AVRUPA SİBER SUÇLAR SÖZLEŞMESİ VE TÜRKİYE'NİN DAHİL OLMA SÜRECİ

Cahit ALİUSTA, Recep BENZER
Gazi Üniversitesi, Bilişim Enstitüsü, Ankara, Türkiye
rbenzer@gazi.edu.tr

ÖZET

Bilişim suçlarıyla mücadelede yaşanan zorlukları bertaraf edebilmesi için ülkelerin aynı farkındalıkta ve hassasiyette olması, maddi ceza ve ceza muhakemesi hukuku mevzuatları arasında uyumluluk sağlanması ve bu yolla bilişim suçluları için sığınma limanlarının yok edilmesi ile uluslararası adli iş birliğinin geliştirilmesi gerektiği anlaşılmış ve bu yönde uluslararası alanda bazı adımlar atıldığı görülmektedir. Atılan adımların en önemlisi olarak Türkiye'nin de taraf olduğu ve bu çalışmanın da konusunu oluşturan Avrupa Siber Suçlar Sözleşmesi'dir. Bilişim suçları ulusal sınırlar içerisinde kalmamaktadır. Bu nedenle bu suçlarla mücadele edilebilmesi, dünya çapında elbirliğiyle etkin bir mücadele yürütülmesi halinde anlam kazanabilecektir. Sözleşme ile amaçlanan yeknesak bir yasal mevzuat temelinde, hızlı ve etkin bir uluslararası adli yardımlaşmanın ne seviyede sağlanabileceği zamanla görülecektir.

Anahtar Kelimeler— Bilişim Suçları, Siber Suç, Avrupa Siber Suçlar Sözleşmesi, Türkiye

The Council of Europe's Convention on Cybercrime and Turkey's Inclusion Process

ABSTRACT

To have the same awareness and sensitivity in order to eliminate the difficulties in the fight against cyber crimes, ensuring compliance between the provisions of material and criminal procedure law and in this way it was understood that international judicial cooperation should be developed with the destruction of asylum ports for cyber criminals. Some international steps have been taken in this direction. The most important of these steps which Turkey is a party and in which form the subject of this work is The Council of Europe's Convention on Cybercrime. Cybercrimes are not within national borders. For this reason, the fight against these crimes can be meaningful if an effective struggle is carried out worldwide. On the basis of a uniform legal legislation intended by the Convention, it will be seen in time that the fast and effective international legal aid can be achieved.

Keywords— Cybercrime, Council of Europe's Convention on Cybercrime, Turkey

1. GİRİŞ

Bilişim teknolojileri ve internetteki gelişmeler son hızla ilerlemektedir. Bununla birlikte bu alanda işlenen suç sayıları hızla artmakta ve her geçen gün farklı şekillerde çeşitli suçlar işlenmektedir. Böylece, gerek günlük gerekse mesleki hayatımızı önemli ölçüde kolaylaştıran internet ve teknoloji aynı zamanda yeni hukuki düzenlemeleri de zorunlu kılan bir problem alanı olarak ortaya çıkmıştır. Gerçekten de bazı hukukçuların karşılaşılan sorunların boyutunu anlatmak için interneti 'Vahşi Batı'ya benzettikleri görülmektedir [1]. Çünkü bu sanal ortam Vahşi Batı'da olduğu gibi sunduğu kolaylıklar ve fırsatlarla suç işlenmesini son derece kolaylaştırmakla birlikte suçlunun takibinin de yapılamadığı bir ortam oluşturmaktadır. İnternet ortamının vahşi batıdan farkı ise sanal alemde olmasıdır. Oysa bu sanal alemde işlenen suçların mağdurlarının karşılaştığı zararlar ise son derece gerçek ve acımasızcadır [1].

Global düzeyde bilişim teknolojileri ve internet gelişmeleri ile ülkemizdeki teknolojik gelişmelerin hangi düzeyde olduğu kıyaslamasına girmeksizin bu kıyaslamanın hukuki açıdan değerlendirilmesi gerekirse, ülkemizin biraz geride olduğu özeleştirisi yapılabilecektir. Ankara Üniversitesi Rektörlüğü, Ankara Barosu, Türk Patent Enstitüsü ve WIPO (World Intellectual Property Organization) işbirliğiyle 12.2.2018 tarihinde Ankara Üniversitesi Rektörlüğü 100. Yıl Konferans Salonunda "Yapay Zeka, Endüstri 4.0 ve Fikri Mülkiyet Hukuku Zirvesi" gerçekleştirilmiştir. Bu zirve, konusu itibariyle ülkemizde gerçekleştirilen ilk zirvedir. Bu zirvede, Avrupalı akademisyenlerin yaptığı sunumlarda, teknolojik gelişmeler karşısında, Avrupa ülkelerinde hukuk dünyasını bu konularda hızlıca revize etmek

