PART 6

MÜCAHİD ÖZBEK

The Impacts of European Cybercrime Convention on Turkish Criminal Law

Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri

ABSTRACT
The European Cybercrime Convention is one of the most significant tools in the fight against cybercrime. The Convention aims to harmonize the domestic legislations of member states and coordinate an effective cooperation among them. Turkey signed the Convention in 2010 and put it into force after its ratification and promulgation in 2014. In this article, the substantial criminal laws and procedural provisions of the Convention are examined in comparison with Turkish domestic law.

KEYWORDS:
Cybercrime, computer crimes, Cybercrime Convention, electronic evidence, judicial cooperation

ÖZET
Siber suçlulukla uluslararası mücadelenin en önemli araçlarından birisi Avrupa Siber Suçlar Sözleşmesidir. Sözleşme taraf devletlerin mevzuatlarını uyumlulaştırmayı ve etkin bir adli işbirliğini koordine etmeyi amaçlamaktadır. Türkiye Sözleşmeyi 2010 yılında imzalamış, 2014 yılında uygun bularak yürürlüğe sokmuştur. Bu makalede Sözleşmenin öngördüğü ceza ve ceza muhakemesi hukuku kuralları Türk mevzuatıyla karşılaştırmalı olarak incelenmektedir.

ANAHTAR KELİMELER:
Siber suçlar, bilişim suçları, Siber Suçlar Sözleşmesi, elektronik delil, adli yardımlaşma

PART 6

1. INTRODUCTION

THE CRIMES COMMITTED BY MEANS OF INFORMATION technology or on the Internet increase in number and diversify each day in parallel with developments on these fields. Therefore, the information technology and the Internet, which in deed make our daily and professional life considerably easier, have become a problem necessitating legal arrangements[1]. So much so that, the Internet is often referred to "Wild West" in order to explain gravity of the problems[2]. Indeed, besides the opportunities it offers, Internet appears to be a ground on which criminals and crimes can avoid prosecution just like in the old Wild West. The only difference is that Internet is a virtual society. However, the harm individuals and corporations are exposed to through crimes committed on the Internet are very real [3].

There is a need to mention the dispute on terms in this subject and clarify our approach before getting into details. The crimes committed through computer systems and in a networking environment, which is also called cyberspace, are named differently by variety of criteria: computer crimes, computer related crimes, crimes committed in cyberspace, cybercrimes. There is no consensus on this matter neither in the international platform nor the national one, and a contradiction among the terms is observed. I prefer to use the term "cybercrime" which is a superior concept including the others in my opinion and the most favored internationally. Cybercrimes can be defined as crimes committed against or by means of computer systems[4].

Currently, cybercrimes are not anymore exceptional forms of delinquency. Right alongside with the relatively new types of crimes against computer systems, the Internet and computer systems became the primary means for many conventional crimes such as fraud, defamation, violation of privacy etc. In addition, identity theft is very common on social media platforms. Each day, millions of transgressive content is produced and distributed. More than half of the companies in an EU survey report that their systems were penetrated from outside. Almost all reported intellectual property violations related to controversial Internet actions. The total amount of loss annually caused by counterfeit credit or bank cards and theft of account information exceeds billions of dollars[5]. A report dated 2015 reveals that cybercrime victims lose 388 billion dollars per year- that

1. GİRİŞ

BİLİŞİM TEKNOLOJİLERİNİN VE İNTERNETİN HIZLI gelişimine paralel olarak bu alanlarda işlenen suçların sayısı hızla artmakta ve her geçen gün yeni suç yöntemleri karşımıza çıkmaktadır. Böylece, günlük ve mesleki hayatımızı önemli ölçüde kolaylaştıran teknoloji ve internet, diğer yandan, yeni hukuki düzenlemeleri zorunlu kılan bir sorun hâline gelmiştir[1]. Öyle ki; bazı hukukçular sorunun boyutlarını anlatmak için interneti "Vahşi Batı"ya benzetmektedir[2]. Gerçekten de internet ortamı tıpkı vahşi batıda olduğu gibi sunduğu çok sayıda kolaylık ve fırsatın yanı sıra suçların ve suçluların takibinin yapılamadığı bir ortam olarak karşımıza çıkmaktadır. Tek fark internet ortamının sanal olmasıdır. Buna mukabil internet ortamında işlenen suçlar dolaysıyla bireylerin ve şirketlerin maruz kaldığı zarar son derece gerçektir[3].

Çalışmamızın başında incelenen konuya ilişkin kavram kargaşasına değinmek ve tercihimizi açıklamak isabetli olacaktır. Siber uzay olarak da ifade edilen ağ ortamlarında ve bilişim sistemleri aracılığıyla işlenen suçlar farklı kriterlere göre farklı şekillerde isimlendirmektedir: bilgisayar suçları, bilişim suçları, sanal ortamda işlenen suçlar, siber suçlar. Bu konuda ne uluslararası ne de ulusal düzeyde bir görüş birliği olduğu ve bir kavram kargaşasının süregittiği görülmektedir. Biz bu konudaki tartışmalar girmeden; diğer kavramları kapsayan bir üst bir kavram olarak gördüğümüz ve uluslararası anlamda en çok itibar gören "siber suç" tabirini kullanmayı tercih ediyoruz. Siber suçlar, siber suçları, bilişim sistemleri aleyhine veya bilişim sistemleri aracılığıyla işlenen suçlar, olarak tanımlanabilir[4].

Bugün siber suçlar istisnai bir suç işleme yöntemi olmaktan çıkmış, bilişim sistemlerine yönelik işlenen ve nispeten yeni suç türlerinin yanı sıra; dolandırıcılık, hakaret, özel hayatın gizliliği ve kişisel verilere karşı suçlar gibi pek çok klasik suç tipi için de internet ortamı ve bilişim araçları birincil işlenme yolu haline gelmiştir. Sosyal medya sitelerinde kimlik hırsızlığı suretiyle kişilik hırsızlıkları yapılmakta, her gün içeriği suç teşkil eden milyonlarca içerik oluşturulmakta ve iletilmektedir. Şirketlerin en az yarısı bilişim sistemlerine dışarıdan müdahale gerçekleştiğini rapor etmekte. Fikri mülkiyet ihlali ve haksız rekabetle ilişkili suç duyurularının neredeyse tamamı internet ortamında gerçekleşmiş saldırılara ilişkin olarak yapılmakta, banka kartlarının kopyalanması ve hesap

makes the cybercrime business more profitable than illegal drug trafficking- and that cybercrime soared 34% last year[6].

States make regulations on their domestic laws in order to combat cyber-criminality and endeavor to prevent it by enacting specific criminal and criminal procedural laws. However, these measures at national level often remain incapable no matter how extensive and effective they seem to be. The difficulty of the fight against cybercrimes and the reasons for the failure of states on this fight can be listed as the following: As cyber-criminality is a pretty new phenomenon, it is not easy to identify crime patterns; therefore most of the actors of criminal justice system are not familiar with the concept[7]. Besides the fact that there is no uniform definition of related terminology in comparative law, the existing ones are not clear enough. There is always geographical distance between offender and victim by the nature of the cybercrimes. The tools used for these crimes require technical expertise and evolve rapidly. Sometimes, it can be very difficult to identify the offender as it is possible to act anonymously[8]. The biggest problem on the fight against cyber-criminality through criminal laws is that even a few countries' omission to make necessary legal arrangements is sufficient for the cyber criminals who are looking for a "liberated zone/shelter"[9].

