PART 9

EVALUATION UNDER TURKISH CRIMINAL LAW OF CRIMES COMMITTED IN THE CYBER WORLD

SİBER DÜNYADA İŞLENEN SUÇLARIN TÜRK CEZA KANUNU KAPSAMINDA DEĞERLENDİRİLMESİ

--

GİZEM AR
İSMAİL ÇAĞLAR

ABSTRACT

Due to the increase in technological systems and access to technology, there is an increase in the rate of crime involving information systems. Moreover, because of the international reach of the internet, illegal actions in the field of information systems easily go beyond countries' borders. Given these developments, the current regulations of our legal system are insufficient for preventing violations committed in the field of informatics or carried out using computer devices. There is therefore a need to introduce national and international regulations. "Crimes in the field of informatics" regulated in the third part of the Turkish Penal Code numbered 5237 titled "Crimes Against Society" has been enacted in order to ensure effective defense against crimes in the field of informatics. In this article, cyber space crimes will be discussed within the scope of Turkish Penal Code No.5237 and other legislation.

KEYWORDS

INFORMATICS, CYBERCRIME, CRIMES ON INFORMATICS, INFORMATION SYSTEMS

ÖZET

Teknolojik sistemlerin ve teknolojiye ulaşılabilirliğin artması sebebiyle bilişim sistemlerine yönelik gerçekleşen suçlarda artış görülmektedir. Üstelik internetin kazandığı uluslararası kimlik sayesinde bilişim sistemleri alanında gerçekleşen hukuka aykırı eylemlerde ülke sınırları dışına taşabilmektedir. Bu kapsamda, bilişim alanında işlenen ya da bilgisayar vasıtaları kullanılarak gerçekleştirilen ihlalleri önlemek bakımından mevzuatımızdaki düzenlemeler yetersiz kaldığından ulusal ve uluslararası birtakım düzenlemeler yapılması ihtiyacı doğmuş ve bilişim alanındaki suçlarla etkin mücadelenin sağlanması için 5237 sayılı Türk Ceza Kanunu'nun "Topluma Karşı Suçlar" başlıklı üçüncü kısmı içerisinde düzenlenen "Bilişim Alanında Suçlar" yasalaşmıştır. Bu çalışmamızda 5237 sayılı Türk Ceza Kanunu ve sair mevzuat kapsamında siber alanda işlenen suçlar ele alınacaktır.

ANAHTAR KELİMELER

BİLİŞİM, SİBER SUÇ, BİLİŞİM SUÇLARI, BİLİŞİM SİSTEMLERİ

PART 9

The types of crimes committed in cyber space are considered computer and internet-specific crimes. It should be noted that the concept of cyber is a superior concept covering not only the internet but also other similar network systems.

Siber alanda işlenen suç türleri bilgisayara ve internete özgü suçlar olarak değerlendirilmektedir. Belirtmek gerekir ki, siber kavramı sadece interneti değil internet ve benzer diğer ağ (network) sistemlerini de kapsayan bir üst kavram olup; mevzuatımızda yer alan düzenlemeler gereği bu çalışmada "bilişim suçu" olarak anılacaktır.

I. INTRODUCTION

The types of crimes committed in cyber space are considered computer and internet-specific crimes. It should be noted that the concept of cyber is a superior concept covering not only the internet but also other similar network systems. In accordance with the regulations in Turkish statute law, this concept will be referred to as "crime on informatics". While it is possible to commit all crimes using information systems, the act of the crime referred to here is any unauthorized and illegal entry into an information system and actions occuring after it.[1] In other words, crimes committed through or against an information system for the purpose of violating personal rights and freedoms, illegally obtaining benefits and financial gains, and gaining interest in favor of organizations and individuals are defined as crimes on informatics together with other crimes related to data or data processing.[2]

While the acceleration of developments in information technologies and the internet has provided great convenience in all areas of life, it has also led to an increase in violations in the cyber world. For this reason, introducing regulations to prevent violations has become inevitable. The cyber world not only makes commiting such crimes easy given the facilities and opportunities it provides, but it also creates an environment where the criminals cannot be followed. It is essential that legislation keeps pace with these developments so that authorities can respond to the innovations that result with developments in information technologies and the internet.[3]