için çalışmalar yapıldığı ve konunun tartışıldığı görülmüştür. Yine benzer haklara yönelik bir tartışma da, insandışı varlıkların telif hakkı sahibi olup olamayacağı konusunda ABD yargısında bir dava açılması üzerine olmuştur. Bu dava, basında da yer aldığı şekliyle 'Monkey Selfie' davasıdır. Bu davanın konusundan kısaca bahsetmek gerekirse, her şey bir doğa fotoğrafçısı olan David Slater'in Endonezya'da bir milli parkta, bir süreliğine fotoğraf makinesini sahipsiz bırakması üzerine yaşanmıştır. Fotoğraf makinesini gören, nadir bir Tepeli Makak Maymunu cinsi olan Naruto fotoğraf makinesinin kurulu olduğu tripotun üzerine çıkarak makinenin deklanşörüne basmış ve kendi özçekimini yapmıştır. Daha sonra bu fotoğrafların yayımlanması üzerine, PETA (Merkezi ABD'de bulunan Dünya'nın en büyük hayvan hakları organizasyonu) ise 2015 yılında Naruto isimli maymun adına Kaliforniya'da dava açarak fotoğraflardan elde edilen telif gelirinin Naruto'ya ait olacağına hükmedilmesini istemiştir. İlk derece mahkemesinde, Naruto'nun dava açamayacağı, davaya devam edemeyeceği gerekçesiyle açılan davanın reddine karar verilmiştir. PETA, davayı temyiz ederek 9. Temyiz Mahkemesi'ne taşımıştır. Ancak karar aşamasında tarafların uzlaşmasıyla dava sonuçlanmış olup anlaşmanın tam içeriği bilinmemekle birlikte, İngiliz fotoğrafçı David Slater'in fotoğraftan elde edilecek telif gelirlerinin %25'ini Naruto'nun yaşadığı maymun tapınağına ödeme taahhüdünü kabul ettiği öğrenilmiştir [2]. Bu davanın, ABD yargısının insandışı varlıkların haklarına ve sorumluluklarına bakışını yansıtması açısından, her ne kadar sona erme şeklinin biraz hayal kırıklığına yol açtığı söylenebilse de, önemli bir yargılama olduğunu belirtmek gerekir. Bu çerçevede, bilişim teknolojilerinin baş döndürücü hızda gelişiyor olmasıyla birlikte yeni suç ve suçlu türleriyle de karşılaşmaktayız. Hukuki altyapının bu gelişmelere cevap verememesi ise çok büyük sorunları beraberinde getirecektir. Bu nedenle bilişim teknolojileri ve internetin gelişimi aynı zamanda hukuki mevzuatın da bu gelişmelere ayak uydurmasını elzem kılmaktadır.

Öncelikle, çalışmanın konusu hakkında yaşanan kavram kargaşasını zikrederek ilgili çalışmaya başlamak daha sağlıklı olacaktır. Ağ ortamında diğer bir ifadeyle siber uzayda bilişim sistemleri aracılığıyla ve bilişim sistemlerine karşı işlenen suçlar farklı şekillerde adlandırılmaktadır. Sanal ortamda işlenen suçlar, siber suçlar, bilgisayar suçları, bilişim suçları, ileri teknoloji suçları… bu adlandırmaların birkaçıdır. 23.11.2001 tarihli Avrupa Siber Suçlar Sözleşmesinde ise bu hususta herhangi bir tanıma yer verilmemiştir. Avrupa Ekonomik Topluluğu'nun 1983 yılındaki 'Bilişim Suçları' tanımı ise günümüzde birçok ülke tarafından esas alınmıştır. Bilişim suçları; bilgileri otomatik işleme tabi tutan veya dataların taşınmasına yarayan bir sisteme karşı veya sistem ile gayri kanuni, ahlakdışı ve yetkisiz icra edilen her türlü davranış olarak tanımlanmıştır [3].

Bilişim suçları günümüzde istisnai bir suç işleme aracı olmaktan çıkmış, bilişim sistemlerine yönelik işlenen suçların yanında; sahtecilik, hakaret, dolandırıcılık, özel hayatın gizliliği ve kişisel verilere karşı suçlar gibi pek çok suç türü sıklıkla bilişim sistemleri aracılığıyla işlenen suçlar haline gelmiştir. Sosyal medya kullanımının büyük oranda artmasıyla birlikte [4] bu sitelerde kullanıcı kimlik hırsızlığı giderek artmaktadır. Yine her geçen gün internet üzerinden klasik suç tiplerinin unsurlarını içeren yeni paylaşımlar yapılmaktadır. Fikri mülkiyet hakkı ve haksız rekabete ilişkin suç duyurularının büyük çoğunluğu sanal ortamda gerçekleşmiş hak ihlallerine yöneliktir. Dünyada banka ve kredi kartlarının kopyalanması ile hesap içeriklerinin elde edilmesi ile çok büyük miktarlarda zararların ortaya çıkarıldığı belirtilmektedir [5]. 2015 yılında yapılan çalışma, bilişim suçu mağdurlarının çok büyük miktarlarda para kaybettiğini, dünyada gerçekleştirilen uyuşturucu ve kara para ticaretinden bile karlı olduğunu ve son bir yılda siber suç oranı %34 arttığı belirtilmektedir [6]. 2017 tarihli bir rapora göreyse, fidye yazılım tehditleri 2016 yılında, 2015 yılına göre %36 artarak günde ortalama 1.270'e ulaşmıştır [7]. Yine siber suçların dünya genelinde verdiği zararın 2021 yılına kadar 6 trilyon dolar olabileceği tahmin edilmektedir [8].

Devletler bilişim suçlarıyla mücadele adına mevzuatlarında düzenlemeler yapmakta, maddi ceza hukuku ve ceza usul hukuku normları getirerek bilişim suçlarını önlemeye çalışmaktadır. Ancak devletlerin ulusal düzeyde aldığı önlemler ve yaptığı düzenlemeler kâğıt üzerinde ne kadar kapsamlı ve etkili görünse de çoğu zaman etkisiz kalmaktadır. Klasik manada bir suçun işlendiği yerin tespiti ile başlayan ceza muhakemesi işlemlerinin siber uzay olarak nitelenen ağ ortamında işlenmesiyle yetki hususunda birtakım sorunlar ortaya çıkmaktadır. Yine bununla beraber bilişim suçları oldukça yeni ve hızlı gelişen bir eğilim olduğundan, suçun işleniş biçimleri hakkında şablonlar çıkarmak mümkün olamamaktadır. Bununla beraber ceza adalet sisteminin birçok aktörü henüz konuya aşina değildir. Bilişim suçlarının mukayeseli hukukta yeknesak bir tanımı olmamakla birlikte mevcut tanımlar da açık ve yeterli tanımlamalar değildir. Bilişim suçlarının özelliği gereği suçun faili ile mağduru arasında mesafe farkı bulunmaktadır. Belirtilen bilişim suçlarının işlendiği bilişim araç ve sistemleri çok teknik ve sürekli değişken olduğu görülmektedir. İnterneti kimliği belli olmayacak şekilde kullandıklarından failleri tespit etme imkanı sınırlı kalmaktadır [1]. Bilişim suçlarıyla mücadelede en büyük sorun ise, bu mücadelenin küresel çapta sağlanması gerekliliğidir. Zira çok az sayıda ülkenin bile mevzuatlarında bu alanda gerekli düzenlemeleri yapmamaları tabiri caizse bir

kurtarılmış bölge arayan bilişim suçluları için yeterli olmaktadır [9].