In order to overcome aforementioned difficulties, the international community have recognized the necessity of same level of awareness and sensibility of the states on the political ground, the harmonization of domestic criminal and criminal procedural laws, the elimination of liberated zones and improvement of international cooperation and some steps have already been taken. The European Cybercrime Convention, to which Turkey is a party of, is one of the most significant steps on that way[10].

In this article, a short history and the structure of the Convention is explained in brief, then the substantial

bilgilerinin çalınması gibi yollarla toplamda milyarlarca dolarlık zararın doğduğu tahmin edilmektedir[5]. 2015 yılına ait bir rapor, siber suç mağdurlarının dünya çapında her yıl 388 milyar dolar kaybettiğini, bu işin küresel çaptaki marihuana, kokain ve eroin ticaretinden daha karlı olduğunu ve son bir yılda siber suçluluğun %34 arttığını ortaya koymaktadır[6].

Devletler siber suçluluk gerçeğiyle mücadele edebilmek adına ulusal hukuk sitemlerinde düzenlemeler yapmakta, özel ceza hukuku ve ceza muhakemesi hukuk kuralları getirerek siber suçluluğu önlemeye çalışmaktadır. Ancak devletlerin ulusal düzeyde aldığı önlemeler ne kadar kapsamlı ve etkili görünse de çoğu zaman etkisiz kalmaktadır. Siber suçlarla hukuki mücadelenin zor olmasının ve devletlerin başarısız olmasının nedenleri şu şekilde sayılabilir: Siber suçluluk oldukça yeni bir fenomen olduğundan, suçun işleniş biçimleri hakkında şablonlar çıkarmak mümkün olmamaktadır ve buna bağlı olarak ceza adaleti sisteminin bir çok aktörü konuya henüz aşina değildir[7]. Siber suçların mukayeseli hukuktaki tanımı yeknesak olmadığı gibi, mevcut tanımlar da her zaman çok net değildir. Siber suçluluğun özelliği gereği fail ile mağdur arasında mekansal mesafe bulunmaktadır. Bu suçların işlendiği araç ve sistem çok teknik ve sürekli değişkendir. İnterneti anonim olarak kullanma fırsatı nedeniyle failleri tespit etme olanağı bazen çok sınırlıdır[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[9].

Siber suçlulukla mücadelede yaşanan yukarıda sayılan zorlukları bertaraf edebilmek adına, siber suçluluk konusunda devletlerin aynı farkındalık ve hassasiyette olması, ulusal ceza ve ceza muhakemesi hukuku mevzuatları arasında uyumluluk sağlanması ve bu yolla siber suçlular için sığınma limanların yok edilmesi ve uluslararası işbirliğinin geliştirilmesi gerekliliği anlaşılmış ve bu yönde uluslararası alanda bazı adımlar atılmıştır. Bu

FOOTNOTE DİPNOT

1 Murat Önok, "Avupa Siber Suçlar Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası Adli İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Arşatırmaları Dergisi* 19/2 (Prof.Dr. Nur Centel'e Armağan) (2013), 1230.
2 Mike Keyser, "The Council of Europe Convention on Cybercrime", *Journal of Transnational Law & Policy* 12:2 (2002), 187; Henry E. Crawford , *Internet Calling: FCC Jurisdiction over Internet Telephony,* 5 COMM. L. CONSPECTUS 43, 43 (1997).
3 Keyser, "The Council of Europe Convention on Cybercrime", 188.
4 Önok, "Avupa Siber Suçlar Sözleşmesi...", 1231.
5 Joginder S. Dhillon & Robert I. Smith, *Defensive Information Operations and Domestic Law: Limitations on Governm ental Investigative Techniques*, 50 A.F. L. REV. 135, 138 (2001).
6 Internet Security Trends Report 2015, Symantec, (08.04.2015). http://www.symantec.com/en/uk/security_response/publica-tions/threatreport.jsp.

criminal laws and procedural provisions of the Convention are examined in comparison with Turkish domestic law and finally essential principles of judicial cooperation regime provided by the Convention are mentioned.

2. EUROPEAN CYBERCRIME CONVENTION

The Council of Europe accepted the European Cybercrime Convention (**"the Convention"**) as the first binding international legal text in this field to harmonize domestic laws and foster international cooperation[11]. The text of the Convention was drafted by the Committee of Experts on Crime in Cyberspace (PC-CY), a committee established by the Council of Europe in 1997. The draft Convention and the Explanatory Report to the Convention were approved by the Parliamentary Assembly and the Committee of Ministers of the Council of Europe and opened for signature on November 23rd, 2001 in Budapest. (This is why the Convention is also known as Budapest Convention.) The Convention has come into force on July 1st, 2004.

adımların en önemlisi Türkiye'nin de taraf olduğu ve makalemizin konusunu oluşturan Avrupa Siber Suçlar Sözleşmesidir[10].

Makalemizde öncelikle kısaca Sözleşmenin tarihi ve yapısı incelenmekte, sonrasında sözleşmede öngörülen ceza hukuku ve ceza muhakemesi hukuku kuralları Türk mevzuatıyla karşılaştırmalı olarak ele alınmakta ve son olarak Sözleşmenin öngördüğü adli yardımlaşma rejiminin temel ilkelerine değinilmektedir.

2. AVRUPA SİBER SUÇLAR SÖZLEŞMESİ

Siber suçlulukla mücadelede mevzuat birliği sağlamak ve uluslararası işbirliğini tesis etmek amacıyla Avrupa Konseyi tarafından hazırlanan Avrupa Siber Suçlar Sözleşmesi (**"Sözleşme"**) bu alandaki ilk uluslararası anlaşmadır[11]. Avrupa Konseyi Bakanlar Kurulu tarafından 1997 yılında kurulan Siber-uzay Suçları Uzmanlar Komitesi (**"PC-CY"**) tarafından dört yıllık bir çalışma sonucunda oluşturulan sözleşme taslağı ve açıklayıcı raporu Avrupa

The Convention's membership is not limited to Council of Europe's members. Until now, 53 states including 21 non-member states (including the USA, Canada, Japan, Montenegro and The Republic of South Africa) signed and 45 states have put it into force. Turkey, a founding member of the Council of Europe, terminally signed the Convention on November 10th, 2010, ratified on September 29th, 2014 and put into force on May 2nd, 2014. The official translation of the Convention's name to Turkish is "Convention on Crimes Committed on Virtual Environment". However, I find the term "Cybercrime Convention" more accurate as adopted by doctrine and prefer to use it on the aforementioned grounds.

The objectives of the Convention can be listed as the following according to the Explanatory Report: To harmonize domestic laws on cybercrime and relevant regulations, to provide procedural powers and regulations related to the prosecution of cybercrimes and other crimes involving electronic evidence and to establish a quick and effective system of cooperation. Although it is subject to criticism for some weakness such as easily allowing reserves, having an heavy going amendment procedure, and the parties not contributing equally and sufficiently at the drafting process; the Convention serves its goals to a great extent by providing a framework legislation on criminal and procedural matters necessary to fight against cybercrime for party states and a convenient platform for a better and faster cooperation among states on the transnational prosecutions[13].