I. GİRİŞ

Siber alanda işlenen suç türleri bilgisayara ve internete özgü suçlar olarak değerlendirilmektedir. Belirtmek gerekir ki, siber kavramı sadece interneti değil internet ve benzer diğer ağ (network) sistemlerini de kapsayan bir üst kavram olup; mevzuatımızda yer alan düzenlemeler gereği bu çalışmada "bilişim suçu" olarak anılacaktır. Tüm suçların bilişim sistemleri kullanılarak işlenmesi mümkün olsa da suçun unsuru bulunan fiil, bilişim sistemine izinsiz olarak ve hukuka aykırı olacak şekilde girilmesi ve sonrasında yapılan eylemlerdir.[1] Diğer bir ifadeyle bilişim sistemleriyle veya bilişim sistemine karşı işlenen, kişisel hak ve hürriyetin ihlal edilmesine, illegal yollardan menfaat ve maddi kazanç elde edilmesine, kuruluş ve kişiler lehinde menfaat sağlanmasına yönelik yapılan, verilerle veya veri işleme ile konu bağlantısı olan suçlar bilişim suçları olarak tanımlanmaktadır.[2]

Bilişim teknolojileri ve internet dünyasındaki gelişmelerin hızlanması hayatın her alanında büyük kolaylıklar sağlarken, sanal alanda gerçekleşen ihlallerin de artmasına sebep olmuştur. Bu nedenle ihlalleri önlemeye yönelik hukuki düzenlemeler yapılması kaçınılmaz hale gelmiştir. Sanal ortam, yarattığı kolaylıklar ve fırsatlarla suç işlenmesini son derece kolaylaştırmanın yanı sıra suçlunun takibinin de yapılamadığı bir ortam oluşturmaktadır. Bilişim teknolojileri ve internetin gelişimi ile meydana gelen yeniliklere hukuk düzenince cevap verilebilmesi için mevzuatın da bu gelişmelere ayak uydurması elzem olmaktadır.[3]

II. HISTORICAL DEVELOPMENT

Informatics is defined by the Turkish Language Association as "The science of processing information, which is the basis of science, which is used by human beings in technical, economic and social fields, especially through electronic machines, informatic."[4] Although there is no common definition of cybercrimes, the most widely accepted definiton comes from the European Economic Community Experts Commission, May 1983, which states cybercrime is "information that is not legal, immoral or in a system that automatically processes information or transfers data, or any unauthorized conduct".[5]

The development of personal computers led to the use of information networks for cybercrimes. The first known cybercrime was committed in the United States of America.[6] This cime on informatics in-

II. TARİHSEL GELİŞİM

Bilişim, Türk Dil Kurumu uyarınca "(i)nsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik."[4] olarak tanımlanmış olup bilişim suçları konusunda herkesin ittifak ettiği bir tanım yoksa da en geniş kabul göreni Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda, "bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" şeklinde tanımlamıştır.[5]

Bilişim ağlarının kullanılmaya başlanmasını, kişisel bilgisayarların geliştirilmesi takip etmiş ve bilişim suçlarına vücut veren eylemler gündeme gelmeye başlamıştır. Bu alanda bilinen ilk bilişim suçu Amerika Birleşik Devletleri'nde gerçekleşmiştir.[6] ABD Minneapo-

FOOTNOTE

1 İç İşleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", https://www.egm.gov.tr/siber/siber-sucnedir (Access Date: 21.07.2020.)

2 İç İşleri Bakanlığı Jandarma Genel Komutanlığı, Suçla Mücadele; "Bilişim Suçu", https://www.jandarma.gov.tr/bilisim-suclari (Access Date: 21.07.2020.)

3 **Cahit Aliusta, Recep Benzer,** "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", International Security Information Engineering Journal, December 2018, Vol:4, No:2, p:35-42.

4 Turkish Language Society https://sozluk.gov.tr/ (Acces Date, 20.07.2020.)

5 **C. Özel,** (2002). Bilişim-İnternet Suçları. Access Date: 20.09.2011, http://www.hukukcu.com/bilimsel/kitaplar/bilişim_internet_suclari.htm 'dan aktaran; Ebru Altunok, Ali Fatih Vural, Bilişim Suçları, see also https://dergipark.org.tr/tr/download/article-file/208853 Access Date: 20.07.2020.