Gerçekten de siber suçlu herhangi bir ülkeden, istediği başka herhangi bir ülkeyi veya bu ülkedeki kişileri hedef alma imkânı bulunmaktadır [10]. Bu nedenden dolayı, doktrinde ifade edildiği gibi, siber suçlara karşı mücadele ya global olacaktır ya da bu mücadelenin hiç anlamı bulunmamaktadır [11]. Birkaç devlet dahi bu mücadeleye katılmazsa, 'forum/jurisdiction shopping' [12] (Bir tarafın kendi lehine en iyi sonucu alabileceği mahkemede dava açması) denilen olgu için bilişim suçlularına imkan sağlanmış olacak ve bu suçlular, mevzuatında en az cezayı öngören veya diğer ülkeler ile adli yardımlaşma anlaşması olmayan ülkeleri tespit ederek faaliyetlerini o ülkelerden devam edeceklerdir [10]. Aynı zamanda iade anlaşmalarında yer alan 'her iki devletçe de cezalandırılabilirlik' koşulu (iadenin gerçekleşebilmesi için, fiilin hem kendisinden iade talep edilen hem de iadeyi talep eden ülkelerde suç teşkil etmesi gerekliliği), bu suçların yargılanmasında devletlerin mevzuatları arasındaki uyumu daha da önemli olmasını ortaya çıkarmaktadır [13].

Bütün bu tehlikeler ve zorluklar, bilişim suçlarıyla mücadelede yasa koyucunun devreye girmesini zorunlu olduğunu göstermektedir. Öte yandan, bilişim suçlarıyla mücadele amacıyla birtakım düzenlemeler yapılırken internetin doğası gereği açık ve özgür olması gerekliliği internet üzerinde temel hak ve özgürlükleri sınırlamada hassas ve dikkatli olunması gerektiği unutulmaması gereken bir gerçektir [14]. Keza, bilişim suçları konusundaki yasal düzenlemelerin suç politikasının, evrensel hukukun genel ilkelerine uygun hareket edilerek oluşturulması gerektiği de vurgulanmalıdır [15].

Bilişim suçlarıyla mücadele, birden çok ülkenin yargı yetkisinin bulunması ve suçun ispatında kullanılacak delillerin elde edilme yöntemlerinin zorluğu ile bu delillerin çok farklı tür ve formatlarda olması nedeniyle klasik adli yardımlaşmadan çok daha hızlı ve yeni yardımlaşma modelleriyle mümkün olabilecektir. Bilişim suçlarıyla mücadelede yaşanan yukarıda ifade edilen zorlukları bertaraf edebilmek adına ülkelerin aynı farkındalıkta olması, maddi ceza ve ceza muhakemesi hukuku mevzuatları arasında uyumluluk sağlanması ve bu yolla bilişim suçluları için sığınma limanlarının yok edilmesi ile uluslararası adli işbirliğinin geliştirilmesi gerektiği ve bu yönde uluslararası alanda birliktelik adımları ortaya konmuştur. Bu adımların en önemlisi Türkiye'nin de taraf olduğu ve bu çalışmanın da konusunu oluşturan Avrupa Siber Suçlar Sözleşmesi'dir [9,16-18].

Tüm bu gelişmelere karşı çözüm amacıyla uluslararası kuruluşlar nezdinde yahut onların destekleriyle STK'lar aracılığıyla birçok girişim olmuştur. 1980'li yılların ortalarından itibaren bu konuda çok sayıda BM tavsiye kararı ile girişimlerde bulunulmuştur [10]. Yine Avrupa Birliği içinde, Konsey'in 2005 yılındaki "Bilişim Sistemleri Aleyhinde Saldırılara dair Avrupa Birliği Çerçeve Kararı" bu konuda önem taşımaktadır [19].

Bilişim suçlarıyla mücadelede Interpol, Europol ve Eurojust'ün çalışmaları da önemlidir. Bu konudaki önemli bir çaba, EUROPOL tarafından Yüksek Teknolojili Suçlar Merkezinin (High Tech Crime Centre) kurulması olmuştur. Keza, 2010 yılında Europol içinde, Avrupa Komisyonu, Eurojust ve AB ülkelerinin siber suçlulukla mücadele birimlerinin başındaki kişilerden oluşan, Avrupa Siber Suç Timi (European Cybercrime Task Force-EUCTF) adlı bir platform kurulmuştur. Buradaki amaç, bilişim suçlarıyla mücadelede AB içinde işbirliğini arttırarak uyumlu bir çalışma yürütmek ve bilişim suçlarının oluşmasında teknolojik gelişmelerden kaynaklanan sorunlara cevap bulmaktır [20].

Avrupa Konseyi bünyesinde, Avrupa Siber Suçlar Sözleşmesi'nin kabulü öncesinde, 1985 yılında bilgisayar suçlarının hukuki yönlerini tartışmak üzere bir Uzman Komitesi atanmış; 1989 yılında Suç Sorunlarına ilişkin Avrupa Komitesi 'Bilgisayarlarla İlişkili Suçlara dair Uzman Raporu'nu kabul edilmiş; Bakanlar Komitesi onayı ile bu suçlara ilişkin 1989 yılında bir Tavsiye Kararı ortaya konulmuştur. 1995 yılında ise sınıraşan bilgisayar suçlarından kaynaklanan sorunlara ilişkin başka bir Tavsiye Kararı daha onaylanmıştır [10].

