aralık 2012 itiabriyle henüz kabul edilmemiştir.

Avrupa Konseyi bünyesinde, Budapeşte Sözleşmesi'nin kabulü öncesinde, 1985'te bilgisayar suçlarının hukuki yönlerini tartışmak üzere bir Uzman Komitesi atanmış; 1989'da Suç Sorunlarına dair Avrupa Komitesi "Bilgisayarlarla İlişkili Suçlara dair Uzman Raporu" kabul etmiş; Bakanlar Komitesi tarafından bu suçlara dair 1989 tarihinde bir Tavsiye Kararı kabul edilmiş, 1995'te ise sınıraşan bilgisayar suçlarından kaynaklanan sorunlara dair başka bir Tavsiye Kararı kabul edilmişti[80].

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) bünyesinde, önceki tarihli çeşitli çalışmalar da bulunmakla birlikte[81], 2002 yılında OECD Konseyi tarafından kabul edilen "Bilgi Sistemleri ve Ağlarının Güvenliği İçin OECD Rehber İlkeleri: Güvenlik Kültürüne Doğru" adlı belgeyi zikretmek gerekir[82].

Dünya ölçeğinde sanayileşmiş 8 büyük devletten (ABD, Almanya, Fransa, İngiltere, İtalya, Japonya, Kanada ve Rusya'dan) oluşan G-8[83], 1997 yılında (o zaman G-7 idi) "Yüksek Teknolojili Suçlara Dair Alt Komite" kurarak siber suçlarla mücadele konusuna eğilmiştir. Daha sonra, bu Devletlerin İçişleri ve Adalet Bakanları, yüksek teknolojili suçlarla mücadele etmek için birtakım ilkeleri ve on hususdan oluşan bir eylem planını kabul etmişlerdir[84]. Belki özellikle vurgulanması gereken bir husus, G8 bünyesinde yaratılan ve uluslararası işbirliği açısından temel bir referans oluşturup, Budapeşte Sözleşmesi'nin 35.maddesinde de yansımasını bulan

---

[76] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69 of 16 March 2005, p. 67.

[77] Bu konuda bkz. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions—Towards a general policy on the fight against cyber crime (COM(2007) 267 final).

[78] Gercke, *Phenomena, challenges and legal response*, s. 128-129.

[79] Gercke, *Phenomena, challenges and legal response*, s. 129.

[80] Gercke, *Phenomena, challenges and legal response*, s. 123-124.

[81] Sınar, Özek Armağanı, s. 769-770.

[82] Burada kabul edilen ilkeler için bkz. Gercke, *Phenomena,challenges and legal response*, s. 136.

[83] Sınar, Özek Armağanı, s. 767.

[84] Detayı ve bunun devamında yapılanlar için bkz. Gercke, *Phenomena, challenges and legal response*, s. 114-115.

'Contact Points Network' anlayışıdır[85]. Bunu ileride detaylı olarak ele alacağız. Yine, G-8 bünyesinde yapılan çeşitli çalışmalarda, dijital "suç sığınaklarının" önlenmesinin önemi (2000), siber suçlarla mücadelede kullanılabilecek usuli araçlar (2001), internetin suç amacıyla kullanılmasını önlemek için global bir kapasitenin yaratılması gereği (2004), siber suçlarla mücadelede etkili karşı-önlemlerin geliştirilmesi gereği (2006), internetin terör amacıyla kullanılması meselesi (2007), gibi konular üzerinde durulmuştur[86].

Siber suçlarla mücadelede INTERPOL, EUROPOL ve EUROJUST'ün çalışmaları önemlidir. Bu konudaki önemli bir çaba, EUROPOL tarafından "High Tech Crime Centre"'ın (Yüksek Teknolojili Suçlar Merkezi) kurulması olup, bu merkezin amacı, Avrupa çapındaki sınıraşan siber suçların soruşturulmasında eşgüdümü sağlamaktır. Keza, 2010 yılında EUROPOL içinde, Avrupa Komisyonu, EUROJUST ve AB ülkelerinin siber suçlulukla mücadele birimlerinin başındaki kişilerden müteşekkil, "European Cybercrime Task Force (EUCTF)" (Avrupa Siber Suç Timi) adlı bir platform kurulmuştur. Buradaki amaç, siber suçlulukla mücadelede, AB içinde uyumlu bir yaklaşımın geliştirilmesinde ve teşvikinde yardımcı olmak ve suç işlemekte siber teknolojinin kullanımından kaynaklanan sorunlara cevap bulmaktır[87].

Çalışmanın kapsamını sınırlı tutabilmek için, bu girişimlerin detayına girmeyeceğiz.

§ 3. 2001 tarihli Siber Suç Sözleşmesi Hakkında Genel Bilgiler

Sözleşme'nin temeli, Suç Sorunlarına dair Avrupa Komitesi'nin (SSAK- European Committee on Crime Problems) 1996'da, Avrupa Konseyi'ne siber suçlara ilişkin bir uzman komitesi kurmasını tavsiye etmesine dayanır[88]. Avrupa Konseyi Bakanlar Komitesi, bu öneriye uygun olarak, Şubat 1997'de "Siber-uzay Suçları Uzman Komitesi"ni (Committee of Experts on Crime in Cyber-space) kurmuştur[89]. Komite'nin görevi, belirli konular[90] üzerinde incelemede bulunarak "bağlayıcı bir hukuki enstrüman" tasarısını hazırlamaktı. Dört yıl boyunca çalışan Komite, Sözleşme tasarısını hazırlamış ve nihai tasarı Haziran 2001'de SSAK tarafından onaylanmış ve daha sonra da Avrupa Konseyi Bakanlar Komitesi tarafından 8 Kasım 2001'de kabul edilmiştir[91]. Devletlerin imzasına 23 Kasım 2001'de Budapeşte'de açılan Siber Suç Sözleşmesi, 1 Temmuz 2004'te yürürlüğe girmiş olup bu alandaki ilk uluslararası antlaşmadır.

---

85 Pedro Verdelho, Discussion paper (draft), s. 5.

86 Gercke, *Phenomena, challenges and legal response*, s. 115.

87 Europol Review - General Report on Europol Activities, European Police Office (2011), s. 48.

88 Explanatory Report to the Convention on Cybercrime, para. 7. Bu kararın gerekçesi için bkz. İçel, İÜHFM, s. 4-5.

89 Explanatory Report to the Convention on Cybercrime, para. 12.

90 Bunlar için bkz. Vatis, s. 208.

91 Sınar, Özek Armağanı, s. 773; Vatis, s. 209.

Türkiye'nin 10/11/2010 tarihinde imzalayıp henüz onaylamadığı Sözleşme'ye, 26/12/2012 itibariyle, ABD de dahil olmak üzere, 38 devlet taraftır[92]. TBMM websitesinde yaptığımız araştırmaya göre, Sözleşme'nin onaylanmasının uygun bulunmasına dair bir kanun tasarısı henüz hazırlanmış ya da görüşülmekte değildir. Türkiye'nin zorluk çektiği noktalardan biri, adli yardım taleplerine, Sözleşme'nin öngördüğü şekilde, hızlandırılmış bazda cevap vermeyi mümkün kılacak teknik altyapının ülke çapında mevcut olmamasıydı. Yakın zamanda, polis ve jandarma altyapısında gerekli güncellemeler yapılarak, bu sorun giderilmiştir. Buna bağlı olarak, Budapeşte Sözleşmesi'nin onay için TBMM'ye sevki öngörülmektedir.

Öte yandan, 28.1.2003'te Strazburg'da kabul edilen, Siber Suç Sözleşmesine Ek Protokol ise, bilgisayar sistemleri aracılığıyla işlenen, ırkçı ve yabancı düşmanlığı güden nitelikli eylemlerin cezalandırılmasını düzenlemektedir. Bazı devletlerin ifade özgürlüğünün kısıtlanmasına dönük endişeleri sebebiyle, ırkçılık ve yabancı düşmanlığının bilişim sistemleri aracılığıyla işlenmesinin cezalandırılması konusunda uzlaşı sağlanamadığından, bu konuyu ayrı bir Protokol'de (Sözleşmeye Ek 1. Protokol) düzenlemek gerekmiştir[93]. 1 Mart 2006'da yürürlüğe giren bu Protokol, Türkiye tarafından henüz imzalanmış değildir.

Budapeşte Sözleşmesi'nin başlıca üç amacı olduğu söylenebilir[94]:

1) Bazı suçların ortak tanımını yapmak suretiyle, ulusal düzeyde mevzuatın uyumlulaştırılmasını mümkün kılmak;

2) Siber suçların soruşturulması açısından, bilişim ortamına uygun düşen ortak yetkileri tanımlayarak, devletler arasındaki muhakeme kurallarının yeknesaklaştırılmasını mümkün kılmak[95];

3) Hem geleneksel hem de yeni türden uluslararası işbirliği yöntemlerini belirleyerek, devletlerin bu hükümleri bir an önce uygulamasını mümkün kılmak. Hemen belirtmek gerekir ki, bazı yeni yetkilere yer verilse de, klasik adli yardımlaşma anlayışının tümüyle ötesine geçilmesini gerektiren bazı yetkilerin verilmesi, ulusal egemenlik ve mülkilik ilkesine bağlı kaygılar sebebiyle, Avrupa Konseyi üyesi devletler arasında bile mutabık kalınan bir konu olamamıştır[96].
Sözleşme dört kısımdan oluşmaktadır:

– İlk Kısımda, Sözleşme'de kullanılan terimler tanımlanmaktadır.

---

92 Türkiye'nin taraf olması gerekip gerekmediğine dair bir değerlendirme için bkz. Sınar, Özek Armağanı, s. 784-786 (yazar, Sözleşme'de tespit ettiği eksikliklere rağmen, Türkiye'nin buna taraf olmasından yanadır).

93 Gercke s.417. Buna karşılık, siber-terör olgusuna Sözleşme'de hiç yer verilmmemiştir ki, bu husus eleştirilmiştir (Karagülmez, s. 451).

94 Csonka s.483; Broadhurst s.418-9; Weber s.426; İçel, İÜHFM, s. 6; Koca, Tekinalp'e Armağan, s. 791; Uçkan/Beceni, s. 382; Aslı Deniz Helvacıoğlu, *Avrupa Konseyi Siber Suç Sözleşmesi – Temel Hükümlerin İncelenmesi*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 279; Lim, s. 331; Ketizmen, s. 50.

95 Bu konuda bkz. Gercke, *Understanding Cybercrime,* s.386 vd.

96 Putnam&Elliott, s. 63.

– İkinci Kısımda, ulusal düzeyde alınacak önlemlere yer verilmektedir. Bu çerçevede, önce maddi ceza hukuku düzenlemeleri bağlamında, birtakım suç tipleri tanımlanmakta[97]; ardından da, ceza muhakemesi hukuku düzenlemeleri bağlamında, birtakım usuli yetkilere yer verilmekte[98] ve yargı yetkisi meselesine dair[99] bazı genel ilkeler[100] belirlenmektedir. Bu noktada, Sözleşme'de düzenlenen suç tiplerinin

[97] "Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar" başlığı altında, yasadışı erişim (m. 2), yasadışı müdahale (m. 3), verilere müdahale (m. 4), sistemlere müdahale (m. 5), cihazların kötüye kullanımı (m. 6); "Bilgisayarlara ilişkin suçlar" başlığı altında, bilgisayarlara ilişkin sahtecilik fiilleri (computer-related forgery - m. 7), bilgisayarlara ilişkin dolandırıcılık fiilleri (computer-related fraud – m. 8); "İçerikle ilgili suçlar" başlığı altında, çocuk pornografisine ilişkin suçlar (m. 9); "Telif haklarının ve benzer hakların ihlaline ilişkin suçlar" başlığı altında, telif haklarının ve benzer hakların ihlaline ilişkin suçlar (m. 10) düzenlenmiştir. Ayrıca, bu suçlara teşebbüsün veya maddi ya da manevi yardımın cezalandırılması da m. 11'de öngörülmüştür. Tüzel kişilerin sorumluluğu m. 12'de düzenlenmiş; m. 13'te ise, m. 2-11'de sayılan fiillerin etkili, orantılı ve caydırıcı yaptırımlarla cezalandırılması öngörülmüştür. Sözleşme'nin maddi ceza hukuku boyutu hk. bilgi için bkz. Sokullu-Akıncı, İÜHFM, s. 12 vd.; Ünver, İÜHFM, s. 91 vd.; Koca, Tekinalp'e Armağan, s. 793 vd.