6 **Levent Kurt,** Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, İstanbul, September 2005, p.157.

DİPNOT

1 İç İşleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", https://www.egm.gov.tr/siber/siber-sucnedir (Erişim Tarihi, 21.07.2020.)

2 İç İşleri Bakanlığı Jandarma Genel Komutanlığı, Suçla Mücadele; "Bilişim Suçu", https://www.jandarma.gov.tr/bilisim-suclari (Erişim Tarihi, 21.07.2020.)

3 **Cahit Aliusta, Recep Benzer,** "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Aralık 2018, Cilt:4, No:2, S:35-42.

4 Türk Dil Kurumu, https://sozluk.gov.tr/ (Erişim Tarihi, 20.07.2020.)

5 **C. Özel,** (2002). Bilişim-İnternet Suçları. Er. Tar. 20.09.2011, http://www.hukukcu.com/bilimsel/kitaplar/bilişim_internet_suclari.htm 'dan aktaran; Ebru Altunok, Ali Fatih Vural, Bilişim Suçları, Erişim için bkz. https://dergipark.org.tr/tr/download/article-file/208853 Er. Tar. 20.07.2020.

6 **Levent Kurt,** Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, İstanbul, Eylül 2005, s.157.

PART 9

THE WORD "SIBER", EQUIVALENT TO "CYBER" IN ENGLISH, HAS MEANINGS PERTINENT TO COMPUTER NETWORKS AND THE INTERNET.

volved the falsification of bank accounts by a computer expert in Minneapolis City Bank, USA. Following this incident, discussions arose regarding the legal regulations involved and a new branch of American law was formed, "Computer Law".[7] The necessity of working on this field of criminal law emerged particularly following the development of the internet, through which the majority of cybercrimes are committed. With the increasingly intensive use of the internet from 1994 for illegal acts, important national and international regulations were introduced.

As cybercrimes are not restricted to national boundaries, the aim is to create uniform legal arrangements in order to effectively defend against these crimes worldwide.[8] One result of the works carried out in this context was the EU Convention on Cybercrime, which entered into force on November 23rd, 2001. Following the signing of this convention by Turkey on November 10th, 2010, Law numbered 6533 dated 22.04.2014 on Approval of Convention on Crimes Committing on a Virtual Platform entered into force, after being published in the Official Gazette dated 05.02.2014, number 28988. Thus, the European Convention on Cybercrime was integrated into Turkish domestic law.

Crimes on informatics were set out in detail in Turkish Penal Code ("TPC") number 5237, which was accepted and enacted on 26th September, 2004. Recognizing the need to continue such studies and to ensure an effective defense against cybercrime, in 2007, Law No. 5651 on the Regulation of Broadcasts on the Internet and Fight Against Crimes Committed Through These Broadcasts and a series of other regulations were brought into force.

III. CYBER CRIMES

Owing to the opportunities offered by information technology and the facilities enabling access to these opportunities all over the world, the intensive and effective use of virtual world tools has increased in both the public and private sector. In addition to the facilities it provides, this development has also led to changes in violations of the law as information systems have begun to be used to commit crimes more usually committe in the traditional way. In parallel with these technological developments, new types of crimes in the field of informatics have emerged.

The word "siber", equivalent to "cyber" in English, has meanings pertinent to computer networks and the internet. Cybercrime therefore, "refers to all crimes that target the security of an information system and the data contained in this system and subject to the illegal seizure of these data".[9] According to the European Commission's definition, "cybercrimes consist of criminal acts committed online using electronic communication networks and information systems."[10] However, since it is possible for every type of crime to be committed through information systems, every crime committed using information systems cannot be defined as a cybercrime and/or crime on informatics.