The Convention is composed of forty-eight articles under four main chapters. The First Chapter defines the cybercrime related terms vital to the Convention. Second Chapter establishes a set of rules that parties have to adopt on national level. In this context, first certain criminal offenses are defined as part of substantial criminal provisions, and then a common set of procedural measures and a set of rules by which parties can assert jurisdiction are laid down. In the Third Chapter of the

Konseyi Genel Kurulu ve Bakanlar Kurulu tarafından onaylanmış ve 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılmıştır. (Bu nedenle sıklıkla Budapeşte Sözleşmesi olarak anılmaktadır.) Sözleşme 1 Temmuz 2004'te yürürlüğe girmiştir.

Avrupa Konseyi üyesi devletlerle sınırlı olmayan Sözleşme, şu ana kadar 21'i Avrupa Konseyi üyesi olmayan (ABD, Kanada, Japonya, Karadağ, Güney Afrika Cumhuriyeti...) 53 devlet tarafından imzalamış, 45 devlet tarafından yürürlüğe sokulmuştur. Avrupa Konseyi kurucu üyesi olan Türkiye 10.11.2010 tarihinde imzaladığı sözleşmeyi nihayet 29.09.2014 tarihinde uygun bularak, 2.05.2014'te yürürlüğe sokmuştur. Sözleşmenin Türkçe'ye resmi tercümesi "Sanal Ortamda İşlenen Suçlar Sözleşmesi" şeklinde yapılmış olup, biz yukarıda da kısaca açıkladığımız gerekçelerle doktrinde de yer etmiş olduğu şekilde Avrupa Siber Suçlar Sözleşmesi tabirini daha doğru buluyor ve tercih ediyoruz.

Sözleşmenin açıklayıcı raporu uyarınca sözleşmenin temel amaçları şu şekilde sayılabilir: Siber suçlarlar ilgili ulusal düzeydeki yasal düzenlemelerin ve bağlantılı hükümlerin uyumlu hale getirilmesi, siber suçların ve elektronik delil içeren diğer klasik suçların soruşturma ve kovuşturulması ile ilgili ulusal usul hukuku yetkilerini ve düzenlemelerini sağlamak ve uluslararası işbirliği alanında hızlı ve etkili bir sistem oluşturmak. Kolay çekince konmasına imkan tanıması, değişiklik rejiminin hantal olması, hazırlık aşamasında taraf devletlerin eşit şekilde ve yeterince temsil edilmemiş olması gibi bazı zayıf yönleri nedeniyle eleştirilse de[12]; sözleşme bu amaçlarına büyük ölçüde hizmet etmekte ve taraf devletlere siber suçlarla mücadele etmek için gerekli maddi ceza hukuku ve usul hukukun temel çatısını sağlamakta ve sınır aşan kovuşturmalar için birbirleriyle süratli bir şekilde koordine olabilmeleri için uygun bir zemin sunmaktadır[13].

Sözleşme kırk sekiz madde ve dört ana bölümden oluşmaktadır. Birinci bölümde Sözleşmede kullanılan siber

FOOTNOTE DİPNOT

7 Francesco Calderoni, *The European legal framework on cybercrime: striving for an effective implementation*, 54 Crime Law Soc Change 339 (2010), 341.
8 Keyser, "The Council of Europe Convention on Cybercrime", 326.
9 Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal* 18/1 (2003), 425.
10 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, (Ankara: Seçkin, 2014), 185; Weber, "The Council of Europe's Convention on Cybercrime", 446; Serdar Havuz, "Avrupa Siber Suçlar Sözleşmesi kapsamında Türkiye'nin Güvenliği", Yayımlanmamış Yüksek Lisans Tezi (2007), 136; Cankat Taşkın, "Bilişim Hukuku Uluslararası Uyuşmazlıklar", *Türkiye Barolar Birliği Dergisi* 85 (2009), 368.
11 Havuz, "...Türkiye'nin Güvenliği", 138.
12 Önok, "Avupa Siber Suçlar Sözleşmesi...", 1246; Weber, "The Council of Europe's Convention on Cybercrime", 444.

Convention, a framework for cooperation in the use of those powers is set out. The Forth Chapter, which is the last, provides the formal and technical provisions related to the application of the Convention.

3. THE SUBSTANTIAL CRIMINAL PROVISIONS OF THE CONVENTION

3.1. In General

In the Second Chapter of the Convention, titled "Measures to be taken- substantive criminal law and procedural law", there are definitions of the offenses committed against, by means of, or in relation with computer systems and related substantive criminal provisions. First nine types of offenses are defined, then supplementary provisions and sanctions are reflected. When the definitions of offenses are examined, the wording and formulation of the structural components of these offenses are determined taking the possibility of emergence of new technologies in the future into account[14].

The offenses defined in the Convention are:

a. Offenses against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices),

b. Computer related offenses (computer-related forgery, computer-related fraud)

c. Content related offenses (offenses related to child pornography)

d. Offenses related to infringements of copyright and related rights.

The parties are supposed to criminalize these offenses in their domestic laws. The Convention does not impose parties to copy the definitions verbatim into their domestic laws. It is only required that the respective domestic laws contain concepts that are "consistent with the principles of the Convention. However certain states, such as Portugal, made the Convention's provisions a part of their domestic law by copying the text of the Convention word by word and ratifying it under the name of "cybercrime law". According to some professors criticizing the Convention for being ineffective, it would be more effective if the Convention would impose a model cybercrime law[15].

suçlarla ilgili temel kavramlar tanımlanmaktadır. İkinci bölümde taraf devletlerin ulusal düzeyde alması gereken önlemlere yer verilmektedir. Bu çerçevede, önce maddi ceza hukuku düzenlemeleri bağlamında, birtakım suç tipleri tanımlanmakta; ardından da, ceza muhakemesi hukuku düzenlemeleri bağlamında, birtakım usuli tedbirlere yer verilmekte ve yargı yetkisine dair bazı genel ilkeler belirlenmektedir. Sözleşmenin 3. bölümünde yukarıda anılan yetkilerin kullanımı bakımından, uluslararası adli yardımlaşmanın çerçevesi çizilmekte; son kısım olan Dördüncü Bölümde ise Sözleşme'nin uygulanmasına dair birtakım usuli ve teknik hükümlere yer verilmektedir.

3. SÖZLEŞEMENİN ÖNGÖRDÜĞÜ MADDİ CEZA HUKUKU HÜKÜMLERİ

3.1. Genel Olarak

Sözleşmenin "ulusal düzeyde alınacak önlemler – maddi hukuk ve usul hukuku" 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 yani maddi hukuk konuları yer almaktadır. Önce dört farklı kategoride gruplanan dokuz suç tipi tanımlanmakta, sonra ilave yükümlülükler ve yaptırımlar belirtilmektedir. 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[14].

Sözleşmede tanımlanan suç tipleri şunlardır:

a. Bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar (yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale, cihazların kötüye kullanımı),

b. Bilgisayar aracılığıyla işlenen sahtecilik suçları ve bilgisayarlar aracılığıyla işlenen dolandırıcılık suçları (sanal sahtecilik ve dolandırıcılık suçları),

c. İçeriğe ilişkin suçlar (çocuk pornografisine ilişkin materyale sahip olmak ve uluslararası düzeyde dağıtımını sağlamak),

d. Fikri mülkiyet haklarının ihlali ve uluslararası düzeyde dağıtımı.

3.2. Position of the Turkish Criminal Law against the Convention

The chapters "Offenses in the field of informatics" and "Offenses against privacy and private life" of the Turkish Criminal Code numbered 5237 (**"TCK"**) criminalize offenses which can be committed against or by means of computer systems. These offenses aren't likely to be committed without help of a computer system. Other than these, in several other chapters of the TCK, there are offenses likely to be committed by means of computer systems although they are not specific computer crimes. Aggravated larceny by means of computer systems and aggravated fraud by means of computer systems can be surveyed as the examples of this type of offenses[16].