[98] Usuli hükümlerin kapsamını belirleyen 14. maddenin ilk fıkrasına göre, taraf Devletler, ceza soruşturma veya kovuşturmasının yapılabilmesi için Sözleşme'nin bu kısmında öngörülen yetki ve usullerin tesisi için gerekli olabilecek yasal ve sair tedbirleri alacaklardır. 21. maddede aksi özellikle belirtilen durumlar hariç olmak üzere, söz konusu yetki ve usuller: a) m. 2-11'de öngörülen fiiller; b) bir bilgisayar sistemi aracılığıyla işlenen diğer adli suçlar; c) adli bir suçun elektronik şekildeki delillerinin toplanması, bakımından uygulanacaktır. 15. maddede ise, bu yetki ve usullerin uygulanmasında kanunen öngörülmesi gereken şart ve güvencelere yer verilmiştir. Özellikle, Avrupa İnsan Hakları Sözleşmesi, BM Kişisel ve Siyasal Haklar Sözleşmesi ve diğer uygulanabilir uluslararası insan hakları araçlarından doğan haklar dahil olmak üzere, temel hak ve özgürlüklerin uygun bir şekilde korunması ve ölçülülük ilkesinin gözetilmesi gereği vurgulanmıştır. 15. maddenin ikinci fıkrasında, bu şart ve güvencelerin, yetki veya usulün niteliğine göre, adli veya diğer bağımsız bir denetim yolunu, yetki ve usullerin uygulanmasını haklı kılan koşulları, bunların kapsamının sınırları ve uygulama süresini içermesi gerektiği belirtilmiştir. Daha sonraki maddelerde ise, şu yetki ve usullere yer verilmiştir: saklanan/depolanmış bilgisayar verilerinin hızlandırılmış korunması (m. 16), trafik verilerinin hızlandırılmış korunması ve kısmi açıklanması (m. 17), ibraz/teslim etme emri (m. 18), saklanan/depolanmış bilgisayar verilerinin aranması ve bunlara elkonulması (m. 19), trafik verilerinin gerçek zamanlı olarak toplanması (m. 20), içerik verilerinin tespiti (ele geçirilmesi anlamında) (m. 21). Bunlar hakkında geniş bilgi için bkz. Keskin, İÜHFM, s. 157 vd.

[99] Bu konuda bkz. Susan W. Brenner, *Cybercrime Jurisdiction*, 46 Crime Law Soc Change 189 (2006); Ray August, *International Cyber-Jurisdiction: A Comparative Analysis,* 39 American Business Law Journal 531 (2002); Lim, s. 18 vd.; Alan Reed, 'Jurisdiction and choice of law in a borderless electronic environment', in: Yaman Akdeniz/Clive Walker/David Wall (ed.), *The Internet, Law and Society* (Longman: Dorchester, 2000), s. 79 vd. Siber suçlarda suçun işlendiği yer sorunu hk. bkz. Özbek, DEÜHFD, s. 113 vd.; Sınar, İnternet ve Ceza Hukuku, s. 127 vd.

[100] Sözleşme'nin 22. maddesine göre, her taraf devlet, m. 2-11'de sayılan fiillerin, a) kendi ülkesinde, b) kendi bayrağını taşıyan bir gemide, c) kendi hukukuna göre tescil edilmiş bir uçağın içinde, d) işlendiği yerin ceza hukukuna göre suç teşkil etmesi veya suçun herhangi bir devletin ülkesel yetkisi dışında işlenmesi durumunda, suçun kendi vatandaşlarınca işlenmesi, ihtimalinde, bu suçlar üzerinde yargı yetkisini icra etmek için gerekli olabilecek yasal ve diğer tedbirleri alacaktır. Bununla birlikte, ikinci fıkraya göre, taraf devlet, b-d bentlerinde sayılan durumlarda, yargı yetkisini hiç kullanmama ya da sadece belirli durumlarda veya şartlar altında kullanma yetkisini saklı tutabilir. Üçüncü fıkraya göre, bir şüphelinin kendi ülkesinde bulunması ve iade talebini müteakiben, sadece vatandaşlık temeline dayalı olarak onu bir başka taraf devlete iade etmemesi durumunda, Sözleşme'nin 24/1. maddesinde belirtilen suçlar üzerinde yargı yetkisi tesis edebilmek için gerekli

ve bunların yapısal unsurlarına ilişkin belirlemelerin, gelecekte ortaya çıkabilecek yeni bilişim teknolojilerini de kapsayabilecek nitelikte, esnek bir üslupla formüle edildiği ifade edilmektedir[101].

– Bu çalışmanın konusunu oluşturan ve 23. maddeyle başlayan 3. Kısımda ise, yukarıda anılan yetkilerin kullanımı bakımından, uluslararası adli yardımlaşmanın çerçevesi çizilmektedir. Bu bakımdan, Sözleşme'ye taraf olan devletler, 2. Kısımda yer alan usuli yetkilere mevzuatlarında yer vermek zorunda oldukları gibi, 3. Kısım sayesinde, sınıraşan siber suçların yabancı devletler tarafından kovuşturulmasında da bu yetkiler onların istifadesine sunulmuş olacaktır[102]. Öte yandan, farklı devletler arasında, siber suçların soruşturulması ve kovuşturulmasında başvurulabilecek yöntemler arasında benzerlik olduğu ölçüde, işbirliği de kolaylaşacaktır[103]. Hemen belirtelim ki, Budapeşte Sözleşmesi, adli yardımlaşmaya dair mevcut diğer antlaşmaların yerini almayı amaçlamayıp onları tamamlamaktadır. Hedefi, söz konusu diğer antlaşmalarla kurulu mevcut rejim kapsamında uygulanmaktır. Bununla birlikte, ilgili devletler arasında bir antlaşma hükmünün yokluğunda uygulanabilecek ilke ve kuralları da (m. 27) belirlemek suretiyle, önemli bir kazanım sağlamaktadır. Bu bakımdan; siber suçlulukla mücadele bakımından, uluslararası adli yardımlaşma konusunu düzenleyen tüm çok taraflı ve ikili antlaşmaların tatbik kabiliyeti, Budapeşte Sözleşmesi'ne taraf devletler açısından aynen devam etmektedir. Örneğin, Türkiye'nin de taraf olduğu, Avrupa Konseyi'nin 1959 tarihli Cezai İşlerde Karşılıklı Adli Yardım Sözleşmesi ve 1960 tarihli Suçluların İadesine Dair Sözleşme; Avrupa Birliği açısından, 2000 tarihli Karşılıklı Adli Yardım Anlaşması ve Avrupa Tutuklama Müzekkeresini öngören Çerçeve Karar[104] gibi belgeler siber suçlulukla mücadele uygulanacaktır. Öte yandan, Sınıraşan Örgütlü Suçluluğa dair Birleşmiş Milletler Sözleşmesi (2000 Palermo Sözleşmesi) ve Ek Protokolleri de uygulanabilecektir.

– Nihayet, 4. Kısımda ise, Sözleşme'nin uygulanmasına dair birtakım usuli ve teknik hükümlere yer verilmektedir.

Aşağıda inceleyeceğimiz üzere, Sözleşme sadece siber suç olarak tanımlanan fiilleri değil; "elektronik şekilde" delil toplanmasını gerektiren tüm suçları, yani bi-

---

olan tedbirleri almalıdır. Dördüncü fıkraya göre, taraf devletin kendi ulusal hukuku uyarınca icra edeceği cezai yargı yetkisi saklı tutulmuştur. Nihayet, son fıkraya göre, bu Sözleşme'de öngörülen bir suça ilişkin olarak birden fazla taraf devlet yargı yetkisine sahip olduğunu iddia ettiğinde, ilgili taraflar, uygun olduğu hallerde, kovuşturma için en uygun yargı merciinin belirlenmesi amacıyla istişare edeceklerdir. Demek ki, "kovuşturulmaların aktarılması yolunda işbirliğine dayalı bir orta yol bulunmaya çalışılmıştır" (Durmuş Tezcan, İnternet Karşısında Özel Hayatın Korunması ve Adli Yardımlaşma, Uluslararası İnternet Hukuku Sempozyumu, DEÜ Yayını, İzmir, 2002, s. 539).

[101] Sınar, Özek Armağanı, s. 778.

[102] Downing, s.761.

[103] Ünver, İÜHFM, s. 144; Grabosky s.214; Picotti & Salvadori s.78.

[104] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, (2002/584/JHA), OJ L 190 of 18/7/2002.

lişim sistemi aracılığıya işlenmiş klasik suç tiplerini, kapsamaktadır[105]. Bu noktada, söz konusu yetkiler çalışmamızın kapsamına girmemekle birlikte, haksızlık içeriği itibariyle cüz'i ihlallerde bile, Sözleşme'nin 2. Kısmında öngörülen ve özel hayatın gizliliğine ağır müdahale teşkil eden bazı soruşturma yetkilerinin kullanılabilmesine ilişkin önemli eleştiriyi vurgulamak isteriz[106]. Bununla birlikte, içerik verilerinin ele geçirilmesi tedbirinin, ancak ağır suçlar bakımından uygulanabileceği, ancak bu son kavramın Sözleşme'de tanımlanmadığı ifade edilmelidir[107].

Bir çok yazarın belirttiği gibi, Sözleşme'nin en önemli bölümü, 3. Kısmıdır[108]. Zira, sınır tanımayan niteliğe sahip, bir çok devlet üzerinde aynı anda işlenebilen ve soruşturulması ile kovuşturulması çok teknik ve zorunlu bir süreç gerektiren, delillerin her an yok olabildiği bir suç türüyle mücadelede, etkin ve çok hızlı uluslararası işbirliğinin varlığı şarttır[109].

Uluslararası işbirliğine dair kısma geçmeden, Sözleşme'ye yönelik bazı genel eleştirilere değinmekte fayda vardır. Birinci eleştiri, Sözleşme'nin 44. maddesinde öngörülen, antlaşmanın tadiline dair zorlu şartlar getiren düzenleme sebebiyle, siber suçluluğun hızla değişen yapısı karşısında, Sözleşme'nin kısa sürede gelişmelerin gerisinde kalma riskidir[110]. Belki, Protokollerle Sözleşme'yi takviye etmek yoluyla bu engel kısmen aşılabilir[111]. Fakat Protokol taslağının hazırlanması, görüşülmesi, kabulü ve yürürlüğe girmesi de zaman alacaktır. Kaldı ki, Ana Sözleşme'ye taraf bazı devletlerin Protokolleri onaylamama ihtimali her zaman mevcuttur.

İkinci eleştiri, çekincelere geniş ölçüde imkan veren Sözleşme rejimi (m. 42) sebebiyle, bazı taraf devletlerin ulusal maddi hukuklarını Sözleşme gerekleriyle uyumlaştırma gereği duymayabileceğidir[112]. Bunun da, en azından söz konusu suçlar açısından, uluslararası işbirliğini daha en baştan imkansız kılacağı ortadadır.

Diğer bir eleştiri, gelişmekte olan devletlerin Sözleşme'nin hazırlanma sürecinde yeterli şekilde temsil edilmemiş olmalarıdır[113]. Keza, sivil toplum örgütlerinin görüşlerinin de yeterli ölçüde alınmadığı ifade edilmektedir[114].

---

[105] Keskin, İÜHFM, s. 158; Helvacıoğlu, s. 294; Uçkan/Beceni, s. 383; Koca, s. 791.

[106] Uçkan/Beceni, s. 383-384.

[107] Keskin, İÜHFM, s. 158. Keza, trafik verilerinin gerçek zamanlı olarak toplanmasında da, taraf devletler, tedbirin uygulanmasını, bazı koşullarla, belirli suç tipleriyle sınırlama hakkına sahiptirler (age, s. 159).

[108] Csonka s.495; Calderoni s.346.

[109] Simion, s.310.

[110] Weber s.442. Hatta, genel olarak, siber suçluluğun hızla değişen teknolojiye dayalı olduğu, geleneksel hukuki süreçlerin ise yavaş ilerlediği, bu bakımdan, çıkarılacak kanunların ya bu değişiklikle baş edebilecek sağlamlıkta olması ya da alternatif denetim mekanizmalarına güvenmemiz gerektiği vurgulanmaktadır, bkz. Moitra s.464.

[111] Sınar, Özek Armağanı, s. 786.

[112] Weber s.444.

[113] Gercke, *Understanding Cybercrime,* s.202.

[114] Uçkan/Beceni, s. 382. Yine bkz. Sınar, Özek Armağanı, s. 783.

Önemli bir eleştiri de, Sözleşme'nin internet hizmet/servis sağlayıcılarına (Internet Service Providers – ISP)[115] fazla ağır bir yük getirdiğidir[116]. Buna göre; bir çok verinin muhafazası gerekecek, adli yardım talepleri sebebiyle servis sağlayıcıların binlerce talebi işleme koyması büyük masraf gerektirip bu da müşterilere daha yüksek hizmet ücretleri olarak yansıtılacak, söz konusu verilerin tutulması ve herhangi bir taraf devletin istemi üzerine temin edilmesi, özel hayat açısından ve şirketlerin "müşteri gizliliği" politikaları açısından sorun arz edecektir[117].

Buna karşılık, özel hayatın gizliliğine dair ciddi itirazlara yol açmış olmakla birlikte[118]; Sözleşme'nin aşırı müdahaleci bir elektronik denetleme sistemi öngörmediği de vurgulanmalıdır. Elbette, birtakım verilere el konulmasına ya da bunların muhafazına ya da bunların açıklanmasına yönelik hükümler mevcuttur; fakat resmi bir ceza soruşturması olmadıkça, gerek servis sağlayıcı gerekse polis tarafından, kişisel iletişimin denetlenmesine yer verilmemiştir[119]. Kaldı ki, 2. Kısımda öngörülen tüm yetkilerin kullanımı, 15. maddede sıkı koşullara bağlanmıştır; ulusal hukuktaki usullere ve güvencelere uyulacaktır, bu usuller de, aralarında Avrupa İnsan Hakları Sözleşmesi ve Birleşmiş Milletler Kişisel ve Siyasal Haklar Uluslararası Sözleşmesi'nin de açıkça sayıldığı, uygulanabilir insan hakları belgelerine ve orantılılık ilkesine uygun olacaktır[120]. Bu nedenle, mahremiyet kavramına veya özel hayatın gizliliğine açıkça yer verilmemesi eleştirilebilir bir husus olsa da[121], bu hakların Sözleşme'de korunmadığını söylemek doğru değildir[122].