2. AVRUPA SİBER SUÇLAR SÖZLEŞMESİ

Sözleşme'nin ilk ortaya çıkışı 1996 yılında Suç Sorunlarına ilişkin Avrupa Komitesi'nin (SSAK- European Committee on Crime Problems) Avrupa Konseyi'ne siber suçlara dair bir uzman komitesi kurmasını tavsiyesine dayandığı ortaya çıkmıştır [15,21]. Avrupa Konseyi Bakanlar Komitesi, bu öneriye uygun olacak şekilde, 1997 yılı şubat ayında 'Siber-uzay Suçları Uzman Komitesi'ni (Committee of Experts on Crime in Cyber-space) kurmuştur [21]. Komite'nin görevi, belirli konular [22] üzerinde incelemede bulunarak bağlayıcı bir hukuki enstrüman hazırlamaktır. Dört yıl boyunca çalışan Komite, Sözleşme tasarısını hazırlamış ve tasarı 2001 yılının haziran ayında SSAK tarafından onaylanmıştır. Daha sonra Avrupa Konseyi Bakanlar Komitesi onayı ile 8.11.2001 tarihinde kabul edilmiştir [14,22]. Devletlerin imzasına 23.11.2001 tarihinde Budapeşte'de açılan Avrupa Siber Suç Sözleşmesi, 1.7.2004 tarihinde yürürlüğe girmiş olup bu alandaki ilk uluslararası sözleşmedir (Bu nedenle sıklıkla Budapeşte Sözleşmesi adıyla anılmaktadır.) Avrupa Konseyi üyesi devletlerin haricinde Sözleşme, şu ana kadar 21'i Avrupa Konseyi üyesi olmayan (ABD, Kanada, Japonya, Karadağ, Güney Afrika

Cumhuriyeti, ..) toplam 68 ülke tarafından imzalamış, 62 devlet tarafından hukuki süreci başlatılmıştır. Avrupa Konseyi kurucu üyesi olan Türkiye 10.11.2010 tarihinde imzaladığı sözleşmeyi nihayet 29.09.2014 tarihinde yürürlüğe girmiştir. Sözleşmenin resmi tercümesi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak belirtilmiştir [23].

Sözleşmenin açıklayıcı raporunda belirtilen temel amaçları şu şekilde sayılabilir:

1. Bilişim suçlarıyla ilgili taraf devletlerin yasal mevzuatlarını ve bağlantılı hükümlerini uyumlu hale getirmek,
2. Siber suçların ve elektronik delil içeren diğer klasik suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku mevzuatına temel oluşturarak uluslararası muhakeme kurallarının yeknesaklaştırılmasını sağlamak,
3. Uluslararası adli yardım ve işbirliği alanında hızlı ve etkili bir sistem oluşturmak.

Gerçekten Sözleşmenin belirtilen bu amaçları çok büyük bir önem ihtiva etmektedir. Buna karşın Sözleşme, kolay çekince konmasına imkan tanıması, değişiklik rejiminin hantal olması, hazırlıklar aşamasında taraf ülkelerin eşit şekilde ve yeterli temsil edilmemiş olması gibi bazı zayıf yönleri nedeniyle eleştirilmektedir [24]. Ancak eleştirilen bu yönlerine rağmen sözleşme, yukarıda sayılan amaçlara büyük ölçüde hizmet etmekte ve taraf devletlere bilişim suçlarıyla mücadele etmek için gerekli maddi ceza hukuku ve usul hukukunun temel çatısını sağlamaktadır. Bununla beraber sınır aşan soruşturma ve kovuşturmalarda devletlerin birbirleriyle hızlı ve etkili bir şekilde koordine olabilmelerine uygun zemin sunmaktadır [1,17].

Budapeşte Sözleşmesi olarak da anılan Avrupa Siber Suçlar Sözleşmesi, 48 madde ve 4 ana bölümden oluşmaktadır. Birinci bölümde, sözleşmede kullanılan bilişim suçlarıyla alakalı terimlerin tanımlarına yer verilmiştir. İkinci bölümde, ulusal düzeyde alınacak önlemlere yer verilmektedir. Bu çerçevede, önce maddi ceza hukuku düzenlemeleri bağlamında, birtakım suç tipleri tanımlanmaktadır. Ardından muhakeme hukuku kapsamında usuli düzenlemelere yer verilmekte ve yargı yetkisi sorununa ilişkin genel ilkeler belirlenmektedir. Sözleşmenin 23. maddesiyle başlayan üçüncü bölümde ise, yukarıda anılan yetkilerin kullanımı bakımından uluslararası adli yardımlaşmanın çerçevesi çizilmektedir. Dördüncü bölümdeyse, Sözleşme'nin uygulanmasına dair birtakım usuli ve teknik hükümler yer almaktadır [24].

2.3. Maddi Ceza Hukuku ve Usul Hukuku Hükümleri

Budapeşte Sözleşmesi'nin "Ulusal Düzeyde Alınacak Tedbirler" başlıklı ikinci bölümünde, hem bilgisayar aracılığıyla işlenen ve bilgisayarların veya bilgisayar sistemlerinin kendisine karşı işlenen suçlar ve bunların tanımlanması ile ilgili hükümler hem de bağlantılı diğer hükümler bir diğer deyişle maddi hukuk konuları bulunmaktadır. Önce dört farklı kategoride gruplanan dokuz suç tipi tanımlanmakta, sonra ilave yükümlülükler ve yaptırımlar bulunmaktadır. Sözleşmede yer alan suç tipleri incelendiğinde, bunların yapısal unsurlarına ilişkin belirlemelerin, gelecekte ortaya çıkabilecek yeni bilişim teknolojilerini de kapsayabilecek nitelikte, esnek bir üslupla formüle edildiği görülmektedir [24]. Sözleşmede tanımlanan suç tipleri şunlardır:

1. Bilgisayar veri veya sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar (yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanımı),
2. Bilgisayarla bağlantılı suçlar (bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık),
3. İçerikle bağlantılı suçlar (çocuk pornografisiyle bağlantılı suçlar),
4. Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar.

Taraf devletler kendi iç mevzuatlarında bu fiilleri suç olarak düzenlemekle yükümlüdürler. Sözleşme, ikinci kısımında düzenlenen bu suç tiplerinin birebir alıntılanarak iç hukuk düzenlemesi haline getirilmesini zorunlu tutmamakta, maddi ceza hukuku mevzuatların içerik anlamında sözleşme düzenlemeleriyle uyumlu olmasını yeterlidir. Ancak, Portekiz gibi bazı taraf ülkeler sözleşmede yer alan ceza hukuku kurallarını neredeyse kelimesi kelimesine tercüme ederek "Siber Suçlar Yasası" adıyla iç hukuklarına dâhil etmişlerdir [25]. Sözleşmeyi geçersiz kalmasına itham eden bazı kişilere göre Sözleşme'nin model bir yasa öngörüp, taraf ülkelere bunu zorlaması daha etkili olabileceği değerlendirilmektedir [9].