As there is a worldwide increase in illegal acts within the virtual world, or cyber space, it is necessary to define cybercrimes by legal order and to determine their status with reard to existing criminal law rules.[11]

A. How Cybercrimes Are Committed

Information systems refer to all kinds of computers and data systems, and, reflecting that, the methods of committing crimes in the cyber world differ. However, the most common methods are as follows:

Trojan Horse: These programs are named according to their features but they all serve the same purpose. The Trojan horse method threatens information security by allowing remote management of a system by tricking users into loading what seems a useful program onto their computer.[12]

Displacement: This is using an authorized or limited access authority password or access code or imitating its unique characteristics.[13]

İNGİLİZCEDE "CYBER" KELİMESİNİN KARŞILIĞI OLAN "SİBER" KELİMESİ, BİLGİSAYAR AĞLARINA AİT OLAN, İNTERNETE AİT OLAN, ANLAMLARI TAŞIMAKTADIR.

lis City Bank'da bilgisayar uzmanı tarafından banka hesaplarında tahrifat yapılması ile ilk kez gündeme geldiği bilinen bilişim suçları, bu olayın ardından hukuki düzenlemelerin de muhatabı olmaya başlamıştır. Bu kapsamda Amerikan Hukukunda "Computer Law" olarak yeni bir hukuk dalı oluşmuştur.[7] Özellikle internetin bulunması ve günümüz itibariyle bilişim suçlarının büyük çoğunluğunun internet vasıtasıyla işlenmesi sebebiyle ceza hukuku alanında bu konu üzerine çalışılmasını gerekli kılmıştır. 1994 yılı ve sonrasında internetin yoğun şekilde kullanılmasıyla hukuka aykırı eylemlerdeki artış sonucu ulusal ve uluslararası alanda ciddi düzenlemeler yapılmıştır.

Bilişim suçlarının ulusal sınırlar içerisinde kalmaması, bu suçlarla dünya çapında etkin şekilde mücadele edilmesini gerekli kıldığından hukuki düzenlemelerin yeknesaklaştırılması amaçlanmıştır.[8] Bu kapsamda yapılan çalışmaların neticesinde 23 Kasım 2001'de Avrupa Siber Suç Sözleşmesi yürürlüğe girmiştir. İlgili sözleşmenin Türkiye tarafından 10 Kasım 2010'da imzalanmasının ardından 22.04.2014'de 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, 02.05.2014 tarihli ve 28988 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Böylece Avrupa Siber Suç Sözleşmesi iç hukukumuza dahil olmuştur.

Bu doğrultuda, bilişim suçlarına detaylı olarak yer verilen 26.09.2004 tarihinde 5237 sayılı Türk Ceza Kanunu ("TCK") kabul edilerek yasalaşmıştır. Bununla sınırlı olmaksızın bu minvaldeki çalışmalar devam etmiş ve 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ve devamında bir dizi düzenleme yürürlüğe girerek siber suçlara ilişkin etkin bir mücadele sağlanması amaçlanmıştır.

III. SİBER SUÇLAR

Tüm dünya genelinde bilişim teknolojisinin sunduğu imkanlar ve bu imkanlara erişimdeki kolaylıklar sayesinde gerek kamusal alanda gerek özel sektörde sanal alemin yoğun ve etkin kullanımı artmıştır. Sağladığı kolaylıkların yanı sıra bu gelişim hukuka aykırılıklarda da birtakım değişiklikler yaratmış, klasik suç tiplerinin işlenme şekillerinde bilişim sistemleri kullanılmaya başlanmış, teknolojik gelişime paralel olarak doğrudan bilişim alanında gerçekleşen yeni suç tipleri ortaya çıkmıştır.

İngilizcede "cyber" kelimesinin karşılığı olan "Siber" kelimesi, bilgisayar ağlarına ait olan, internete ait olan, anlamları taşımaktadır. Bu bağlamda "siber suçlar, bir bilişim sisteminin güvenliğini ve bilişim sistemi içerisinde yer alan verileri hedef alan ve bu verilerin hukuka aykırı olarak ele geçirilmesini konu alan bütün suçları" ifade eder.[9] Avrupa Komisyonunun yaptığı tanıma göre ise, "siber suçlar elektronik iletişim ağları ve bilgi sistemleri kullanılarak çevrimiçi olarak işlenen suç işlemlerinden oluşur." [10] Ancak her suç tipinin bilişim sistemleri aracılığıyla işlenmesi mümkün olduğundan, bilişim sistemi kullanılarak işlenen her suç siber suç ve/veya bilişim suçu olarak değerlendirilemeyecektir.