Öte yandan, servis sağlayıcıların trafik verilerini düzenli olarak toplama ve belirli bir süreyle saklama zorunluluğuna dair bir hüküm, üzerinde uzlaşı sağlanamaması sebebiyle Sözleşme'ye konulmamıştır[123].

---

[115] Bunlar, kullanıcıların internete "erişimini sağlayan ve/veya elektronik hizmetlerin kullanıcıların kullanımına sunulmasına aracılık eden gerçek veya tüzel kişiler"dir (bkz. Avşar/Öngören, s. 118). Servis sağlayıcısı, "kendi bilgisayarlarını kullanıcıların internet'e ulaşabilmeleri için bir giriş kapısı (gateway) olarak hizmete sunan internet süjesi"dir (Sınar, İnternet ve Ceza Hukuku, s. 41). Türk Hukuku bakımından bkz. 5651 sayılı 'İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un m. 2/1-e hükmü. Siber Suç Sözleşmesi'nde ise, kavram, "hizmetlerinden faydalanan kullanıcılara bir bilgisayar aracılığıyla iletişim kurma imkânı sağlayan her türlü kamu ve özel sektör tüzel kişisi, ve söz konusu iletişim hizmeti veya bu hizmetin kullanıcıları adına bilgisayar verilerini işleyen ve saklayan diğer her türlü kişi ve kuruluş" olarak tanımlanmıştır (m. 1).

[116] Vatis, s. 218; Uçkan/Beceni, s. 382.

[117] Keyser s.325. Yine bkz. Sınar, Özek Armağanı, s. 780.

[118] Csonka s.490; Vatis, s. 218; Uçkan/Beceni, s. 382; Lim, s. 332.

[119] Csonka s.490; Broadhurst s.421.

[120] İçel, İÜHFM, s. 6-7; Keskin, İÜHFM, s. 160-161. Bu nedenle, temel hak ve özgürlüklere aykırı adli yardım taleplerinin yerine getirilmek zorunda kalınacağı yönündeki eleştiriye (Uçkan/Beceni, s. 385) katılmıyoruz.

[121] Bu yönde Uçkan/Beceni, s. 382.

[122] Fakat, bu husus, belki, kamusal otorite ile bireysel hak ve özgürlükler arasındaki denge bağlamında, Sözleşme'nin ilk değer lehine taraflı davrandığı yönündeki eleştirilere (Sınar, Özek Armağanı, s. 781) haklılık kazandırabilir.

[123] Csonka s.491.

§ 4. Uluslararası Adli Yardımlaşma

I. Adli Yardımlaşma Konusunda Türk Uygulamasına Dair Genel Bilgi

Sözleşme'de yer alan konuya dair hükümlere geçmeden önce, adli yardımlaşma hususundaki Türk uygulamasını kısaca belirtmek isteriz[124].

Almanya, Avusturya, İsviçre gibi bazı devletlerin aksine, Türk yasakoyucusu, adli yardımlaşmanın çeşitli yönlerini düzenleyen bağımsız bir genel kanunu yürürlüğe koymayı seçmemiştir[125]. Yurtdışında sürdürülen muhakeme işlemlerine ilişkin olarak kendilerinden adli yardım talep edilmesi durumunda, Türk ulusal makamlarının takip etmesi gereken usule ilişkin olarak da yasal düzenleme mevcut değildir. Bu bakımdan, genel olarak uygulanabilir bir çerçeve yoktur; farklı işbirliği türlerine dair kurallar, Türkiye'nin tarafı olduğu çok-taraflı ya da iki-taraflı uluslararası antlaşmalarda veya bu antlaşmalara uygun olarak yürürlüğe konulmuş ulusal düzenlemelerde yer almaktadır. Buna ilaveten, geri vermeye ilişkin kurallar, Anayasa'nın 38. maddesinde ve 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun 18. maddesinde yer almaktadır. Genel olarak, farklı türlerde işbirliğini ele alan özel bir düzenleme yapılmasında fayda olduğu söylenebilir[126].

Uygulamada, adli işbirliğine dair taleplerin hazırlanmasında ve yerine getirilmesinde, Adalet Bakanlığı merkezi role sahiptir. Talepler, genel olarak, 1959 tarihli **Ceza İşlerinde Karşılıklı Adli Yardımlaşmaya dair Avrupa Sözleşmesi** çerçevesinde yerine getirilmektedir.

1984 tarihli ve 2992 sayılı Adalet Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin Değiştirilerek Kabulü Hakkında Kanun'un 13/A maddesine göre, "Hukuki ve cezai konularda uluslararası adli yardımlaşma; tebligat, istinabe, suçluların iadesi, hükümlülerin transferi, kovuşturmaların aktarılması işlemlerini yapmak", Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün (UHDİGM) görevleri arasına girer. Müdürlük, adli yardım taleplerini almakta ve gerekli mercilere yönlendirmektedir. Bu görev, Türkiye'nin konuya ilişkin taraf olduğu çok taraflı ve ikili antlaşmalar doğrultusunda yürütülmektedir. Uygulanabilir

---

[124] Bu kısım, daha önceki bir konferansta sunduğumuz metinden özetlenmiştir (R.M. Önok, **'International Judicial Co-operation in Criminal Matters', Fight Against Fraud and Corruption: Strengthening Cooperation Between Turkish Authorities and EU Institutions, ERA (Academy of European Law) in partnership with the Istanbul Kültür University (co-financed by the European Commission (OLAF)), İstanbul, 29-30 Nisan 2010).**

[125] Tezcan/Erdem/Önok, Uluslararası Ceza, s. 181.

[126] Bkz. bu yönde Feridun Yenisey, *Milletlerarası Ceza Hukukunda Yeni Gelişmeler*, Ceza Hukuku Günleri, 70. Yılında Türk Ceza Kanunu - Genel Hükümler, İstanbul, 1998, s. 52; Tezcan/Erdem/Önok, Uluslararası Ceza, s. 181; Fatih S. Mahmutoğlu, *Suçluların Geri Verilmesi*, Ceza Hukuku Günleri, 70. Yılında Türk Ceza Kanunu - Genel Hükümler, İstanbul, 1998, s. 66; Faruk Turhan, *Die Rechtsstellung des Auszuliefernden nach türkischem Recht unter rechtsvergleichender Berücksichtigung des deutschen Rechts,* Frankfurt am Main, 1993, s. 43, 304-305.

bir antlaşma hükmünün yokluğunda ise, uluslararası örfi hukuka ve mütekabiliyet ilkesi esaslarına göre hareket edilmektedir.

UHDİGM'in konuya dair genelgeleri uygulamada önemli yere sahiptir. Bu konuda, 1.3.2008 tarihli ve 69/1 sayılı "Cezai İşlere İlişkin Uluslararası İşbirliğinde Adli Makamlarımızca Dikkat Edilmesi Gereken Hususlar"a dair genelge yol göstericidir. Keza, 1.3.2008 tarihli ve 66/1 sayılı "Adli Yardım Taleplerinin İletilmesine İlişkin Avrupa Sözleşmesinin Uygulanması" hakkındaki genelge de önemlidir.

Genel olarak, uygulamada, adli işbirliği konusunda Türkiye'nin pozitif bir yaklaşım sergilediği, gelen taleplerin esnek ve işbirlikçi bir şekilde yerine getirildiği belirtilmektedir[127].

Cezai işlerde adli yardımlaşmaya dair Türkiye'nin taraf olduğu çok sayıda uluslararası antlaşma mevcuttur. Bunlardan bazıları şunlardır[128]:

- Suçluların İadesine Dair Avrupa Sözleşmesi (18.4.1960, 18.4.1960)[129],

- Ceza İşlerinde Karşılıklı Adli Yardımlaşmaya Dair Avrupa Sözleşmesi[130] (12.6.1962, 22.9.1969),

- Ceza Kovuşturmalarının Aktarılmasına Dair Avrupa Sözleşmesi (30.3.1978, 28.1.1979),

- Ceza Yargılarının Uluslararası Değeri Konusunda Avrupa Sözleşmesi (26.7.1974, 28.1.1979),

- Terörizmin Önlenmesine Dair Avrupa Sözleşmesi (4.8.1978, 20.8.1981),

- Hükümlülerin Nakline Dair Sözleşme (1.7.1985, 1.1.1988);

- Suçtan Kaynaklanan Gelirlerin Aklanması, Araştırılması, Ele Geçirilmesi ve El Konulmasına İlişkin Avrupa Konseyi Sözleşmesi (1.9.1993, 1.2.2005),

- Yolsuzluğa Dair Ceza Hukuku Sözleşmesi (1.7.2002, 1.7.2004),

- Terörizmin Önlenmesine Dair Avrupa Konseyi Sözleşmesi (1.6.2007, 23.3.2012, yürürlük 1.7.2012).

Nihayet, Türkiye'nin taraf olduğu, 40 civarında ikili iade antlaşması veya genel adli yardımlaşma antlaşması mevcuttur[131].

---

[127] CyberCrime@IPA project, Turkey Country profile (Version 25 January 2011), (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/cyber_cp_Turkey_2011_January.pdf) [son erişim 10.10.2011].

[128] Gösterilen ilk tarih, antlaşmanın uluslararası alanda yürürlüğe girme tarihi, ikincisi ise, Türkiye bakımından yürürlüğe girme tarihidir.

[129] Türkiye, İkinci Ek Protokolü de 1992 tarihinde onaylamıştır.

[130] Türkiye 1978 tarihli Ek Protokolü de onaylamıştır.

[131] http://www.uhdigm.adalet.gov.tr/sozlesmeler/ikitaraflisoz/ikili.html

II. Siber Suç Sözleşmesi'ne göre Uluslararası Adli Yardımlaşma Konusundaki Temel İlkeler

Budapeşte Sözleşmesi'nin 23. maddesine göre, uluslararası işbirliği konusunda öngörülen temel ilkeler şunlardır[132]:

- Taraf Devletler mümkün olan en geniş biçimde işbirliği yapacaklardır. Bu çerçevede, bilgi ve delillerin hızlı akışı önündeki engeller asgariye indirilecektir. Elbette, burada somut bir yükümlülük öngören bir hükümden ziyade, çerçeve bir hüküm getirilmiştir. Sonraki hükümlerde bu çerçevenin içi doldurulmaya çalışılmıştır.

- Bu işbirliği yükümlülüğü, hem bilgisayar sistemleri ve verilerine ilişkin tüm suçları hem de bir bilgisayar sistemi aracılığıyla işlenmeyen, sıradan bir suçun delillerinin elektronik şekilde toplanması bakımından mevcuttur[133]. Bu bakımdan, Sözleşme'nin uygulama alanı oldukça geniştir. Gerçekten, Sözleşme'nin önemli bir özelliği, usuli nitelikli hükümlerinin bir çoğunun uygulama alanının siber suçlarla sınırlı olmaması, "elektronik şekilde" (*in electronic form*) delil toplanması gereken herhangi bir suçu kapsamasıdır[134].

- Siber Suç Sözleşmesi'nin uluslararası işbirliğine dair 3. Kısım hükümleri, cezai işlerde adli yardımlaşma ve bu arada iadeye ilişkin olan, uluslararası çok taraflı antlaşma hükümlerine ve aynı konudaki iki taraflı antlaşmalara göre üstün değildir. Bu bakımdan, karşılıklı adli yardımlaşmaya dair mevcut çok taraflı ve ikili antlaşmalarla öngörülen rejimler aynen korunmuştur; bunların yerine yeni bir rejim yaratılmış değildir[135]. Bunun sebebi, söz konusu sözleşmelerin zaten cezai işlerde delil elde etmeye yönelik olarak özellikle tasarlanmış, yeni türden antlaşmalar olmasıdır[136]. Bununla birlikte, aksi öngörülmedikçe, mevcut antlaşma hükümlerinin uygulama önceliğine sahip olması, Siber Suç Sözleşmesi'ne taraf olmanın faydalarını azaltan bir unsur olarak değerlendirilmiştir[137].

- Hatta, antlaşma hükümleri, uluslararası işbirliğine dair ulusal mevzuat hükümlerine de üstün değildir[138], her bir devletin kendi kuralları da, bir kaç istisna dışında, uygulanmaya devam edecektir.

---

[132] Weber, s. 433.

[133] Explanatory Report to the Convention on Cybercrime, para. 243; Broadhurst s.421; Csonka s.495.

[134] Vatis, s. 208; Uçkan/Beceni, s. 383.

[135] Gercke, *Understanding Cybercrime,* s.463.

[136] Weber, s.442.

[137] Weber, s.442.

[138] Explanatory Report to the Convention on Cybercrime, para. 244. Kaldı ki, uluslararası hukuk bakımından önemli olan, uluslararası alanda yüklenilen yükümlülüklerin bir şekilde ifa edilmesidir. Bunun modalitesini belirlemek ise iç hukuka kalmıştır. Bu bağlamda, antlaşmaların ulusal hukuktaki yeri (ve normlar hiyerarşisindeki sıralaması) da, her bir devletin kendi iç hukuk kurallarına göre belirlenir (bkz. Antonio Cassese, *International Law* (2nd ed, Oxford: Oxford University Press, 2005), s.218; Rebecca M.M. Wallace & Olga Martin-Ortega, *International Law* (6th ed., Cornwall: Sweet & Maxwell, 2009) s.38).