An exhaustive mapping of current Turkish law against the provisions of the Convention, and a comparison of equivalent provisions one by one is beyond the scope of this paper. Thus, with the presumption that the audience have basic knowledge on the related provisions of the Turkish criminal law and the Convention, we confine this study to a general comparison of the Convention and the current Turkish law within the frame of the offense categories adopted by the Convention and to determination of deficiencies and inadequacies of Turkish law in view of the Convention.

The analogous in Turkish law, of the offenses against the confidentiality, integrity and availability of computer data and systems that are set out in the first category are the articles 243 and 244 of the TCK[17]. However, these articles do not cover the provisions of the Convention and, in many aspects, do not provide regulations necessary to comply with the Convention.

The Article 243 of the TCK, which is the equivalent the offense of illegal access, criminalizes action of "unlawfully accessing to and remaining within a computer system". Whereas, according to convention the action of "accessing" is necessary and sufficient to commit the crime. The formulation of TCK is not compatible with the Convention because it determines the scope of the of-

Taraf devletler bu fiilleri suç haline getirmekle yükümlüdürler. Sözleşme, ikinci bölümde düzenlenen bu suç tiplerinin bire bir alıntılanarak iç hukuk kuralı haline getirilmesini zorunlu tutmamakta, ulusal ceza hukuku mevzuatların içerik anlamında sözleşme düzenlemeleriyle uyumlu olmasını yeterli görmektedir. Buna karşın Portekiz gibi bazı taraf devletler sözleşmede yer alan ceza hukuku kurallarını neredeyse kelimesi kelimesine tercüme ederek "Siber Suçlar Yasası" adıyla iç hukuklarına dahil etmişlerdir. Sözleşmeyi etkisizlikle itham eden bazı yazarlara göre Sözleşme'nin model bir yasa öngörüp, taraf devletlere bunu dayatması daha etkili bir olabilirdi[15].

3.2.Türk Ceza Hukukunun Sözleşme Karşısındaki Durumu

5237 sayılı Türk Ceza Kanunu'nda (**"TCK"**) "bilişim alanında suçlar" ve "*özel hayata ve hayatın gizli alanına karşı suçlar*" bölümlerinde bilişim sistemleriyle veya bunlara karşı işlenen, özellikle günümüzde söz konusu sistemler kullanılmadan işlenebilme olanakları çok kısıtlı olan hatta mümkün olmayan suçlar düzenlenmiştir. Bunların yanı sıra TCK'nın çeşitli bölümlerinde bilişim sistemleriyle işlenmesi olanaklı olan suç tiplerine de yer verilmiştir. Örneğin bilişim sistemleri aracılığıyla gerçekleştirilen dolandırıcılık ve hırsızlık suçları bunların en önemli örnekleridir[16].

Sözleşmede öngörülen suç tiplerinin ve Türk Ceza Mevzuatında yer alan muadillerinin teker teker açıklanması ve karşılaştırılması bu çalışmanın öngörülen hacminden çok daha fazlasını gerektirmektedir. Bu nedenle Sözleşme ve Türk ceza mevzuatının ilgili hükümlerinin okuyucu tarafından bilindiği varsayımıyla, Sözleşmede benimsenen suç kategorileri üzerinden genel bir karşılaştırma yapmak ve Türk mevzuatının eksik ya da yetersiz kaldığı noktaları belirtmekle yetineceğiz.

Birinci kategoriyi oluşturan bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçların Türk hukukundaki karşılığı TCK'nın 243 ve 244. maddeleridir[17]. Ancak bu maddeler Sözleşme düzenlemesiyle uyumluluk arz etmemekte, Türkiye'nin

FOOTNOTE DİPNOT

13 Havuz, "...Türkiye'nin Güvenliği", 145; Keyser, "The Council of Europe Convention on Cybercrime", 325.
14 Önok, "Avupa Siber Suçlar Sözleşmesi...", 1244.
15 Weber, "The Council of Europe's Convention on Cybercrime", 444; Önok, "Avupa Siber Suçlar Sözleşmesi...", 1245.
16 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 328.

fense narrower. The term "and" in the Article 243 needs to be changed with the term "or" in order to resolve this incompatibility[18].

The illegal interception, data interference, and system interference offenses in the first category are covered by the Article 244 of the TCK, which substantially complies with the requirements of the Convention. Given that, the Article 244 falls short of the requirements for lack of criminalization of action of the interception without right within the same scope with the Convention. Whereas the Convention criminalize all kinds of illegal interception to protected computer data, including electromagnetic emissions from a computer system carrying such computer data, the Article 244 criminalize only illegal interception by means of computer systems and thus; excludes actions by means of electromagnetic devices and technologies to be invented in the future. In order for Article 244 of TCK to be fully compatible with the Convention, it needs to be amended as criminalizing all kinds of illegal interception without any limitation.

In respect of the category of the offenses against the confidentiality, integrity and availability of computer data and

Sözleşmeye taraf olmakla üstlendiği yükümlülüğü birçok açıdan karşılamamaktadır.

Yasadışı erişim suçunun karşılığı olan TCK'nın 243. maddesi bilişim sistemlerine "*hukuka aykırı olarak girme ve orada kalmaya devam etme*" eylemini suç olarak düzenlemektedir. Oysa Sözleşme'de yalnızca "girme" eyleminin suçun oluşumu için yeterli olduğu görülmektedir. TCK'daki düzenleme suçu daha kısıtlı bir kapsamda tanımlaması itibariyle Sözleşme hükmüyle uyumlu değildir. Bu uyumsuzluğu gidermek için TCK'nın 243. Maddesi metninde yer alan "ve" ifadesi "veya" olarak değiştirilmelidir[18].

Birinci kategoride yer alan yasadışı müdahale, verilere müdahale, sistemlere müdahale suçlarının karşılığı TCK 244. madde hükmüdür ve Sözleşmeyle büyük ölçüde uyumludur. Ancak 244. madde "veri iletimine haksız surette dahil olma" eylemi bakımından eksik kalmaktadır. Sözleşme, verilere elektronik, elektromanyetik yollar dahil olmak üzere her türlü müdahaleyi suç saymakta iken TCK 244. madde hükmü, verilere yalnızca bilişim sistemi aracılığıyla yapılan müdahaleleri düzenlemiş ve bu surette elektromanyetik araçlarla veya ileride gelişti-

systems, the largest gap in Turkish criminal law is that there is no law criminalizing misuse of devices[19]. The offense of misuse of devices is provided in the article 6 of the Convention. In this article, production, sale, procurement for use, import, distribution or otherwise making available of devices, computer passwords, access codes, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offenses established in the Convention are counted as criminal offenses. As the Turkish criminal law adheres to the principle of non-criminalization of preparatory actions, any law provides a regulation as necessitated by the Convention. Whereas, an effective struggle against some specific offenses like those related to counterfeit bank and credit cards and massive circulation of epidemical malicious software might possible only if the perpetrators are caught in preparatory actions and charged. Indeed, many law enforcement officers and prosecutors struggling against cybercrimes in the field complain that the non-criminalization of preparatory actions of computer crimes stands as a significant obstacle in their fight against criminals and makes their efforts meaningless. This is why the Convention recognized an exception to the general principle of non-criminalization of preparatory actions in favor of cybercrimes. In order to provide a convenient infrastructure for the fight against cybercrime and to comply with the requirements of the Convention, TCK needs to be amended in parallel to the Article 6 of the Convention.