İnternet ağlarının tüm dünyayı sarması siber alan olarak isimlendirilen sanal alemdeki hukuka aykırılıkların artmasına sebep olduğu için siber suçların hukuk düzeni tarafından tanımlanması ve ceza hukukunda mevcut kurallar karşısındaki konumlarının belirlenmesini gerekli kılmıştır.[11]

A. Siber Suçların İşleniş Şekilleri

Her türlü bilgisayar ve veri sistemini ifade eden bilişim sistemlerindeki gelişime paralel olarak siber dünyada işlenen suçların işleniş şekilleri de birlikte farklılık arz etmektedir. Ancak en bilinen yöntemler aşağıdaki şekildedir:

Truva Atı: bu programlar özelliklerine göre değişik isimlerle adlandırılsa da hepsi aynı amaca hizmet etmektedir. Truva atı yöntemi, yararlı gibi görünen bilgisayar programlarının arkasında yer alan gizli kod ile sistemi ele geçirerek uzaktan yönetim sağlayarak bilişim güvenliğini tehdit etmektedir.[12]

Yerine Geçme; yetkili veya sınırlı erişim yetkisi olan kişinin, parola veya erişim kodunun yazılması veya ona özgü niteliklerin taklit edilmesidir. [13]

FOOTNOTE

7 Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınları, Ankara, September 2015, p.114.

8 Cahit Aliusta, Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, December 2018, Vol:4, No:2, p.35-42.

9 İç İşleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", https://www.egm.gov.tr/siber/siber-sucnedir (Access Date: 21.07.2020.)

10 Süleyman Yılmaz / Gökçe Filiz Çavuşoğlu, Kişisel Verileri Koruma Hukuku, Yetkin Basımevi, Ankara, 2020, p.147.

11 Oğuz Turhan, "Bilgisayar Ağları ile İlgili Suçlar", Başbakanlık Devlet PlanlamaTeşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara, April 2006, p. 32.

12 Ibid., pg. 56.

13 Levent Kurt, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması Seçkin Yayınları, İstanbul, 2005, p. 60-77.

DİPNOT

7 Murat Volkan Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınları, Ankara, Eylül 2015, s.114.

8 Cahit Aliusta, Recep Benzer, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Aralık 2018, Cilt:4, No:2, s.35-42.

9 İç İşleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", https://www.egm.gov.tr/siber/siber-sucnedir (Erişim Tarihi, 21.07.2020.)

10 Süleyman Yılmaz / Gökçe Filiz Çavuşoğlu, Kişisel Verileri Koruma Hukuku, Yetkin Basımevi, Ankara, 2020, s.147.

11 Oğuz Turhan, "Bilgisayar Ağları ile İlgili Suçlar", Başbakanlık Devlet PlanlamaTeşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara, Nisan 2006, s. 32.

12 Ibid., s. 56.

13 Levent Kurt, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması Seçkin Yayınları, İstanbul, 2005, s. 60-77.

PART 9

Network Worms: These are programs that can run themselves, without the need for user intervention. They enter the system by bypassing the firewall (for example, where easy passwords are used) and accessing the information network.

Unwanted Electronic Messages: Spam, technically, is the sending of large numbers of copies of the same compelling message over the internet to people who have not requested the message.

Other methods include trash, eavesdropping, data spoofing, scanning, super hit, salami technique, secret doors, asynchronous attacks, software bombs, wolves, bug ware computer viruses, piggyback, logic bombs, credit card frauds, rabbits, chameleons, fake messages, etc.

IV. CRIMES ON INFORMATICS UNDER TURKISH CRIMINAL LAW NO 5237

Crimes on informatics within the scope of the TPC (Turkish Penal Code) are regulated in the section titled "Crimes in the Field of Information". The crimes set out in this section are crimes that can be committed with information systems, for example theft and fraud. However, it should be noted that this distinction is not always clear as new forms of crime emerge as technology develops.