III. Siber Suç Sözleşmesi'nde Öngörülen Adli Yardımlaşma Usulleri

En temel yardımlaşma türü olan geri verme bakımından, genel kurallar, Budapeşte Sözleşmesi'nin 24. maddesinde öngörülmüştür.

– İade yükümlülüğü, sadece belirli ağırlıktaki suçlar açısından mevcuttur. Buna göre, 24. madde; Sözleşme'nin 2.-11. maddeleri arasında yer alıp, her iki taraf devletin yasalarına göre üst sınırı en az bir yıl hapis cezasını gerektiren suçlar bakımından uygulanır (m. 24/1). Bazı suçlar bakımından[139], taraf devletlerin daha kısa süreli hapis cezası öngörmesi mümkün olduğundan, bir yıllık azami sınır getirilmiştir[140]. Burada önemli olan, kanunda öngörülen soyut ceza olup, somut olayda hükmolunan cezaya bakılmaz[141]. Öte yandan, yine sair antlaşma hükümleri saklı tutulduğundan, belirli devletler arasındaki ilişkide, daha yüksek bir ceza sınırını öngören bir düzenleme mevcutsa, uygulanmaya devam edecektir. Bazı suç tiplerini de kapsayan belirli hükümler bakımından çekince koyma imkanı Sözleşme'de tanındığından, iade, çifte cezalandırılabilirlik (*double criminality*) koşuluna bağlanmıştır[142].

– Maddenin ikinci fıkrasına göre, 1. fıkrada tanımlanan suçlar, taraf devletler arasında mevcut ve ileride akdedilebilecek tüm iade antlaşmalarında, iadesi mümkün suçlar olarak düzenlenecektir.

– Maddenin üçüncü fıkrasına göre, aralarında iade antlaşması olmadığı ya da mevcut antlaşma işbu Sözleşme'de öngörülen suçları kapsamadığı takdirde, diğer bir taraf devletin iade talebini yerine getiremeyen taraf bir devlet, işbu Sözleşmeyi yasal dayanak yaparak, iadeyi gerçekleştirebilir. Fakat bunu yapmak zorunda da değildir.

- Maddenin beşinci fıkrasına göre, iadenin gerçekleştirilmesi, yürürlükteki ikili antlaşmalarda ve ulusal mevzuatta yer alan hükümlerde aranan koşulların gerçekleşmesine bağlıdır. Bu bakımdan, Türkiye ileride Budapeşte Sözleşmesi'ne taraf olursa, Suçluların İadesine Dair Avrupa Sözleşmesi ve TCK m. 18'de yer alan sınırlamaları uygulayabilecektir.

- Maddenin altıncı fıkrasında, "aut dedere aut judicare" (ya iade et ya yargıla) ilkesine yer verilmiştir. Kendisinden iade talep edilen devletin vatandaşı olduğu için iadesi kabul edilmeyen şahsın yargılanmasını, talep eden taraf devlet isteyebilir. Bu durumda, talebi alan devlet, davayı kovuşturulmak üzere kendi yetkili mercilerine havale etmelidir. Böyle bir talep gelmezse, talep edilen devletin bu konuda bir yükümlülüğü olmaz. Hatta, böyle bir talebin varlığında bile, bu kişi hakkında kovuşturma yapma yükümlülüğü yoktur; talep edilen devlet, nihai sonucu talep eden devlete bildirecektir[143]. Türkiye Sözleşme'ye taraf olduğunda, her ne kadar Sözleşme

[139] Örneğin 2. maddedeki izinsiz erişim ve 4. maddedeki verilere müdahale gibi.
[140] Keyser, s.317.
[141] Explanatory Report to the Convention on Cybercrime, para. 245.
[142] Gercke, *Understanding Cybercrime,* s. 463.
[143] Vatis, s. 214.

hükümleri iç hukukumuzun parçası haline gelse de, uygulamada kolaylık ve açıklık sağlaması bakımından, TCK m. 18'de, bu fıkraya paralel bir düzenleme yapılabilir.

Karşılıklı yardımlaşmaya dair genel ilkelere 25. maddede yer verilmiştir:

- Maddenin 1. fıkrasına göre, yardımlaşma "mümkün olan en geniş ölçüde" gerçekleştirilecektir. Burada da, işbirliği yükümlülüğü, hem bilgisayar sistemleri ve verilerine ilişkin tüm suçlar hem de bir bilgisayar sistemi aracılığıyla işlenmeyen, sıradan bir suçun delillerinin elektronik şekilde toplanması bakımından mevcuttur.

- Maddenin ikinci fıkrasına göre, taraf devletler, 27.-35. maddeler arasında yer alan yükümlülüklerin yerine getirilebilmesini mümkün kılacak yasal ve sair tedbirleri almakla yükümlü kılınmışlardır. Sözleşmeye dair açıklayıcı rapora göre[144], devletlerin bu hükümleri doğrudan uygulanabilir olarak addederek[145], adli yardımlaşmaya dair mevcut mevzuatlarında yeterli esnekliğe sahip oldukları için, Sözleşme'de öngörülen karşılıklı yardımlaşma tedbirlerini yerine getirebilmeleri beklenmektedir. Bu mümkün değilse, bunu mümkün kılacak ulusal düzenlemeler en kısa sürede yapılmalıdır[146]. Türk Hukuku bakımından, ileride Sözleşme'ye taraf olması durumunda, m. 18, 19, 21'de yer alan ve ulusal hukukta yer verilmesi gereken tedbirlere dair hükümler, yeterince somut ve doğrudan uygulanabilir olduklarından, Türkiye açısından gerekli yasal dayanağı sağlayacaktır. Buna karşılık, m. 16, 17 ve 20 açısından[147], bunların uygulanmasını mümkün kılacak düzenlemelere (ve idari yapılandırmaya) ihtiyaç olacaktır. Bu bakımdan, hangi mercilerin bu konuda karar vermeye yetkili oldukları, izlenecek prosedür, tedbiri uygulamaya yetkili makamın belirlenmesi gibi hususların kanunla düzenlenmesi gerekecektir.

- Maddenin üçüncü fıkrasında, acil durumlarda, adli yardımlaşma taleplerinin yapılmasında ve buna ilişkin iletişimlerde, faks ve elektronik posta gibi hızlı iletişim araçlarına başvurulması mümkün kılınmaktadır. Bunun için, ilgili yöntemin güvenlik ve doğruluk açısından güvenilir olması aranmaktadır. Bu hüküm, bilgisayarda saklanan verilerin geçici olabilmesi ve kolaylıkla kaybolabilmesi açısından

---

144 Bizdeki "Genel Gerekçe"ye tekabul ettiği söylenebilir (bkz. İçel, İÜHFM, s. 6).

145 Yani, taraf Devletlerin, söz konusu maddelerde yer alan yükümlülüklerin iç hukukta uygulanabilecek şekilde somut ve belirli olduğunu ve bunların uygulanabilmesi için ayrıca ulusal alanda düzenleme yapmanın gerekli olmadığını kabul etmeleri beklenmektedir (Melda Sur, *Uluslararası Hukukun Esasları*, 4. Baskı, İstanbul, 2010, s. 52).

146 Explanatory Report to the Convention on Cybercrime, para. 255. Örneğin, uluslararası hukuk ile ulusal hukuk arasındaki ilişkide dualizmi (ikici görüşü) kabul eden, ABD gibi bir devlet bakımından, uluslararası antlaşmaların iç hukuk sisteminin bir parçasına dönüştürülmeksizin, iç hukukta doğrudan uygulanabilirliği hiç bir zaman söz konusu değildir (Hüseyin Pazarcı, *Uluslararası Hukuk*, 9. Bası, Ankara, 2010, s. 19; Yusuf Aksar, *Teoride ve Uygulamada Uluslararası Hukuk* – I, Ankara, 2012, s. 173).

147 Saklanan/depolanmış bilgisayar verilerinin hızlandırılmış korunması (m. 16), trafik verilerinin hızlandırılmış korunması ve kısmi açıklanması (m. 17), trafik verilerinin gerçek zamanlı olarak toplanması (m. 20).

önemlidir[148]. Acil durumlarda, gerek talebin yapılmasında gerekse cevabın verilmesinde hızlı iletişim yöntemlerine başvurulabilecektir. Daha sonra, bu talebin resmi yollarla teyit edilmesi istenebilecektir. Maddede sayılan faks ve elektronik posta, örnek niteliğindedir; olayın mahiyetine uygun düştüğü ölçüde, başka yöntemlere de başvurulabilir. Fakat, her koşulda, ulusal hukuk bu yöndeki talepleri yerine getirmeyi mümkün kılacak şekilde düzenleme içermelidir[149]. Bu bakımdan, Türkiye'nin Sözleşme'ye taraf olması durumunda, söz konusu yükümlülükleri yerine getirebilmemizi sağlayacak hukuki düzenlemeler mutlaka yapılmalıdır.

- Maddenin dördüncü fıkrasına göre, karşılıklı yardımlaşma, Sözleşme'nin bu kısmında aksi açıkça öngörülmedikçe, yürürlükteki ikili antlaşmalarda ve ulusal mevzuatta yer alan hükümlerde aranan koşullar çerçevesinde yürütülür. Bu düzenleme sayesinde, yardım talebinin konusu olabilecek şahısların temel haklarının korunması açısından güvence sağlanmış olacaktır[150]. Zira, özellikle ulusal düzenlemelerde bu konuda birtakım kısıtlamalar mevcuttur. Her ne kadar ulusal mevzuata atıf yapılmış ise de, bazı durumlarda (örneğin, m. 27), ikili bir antlaşma yoksa, ulusal hukuk yerine, doğrudan m. 25 hükümleri uygulanacaktır. Örneğin, saklanan bilgisayar verilerinin korunması açısından, yardımlaşma talebi "çifte cezalandırılabilirlik" koşuluna bağlı olarak reddedilemez. Zaten bu durumda, verinin içeriği öğrenilmemektedir; ileride, buna yönelik bir istem, adli yardımlaşma talebine konu olacak ve bu noktada "çifte cezalandırılabilirlik" koşuluna bağlı olarak, talep reddedilebilecektir[151]. Yine, 2.-11. maddeler arasında sayılan suçlara dair yardımlaşma talepleri bakımından, talebin mali bir suça ilişkin olduğu gerekçesine dayanarak, salt bu nedenle reddedilmesi mümkün değildir.

- Maddenin 5. fıkrası ise, ulusal mevzuatta aranabilecek "çifte cezalandırılabilirlik" koşulu açısından bir sınırlama getirmektedir. Buna göre, fiilin hukuki nitelendirilmesi, yani her iki ülkede aynı şekilde tavsif edilmiş olması önemli olmayıp, suçun maddi unsurunu oluşturan davranışın her iki ülke kanunlarında ceza hukuku anlamında suç oluşturması yeterlidir. Kaldı ki, Sözleşme'ye taraf devletler, zaten 2.-11. madde arasında sayılan suçları ulusal hukuklarında düzenlemekle yükümlüdürler, bu bakımdan "çifte cezalandırılabilirlik" koşulu gerçekleşmiş olacaktır[152]. Birden çok ülkeyi ilgilendiren siber suçlarda, bunlardan birinde bile fiilin suç olarak düzenlenmemiş olması durumunda adli işbirliğinin olanaksız hale geldiği düşünüldüğünde[153], bu hükmün önemi açıktır.

---

[148] Grabosky, s. 214; Weber, s. 434; International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 3.

[149] Explanatory Report to the Convention on Cybercrime, para. 256.

[150] International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 3; Calderoni, s. 348.

[151] Calderoni, s. 349.

[152] International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 4.

[153] Csonka, s. 478.

26. maddede, "anında iletilen bilgiler" (*spontaneous information*) düzenlenmiştir:

- Buna göre, bazı durumlarda, soruşturma ya da kovuşturmayı yürüten devletin varlığından bile haberdar olmadığı, başka bir devlette bulunan bilgiler mevcut olabilir. Bu durumda, haliyle, adli yardım talebi söz konusu olamayacaktır[154]. İşte, başka bir devletin yürüttüğü soruşturma ya da kovuşturmada yardımcı olabilecek bilgilere sahip olduğunu düşünen devlet, kendisinden talepte bulunulmaksızın ve ulusal hukukun izin verdiği ölçüler içerisinde, söz konusu bilgiyi ilgili devlete yollayabilecektir. Fakat, bu aşamada, bu konuda bir mecburiyet söz konusu değildir. Bilgiyi gönderen devlet, bilginin gizli tutulmasını isteyebilir. Bunun amacı, kendi yürüttüğü soruşturmanın zarar görmesini önlemektir[155].