3. TÜRK CEZA MEVZUATININ SÖZLEŞME KARŞISINDAKİ DURUMU

5237 sayılı Türk Ceza Kanunu'nda "bilişim alanında suçlar" ve "özel hayata ve hayatın gizli alanına karşı suçlar" kısmında bilişim sistemleriyle veya bunlara karşı işlenen, özellikle günümüzde söz konusu sistemler kullanılmadan işlenebilme olanakları çok kısıtlı olan hatta mümkün olmayan suçlar düzenlemeye alınmıştır. Bunların yanı sıra 5237 sayılı yasanın ve sair mevzuat hükümlerinin çeşitli bölümlerinde bilişim sistemleriyle işlenmesi olanaklı olan suç tiplerine de belirtilmiştir. Örnek verecek olursak, bilişim sistemleri vasıtasıyla gerçekleştirilen dolandırıcılık ve hırsızlık suçları bunların en önemlileridir [16].

Sözleşmenin birinci başlığında düzenlenen bilgisayar veri veya sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçların Türk hukukundaki karşılığı 5237 sayılı yasanın 243, 244 ve 245/A

maddeleri olarak görülmektedir. Ancak bu maddelerin kanunda düzenlendiği ilk hali, Sözleşme hükümleriyle uyumluluk arz etmemekte ve Türkiye'nin Sözleşmeye taraf olmakla üstlendiği yükümlülüğü birçok açıdan karşılamamaktaydı. Yasadışı erişim suçunun karşılığı olan 5237 sayılı yasanın 243. maddesi ilk haliyle bilişim sistemlerine "hukuka aykırı olarak girme ve orada kalmaya devam etme" eylemini suç olarak düzenlemekteydi. Oysa Sözleşmede yalnızca "girme" eyleminin suçun oluşumu için yeterli olduğu görülmektedir. 5237 sayılı Yasa'daki düzenleme, suçu daha kısıtlı bir kapsamda tanımlaması itibarıyla Sözleşme hükmüyle uyumlu değildi. Bu uyumsuzluğu gidermek için 24.3.2016 tarihli ve 6698 sayılı yasanın 30. maddesiyle 5237 sayılı yasanın 243. maddesi metninde yer alan "ve" ifadesi "veya" olarak değiştirilmiştir. Bu değişiklikle birlikte birçok eleştiriye maruz kalan mezkur mevzuat hükmü, Budapeşte Sözleşmesi ile uyumlu hale getirilmiştir.

Sözleşme'nin 4. ve 5. maddelerinde yer alan "verilere müdahale" ve "sisteme müdahale" suçlarının karşılığı 5237 sayılı yasanın 244. maddesi olup Sözleşme ile büyük ölçüde uyumludur. Sözleşme'nin 3. maddesinde düzenlenen "yasadışı araya girme" suçu ise ilk haliyle 5237 sayılı Yasa'da yer almamasına karşın, kanun koyucu tarafından 24.3.2016 tarihli ve 6698 sayılı yasanın 30. maddesi ile 5237 sayılı yasanın 243. maddesine eklenen 4. fıkra ile düzenlenmiştir.

Bilgisayar veri veya sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar kategorisi anlamında Türk ceza mevzuatının ilk halindeki en önemli eksikliği cihazların kötüye kullanımını suç sayan herhangi bir hükmün bulunmamasıydı. Cihazların kötüye kullanımı suçu, Sözleşme'nin 6. maddesinde yer almaktadır. Söz konusu maddede, kanunda suç olarak sayılan eylemlerde kullanımı amacıyla cihazların, şifrelerin veya erişim verilerinin üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi suç olarak düzenlenmiştir. Türk ceza hukukunda hazırlık hareketlerinin cezalandırılmaması ilkesi esas olduğu için bu yönde herhangi bir hüküm bulunmamaktaydı. Özellikle kredi kartlarının kopyalanması, zararlı yazılımların yayılması gibi suç içeren fiillerle etkin mücadele ancak hazırlık hareketleri aşamasında faillerin tespit edilip cezalandırılabilmelerinin mümkün olmasıyla sağlanabilecektir. Bu nedenle bilişim suçlarıyla etkin bir şekilde mücadele edilebilmesi ve sözleşmeye uyumluluğun sağlanması adına 24.3.2016 tarihli ve 6698 sayılı yasanın 30. maddesi ile 5237 sayılı yasaya eklenen 245/A maddesi ile Sözleşme'nin 6. maddesine uygun bir hüküm mevzuatımıza girmiştir.

Sözleşme'nin "bilgisayarla bağlantılı suçlar" şeklinde düzenlenen ikinci başlığında yer alan 'Bilgisayarla bağlantılı sahtecilik' ve 'Bilgisayarlarla bağlantılı dolandırıcılık' suçlarının Türk mevzuatında 5237 sayılı yasanın 244 ve 245. maddeleri ile bilişim sitemleri aracılığıyla gerçekleştirilen dolandırıcılığa ilişkin mezkûr yasanın 158. maddesinde ve belgede sahteciliğe ilişkin düzenleme de aynı yasanın 204 ve 212. maddeleri arasında düzenlenmiştir. Yine 5237 sayılı yasanın 142. maddesinde düzenlenen suç kapsamında da suçun bilişim sistemleri aracılığıyla işlenmesi nitelikli hal olarak sayılmıştır. 5070 sayılı yasanın 16. ve 17. maddeleri de bilişim sistemleri aracılığıyla işlenen suçlara ilişkin düzenlemeler içermektedir. Bu haliyle mevzuatımız Sözleşme'nin ikinci başlığındaki düzenlemeleri büyük ölçüde karşılamaktadır.