The analogous of the offenses of computer-related forgery and computer-related fraud established in the second category are the Article 244 on data interference, Article 158/1-f on fraud by means of computer systems and the articles from 204 to 212 on forgery of documents. Despite the fact that these articles cover the most of the related provisions of the Convention, the confinement of the electronic documents that can be subject to fraud by alteration, suppression or distortion of electronic data, to those signed with electronic signature remains as a defect. Although the current provisions of Turkish law are believed to be fully compatible with those imposed by the Conven-

rilecek başka yöntemlerle gerçekleştirilecek müdahaleleri kapsam dışında bırakmıştır. Türk mevzuatının sözleşmeyle uyumlu hale getirilmesi için TCK 244. madde metni bilişim verilerine yönelik her türlü araya girme eylemini suç sayacak şekilde değiştirilmelidir.

Bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar kategorisi anlamında Türk ceza mevzuatının en önemli eksikliği cihazların kötüye kullanımını suç sayan herhangi bir hükmün bulunmamasıdır[19]. Cihazların kötüye kullanımını Sözleşmenin 6. maddesinde düzenlemektedir. Söz konusu madde ile kanunda suç olarak düzenlenen eylemlerin işlenmesine yarayan cihazların, şifrelerin, erişim kodlarının üretilmesi, satılması, ithal edilmesi, dağıtımı, kullanım amaçlı tedariki veya başka şekilde erişilebilir hale getirilmesinin taraf devletlerin iç hukukunda suç olarak düzenlenmesi belirtilmiştir. Türk ceza hukukunda hazırlık hareketlerinin cezalandırılmaması ilkesi esas olduğu için bu yönde herhangi bir hüküm bulunmamaktadır. Özellikle kredi kartlarının kopyalanması, zararlı yazılımların kitlesel olarak yayılması gibi suç türleriyle etkin mücadele ancak hazırlık hareketleri aşamasında faillerin tespit edilip cezalandırılabilmelerinin mümkün olmasına bağlıdır. Uygulamada siber suçlarla mücadele eden pek çok polis ve savcı da, hazırlık hareketlerinin cezalandırılmamasının kendileri için önemli bir engel teşkil ettiğini ve siber suçlarla mücadeleyi anlamsız hale getirdiğini ifade etmektedir. Sözleşme siber suçlar bakımından bu özel durumu dikkate alarak, hazırlık hareketlerinin cezalandırılmaması kuralına siber suçlar bakımından istisna getirmiştir. Siber suçlarla etkin bir şekilde mücadele edilebilmesi ve Sözleşmeye uyumluluğun sağlanması adına TCK'ya Sözleşmenin 6. maddesine paralel bir hüküm getirilmelidir.

İkinci kategoride yer alan bilgisayar aracılığıyla işlenen sahtecilik suçları ve bilgisayarlar aracılığıyla işlenen dolandırıcılık suçlarının (sanal sahtecilik ve dolandırıcılık) Türk mevzuatındaki karşılığı TCK'nın verilere müdahaleye ilişkin 244. maddesi, bilişim sitemleri aracılığıyla gerçekleştirilen dolandırıcılığa ilişkin 158/1-f hükmü,

FOOTNOTE DİPNOT

17 Havuz, "...Türkiye'nin Güvenliği", 142.
18 Murat Volkan Dülger, "Avrupa Siber Suç Sözleşmesi ile Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nun Karşılaştırılması", 7.
19 Dülger, "Avrupa Siber Suç Sözleşmesi ile Türk Ceza Kanunu ve Ceza Muhakemesi Kanunu'nun Karşılaştırılması", 13.
20 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 188.
21 Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 660.

tion by some[20], in my opinion, an explicit and extensive amendment of related articles considering the statement and the intendment of the Convention would be more appropriate.

Offenses related to possession and distribution of child pornography, set out under the third category called content related offenses, are provided by the Article 226 of TCK on offenses related obscenity in Turkish criminal law. The article defines several types of obscenity as criminal offense and points out the sanctions. Although it is not specific to it, in practice the Article 226 is mostly used against offenses related to child pornography. However, the lack of specific regulations on child pornography in accordance with the Convention constitutes a deficiency of Turkish criminal law[21]. There is a need to mention that, sometimes the lack of specific regulation on child pornography causes problems on the diplomatic relations of Turkey. This third category is ostensibly supplemented by a new protocol adopted November 7th, 2002 making any dissemination of racist or xenophobic material through computer systems a criminal offense[22]. Turkey hasn't yet signed this protocol which entered into force on March 1st, 2006.

ve belgede sahteciliğe ilişkin 204 ila 212 maddeleridir. Bu maddeler sözleşmedeki düzenlemeleri büyük ölçüde karşılamakla birlikte, elektronik ortamda gerçekleştirilen verilerin değiştirilmesi, yok edilmesi veya tahrif edilmesi hareketlerinin, elektronik imzalı bir belge söz konusu olmadıkça belgede sahtecilik suçunun konusu oluşturamaması bir eksiklik olarak göze çarpmaktadır. Mevcut hükümlerin Sözleşmeyi karşıladığını savunan yazarlar olsa da[20], biz Sözleşme'nin ifadesini esas alan daha açık ve daha kapsamlı bir düzenlemenin daha isabetli olacağı kanaatindeyiz.

İçeriğe ilişkin suçlar olarak ifade edilen ve üçüncü kategoriyi oluşturan çocuk pornografisine ilişkin materyale sahip olmak ve uluslararası düzeyde dağıtımını sağlamak suçunun Türk ceza hukukundaki karşılığı TCK'nın 226. maddesinde düzenlenen müstehcenlik suçudur. Maddede her türlü müstehcenlik eylemi suç olarak tanımlanıp yaptırıma bağlanmıştır. Bu madde çocuk pornografisine özel olmamasına rağmen uygulamada en çok çocuk pornografisi suçlarında kullanılmaktadır. Bununla beraber çocuk pornografisinin özellikle Sözleşmenin ilgili maddeleri örnek alınarak ayrı bir suç tipi olarak düzenlenmeyişi TCK açısından önemli bir eksiklik oluşturmaktadır[21].

With regards to the last category of offense on infringements of copyright and related rights, the analogous provisions of the Law on Intellectual and Artistic Works provide the protection platform necessary to comply with the Convention.

4. PROCEDURAL PROVISIONS OF THE CONVENTION

4.1. In General

The criminal procedural provisions of the Convention are established in the Articles from 14 to 21. The articles and provided protective measures are as follows:

a. Article 16; expedited preservation of stored computer data,

b. Article 17; expedited preservation and partial disclosure of traffic data,

c. Article 18; production order,

d. Article 19; search and seizure of computer data,

e. Article 20; real-time collection of traffic data,

f. Article 21; interception of content data.

These measures provided by the Convention are actually various types of conventional search and seizure measure, developed in consideration of the nature of cybercrimes[23]. Because of the difficulties submitted by the speed and form of cybercrimes, the Convention regulates these specific procedural tools and requires the parties to create equivalent measures at national level[24]. It must be known that, it is not possible for these measures to be considered as general preventive powers, since they can only be applied within a determined investigation[25].