27. maddede, uygulanabilir uluslararası antlaşmaların yokluğunda, karşılıklı yardımlaşma talebine ilişkin usuller düzenlenmiştir:

- Avrupalı devletlerin yararlanabileceği bir çok ortak antlaşma zaten mevcuttur. Buna karşılık, Budapeşte Sözleşmesi'ne, Avrupa Konseyi'ne taraf olmayan devletler de taraf olabilecektir ve bunların söz konusu diğer adli yardımlaşma sözleşmelerine taraf olması mümkün değildir. Böyle durumlarda, aralarında uygulanabilir ortak bir antlaşma mevcut olmayan devletler açısından, adli yardımlaşmanın temel prensipleri m. 27'de düzenlenmiştir[156]. Yani, bu Sözleşme, aralarında özel bir antlaşma bulunmayan taraf devletler açısından, karşılıklı adli yardımlaşma antlaşması işlevini görecektir[157]. Demek ki, Sözleşme'nin rolü ikincildir: şayet ilgili devletler arasında bu konuda uygulanabilir çok taraflı ya da ikili antlaşma mevcutsa, kural olarak o antlaşmalar uygulanmaya devam edecektir; fakat ilgili taraflar, söz konusu antlaşma yerine işbu Sözleşmenin bu hükmünün bir kısmını ya da tümünü uygulamayı kararlaştırabilirler. Böylece, mevcut karşılıklı adli yardım antlaşmaları ile kurulan rejimin sürdürülmesi daha pratik görülmüştür[158]. Bu bakımdan, Türkiye ileride Sözleşme'ye taraf olsa bile, Sözleşme'nin 3. Kısmında öngörülen yardımlaşma türlerinin çoğu, yine Avrupa Konseyi'nin Ceza İşlerinde Karşılıklı Adli Yardımlaşma Sözleşmesi'ne göre gerçekleştirilmeye devam edecektir[159]. Öte yandan, siber suçların giderek artan sıklıkla organize olarak işlendiği düşünülecek olursa[160],

---

154 Keyser, s. 318.

155 Gercke, *Understanding Cybercrime,* s. 466.

156 International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 5; Keyser, s. 318.

157 Downing, s. 761.

158 Calderoni, s. 348.

159 Explanatory Report to the Convention on Cybercrime, para. 262.

160 Palermo Sözleşmesi'nde tanımlanan "örgütlü suç grubu", "ciddi suç" gibi terimlerde yer alan unsurların siber suçluluğun arz ettiği görünüme uygun olduğu hk. bkz. Simion s. 308. Yine bkz. Broadhurst, s.417-418 (siber suçluluğun bir çok olağan görünüm şekli, "ciddi suç" tanımının unsurlarını taşımaktadır).

Türkiye'nin taraf olduğu 2000 tarihli Sınıraşan Örgütlü Suçluluğa dair Birleşmiş Milletler Palermo Sözleşmesi de önemlidir, orada yer alan işbirliği yöntemlerine de başvurmak mümkündür. Özellikle, Türkiye ile ilgili devlet arasında ikili bir antlaşma mevcut olmadığında, diğer devletin de buna taraf olması durumunda, Palermo Sözleşmesi iyi bir dayanak olabilecektir. Keza, ikili antlaşmalar mevcutsa, bunlar uygulanacaktır. Bununla birlikte, Sözleşme'nin 29 vd. maddelerinde, bilişim suçları ya da bilgisayarla bağlantılı suçlar açısından öngörülen bazı özel tedbirlere ilişkin hükümler, söz konusu çok taraflı ya da ikili antlaşmalarla kurulan mevcut rejimi takviye edecektir. Demek ki, 27. madde hükümleri, uygulanabilir çok taraflı ya da ikili bir antlaşmanın yokluğunda, ulusal mevzuat hükümlerinin yerine uygulanacaktır. Bununla birlikte, bir çok devletin ulusal mevzuatında yer alan, adli yardımlaşmaya dair, örneğin, tanık ifadesinin alınması, bazı resmi belgelerin temini, müsadere konusunda yardım gibi, bazı hükümlere 27. maddede yer verilmemiştir. Bu durumlarda, m. 25/4 gereği, kendisinden talepte bulunulan devletin ulusal mevzuatına göre işlem yapılacaktır[161].

- İkinci fıkraya göre, taraf devletler, yardım taleplerinde bulunmak, bu taleplere cevap vermek, bu taleplerin gereğini yerine getirmek ya da bunların gereğini yerine getirecek mercilere bu talepleri iletmekle görevli, merkezi bir merci ya da merciler belirleyecektir; söz konusu merciler birbirleriyle doğrudan haberleşeceklerdir. Buna mukabil, dokuzuncu fıkraya göre, acil durumlarda, yardım talepleri ya da bu taleplere ilişkin yazışmalar, doğrudan, talep eden tarafın adli mercileri aracılığıyla, kendisinden yardım talep edilen tarafın adli mercilerine iletilebilir. Tüm bu hükümlerin amacı, işlemlerin hızlı yürütülmesini sağlayabilmektir[162]. Uygulamaya bakarsak, en sıklıkla başvurulan formül, Adalet Bakanlığı'nı merkezi yetkili olarak tayin etmektir. Ancak, Emniyet Teşkilatı içindeki bir birimi belirleyen ülkeler de mevcuttur, örneğin, Ermenistan ve Norveç gibi. Bunun yanı sıra, örneğin, Azerbaycan ise, Ulusal Güvenlik Bakanlığı'nı tayin etmiştir. Bazı devletler ise, ceza muhakemesinin farklı aşamalarına göre ayrımlar yapmışlardır. Örneğin, Bulgaristan, yargılama aşamasında Adalet Bakanlığı'nı, bundan önce ise, Yüksek Mahkeme[163] Başsavcılığı'nı; Macaristan, ceza muhakemesi başlamadan önce, polis teşkilatı içindeki bir birimi, başladıktan sonra, Macaristan Başsavcılığı'nı; Moldova, ceza kovuşturması aşamasında Başsavcılık makamını, infaz aşamasında ise Adalet Bakanlığı'nı; Romanya, soruşturma aşamasında Yüksek Mahkeme[164] Başsavcılık makamını, yargılama ve infaz aşamasında Adalet Bakanlığı'nı tayin etmiştir[165].

---

[161] Explanatory Report to the Convention on Cybercrime, para. 264.

[162] Keyser, s. 318.

[163] Bizdeki Yargıtay'a tekabül etmektedir.

[164] Bizdeki Yargıtay'a tekabül etmektedir.

[165] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp (son erişim 10.10.2011).

- Üçüncü fıkraya göre, bu maddeye göre yapılacak yardımlaşma talepleri, talep edilen devletin yasalarına uygun olmaması haricinde, talep eden devletin öngördüğü prosedürlere göre yerine getirilecektir. Buradaki amaç, talep eden devletin ulusal mevzuatında öngörülen delil elde etme yöntemlerine uygun hareket edilmesi, böylece, elde edilen delillerin kendi mahkemeleri nezdinde kullanılabilmesini sağlamaktır[166]. Talep edilen işlem bakımından, kendisinden talepte bulunulan devletin konuya dair temel kurallarına riayet edilecektir. Fakat bazı durumlarda, talepte bulunan devlet kanununa göre delilin geçerli olması için, bazı ilave teknik şartlar aranmış olabilir, örneğin, tanıklıktan önce yemin verdirilmesi gibi. İşte, bu gibi durumlarda, talepte bulunan devletin kanunlarına göre aranan bu şarta riayet edilerek, yardımlaşma talebi yerine getirilecektir; kendisinden talepte bulunulan devlet, kendi kanununda böyle bir usule imkan veren bir hükmün yer almadığından bahisle, talep eden devletin uygulanmasını istediği usulü yerine getirmeyi reddedemeyecektir[167]. Bu hüküm, Anayasa m. 38'de, çok katı bir delil yasağı kuralına sahip olan Türkiye açısından özellikle önem taşımaktadır.

- Dördüncü fıkrada ise, yardımlaşma talebinin reddedilmesini mümkün kılan sebepler sayılmıştır. Bunlar iki tanedir: a) Suçun, talepte bulunulan devlet tarafından siyasi suç ya da siyasi suçla bağlantılı suç olarak kabul edilmesi; b) talebin yerine getirilmesinin, talepte bulunulan devlet tarafından, kendi egemenliğine, güvenliğine, kamu düzenine veya diğer temel yararlarına zarar verebilecek mahiyette mütalaa edilmesi. "Diğer temel yararlar" kavramının dar yorumlanması gerekecektir[168]. Fakat kavramın içeriğini somut olarak belirlemek de mümkün değildir. Doktrinde, yardımlaşma talebinin reddedilmesini mümkün kılan nedenlerin azaltılması gerektiği; özellikle b) bendi altındaki red sebeplerinin, spesifik ve inandırıcı nedenler sunmaksızın talebi reddedebilmek bakımından fazla esneklik sağladığı, en azından red nedenlerinin yazılı olarak bildirilmesi gerektiği yönünde bir değişikliğin yapılması savunulmaktadır[169].

- Beşinci fıkraya göre, kendisinden talepte bulunulan taraf, şayet yardım talebine dair işlem yapması kendi yetkili mercilerince sürdürülmekte olan bir cezai soruşturmaya ya da kovuşturmaya zarar verebilecekse, bu talebe ilişkin işlemleri geciktirebilir. Ayrıca, 6. fıkraya göre, bu talep kısmen ya da koşullara bağlı olarak yerine getirilebilir.

28. maddeye göreyse, kendisinden talepte bulunulan devlet, temin ettiği bilgilerin kullanımı açısından, bunların sadece talepte belirtilen soruşturma ya da işlemde kullanılması yönünde sınırlama getirebilecek ve gizlilik koşuluna uyulmasını talep edebilecektir. Belirtelim ki, ancak taraflar arasında başka bir antlaşma hükmü

[166] Keyser, s. 319.
[167] Explanatory Report to the Convention on Cybercrime, para. 267.
[168] Gercke, *Understanding Cybercrime,* s. 467.
[169] Vatis, s. 221.

yoksa, bu madde uygulanabilecektir[170]. Hukukun genel ilkeleri gereği, gizlilik gerekçesiyle, sanığın lehine olan delillerin savunma makamından saklanması mümkün değildir. Ayrıca, duruşmada kullanılacak bilgiler bakımından, bunların zaten yargılamada aleni hale gelecek olması sebebiyle, bu aşamada gizlilik koşulu öne sürmek mümkün değildir[171].

Sözleşmenin 29. ve devamı maddelerinde, İkinci Kısım'da yer alan bazı tedbirlerin, uluslararası işbirliği bakımından yansımasına yer verilmiştir. Zira, m. 16 vd.nda yer verilen önlemler, devletlerin egemenliği gereği, ancak devletin kendi ülkesi üzerinde uygulanabilir. Yurt dışında delil toplamak gerekiyorsa, adli yardımlaşma talep etmek gerekecektir[172]. İşte, m. 29 vd. hükümleri de, bu hususun pratik ve hızlı bir şekilde gerçekleşebilmesini temine yöneliktir. Çalışmanın kapsamını fazla genişletmemek amacıyla, bu konularda sadece birtakım genel bilgiler verilecek ve bazı önemli noktalara değinilecektir.

29. maddede, saklanan/depolanmış bilgisayar verilerinin korunması bakımından hızlandırılmış bir prosedür öngörülmüştür.

- Düzenlenen husus, ileride adli yardımlaşma talebine konu olacak (örneğin, elkonulması istenecek) birtakım verilerin muhafazasını sağlamak için[173], taraf bir devletin, diğer bir taraf devletten acil talepte bulunmasıdır. Bu, 16. maddede yer verilen hükmün yansımasıdır[174]. Bu hükmün amacı, nispeten uzun sürebilecek, resmi bir adli yardımlaşma talebinin infazı süreci boyunca, her an kaybolabilecek mahiyetteki verilerin korunmasını sağlamaktır[175]. Gerçekten, klasik adli yardımlaşma prosedüründe, resmi talepname hazırlanıp, talep edilen devletin yetkili merciine gönderilmeli, o merci de bunu kendi ülkesindeki yetkili birime göndermeli, bu birim de talebi onaylayıp yerine getirmelidir. Bu, bazen aylarca sürebilir. Oysa, trafik verileri ve diğer önemli bilgiler çoğu *server*'da[176] geçici olarak saklanır ve bunlara derhal el konulmazsa, geriye dönüşü olmayan biçimde kaybolabilir. Bu nedenle, acil eylemi mümkün kılan, hızlandırılmış bir formül bulmak elzemdir[177]. 29. maddede buna imkan verilmiştir. Bu bağlamda, veriyi muhafaza eden kişiden verilerin içeriğinin elde edilmesi istenmeyip, sadece muhafazası (yani, silinmemesi) istenebildiğinden, bu yöntem hem çabuktur hem de ilgili kişinin özel hayatını korumak

[170] Picotti & Salvadori, s. 66; Keyser, s. 319.
[171] Explanatory Report to the Convention on Cybercrime, para. 278.
[172] Gercke, *Understanding Cybercrime,* s. 468.
[173] Keskin, İÜHFM, s. 161.
[174] Helvacıoğlu, s. 296. Bu koruma tedbiri için bkz. Keskin, İÜHFM, s. 161 vd.
[175] Explanatory Report to the Convention on Cybercrime, para. 282; Keskin, İÜHFM, s. 161; Csonka, s. 481; Picotti & Salvadori, s. 67.
[176] *Server* (sunucu), diğer bilgisayarlara hizmet sağlayan bir bilgisayar veya programdır (Avşar/Öngören, s. 119).
[177] Putnam&Elliott, s. 62.

açısından daha güvencelidir, zira, verinin içeriği öğrenilmemektedir[178]. Burada, genellikle internet servis sağlayıcı düzeyinde uygulanan, verinin muhafazası söz konusu olan, geçici bir önlem düzenlenmiştir. Verinin açıklanması ise, sonraki aşama olup çoğu zaman adli yardımlaşma talebinde bulunulmasını gerektirecektir[179]. Bu istemlerin, aşağıda ele alınacak 24/7 ağı (7 gün, 24 saat hizmet verecek ağ) aracılığıyla yapılması beklenmelidir.