İçerikle bağlantılı suçlar olarak ifade edilen üçüncü başlıkta çocuk pornografisiyle bağlantılı suçlar düzenlenmiştir. Türk ceza hukukundaki karşılığı ise 5237 sayılı yasanın 226. maddesindeki müstehcenlik suçudur. Maddede suç teşkil eden müstehcenlik eylemleri tanımlanıp yaptırıma bağlanmıştır. Çocuk pornografisinin özellikle Sözleşme'nin ilgili maddeleri örnek alınarak ayrı bir suç tipi olarak düzenlenmeyişi Türk Ceza Hukuku açısından önemli bir eksiklik oluşturmaktadır [16]. Üçüncü başlıkta düzenlenen suç kapsamı Sözleşme'ye 2003 yılında eklenen ve her türlü ırkçı ve yabancı düşmanı içeriğin bilişim sistemleri aracılığıyla yayılmasının suç sayılmasını öngören Ek Protokol ile genişletilmiştir [9]. 1.3.2006 tarihinde yürürlüğe giren bu Protokol, 19.4.2016 tarihinde Türkiye tarafından imzalanmış olmakla birlikte henüz onaylanmamıştır.

Son suç kategorisi olan fikri mülkiyet haklarının ihlali ve uluslararası düzeyde dağıtımı bakımından, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 71 ve 72. madde hükümleri sözleşmeyle uyumludur ve yeteri ölçüde bir koruma ortamı sağlamaktadır.

4. SÖZLEŞMEDEKİ USUL HUKUKU DÜZENLEMELERİ

Avrupa Siber Suçlar Sözleşmesi'nde ceza muhakemesine ilişkin yasal düzenlemeler 14 ve 21. maddeler arasında düzenlenmiştir. Söz konusu maddeler ve içerdiği koruma tedbirleri:

1. 16. madde; "depolanan bilgisayar verisinin süratli şekilde korunması"
2. 17. madde; "trafik verisinin süratli şekilde korunması ve kısmen açıklanması"
3. 18. madde; "üretim emri"
4. 19. madde; "depolanmış bilgisayar verilerinin aranması ve bunlara el konulması"
5. 20 madde; "trafik verilerinin gerçek zamanlı toplanması"
6. 21. madde; "içerik verilerinin takibi"

Sözleşmede bulunan bu tedbirler klasik arama/el koyma tedbirinin, bilişim suçlarının niteliği göz önüne alınarak geliştirilmiş birer çeşididir [26]. Ancak bilişim suçlarını takip etmenin zaman ve mekân itibariyle oluşturduğu zorluklardan dolayı bu tedbirler Sözleşme tarafından ayrıntılı olarak düzenlenmiş ve taraf devletlere bu hükümlerle uyumlu tedbirleri alma sorumluluğu ve yükümlülüğü zorunlu hale getirilmiştir [21].

Özellikle belirtilmelidir ki, bu tedbirlere "önleyici kolluk faaliyeti" olarak başvurmak mümkün değildir. Bu tedbirler ancak somut bir ceza soruşturmasının varlığı halinde uygulanabileceği görülmektedir [26]. Bu tedbirler elektronik ortamda depolanmış ya da iletişim sürecinde bulunan trafik verileri, içerik verileri ve abone verilerini de içeren her türlü bilgisayar verisiyle ilgilidir [26]. Sözleşme, koruma tedbirlerinin kapsamını Sözleşmede yer alan suç tipleriyle hatta bilişim suçları ile sınırlı tutmamış, 20 ve 21. madde tedbirleri hariç olmak üzere herhangi bir suçun elektronik ortamdaki delillerinin toplanması amacıyla da bu tedbirlere başvurulabileceğini belirtmiştir [21].

5. TÜRK CEZA MUHAKEMESİ HUKUKUNUN SÖZLEŞME KARŞISINDAKİ DURUMU

Türk ceza muhakemesi hukukunda bilişim sistemlerine yönelik tek usuli düzenleme 5271 sayılı Ceza Muhakemesi Kanunu'nda yer almaktadır. 5271 sayılı yasanın 134. maddesinde düzenlenen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı maddesiyle aynı yasanın Beşinci bölümünde düzenlenen "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" başlıklı 135. vd. maddelerindeki tedbirler bilişim suçları bakımından uygulanmaktadır. Bilişim suçlarının yukarıda değindiğimiz karmaşık ve teknik yapısıyla bu suçlarla mücadelenin zorlukları göz önüne alındığında, Türk ceza muhakemesi hukukunun bu konuda oldukça geri ve eksik olduğunu söylemek yanlış olmaz.

Sözleşme ile karşılaştırıldığında; 16. maddede yer alan 'Depolanan bilgisayar verisinin süratli şekilde korunması' ve 17. maddede yer alan 'Trafik verisinin süratli şekilde korunması ve kısmen açıklanması' tedbirlerinin Türk ceza muhakemesi hukukunda bir karşılığı olmadığı yapılan inceleme ile görülmektedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da yer alan düzenlemelerin somut bir suç soruşturmasında başvurulacak ceza muhakemesi tedbirleri değil, idari tedbirler olduğu ve dolayısıyla Sözleşme'de öngörülen tedbirleri karşılamadığını belirtmek gerekmektedir [27]. Sözleşme'nin 18. maddesindeki 'Üretim emri' ve 19. maddesindeki 'Depolanmış bilgisayar verilerinin aranması ve bunlara el konulması' tedbirlerinin Türk hukukundaki karşılığı 5271 sayılı yasanın 134. Maddesi olduğu görülmektedir. Zaten klasik suçlar bakımından uygulamada son derece eksik ve sorunlu bulunan mezkur yasanın 134. maddesi, Sözleşme'de düzenlenen usul hükümlerini tam anlamıyla karşılayamamaktadır.