The subject of these protective measures can be all kinds of electronic data, including traffic data, content data and subscriber information, stored in a computer system or being transmitted from one to another[26]. The scope of these procedural measures is not limited to the offenses established by the Convention, nor cybercrimes; these measures, except those in the articles 20 and 21 can be applied for any crime involving electronic evidence[27].

Çocuk pornografisinin ayrı olarak düzenlenmeyişinin Türkiye'nin diplomatik ilişkilerinde de bir sorun olarak karşısına çıktığını belirtmek gerekir. Üçüncü suç kategori, sözleşemeye 2003 yılında eklenen ve her türlü ırkçı ve yabancı düşmanı içeriğin bilişim sistemleri aracılığıyla yayılmasının suç sayılmasını öngören Ek Protokol ile genişletilmiştir[22]. 1 Mart 2006'da yürürlüğe giren bu Protokol, Türkiye tarafından henüz imzalanmış değildir.

Son suç kategorisi olan fikri mülkiyet haklarının ihlali ve uluslararası düzeyde dağıtımı bakımından, Fikir ve Sanat Eserlerinin Korunması Hakkında Kanun'un hükümleri sözleşmeye uyumludur ve yeteri ölçüde bir koruma zemini sunmaktadır.

4. SÖZLEŞMENİN ÖNGÖRDÜĞÜ USUL HUKUKU KURALLARI

4.1. Genel Olarak

Avrupa Siber Suç Sözleşmesi'nde ceza muhakemesine ilişkin düzenlemeler 14 ila 21. maddeler arasında düzenlemektedir. Söz konusu maddeler ve içerdiği koruma tedbirleri şunlardır:

a. 16. madde; "depolanmış bilgisayar verilerinin hızlı bir biçimde korunması tedbiri",

b. 17. madde; "trafik verilerinin hızlı bir biçimde korunması ve kısmen açıklanması tedbiri",

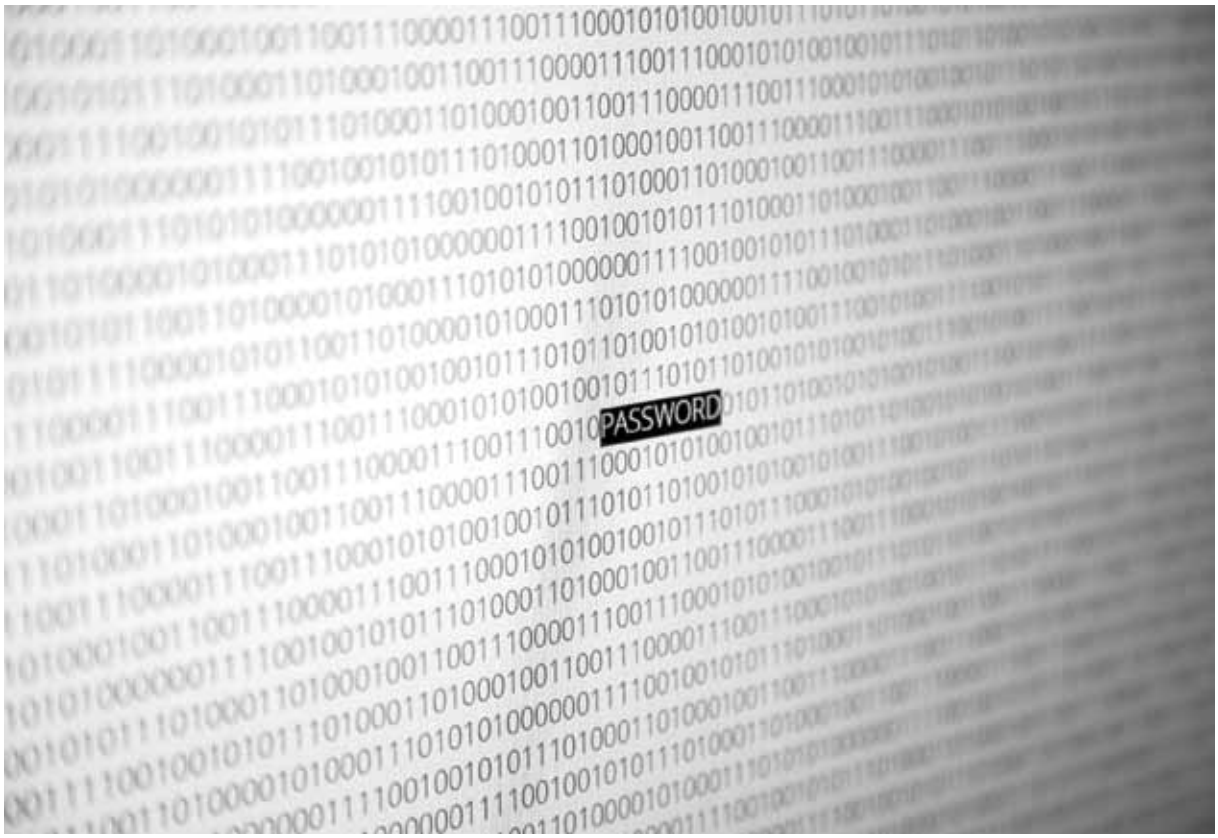
c. 18. madde; "üretim emri",

d. 19. madde; "depolanmış bilgisayar verilerinin aranması ve bunlara el konulması tedbiri",

e. 20 madde; "trafik verilerinin gerçek zamanlı toplanması tedbiri",

f. 21. madde; "içerik verilerinin yolunun kesilip ele geçirilmesi tedbiri".

Sözleşmede yer alan bu tedbirler klasik arama el koyma tedbirinin, siber suçların niteliği göz önüne alınarak geliştirilmiş birer çeşididir[23]. Ancak siber suçları takip etmenin hız ve ortam itibariyle arz ettiği zorluklar itibariyle bu tedbirler Sözleşme tarafından ayrıntılı olarak düzenlenmiş ve taraf devletlere bu hükümlerle uyumlu tedbirleri alma yükümlülüğü getirilmiştir[24]. Belirtilmelidir ki; bu tedbirlere genel bir izleme tedbiri şeklinde "*ön-*



4.2. Position of the Turkish Criminal Procedural Law Against the Convention

The unique specific procedural provision in the Turkish criminal procedural law is the Article 134, titled "*Search in computers, computer programs and logs, copying and seizure*", of the Turkish Criminal Procedure Code (**"CMK"**). Also the measures set out in articles from 135 to 138 of the section titled "*Surveillance of communications through telecommunication facilities*" of the CMK are often applied in investigations of cybercrimes. Considering the technical and complex disposition of cybercrimes and aforementioned difficulties of their prosecution, Turkish criminal procedural law can be evaluated as insufficient and sketchy.

In comparison with the provisions establishing procedural laws of the Convention, there is no equivalent of the Article 16 on expedited preservation of stored computer data and the Article 17 on expedited preservation and partial disclosure of traffic data in Turkish criminal procedural law. It would be beneficial to remind that the provisions of the Law numbered 5651 on the Regula-

leyici kolluk görevi" olarak başvurmak mümkün değildir, bu tedbirler ancak somut bir ceza soruşturmasının varlığı halinde uygulanabilecektir[25].