- 29. maddenin ikinci fıkrasında, böyle bir talepnamede yer alacak hususlar detaylı bir şekilde düzenlenmiştir. Bu bağlamda, cezai soruşturmaya ya da işleme konu olan suç ve ilgili vakıaların kısa bir özeti belirtilmelidir. Ayrıca, verilerin korunmasının neden gerekli olduğu da açıklanmalıdır.

- 29. maddenin üçüncü ve dördüncü fıkrasında, bu talebin yerine getirilmesi bakımından, çifte cezalandırılabilirlik koşulu, m. 2-11 arasında yer alan suçlar açısından[180] kaldırılmıştır. Bunun sebebi, hem söz konusu önlemin özel hayat bakımından ciddi bir müdahale oluşturmaması hem de çifte cezalandırılabilirlik koşulunun gerçekleştiği tespit edilene kadar geçecek sürede verinin kaybedilmesinin olası olmasıdır[181].

- 29. maddenin beşinci fıkrasında, talebin reddedilme sebepleri belirtilmiştir: Bu hükme göre; a) Suçun, talepte bulunulan devlet tarafından siyasi suç ya da siyasi suçla bağlantılı suç olarak kabul edilmesi; b) talebin yerine getirilmesinin, talepte bulunulan devlet tarafından, kendi egemenliğine, güvenliğine, kamu düzenine veya diğer temel yararlarına zarar verebilecek mahiyette mütalaa edilmesi.

- 29. maddenin yedinci fıkrasına göre, talebe cevaben başvurulan muhafaza işlemi en az 60 günlük süreyi kapsamalıdır; diğer bir deyişle, veriler en az 60 gün muhafaza edilmelidir. Bunun maksadı, gerçekleştirilmesi istenen asıl işleme dair adli yardım talebinin hazırlanabilmesini sağlamaktır. Söz konusu talep alındıktan sonra da, talebe dair karar verilenceye kadar veriler korunacaktır. Uygulamada, bu sürenin çok kısa olduğu, evrak üzerinden birçok işlemin yapılmasının zorunlu olması karşısında, resmi adli yardım talepnamesini hazırlamanın çok daha uzun sürebildiği dile getirilmektedir[182].

30. maddede, korunan trafik verilerinin açıklanması bakımından hızlandırılmış bir prosedür öngörülmüştür. 17. maddede yer alan trafik verilerinin hızlı muhafazası ve kısmi olarak açıklanmasının[183] bir yansıması olan 30. maddeye göre;

---

[178] Picotti & Salvadori, s. 67.

[179] International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 6.

[180] Bu suçlar için bkz. dipnot 97.

[181] Explanatory Report to the Convention on Cybercrime, para. 285. Eleştiri için bkz. Uçkan/Beceni, s. 384.

[182] Pedro Verdelho, Discussion paper (draft), s. 30.

[183] Bilgi için bkz. Keskin, İÜHFM, s. 165-166.

bu konuda iletilen talebin yerine getirilmesi sırasında, kendisinden yardım talep edilen devlet, tebdir konusu iletişimin aktarılmasında başka bir ülkedeki hizmet sağlayıcının devrede olduğunu anlarsa, talepte bulunan devlete, ilgili hizmet sağlayıcısının ve verilerin aktarıldığı yolun teşhis edilmesi için gerekli olan ölçüde, trafik verisini en kısa sürede açıklamalıdır. Bu hükmün sebebi, verinin genellikle bir çok ülkeden geçmesidir; bu bakımdan, verinin muhafazası için tek bir devletten talepte bulunmak yetmez, zincirdeki tüm ülkeler veya *server*'lar bakımından harekete geçmek gerekir. Bunun mümkün olması için de, söz konusu bilgi gerekli olacaktır[184].

31. maddede, saklanan bilgisayar verilerine erişime dair karşılıklı yardımlaşma düzenlenmiştir. Burada söz konusu olan, bazı verilerin aranması, bunlara erişilmesi, el konulması ya da bunların benzer şekilde güvence altına alınması ya da açıklanması amacıyla, taraf bir devletin diğer bir taraf devletten talepte bulunmasıdır. Yine, bazı durumlarda (f. 3) hızlandırılmış prosedürlere başvurulması mümkün kılınmıştır[185].

32. maddede, çok tartışmalı bir konu olan, bilgisayarda saklanan verilere sınır ötesinden erişim meselesi ele alınmıştır. Kapsamlı tartışmalar sonucunda, bu konuda kısıtlı bir düzenlemeye gidilmiş ve sadece iki durumda bu yetki tanınmıştır:

1) Her bir taraf devlet, diğer taraf devletin iznini almaksızın, herkesin kullanabileceği bir kaynakta bulunan, kullanımı herkese açık bilgisayar verilerine, bu veriler nerede yer alırsa alsın, ulaşabilecektir. Örneğin, herkese açık bir websitesindeki bilgilerin sınır ötesinden elde edilmesi durumunda, herhangi bir sakınca olmadığı ortadadır.

2) Şayet kamunun erişimine açık olmayan ve başka bir taraf Devletin sınırları dahilinde saklanan veriler söz konusu ise, bu verilerin ulusal sınırlar içinde bulunan bir bilgisayar sistemi aracılığıyla elde edilebilmesi, rıza koşuluna bağlanmıştır. Buna göre, söz konusu bilgisayar sistemi üzerinden bu verileri açıklama yetkisine sahip olan kişinin yasal rızası (*lawful and voluntary consent*) aranacaktır.

Demek ki, taraf bir devletin, diğer taraf devletin izni olmaksızın, tek taraflı olarak, sınır ötesinde saklanan verilere erişimi konusundaki yetkisi kısıtlıdır. Bu bakımdan, "*remote extraterritorial search*" denilen, başka bir ülkede bulunan verilerin elde edilmesine yönelik faaliyetler sınırlandırılmıştır. Bu yönüyle, Ekim 1999'da G-8 tarafından kabul edilen "Saklanan Bilgisayar Verilerine Sınırötesi Erişime Dair İlkeler"de (Principles on Transborder Access to Stored Computer Data) yer verilen kuralın ötesine geçilememiştir. Ancak Sözleşme'nin bu iki durumun dışında, başka türden tek taraflı erişim yetkisini *yasaklamadığı* da vurgulanmalıdır[186].

---

[184] International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 8.

[185] Fakat bkz. Vatis, s. 216 (bu talebin, m. 31/2'de yapılan atıf gereği, m. 23'de öngörülen kurallar ve düzenlemeler uyarınca reddedilebilmesi ya da yerine getirilmesinin ertelenebilmesi mümkün gözükmektedir.)

[186] Vatis, s. 217.

Bu hüküm yine de ciddi bir şekilde eleştirilmektedir. Bir görüşe göre, bireyin rızasıyla, devletlerin egemenliği ilkesine aykırı olarak, başka bir devletin ülkesinde yargı yetkisi kullanılmaktadır[187]. Bununla birlikte, Sözleşme'ye taraf olmayı seçen devletlerin, kendi rızalarıyla bu işleme izin verdikleri söylenebilecektir.

33. maddede, şüphelinin kimliğini deşifre edebilmek için çok önemli olan bir önleme[188], yani, trafik verilerinin gerçek zamanlı olarak toplanmasına yer verilmiştir. Gerçekten de, bir siber saldırının kaynağını belirlemek, fail henüz *online* (çevrimiçi) iken en kolay bir şekilde mümkündür[189]. Bunun gerçekleştirilme usulü, ulusal hukuk tarafından belirlenecektir. Ancak, ikinci fıkrada önemli bir hususa yer verilmiştir: ulusal hukukta bu tedbirin uygulanılmasına izin verilen davalara benzer türden suçlar söz konusu ise, yardım talebi yerine getirilmelidir[190]. Yani, ulusal hukukta öngörülenden daha dar bir uygulama alanı söz konusu olmamalıdır.

34. maddede, özel hayata çok daha ağır bir müdahale teşkil eden[191], içerikle ilgili verilerin bu hükme göre denetlenmesi ve kaydedilmesine yer verilmiştir. Burada, uygulanabilir antlaşmalar ve ulusal hukukun öngördüğü ölçüler çerçevesinde bu tedbire başvurulabileceği ifade edilmiştir. Bu noktada, Sözleşme'nin herhangi bir yenilik getirmediğini ve mevcut rejimlere yollama yaptığını belirtmek gerekir. Tedbir, yine her bir devletin ulusal kuralları çerçevesinde icra edilecektir. Bununla birlikte, aynı türden suçu kendisi kovuşturduğu zaman bu tedbire başvurabilen bir devletin, başka bir devletten talep geldiği zaman içeriğin denetlenmesi ve kaydedilmesi konusunda yardım sağlamak zorunda olmadığı; başka bir devletin yardım talebini yerine getirmesini engelleyen yargı yetkisine dair bazı koşulların var olabileceği, ifade edilmektedir[192].

Nihayet, 35. maddeye göre, her bir taraf devlet, bilgisayar sistemleri ve verilerine dair suçların soruşturulması ya da kovuşturulmasında ya da bir suçun elektronik formattaki delillerinin toplanmasında, derhal yardım teminini mümkün kılmak amacıyla, haftada yedi gün ve yirmi dört saat müsait olacak bir irtibat noktası tayin edecektir (24/7 network).

- Bu hüküm, adli yardımlaşmanın hızlı ve etkin biçimde gerçekleştirilebilmesi yönünden çok önemlidir. Düzenleme, G-8 tarafından 1997'de yaratılan ve bugün

---

[187] Gercke, *Understanding Cybercrime,* s. 470; Uçkan/Beceni, s. 388. En ağır eleştiri Rusya'dan gelmektedir, bkz. Vatis, s. 218.

[188] Keskin, İÜHFM, s. 159; Picotti & Salvadori, s. 68; Vatis, s. 217; Helvacıoğlu, s. 297.

[189] Putnam&Elliott, s. 62, dn. 49.

[190] Bu bakımdan, "bir ülkenin politik amaçlar doğrultusunda başka bir ülkede faaliyet gösteren muhaliflerinin faaliyetlerini bu ülkenin yetkilileri kanalıyla" denetleyebilmesine olanak sağlandığı yönündeki eleştiriye de (Uçkan/Beceni, s. 385) katılmıyoruz, zira, suç teşkil etmeyen bir faaliyet bakımından yardım talep edilmişse, m. 33/2'nin aksi yorumundan, kendisinden talep edilen devletin yardım etmek zorunda olmadığı anlaşılmaktadır.

[191] Broadhurst, s. 421.

[192] Vatis, s. 217.

50 civarında ülkeyi kapsayan, İrtibat Noktaları Ağı (Network of Contact Points) tecrübesine dayanmaktadır[193]. G-8'deki amaç da, yüksek teknoloji ürünü suçluluk konusunda uzman kişilerden oluşan, dünya çapında bir iletişim ağı yaratmaktı; böylece, şüphelilerin yerini tespit etmek ve onları yargılayabilmek açısından elzem olan, elektronik delillerin derhal muhafaza altına alınması mümkün olabilecekti[194]. Belirtelim ki, AB Konseyi'nin 2005/222/JHA sayılı, 24.2.2005 tarihli Çerçeve Kararı ile, tüm AB üyesi devletlerin "mevcut" irtibat noktası ağından yararlanmaları zorunlu hale getirilmiştir. Aslında, karara bakınca, G-8 bünyesinde mevcut ağın kast edildiği anlaşılmaktadır[195]. Belirtelim ki, G-8 bünyesindeki ağ ile Budapeşte Sözleşmesi gereğince tayin edilmesi gereken irtibat noktalarının örtüşmesi faydalı olacaktır[196]. Bu birim, diğer mevcut işbirliği kanallarının yerini almayıp onları takviye edecektir[197]. Buradaki amaç, geleneksel işbirliği yöntemlerinin yetersiz kaldığı için çok çabuk bir cevabı gerekli kılan siber suçlulukla mücadele konusunda elverişli bir yöntemin yaratılmasıdır[198]. Hem tek bir irtibat noktası belirlenerek iletişim süreci hem de irtibat noktasına bazı soruşturma işlemlerini bizzat yapabilmesi imkanı tanınarak soruşturma süreci hızlandırılacaktır[199]. Budapeşte Sözleşmesi ile kurulan irtibat noktaları 7 gün, 24 saat ulaşılabilir olacaktır. Böylece, derhal veri saklanması yönünde diğer bir devletten gelen acil bir talep, söz konusu devletin irtibat noktası aracılığıyla, doğrudan telefon ya da e-mail yoluyla, ilgili devlet tarafından görevlendirilen kişi ya da birime derhal iletilebilecektir[200]. Dünyanın farklı bir ucundan ve apayrı bir saat diliminden yardım talebi geldiğinde, kendisinden yardım talep edilen ülkede saat gecenin üçü, dördü olabilecektir; bu, siber suçlulukla mücadelede adli işbirliğinde sıklıkla rastlanabilecek, olağan bir durumdur. Bu nedenle, normal çalışma saatleri mefhumu geçersiz hale gelmekte, 24 saat hazır bulunacak birimlere ihtiyaç duyulmaktadır[201].