Sözleşme'nin 20. maddesinde düzenlenen 'Trafik verilerinin gerçek zamanlı toplanması' ve 21. maddede düzenlenen 'İçerik verilerinin takibi' tedbirlerinin de Türk hukukunda doğrudan bir karşılığı olmayıp; telekomünikasyon yoluyla yapılan iletişimin denetlenmesine ilişkin 5271 sayılı yasanın 135. maddesi hükmüne başvurulmaktadır. Ancak 135. madde hükmü, Sözleşme'nin 20 ve 21. maddelerindeki tedbirleri tam olarak karşılayamamaktadır. Bu düzenlemeler arasındaki fark teknik detaylara girmeksizin sade bir şekilde açıklanacak olursa, 5271 sayılı yasanın 135. madde hükmü yalnızca kişilerarası iletişimin denetlenmesine olanak sağlamaktadır. Yani iki gerçek kişi arasında geçen konuşma eyleminin bulunması mecburdur. Oysa Sözleşme'nin 20 ve 21. maddelerinde düzenlenen ve olması gereken tedbirler, bilişim sistemleri arasındaki her türlü veri iletişimini kapsamaktadır. Görüldüğü üzere Türk ceza muhakemesi hukukunun bilişim alanında öngördüğü tedbirler Sözleşme'nin öngördüğü standartların çok gerisindedir. Sözleşmeye uyum sağlanması ve bilişim suçlarıyla etkin bir mücadelenin yürütülebilmesi için ceza muhakemesi hukukunda bir an önce sözleşmeye uygun kanuni değişikliklerin gerçekleştirilmesi gerekmektedir.

6. SÖZLEŞMEDE DÜZENLENEN ADLİ YARDIMLAŞMANIN ESASLARI

Budapeşte Sözleşmesi'nin en önemli bölümü, bilişim suçlarıyla mücadelede adli yardımlaşma hükümlerini içeren 3. bölümdür. Zira sınır tanımayan bir özelliğe sahip, birçok ülke üzerinde aynı anda işlenebilen, soruşturulması ile kovuşturulması çok teknik ve zorlu bir süreç olmasını gerektiren ve delillerin çabuk kaybolabildiği bu suç türleriyle mücadelede etkin ve çok hızlı bir uluslararası işbirliği olmazsa olmazdır.

Bu kapsamda, Avrupa Siber Suçlar Sözleşmesi, birincil maksadı olan etkin bir uluslararası adli yardımlaşmanın gerçekleşebilmesi adına üçüncü bölümde adli yardımlaşmaya ilişkin birtakım genel ilkeler ve özel usuller getirdiği görülmektedir. Sözleşme, adli yardımlaşmaya dair mevcut diğer anlaşmaların yerini almayı amaçlanmadığı görülmektedir. Hedefi, söz konusu diğer anlaşmalarla kurulu mevcut rejim kapsamında uygulanmaktır. Ayrıca, taraf ülkeler arasında bir anlaşma hükmünün yokluğunda uygulanabilecek ilke ve kuralları da belirlemek suretiyle önemli bir kazanım sağlayacaktır [24].

Sözleşmenin 23. maddesi adli yardımlaşmaya ilişkin genel ilkeleri ortaya koymaktadır. Bu sonuca göre, taraf devletler arasında adli yardımlaşma birbirleriyle mümkün olan en geniş biçimde sağlanmalı, işbirliğinin bilişim sistemleriyle ilişkili suçlarla birlikte delilleri elektronik ortamda bulunan diğer suçları da kapsayacak şekilde uygulanmalı ve adli yardımlaşma hem yerel ve uluslararası anlaşmalar uyarınca yürütülen şekliyle hem de Sözleşme'nin öngördüğü usullere uygun olarak ortaya konacaktır [28].

Sözleşme, genel ilkelerin dışında etkin bir adli yardımlaşma sistemini tesis etmek amacıyla bazı özel yardımlaşma usulleri de ortaya koymaktadır. Bu özel hükümler, ulusal düzeyde alınması gereken usuli tedbirlerin uluslararası temelleridir. Bunlar, Sözleşme'nin "Özel Hükümler" başlıklı İkinci Kısmında 'depolanan bilgisayar verilerinin süratli şekilde korunması' başlıklı 29. maddesinde, 'korunan trafik verilerinin süratli şekilde açıklanması' başlıklı 30. maddesinde ve 'depolanan bilgisayar verilerine erişim konusunda karşılıklı yardımlaşma' başlıklı 31. maddesinde düzenlenen usuli hükümlerdir. Sözleşme'nin 35. maddesinde taraf devletlerden her birine 7 gün 24 saat erişilebilecek bir irtibat noktalarının kurulması yükümlülüğü getirilmiştir. Türkiye için 7/24 irtibat noktası EGM Siber Suçlarla Mücadele Daire Başkanlığı olarak belirlenmiştir. Bunun yanında, adli yardımlaşma konusunda merkezi makam olan Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü'nün de anılan Başkanlık ile birlikte 7/24 irtibat noktası olması yönünde girişimler öngörülmektedir [24].

7. SONUÇ

Bilişim suçları, ulusal sınırlar içerisinde kalmamaktadır. Bu nedenle bu suçlarla mücadele edilebilmesi, dünya çapında elbirliğiyle etkin bir mücadele yürütülmesi halinde anlam kazanabilecektir.

Bilişim suçlarıyla mücadelede yaşanan zorlukları bertaraf edebilmek adına devletlerin aynı farkındalıkta ve hassasiyette olması, maddi ceza ve ceza muhakemesi hukuku mevzuatları arasında uyumluluk sağlanması ve bu yolla bilişim suçluları için sığınma limanlarının yok edilmesi ile uluslararası adli iş birliğinin geliştirilmesi gerektiği anlaşılmış ve bu yönde uluslararası alanda bazı adımlar atılmıştır. Bu adımların en önemlisi Türkiye'nin de taraf olduğu ve bu çalışmanın da konusunu oluşturan Avrupa Siber Suçlar Sözleşmesi'dir. Bilişim suçları ulusal sınırlar içerisinde kalmamaktadır. Bu nedenle bu suçlarla mücadele edilebilmesi, dünya çapında elbirliğiyle etkin bir mücadele yürütülmesi halinde anlam kazanabilecektir.