Sözleşmede düzenlenen koruma tedbirleri elektronik ortamda depolanmış, ya da halen iletişim sürecinde bulunan, trafik verileri, içerik verileri ve abone verilerini de içeren her türlü bilgisayar verisiyle ilgilidir[26]. Sözleşme, düzenlediği koruma tedbirlerin kapsamını sözleşmede yer alan suç tipleriyle hatta siber suçlarla sınırlı tutmamış, 20 ve 21. maddelerdeki tedbirler hariç olmak üzere herhangi bir suçun elektronik ortamda bulunan delillerinin toplanması amacıyla da bu tedbirlere başvurulabileceğini belirtmiştir[27].

4.2. Türk Ceza Muhakemesi Hukukunun Sözleşme Karşısındaki Durumu

Türk ceza muhakemesi hukukunda bilişim sistemlerine yönelik tek usuli düzenleme Ceza Muhakemesi Kanunu'nun (**"CMK"**) "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*" başlıklı 134. maddesidir. CMK'nın "*Telekomüni-*

tion of Publications on the Internet and Suppression of Crimes Committed by means of such publications, apparently similar to those in the Convention, are administrative measures; not criminal procedural, thus they cannot be applied in a determined criminal investigation. Therefore, these measures do not cover the measures provided by the Convention[28].

The analogous of the production order measure set in the Article 18 and the search and seizure of computer data set in the article 19 is the article 134 of the CMK in Turkish law. While the Article 134 of the CMK satisfies the requirements of the Convention thanks to its non-rigid disposition[29]; it seems insufficient and problematical with regard to the practice[30].

Whereas the real-time collection of traffic data measure of the Article 20 and the interception of content data measure of the Article 21 cannot be traced in the Turkish law as there are no exact equivalents of them; the article 135 of CMK on "interception of communications through telecommunication facilities" is applied instead. But the regulation provided in the Article 134 of CMK doesn't exactly cover the Articles 20 and 21 of the Convention. To explain the differences between them by simplifying and omitting technical details: The Article 135 of the Convention permits only surveillance of communications between real persons. In another word, there has to be a human communication process in form of dialog. However the measures established in the Articles 20 and 21 of the Convention, with good reason, include all types of data communication between computer systems.

As shown above, the provisions of the Turkish criminal procedural law on cybercrimes are far behind the standards determined and imposed by the Convention. The necessary amendments on the CMK need to be done urgently, in order to comply with the Convention and to perform an effective fight against cybercrimes.

kasyon Yoluyla Yapılan İletişimin Denetlenmesi" başlıklı Beşinci bölümünde 135 ila 138 maddelinde düzenlenen tedbirler de bilişim sistemleri bakımından sıkça uygulanmaktadır. Siber suçların yukarıda tekraren değindiğimiz karmaşık ve teknik yapısı ve bunlarla mücadelenin zorlukları göz önüne alındığında Türk ceza muhakemesi hukukunun bu konuda oldukça geri ve eksik olduğunu söylemek gerekir.

Sözleşmeyle karşılaştırıldığında; 16. maddede yer alan depolanmış bilgisayar verilerinin hızlı bir biçimde korunması ve 17. maddede yer alan trafik verilerinin hızlı bir biçimde korunması ve kısmen açıklanması tedbirlerinin Türk ceza muhakemesi hukukunda bir karşılığı olmadığı 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 Sözleşmede öngörülen tedbirleri karşılamadığını belirtmekte fayda vardır[28].

18. maddede düzenlenen üretim emri ve 19. maddede depolanmış bilgisayar verilerinin aranması ve bunlara el konulması tedbirlerinin Türk hukukundaki karşılığı CMK'nın 134. maddesidir. 134. madde, sözleşmenin esnek düzenlemesi sayesinde sözleşmenin ilgili hükümlerini gereğini yerine getirmekle birlikte[29]; bu madde uygulama bakımından son derece eksik ve sorunlu bulunmaktadır[30].

20. maddede düzenlenen trafik verilerinin gerçek zamanlı toplanması ve 21. Maddede düzenlenen içerik verilerinin yolunun kesilip ele geçirilmesi tedbirlerinin de Türk hukukunda doğrudan bir karşılığı olmayıp; telekomünikasyon yoluyla yapılan iletişimin denetlenmesine ilişkin CMK'nın 135. maddesi hükmüne başvurulmaktadır. 135. maddenin düzenlemesi Sözleşmenin 20 ve 21. maddelerindeki tedbirleri tam olarak karşılamamaktadır. Bunların arasındaki farkı teknik detaylara girmek-

FOOTNOTE DİPNOT

22 Weber, "The Council of Europe's Convention on Cybercrime", 431.
23 Serap Keskin, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* LIX(2001), 156.
24 Explanatory Report of the Comm. of Ministers [of the Conventio n on Cybercrime], 109th Sess. (adopted on Nov. 8 , 2001).
25 Keskin, "..Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", 157; Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*, 198.
26 Keskin, "..Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", 157; Keyser, "The Council of Europe's Convention on Cybercrime", 312.
27 Explanatory Report of the Comm. of Ministers [of the Convention on Cybercrime].
28 Cybercrime Legistlation Country Profiles, Council of Europe, (08.04.2015), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp.

5. ESSENTIALS OF THE JUDICIAL COOPERATION REGIME

The Third Chapter of The European Cybercrime Convention establishes the general principles of international cooperation and provides some specific mutual assistance provisions in order to accomplish one of its very first goals: fostering international judicial cooperation. The convention doesn't aim to substitute existing treaties on international cooperation; it sets forth a regime to be applied within the frame of the system sustained by existing treaties. In addition to this, it makes a significant contribution by determining rules to follow in the absence of applicable legal instruments among the parties[31].

The article 23 of the Convention outlines general principles of mutual legal assistance: First, international cooperation will be provided among states "to the widest extent possible". Second, the obligation to cooperate extends not only to the crimes established in the Convention, but also to the collection of electronic evidence whenever it relates to a criminal offense. Third, the international cooperation is to be performed in accordance

sizin basite indirgeyerek açıklayacak olursak: CMK 135 hükmü yalnızca kişiler arası iletişimin denetlenmesine olanak sağlamaktadır. Yani iki gerçek kişinin konuşma eylemini ifade eden bir diyalog süreci bulunmak mecburiyetindedir. Oysa Sözleşmenin 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 Sözleşmenin öngördüğü standartların çok gerisindedir. Sözleşmeye uyum sağlanması ve siber suçlarla etkin bir mücadelenin yürütülebilmesi için Ceza Muhakemesi Kanunu'nda bir an önce sözleşmeye paralel değişikliklerin yapılması gerekmektedir.

5. ADLİ YARDIMLAŞMA REJİMİNİN ESASLARI

Avrupa Siber Suçlar Sözleşmesi, birincil amacı olan etkin bir uluslararası adli yardımlaşmanın gerçekleşebilmesi adına üçüncü bölümde adli yardımlaşmaya ilişkin bir takım genel ilkeler ve özel usuller getirmektedir. Sözleşme, adli yardımlaşmaya dair mevcut diğer antlaşmaların yerini almayı amaçlamamaktadır. Hedefi, söz konusu diğer

with both the Convention and preexisting provisions of international agreements on these issues[32].

Besides the general principles, The Convention provides also specific provisions on mutual legal assistance in order to constitute an independently applicable cooperation system. These specific provisions mirror the procedural powers that states required to have at national level. These specific mutual assistance provisions include expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing stored computer data, real time collection of traffic data and interception of content data.

The article 35 of the Convention obligates parties to designate point of contacts that are available 24 hours a day 7 days a week. The 24/7 contact point of Turkey is the Department for Fighting Cybercrime, Directorate General of Security. On the other hand, codetermination of the Directorate General for International Law and Foreign Relations of the Ministry of Justice, the central authority on international legal assistance, is intended[33].