- 35. maddenin ikinci fıkrasına göre, bu irtibat noktası, diğer tarafların irtibat noktalarıyla hızlı iletişim kuracak kapasiteye sahip olmalıdır. Diğer bir deyişle, soyut olarak bir kimsenin ya da merciin tayin edilmesi yetmez, söz konusu irtibat noktasının gerekli şekilde teçhizatlandırılması da şarttır. Zaten, üçüncü fıkraya göre, söz konusu ağın işleyişini kolaylaştırmak açısından, eğitimli ve donatılmış

[193] Project on Cybercrime - Final Report (September 2006-February 2009), Prepared by the Economic Crime Divison of the Directorate General of Human Rights and Legal Affairs, s. 32; Csonka s.496; Helvacıoğlu, s. 298.

[194] Pedro Verdelho, Discussion paper (draft), s. 13.

[195] Pedro Verdelho, Discussion paper (draft), s. 14.

[196] Bu konuda çalışıldığına dair bkz. Calderoni, s. 349.

[197] International Co-operation under the Convention on Cybercrime (Version 18 August 2009), Project on Cybercrime, s. 9; Broadhurst, s. 421; Csonka, s. 496.

[198] Explanatory Report to the Convention on Cybercrime, para. 298; Buono, s. 210.

[199] Gercke, *Understanding Cybercrime,* s. 473.

[200] Pedro Verdelho, Discussion paper (draft), s. 13.

[201] Csonka, s. 480.

personelin mevcut olması sağlanacaktır. Bu bakımdan, irtibat noktasının teknolojik donanımının en üst düzeyde olması ve ilgili personelin de bu konuda uzman olması gerekecektir[202].

- İrtibat noktasının idari yapı dahilinde nasıl konumlandırılacağı, ilgili devlete kalmıştır[203]. Türkiye örneğinden düşünürsek, Adalet Bakanlığı içindeki UHDİGM olabileceği gibi, emniyet teşkilatı içerisinde bir birim de olabilir. Bu bakımdan, irtibat noktasının bizzat kendisi adli yardım talebini yerine getirmek zorunda değildir; ilgili kuruma meseleyi havale edecek bir organ da olabilir. Her durumda, irtibat noktası, hem siber saldırıları durdurmak ve izini tespit etmek açısından teknik yardım sunacak hem de bazı uluslararası adli yardımlaşma işlevlerini yerine getirecektir[204]. Bu bakımdan, teknik bilgi ve tecrübe önemli olduğu kadar, diğer bir çok devletlerin irtibat noktalarıyla temaslar kurulacağından, geniş bir yabancı dil yelpazesi de elzemdir. Öte yandan, irtibat noktası, şayet polis teşkilatı içinde yer alacaksa, adli yardımlaşma taleplerini yerine getirecek yetkili idari makamla hızlı ve koordine şekilde çalışmaya da muktedir olmalıdır[205]. Aksi takdirde, hem kendisi istenilen işlemi yerine getirme yetkisine sahip olmaz hem de yetkili mercie talebin iletilmesinde zaman kaybedilirse, artık çok geç olabilir. Uygulamaya bakıldığında[206], genellikle polisin irtibat noktası olarak belirlendiği gözlemlenmekle birlikte, çok farklı mercilerin tayin edildiği göze çarpmaktadır: a) emniyet teşkilatı ya da içindeki bir birimi tayin eden (Arnavutluk, Ermenistan, Danimarka, Estonya, Almanya, Macaristan, İzlanda, Letonya, Litvanya, Slovakya), b) Adalet Bakanlığı'nı tayin eden (Kıbrıs R.K.), c) başka bir Bakanlığı tayin eden (Azerbaycan: Ulusal Güvenlik Bakanlığı, Bulgaristan: İçişleri Bakanlığına bağlı özel bir birim, Moldova: İçişleri Bakanlığı'na bağlı özel bir birim, Slovenya), d) İstihbarat Birimi'ni tayin eden (Finlandiya), e) ayrı bir uzman birimi tayin eden (Fransa, Norveç, Romanya: Yüksek Mahkeme'ye bağlı özel bir birim), f) Savcılık Makamı'nı tayin eden (İtalya: Roma Başsavcısı, Hollanda, Sırbistan, Makedonya (Eski Yugoslav Cumhuriyeti) ülkeler bulunmaktadır. Öte yandan, 24/7 ağına katılmak için, Sözleşme'yi imzalamanın ya da buna taraf olmanın gerekmediği, Sözleşme'nin 46. maddesi uyarınca kurulan Siber Suç Sözleşmesi Komitesi (T-CY) tarafından vurgulanmıştır[207].

---

[202] Teknolojik donanımın önemi hususunda bkz. Özcan, s. 334.

[203] Csonka, s. 496.

[204] Explanatory Report to the Convention on Cybercrime, para. 300.

[205] Csonka s.496.

[206] http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp (son erişim 10.10.2011).

[207] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

SONUÇ

Siber suçlarla mücadele konusunda, çeşitli uluslararası örgütler ve kuruluşlar nezdinde, yine dünya çapında bir çok STK'nin inisiyatifiyle, aynı anda yürütülen onlarca faaliyet olması, sorunun hem ciddiyetini hem de buna cevaben istenilen çözümün bulunulmasında ne kadar çok çaba vermek gerektiğini göstermektedir. Bugüne kadar sağlanan gelişme kayda değer olmakla birlikte, siber suçlulukla etkin bir mücadelede, yolun başında olduğumuz söylenmelidir[208].

Siber suçun tanımı ve içeriği hakkında henüz bir uzlaşı sağlanmış değildir. Nitekim, 2001 Siber Suç Sözleşmesi'nde de bir tanım verilmemiştir. Bununla birlikte, birtakım suç tiplerini ulusal hukukta düzenleme yükümlülüğü getirilmiştir. Çifte cezalandırılabilirlik koşulunun, en azından Sözleşme'de tanımlanan söz konusu suçlar açısından devre dışı bırakılması, önemli bir gelişmedir[209]. Buna karşılık, henüz az sayıda devletin Sözleşme'ye taraf olması ve siber suçlara dair ulusal mevzuatların da yeknesak olmaktan uzak olması karşısında, geleneksel adli işbirliği imkanları bakımından, çifte cezalandırılabilirlik koşulu önemli bir engel oluşturmaya devam edecektir. Öte yandan, talep ettiği yardımı alamayan devletlerin tazminat elde edebileceği bir zorlayıcı mekanizma da yoktur[210].

Siber suçlulukla mücadelede, faillerin hiç bir "sığınak" bulamamasının önemini belirtmiştik. Bu sorunun önüne geçmek için BM Genel Kurulu tarafından kabul edilen 55/63 ve 56/121 sayılı kararlara dikkat çekmek gerekir (*Combating the Criminal Misuse of Information Technologies*). Ne var ki, BM Genel Kurul kararları tavsiye niteliğinde olup bağlayıcı değildir. Konuya ilişkin, BM bünyesinde bağlayıcı bir sözleşme hazırlama çalışmaları ise sürmektedir[211]. Bunun sonuç vermesi ise, kolay gözükmemektedir; zira, dijital anlamda gelişmiş bir çok ülkenin tercihinin, Budapeşte Sözleşmesi'ni daha çok sayıda ülkeye genişletip bunun etkinliğini görmeyi beklemek yönünde olduğu söylenmektedir[212]. Kaldı ki, bir görüşe göre, uzun süre ve büyük çaba gerektiren ikinci bir sözleşme hazırlamaktansa, Avrupa

---

[208] Broadhurst, s. 409.

[209] Her ne kadar bu husus doktrinde (Uçkan/Beceni, s. 384) eleştirilmişse de, çifte cezalandırılabirlik koşulunun genel olarak, tümüyle kaldırılmadığı ve bu konuda önemli sınırlamalar olduğu da ifade edilmelidir. Bu sınırlamaları çalışmamızda yeri geldikçe incelemiş bulunuyoruz. Kaldı ki, Sözleşme'ye taraf bir devlet, zaten m. 2-11'de yer alan fiilleri mevzuatında cezalandırmak konusunda uluslararası yükümlülük altına girmiştir.

[210] Vatis, s. 220.

[211] Birleşmiş Milletler Uyuşturucu ve Suç Ofisi de, yakın zamanda, siber suçlara karşı global bir sözleşmenin geliştirilmesi lehinde görüş beyan etmiştir. Bkz. Secretariat of the United Nations Office on Drugs and Crime (UNODC), *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime,* Working Paper submitted to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (22 Ocak 2010), s. 15 (http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf) [son erişim 15.11.2012].

[212] Broadhurst, s. 409.

Konseyi Sözleşmesi'ne global katılımı sağlamaya çalışmak tercih edilmelidir[213]. Keza, AB'nin de tercihinin bu yönde olduğu bilinmektedir[214]. Öte yandan, Budapeşte Sözleşmesi'nin sunduğu hazır bir çerçeve mevcutken, BM bünyesinde, ondan daha iyi bir enstrüman hazırlama gayretine girişilmeyebileceği, Avrupa Konseyi Sözleşmesi'nin çok benzeriyle yetinilebileceği endişesi de dile getirilmektedir[215].

Siber suçluların sığınabileceği güvenli limanlar bulmalarını önlemek açısından, gelişmekte olan ya da az gelişmiş ülkelerin de bu mücadeleye dahil olmaları yönünde ikna edilmeleri gerekmektedir. Oysa, teknolojik gelişme düzeyi düşük olduğu için, bu fenomenden kayda değer bir zarar görmeyen devletlerin, bu konuya enerji ve kaynak yatırmalarını beklemek, her zaman kolay değildir. Kaldı ki, buna muktedir olmayan, "iflas etmiş" devletler de mevcuttur[216]. Yine, adli yardımlaşma talebinden doğan masrafların, bazen talep eden devletçe karşılanmakla beraber, talebi yerine getiren devlete ait olması da, yardımlaşma konusunda bir isteksizliğe yol açabilmektedir[217]. Bunun da ötesinde, bazı devletlerin siyasi saiklerle ya da menfaat amacıyla, siber suçluluğa zaman zaman kasten göz yumması da gündeme gelebilir[218].

Bu noktada, bazı devletlerin siber suçluluğun ortaya çıkardığı tehdide karşı gerekli refleksi göstermemeleri karşısında, bilişim teknolojilerine bağımlı ve saldırılar karşısında daha hassas olan güçlü devletlerin, siyasi taktiklere başvurması gerektiği söylenmektedir[219]. Bu, bölgesel ve uluslararası düzeyde siyasi baskı yapmaktan, ekonomik bakımdan güçsüz devletlere, teknolojik transfer yardımı gibi teşviklerde bulunmayı içeren bir dış politikanın izlenmesine kadar uzanabilir. Siber suçla mücadele mevzuatının oluşturulmasında, bu konuda engin tecrübesi bulunan devletlerin, henüz yolun başında olan devletlere azami surette yardım etmesi, bu anlamda gereklidir[220].

Genel bir durum değerlendirmesi yapmak gerekirse, Siber Suç Sözleşmesi çok önemli bir adım olmakla birlikte, henüz sadece bir başlangıçtan ibarettir[221]. Kaldı ki, içeriğini globalleştirme amacıyla Avrupa Konseyi üyesi olmayan devletlere açık olsa da, Sözleşme bölgesel bir araç olup, kendi bölgesinde bile henüz genel kabul

[213] Downing, s.762.

[214] Buono, s. 208 (bu konuda bkz. The Stockholm Programme—An open and secure Europe serving and protecting the citizens. Presidency Conclusions—Brussels, 10–11 December 2009 (Council of the European Union, Brussels 3 March 2010, doc 5731/10, s. 79). Avrupa Konseyi de bu yönde görüş beyan etmektedir (bkz. Vatis, s. 219).

[215] Calderoni, s. 351.

[216] Broadhurst, s. 410. Genel olarak, ekonomik güçlükler sebebiyle siber suçlulukla mücadeleye yeterli kaynak ayıramayan devletlerin siber suçlular için cazibe merkezi olacağı yönünde bkz. Bell s. 317.

[217] Grabosky, s. 217.

[218] Allan, s. 155.

[219] Putnam&Elliott, s. 52.

[220] Grabosky, s. 220.

[221] Benzer yönde Simion, s. 310.

görmüş değildir. Uzun vadede de, global katılım beklenmemektedir[222]; zaten taraf olma süreci de hızlı işlememektedir[223]. Rusya ve Çin gibi, bir çok siber saldırının kaynağı olan ülkelerin Sözleşme'ye taraf olmaması da endişe sebebidir[224]. Taraf olan Devletlerin de Sözleşme gereklerini ne ölçüde iç hukuklarına aktardıkları, tartışmaya açıktır[225].