Ülkelerin maddi ceza ve ceza muhakemesi hukuku mevzuatlarının farklı olması uluslararası etkin bir mücadeleye engel teşkil etmektedir. Bu sorunu aşmak adına adım atan ilk bağlayıcı uluslararası metin Avrupa Siber Suçlar Sözleşmesi'dir. Eleştirilen yönleri olmasına karşın Sözleşme bilişim suçlarıyla mücadelenin en önemli enstrümanıdır [1,9,16]. Sözleşme'nin en temel amaçlarından birisi ilgili konularda ulusal mevzuatların uyumlulaştırılmasının sağlanmasıdır. Bu nedenle taraf devletlere iç hukuklarında Sözleşme'de öngörülen maddi ve usuli ceza hukuku kurallarına uygun düzenlemeler yapma yükümlülüğü getirmiştir.

Netice olarak aşağıdaki hususlara dikkat edilmesi bu sürecin hızlanmasına katkılar sağlayacaktır. Bunlar;

1. Budapeşte Sözleşmesi'nin bilişim suçlarıyla mücadele konusunda çok önemli bir adımdır. Sözleşme ile amaçlanan yeknesak bir yasal mevzuat temelinde, hızlı ve etkin bir uluslararası adli yardımlaşma ortamı oluşturulmalıdır.
2. Siber tehdit ve tehlikelerin her ülkenin problemidir. Gelecekte bu daha da önemli bir problem haline gelecektir. Dolayısıyla ülkelerin, hem yasal düzenlemeleri uyumlu hale getirmelerinin yanında hem uluslararası işbirlikleri düzeylerini arttırmaları hem de tehdit istihbaratı yapılabilmesi içinde çalışmalar yürütmelidirler.
3. Ülkelerin hukuki süreçlerdeki problemleri görmeleri için ortak siber güvenlik tatbikatları yapılması ve bu deneyimlerden faydalanılması, uyum sürecini hızlandıracaktır.

KAYNAKLAR

[1] M. Keyser, "The Council of Europe Convention on Cybercrime", Journal of Transnational Law & Policy. 12(2):131-170. 2002.

[2] A. Guadamuz, "Can the monkey selfie case teach us anything about copyright law?", Wipo Magazine https://www.wipo.int/wipo_magazine/en/2018/01/article_0007.html adresinden erişildi. (14.12.2018).

[3] A.K. Ekizer, "Bilişim Suçları (Siber Suçlar)", https://www.ekizer.net adresinden erişildi. (08.12.2018).

[4] H. Bayrak, "Dünya'da İnternet Kullanımı ve Sosyal Medya İstatistikleri- 2. Çeyrek Raporu", https://dijilopedi.com/dunyada-internet kullanimi-ve-sosyal-medya-istatistikleri-2-ceyrek-raporu/ adresinden erişildi. (15.12.2018).

[5] J.S. Dhillon and R.I. Smith, "Defensive Information Operations and Domestic Law: Limitations on Governm ental Investigative Techniques", 50 A.F. L. REV. 135, 138. 2001.

[6] Symantec, "Internet Security Trends Report 2015, Symantec", http://www.symantec.com/en/

uk/security_response/publications/threatreport.jsp adresinden erişilmiştir. (08.12.2018).

[7] Symantec, "Internet Security Threat Report 2017, Symantec," https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf adresinden erişilmiştir. (15.12.2018).

[8] S. Cantürk, "Bireysel Siber Farkındalık Araştırması", https://home.kpmg.com/tr/tr/home/gorusler/2018/05/bireysel-siber-farkindalik_arastirmasi.html adresinden erişilmiştir (15.12.2018).

[9] A.M. Weber, "The Council of Europe's Convention on Cybercrime", Berkeley Technology Law Journal. 18(1):425-446. 2003.

[10] M. Gercke, "Understanding cybercrime: phenomena, challenges and legal response" International Telecommunication Union, 366, 2012.

[11] G. Esposito, "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, 412. 2004.

[12] M. Webster, "Forum shopping" www.merriam-webster.com/legal/forum_shopping adresinden erişilmiştir (15.12.2018).

[13] G. Allan, "Responding to Cybercrime: A Delicate Blend of the Orthodox and the Alternative", 2005 N. Z. L. Rev. 149, s.153, 2005.

[14] H. Sınar, "İnternet ve Ceza Hukuku" Beta Basım Yayın, s.160, 2001.

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

[16] M.V. Dülger, "Bilişim Suçları ve İnternet İletişim Hukuku", Ankara: Seçkin, 2014.

[17] S. Havuz, "Avrupa Siber Suçlar Sözleşmesi kapsamında Türkiye'nin Güvenliği", Yayımlanmamış Yüksek Lisans Tezi. Harp Akademileri Komutanlığı, 2007.

[18] C. Taşkın, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", Türkiye Barolar Birliği Dergisi, 85:332-372. 2009.

[19] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, OJ L 69 of 16 March 2005, p. 67. 2005. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32005F0222 adresinden erişilmiştir. (15.12.2018).

[20] Europol Review - General Report on Europol Activities, European Police Office (2011), s. 48. https://www.europol.europa.eu/sites/default/files/documents/en_europolreview.pdf adresinden erişilmiştir. (15.12.2018).

[21] Council of Europe, Explanatory Report to the Convention on Cybercrime, https://rm.coe.int/16800cce5b adresinden erişilmiştir. (15.12.2018).

[22] M.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" cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf adresinden erişilmiştir. (15.12.2018).

[23] Council of Europe, coe.int/ en/web/conventions/full-list/conventions/treaty/185/signatures?pauth=7mZsVgAk adresinden erişilmiştir. (15.12.2018).

[24] M. Önok, "Avrupa Siber Suçlar Sözleşmesi ışığında siber suçlarla mücadele uluslararası işbirliği", Hukuk Araştırmaları Dergisi. 1229-1269. 2013.

[25] M. Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri", Article Letter Summer. 73-88. 2015.

[26] S. Keskin, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası LIX, 59 (1-2): 155-180. 2001.

[27] Cybercrime Legistlation Country Profiles, Council ofEurope,coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp. adresinden erişilmiştir. (08.04.2015).

[28] Council of Europe, International Cooperation under the Convention on Cybercrime, Project on Cybercrime, Council of Europe. https://rm.coe.int/1680304352 adresinden erişilmiştir. (15.12.2018).