6. CONCLUSION

Cybercrimes are not confined within national borders. The performance of a common global policy in cooperation against cybercrimes is paramount for the struggles to be meaningful. Differing legal systems and disparities in the law often present major obstacles for a well-coordinated fight against cybercrimes. The European Cybercrime Convention is the first binding legal instrument, a first step to solve these problems. Despites its failings and imperfections, the Convention is the most important instrument in fight against cybercrime[34].

One of the primary objectives of the Convention is to harmonize national laws of the states. In this direction, the Convention puts the parties under obligation of making necessary regulations in parallel to those provided in the Convention. While Turkey has signed the Conven-

antlaşmalarla kurulu mevcut rejim kapsamında uygulanmaktır. Bununla birlikte, ilgili devletler arasında bir antlaşma hükmünün yokluğunda uygulanabilecek ilke ve kuralları da belirlemek suretiyle, önemli bir kazanım sağlamaktadır[31].
Sözleşmenin 23. maddesi adli yardımlaşmaya ilişkin genel ilkeleri saymaktadır. Buna göre, taraflar arasında adli yardımlaşma mümkün olan en geniş ölçekte sağlanacak, işbirliğinin bilişim sistemleriyle ilişkili tüm suçlar ve delilleri elektronik ortamda bulunan diğer suçları kapsayacak şekilde uygulanacak ve adli yardımlaşma hem yerel ve uluslararası belgeler uyarınca yürütülen mevcut rejime hem de Sözleşmenin öngördüğü usullere uygun olarak gerçekleştirilecektir[32].

Sözleşme, genel ilkelerin dışında etkin bir adli yardımlaşma sistemini tesis etmek amacıyla bazı özel yardımlaşma usulleri de getirmektedir. Bu özel hükümler, ulusal düzeyde alınması gereken usuli tedbirlerin uluslararası birer yansımasıdır. Bunlar saklanan/depolanmış bilgisayar verilerinin korunması, korunan trafik verilerinin açıklanması, saklanan bilgisayar verilerine ve bilgisayarda saklanan verilere sınır ötesinden erişime dair hızlandırılmış yardımlaşma usulleridir.

Sözleşmenin 35. maddesinde taraf devletlerden her birine 7 gün 24 saat hizmet verebilen irtibat noktalarının kurulması yükümlülüğü getirilmiştir. Türkiye için 7/24 irtibat noktası Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı'dır. Ancak 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 bulunmaktadır[33].

6. SONUÇ

Siber suçlar ulusal sınırlar içerisinde kalmamaktadır. Bunlarla mücadele edilebilmesi dünya çapında elbirliğiyle etkin bir mücadele yürütmesi halinde anlamlı olabilmektedir. Ülkelerin ulusal ceza ve ceza muhakemesi

FOOTNOTE DİPNOT

29 Keskin, "..Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", 156.
30 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 707-714.
31 Önok, "Avupa Siber Suçlar Sözleşmesi...", 1244.
32 International Cooperation under the Convention on Cybercrime, Project on Cybercrime, Council of Europe.
33 Önok, "Avupa Siber Suçlar Sözleşmesi...", 1262.
34 Weber, "The Council of Europe's Convention on Cybercrime", 446; Keyser, "The Council of Europe Convention on Cybercrime", 326; Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, 177.

tion and put it into force, amendments to several points both in substantial criminal law and criminal procedural law remain undone.

In order for Turkish Law to be in accord with the Convention in terms of both the criminal law and criminal procedural law, an extensive amendment proposal is being prepared by the Directorate General for Laws of the Ministry Justice with the intention of both being in compliance with the Convention and providing a convenient ground to combat cybercrimes by making necessary legal changes. ■

hukuku mevzuatlarının farklı olması iyi koordine edilmiş bir mücadeleye engel teşkil etmektedir. Bu sorunu aşmak adına adım atan ilk bağlayıcı uluslararası metin Avrupa Siber Suçlar Sözleşmesidir. Eksik ve yetersiz yönleri olmasına karşın Sözleşme siber suçlulukla mücadelenin en önemli enstrümanıdır[34].

Sözleşmenin en önemli amaçlarından birisi ilgili konularda ulusal mevzuatların uyumlulaştırılmasıdır. Bu doğrultuda taraf devletlere iç hukuklarında sözleşmede öngörülen maddi ve usuli ceza hukuku kurallarına paralel düzenlemeler yapma yükümlülüğü getirmiştir. Türkiye sözleşmeyi imzalayıp yürürlüğe koymuş olmakla birlikte gerek maddi ceza hukuku anlamında gerek muhakeme hukuku anlamında birçok noktada değişiklikler ve yeni düzenlemeler yapılması gerekmektedir.

Türk mevzuatının gerek maddi ceza hukuku gerek ceza muhakemesi hukuku anlamında Sözleşmeye uyumlu hale getirilmesi için halihazırda Adalet Bakanlığı Kanunlar Genel Müdürlüğü kapsamında kapsamlı bir yasa değişikliğine yönelik kanun tasarısı hazırlıkları sürdürülmekte ve en yakın zamanda ilgili yasa değişiklikleri yapılarak hem Sözleşme uyarınca üstlenilen sorumluluğun yerine getirilmesi hem de siber suçlarla etkin mücadele adına mevzuatın elverişli hale getirilmesi amaçlanmaktadır. ■

BIBLIOGRAPHY KAYNAKÇA

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

Crawford ,Henry E. "Internet Calling: FCC Jurisdiction over Internet Telephony". 5 COMM. L. CONSPECTUS 43, 43 (1997).

Cybercrime Legistlation Country Profiles, Council of Europe, (08.04.2015), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/CountryProfiles/default_en.asp.

Dhillon, Joginder S. & Smith, Robert I. "Defensive Information Operations and Domestic Law: Limitations on Governm ental Investigative Techniques". 50 A.F. L. REV. 135, 138 (2001).

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

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin, 2014.

Explanatory Report of the Comm. of Ministers [of the Conventio n on Cybercrime], 109th Sess. (adopted on Nov. 8 , 2001).

Havuz, Serdar. "Avrupa Siber Suçlar Sözleşmesi kapsamında Türkiye'nin Güvenliği". Yayımlanmamış Yüksek Lisans Tezi (2007).

International Cooperation under the Convention on Cybercrime, Project on Cybercrime, Council of Europe.

Internet Security Trends Report 2015, Symantec. (08.04.2015). http://www.symantec.com/en/uk/security_response/publica-tions/threatreport.jsp.

Keskin, Serap. "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi". *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası* LIX (2001).

Keyser, Mike. "The Council of Europe Convention on Cybercrime". *Journal of Transnatıonal Law & Policy* 12:2 (2002), 287-326.

Önok, Murat. "Avupa Siber Suçlar Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası Adli İşbirliği." *Marmara Üniversitesi Hukuk Fakültesi Hukuk Arşatırmaları Dergisi* 19/2 (Prof.Dr. Nur Centel'e Armağan) (2013), 1229-1269.

Taşkın, Ş. Cankat. "Bilişim Hukuku Uluslararası Uyuşmazlıklar". *Türkiye Barolar Birliği Dergisi* 85 (2009).

Weber, Amalie M. "The Council of Europe's Convention on Cybercrime". *Berkeley Technology Law Journal* 18/1 (2003).