Bu bakımlardan da, siber suçla mücadelenin dünya çapında sonuç verebilmesi açısından, BM'nin katkısı vazgeçilmez bir öneme sahiptir[226]. Gerçi, taraf olmayı seçmeyen devletler açısından bile, Budapeşte Sözleşmesi'nin katkısı büyüktür, zira, siber suçlara dair ulusal mevzuatını oluşturmak isteyen tüm devletler bakımından bu Sözleşme temel bir referans ve gösterge teşkil edecektir[227]. Fakat yine de, devletlerin taraf olmayı seçtikleri, bağlayıcı bir antlaşmanın önemi apayrıdır. Bu bağlamda, Amerikan Devletleri Örgütü'nün, üye devletlerine yönelik, Amerikan devletleri arasında bir Siber Suç Sözleşmesi yapılmasına dair tavsiyesinin[228] de devamının gelmesi ümit edilmektedir.

Son bir husus olarak; diğer suçluluk türlerinden daha fazla bir ölçüde, siber suçlar bakımından, ceza hukukuna alternatif kontrol mekanizmaları ön plana çıkarılabilir[229]. Bu bağlamda, suçun ortaya çıkmasından sonra bunun cezalandırılmasına yönelik klasik anlayışın yetersiz kalması kaçınılmaz olduğundan, diğer tedbirlerin dışında, devletle özel sektör arasındaki işbirliğine, bireylerle şirketlerin kendilerini koruyucu önlemlere yatırım yapmasına[230], etkili bir etik eğitime dayalı, suçun önlenmesine yönelik bir modele önem verilmesi tavsiye edilmektedir[231].

Netice olarak; Budapeşte Sözleşmesi'nin siber suçlarla mücadele konusunda

---

[222] Csonka, P. (2005), "The council of Europe Convention on cybercrime: a response to the challenge of the new age?", in Broadhurst, R. and Grabosky, P. (Eds), Cyber-crime: The Challenge in Asia, University of Hong Kong Press, Hong Kong, s. 326'dan naklen Broadhurst s.416; Calderoni, s. 350.

[223] Gercke, *Understanding Cybercrime,* s. 201. Keza, bazı taraf devletler, mevcut kanunlarıyla ya da ceza hukuku anlayışlarıyla bağdaşmadığı için, bazı hükümlerin gereğini mevzuatlarında yapmayabilirler (Allan, s.155). Buna karşılık, bir görüşe göre, diğer uluslararası enstrümanlara göre onaylama süreci daha hızlıdır (Calderoni, s. 350).

[224] Vatis, s. 220. Yine bkz. Helvacıoğlu, s. 299.

[225] Gercke, *Understanding Cybercrime,* s. 202; AB çerçevesinde, 2005 tarihli Çerçeve Karar'ın uygulanmasına dair endişeler bakımından bkz. Calderoni, s. 352. Avrupa Konseyi, Sözleşme'ye taraf olan devletlerin bunun gereğini iç hukukta yerine getirip getirmediklerini henüz değerlendirmemiştir (Gercke, *Phenomena,challenges and legal response*, s. 125).

[226] Benzer yönde Simion, s. 311.

[227] Downing, s. 761; Calderoni, s. 351. Türkiye açısından aynı yönde bkz. Özen/Baştürk, s. 307. Bu konuda örnekler için bkz. Gercke, *Phenomena,challenges and legal response*, s. 124.

[228] http://www.oas.org/juridico/english/cyber.htm [son erişim 12.10.2011].

[229] Bu konuda bkz. Allan 168 vd. Yine bkz. Sınar, İnternet ve Ceza Hukuku, s. 52-53; Elliott&Putnam, s. 67; Picotti & Salvadori, s.79.

[230] Dülger, s. 320-322; Özcan, s. 335-336; Taşkın, s. 177-178. Özdenetim mekanizmaları hk. bkz. Uçkan/Beceni, s. 376 vd.; yine bkz. Tezcan, Sempozyum, s. 535-537.

[231] Brenner in Rutgers Computer & Tech. L.J., s.40 vd. Yine bkz. Bell, s. 321-2; Buono, s. 210.

çok önemli bir atılım teşkil ettiği tartışmadan uzaktır[232]. Bununla birlikte, hükümlerinin taraf devletlerce iç hukuka gerçekten ve tümüyle dahil edilip edilmediğini görmek ve Sözleşme'nin nasıl sonuç vereceğini tespit etmek zamanı gerektirmektedir[233].

KAYNAKÇA

A. Caner Yenidünya/Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, İstanbul, 2003.

Ali Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, 3. Baskı, Ankara, 2011.

Amalie M. Weber, "*The Council of Europe's Convention on Cybercrime",* 18 Berkeley Technology Law Journal 425 (2003).

Antonio Cassese. *International Law* (2nd ed, Oxford: Oxford University Press, 2005).

Aslı Deniz Helvacıoğlu, *Avrupa Konseyi Siber Suç Sözleşmesi – Temel Hükümlerin İncelenmesi*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

B. Zakir Avşar/Gürsel Öngören, *Bilişim Hukuku*, Türkiye Bankalar Birliği, İstanbul, 2010.

Berrin Bozdoğan Akbulut, "*Bilişim Suçları"*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Milenyum Armağanı, Cilt 8, Sayı 1-2, 2000.

Cevat Özel, *Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

David R. Johnson & David G. Post, "*Law and Borders – The Rise of Law in Cyberspace",* 48 STAN.L.REV. 1367 (1996).

Durmuş Tezcan/Mustafa Ruhan Erdem/R. Murat Önok, *Uluslararası Ceza Hukuku*, Ankara, 2009.

Durmuş Tezcan, İnternet Karşısında Özel Hayatın Korunması ve Adli Yardımlaşma, Uluslararası İnternet Hukuku Sempozyumu, DEÜ Yayını, İzmir, 2002.

Europol Review - General Report on Europol Activities, European Police Office (2011).

Faruk Turhan, *Die Rechtsstellung des Auszuliefernden nach türkischem Recht unter rechtsvergleichender Berücksichtigung des deutschen Rechts,* Frankfurt am Main, 1993.

[232] Calderoni, s. 355.

[233] Ancak tesirin başlangıç itibariyle olumlu olduğuna dair veriler için bkz. Vatis, s. 220.

Fatih S. Mahmutoğlu, "*Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu",* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001.

Fatih S. Mahmutoğlu, *Suçluların Geri Verilmesi*, Ceza Hukuku Günleri, 70. Yılında Türk Ceza Kanunu - Genel Hükümler, İstanbul, 1998.

Feridun Yenisey, İnternet Suçlarının Yeni İşleniş Biçimleri, Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayını, İzmir, 2002.

Feridun Yenisey, *Milletlerarası Ceza Hukukunda Yeni Gelişmeler*, Ceza Hukuku Günleri, 70. Yılında Türk Ceza Kanunu - Genel Hükümler, İstanbul, 1998.

Fikret İlkiz, İnternet *Ortamında Yayınlar,* İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

Francesco Calderoni, "*The European legal framework on cybercrime: striving for an effective implementation"*, 54 Crime Law Soc Change 339 (2010).

Füsun Sokullu-Akıncı, "*Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001.

Gregor Allan, "*Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative"*, 2005 N.Z. L. Rev. 149 (2005).

Gregor Urbas, "*Criminalising Computer Misconduct: Some Legal and Philosophical Problems",* 14 Asia Pac. L. Rev. 95 (2006).

Hasan Sınar, "*Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme"*, Prof. Dr. Çetin Özek Armağanı, İstanbul, 2004.

Hasan Sınar, İnternet ve Ceza Hukuku, İstanbul, 2001.

Hatice Akıncı/A. Emre Alıç/ Cüneyd Er, *Türk Ceza Kanunu ve Bilişim Suçları*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

Hüseyin Pazarcı, *Uluslararası Hukuk*, 9. Bası, Ankara, 2010.

İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* Ankara, 2008.

James Crawford. *Brownlie's Principles of Public International Law* (8th ed., Oxford: Oxford University Press, 2012).

Kayıhan İçel, "*Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri",* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001.

Kim-Kwang Raymond Choo, "*Organised crime groups in cyberspace: a typology",* 11 Trends Organ Crim 270 (2008).

Laviero Buono, "*Investigating and prosecuting crimes in cyberspace: European training schemes for judges and prosecutors",* 11 ERA Forum 207 (2010).

Leyla Keser Berber, *Adli Bilişim (Computer Forensic)*, Ankara, 2004.

Lorenzo Picotti & İvan Salvadori, *National legislation implementing the Convention on Cybercrime – Comparative Analysis and good practices*, Discussion paper, Version 28 August 2008.

Mahmut Koca, "*Avrupa Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku*", Bilgi Toplumunda Hukuk, Prof. Dr. Ünal Tekinalp'e Armağan, Cilt III, 2003.

Malcolm N. Shaw. *International Law* (6th ed., New York: Cambridge University Press, 2008).

Marco Gercke, *Understanding cybercrime: phenomena, challenges and legal response*, September 2012, ITU 2012 (www.itu.int/ITU-D/cyb/cybersecurity/legislation.html).

Marco Gercke, *Understanding Cybercrime. A Guide for Developing Countries,* 2nd ed. (Draft March 2011).

Marco Gercke, "*Europe's Legal Approaches to Cybercrime*", 10 ERA Forum 409 (2009).

Martin Dixon. *Textbook on International Law* (6th ed., Oxford: Oxford University Press, 2007).

Mehmet Özcan, *Siber Terörizm ve Ulusal Güvenlik*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004

Melda Sur, *Uluslararası Hukukun Esasları*, 4. Baskı, İstanbul, 2010.

Michael A. Vatis, *The Council of Europe Convention on Cybercrime*, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf).

Mike Keyser, "*The Council of Europe Convention on Cybercrime",* 12 J. Transnational Law & Policy 287 (2003).

Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara, 2008.

Muharrem Özen/İhsan Baştürk, *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku*, Ankara, 2011.

Murat Volkan Dülger, *Bilişim Suçları*, Ankara, 2004.

Özgür Uçkan/Yasin Beceni, *Bilişim-İletişim Teknolojileri ve Ceza Hukuku*, İnternet ve Hukuk (derleyen Yeşim M. Atamer), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

Pedro Verdelho, *The effectiveness of international co-operation against cybercrime: examples of good practice*, Discussion paper (draft) prepared within the framework of the Project on Cybercrime of the Council of Europe, 2008.

Peter Csonka, "*The Council of Europe's Convention on Cyber-Crime and Other European Initiatives",* Revue internationale de droit pénal, 2006/3 Vol. 77, p. 473-501 (DOI : 10.3917/ridp.773.0473).

Peter Grabosky, "*Requirements of Prosecution Services to Deal with Cyber Crime",* 47 Crime Law Soc Change 201 (2007).

Project on Cybercrime - Final Report (September 2006-February 2009), Prepared by the Economic Crime Divison of the Directorate General of Human Rights and Legal Affairs.

R. Yılmaz Yazıcıoğlu, *Bilgisayar Suçları – Kriminolojik, Sosyolojik ve Hukukî Boyutlarıyla*, İstanbul, 1997.

R.E. Bell, "*The Prosecution of Computer Crime",* 9 Journal of Financial Crime 308 (2002).

Raluca Simion, "*Cybercrime and its challenges between reality and fiction. Where do we actually stand?",* Rivista di Criminologia, Vittimologia e Sicurezza, Vol. III- N. 3, Vol. IV, N. 1- Settembre 2009-Aprile 2010.

Ray August, "*International Cyber-Jurisdiction: A Comparative Analysis",* 39 American Business Law Journal 531 (2002).

Rebecca M.M. Wallace & Olga Martin-Ortega. *International Law* (6th ed., Cornwall: Sweet & Maxwell, 2009).

Richard W. Downing, "*Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime",* 43 Colum. J. Transnat'l L. 705 (2004-2005).

Roderic Broadhurst, *"Developments in the global law enforcement of cyber-crime"*, 29 Policing: An International Journal of Police Strategies & Management (2006).

Secretariat of the United Nations Office on Drugs and Crime (UNODC), *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime,* Working Paper submitted to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (22 Ocak 2010).

Serap Keskin, "*Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001.

Soumyo D. Moitra, "*Developing Policies for Cybercrime"*, 13 Eur. J. Crime Crim. L. & Crim. Just. 435 (2005).

Susan W. Brenner, "*Cybercrime Jurisdiction"*, 46 Crime Law Soc Change 189 (2006).

Susan W. Brenner, "*Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?",* 30 Rutgers Computer & Tech. L.J. 1 (2004).

Şaban Cankat Taşkın, *Bilişim Suçları*, İstanbul, 2008.

The Stockholm Programme—An open and secure Europe serving and protecting the citizens. Presidency Conclusions—Brussels, 10–11 December 2009, Council of the European Union, Brussels 3 March 2010, doc 5731/10.

Tonya L. Putnam & David D. Elliott, "International Responses to Cyber Crime", in Abraham Sofaer and Seymour Goodman (eds.), *Transnational Dimension of Cyber Crime and Terrorism,* 2001.

Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları*"*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt 4, Sayı 1, 2002.

Yee Fen Lim, *Cyberspace Law, Commentaries and Materials*, Oxford University Press, 2002.

Yener Ünver, "*Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısı'nın İnternet Açısından Değerlendirilmesi"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt: LIX, Sayı: 1-2, 2001.

Yılmaz Yazıcıoğlu, *TCK 2000 Tasarısında Bilişim Şebekeleri Vasıtasıyla İşlenen Suçlar,* Uluslararası İnternet Hukuku Sempozyumu, DEÜ Yayını, İzmir, 2002.

Yusuf Aksar, *Teoride ve Uygulamada Uluslararası Hukuk* – I, Ankara, 2012.