It is possible to evaluate cybercrimes under the TPC in two separate categories. Crimes on Informatics includes Access to data processing system (TPC Art. 243); Hindrance or destruction of the system, deletion or alteration of data (TPC Art. 244); Improper use of bank or credit cards (TPC Art. 245); and illegal devices or programs (Art.245/A). The second category is Crimes that Can Be Committed through Informatics. These crimes are Defamation (TPC Art.125); Violation of communicational secrecy (TPC Art. 132); Tapping and recording conversations between individuals (TPC Art.133); Violation of privacy (TPC Art.134); Recording of personal data (TPC Art.135); Unlawful delivery or acquisition of data (TPC Art.136); Theft (TPC Art. 142/2-e); and Qualified form of fraud (TPC Art. 158/1-f). The following sections of this article will discuss crimes regulated under "Crimes in the Field of Informatics" in the TPC.

A. Access to data processing systems

Article 243 of the TPC regulates that:
(1) Any person who unlawfully enters a part or whole of data processing system or remains there is punished with imprisonment up to one year, or imposed punitive fine. (2) In cases where the offenses defined in the above subsection involve systems that are benefited against charge, the punishment to be imposed is increased up to one half. (3) If such act results with deletion or alteration of data within the content of the system, the person responsible for such failure is sentenced to imprisonment from six months up to two years.[14]

In the preamble of the TPC Article in question, an information system is defined as a magnetic system that allows data to be automatically processed after collecting and placing it. With this regulation, the legislator has protected the security of information systems and criminalizes illegally entering the whole or part of an information system. Regardless of whether a person entered the system illegally to obtain certain data, a crime naturally occurs if the system is entered unfairly and deliberately.[15]

Ağ Solucanları; kullanıcı müdahalesi gerekmeden, kendi kendini çalıştırabilen, bilişim ağında ulaştıkları sistemin güvenlik duvarıyla karşılaştıklarında iyi oluşturulmamış güvenlik duvarını (kolay şifreler gibi) aşarak sisteme giren programlardır.

İstem Dışı Alınan Elektronik İletiler; Spam teknik olarak, internet üzerinde aynı mesajın çok sayıdaki kopyasının, bu mesajı alma talebinde bulunmayan kişilere zorlayıcı olarak gönderilmesidir.

Diğer Yöntemler ise, çöpe dalma, gizlice dinleme, veri aldatmacası, tarama, süper darbe, salam tekniği, gizli kapılar, eş zamansız saldırılar, yazılım bombaları, kurtlar, bug ware bilgisayar virüsleri, sırtlama, mantık bombaları, kredi kartı sahtekârlıkları, tavşanlar, bukalemun, sahte iletiler vb. olarak özetlenebilir.

IV. 5237 SAYILI TÜRK CEZA KANUNU KAPSAMINDA BİLİŞİM SUÇLARI

TCK kapsamında bilişim suçları, "Bilişim Alanında Suçlar" bölümünde düzenlenmiştir. Bu bölümlerde düzenlenen suçlar bilişim sistemiyle işlenebilen suçlardır. Bunların yanı sıra TCK'da düzenlenen bazı suç tiplerinin bilişim sistemleri aracılığıyla işlenebilmesi de mümkündür. Hırsızlık ve dolandırıcılık suçları bilişim sistemleri kullanılarak işlenebilecek suç tiplerine örnek verilebilecektir. Ancak belirtmek gerekir ki, gelişen teknoloji sebebiyle yeni suç işleniş şekillerinin ortaya çıkması söz konusu olduğundan bu ayrım net bir ayrım değildir.

TCK kapsamındaki bilişim suçlarını iki ayrı kategoride değerlendirmek mümkündür. Bilişim Alanında İşlenen Suçlar; bilişim sistemine girme (TCK m.243), sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK m.244), banka veya kredi kartlarının kötüye kullanılması (TCK m. 245), yasak cihaz veya programlar (m.245/A). Bunun dışında ikinci kategori ise bilişim Yoluyla İşlenebilen Suçlardır. Bunlar ise, hakaret (TCK m.125), haberleşmenin gizliliğini ihlal (TCK m. 132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (TCK m.133), özel hayatın gizliliğini ihlal (TCK m.134), kişisel verilerin kaydedilmesi (TCK m.135), verileri hukuka aykırı olarak verme veya ele geçirme (TCK m.136), hırsızlık (TCK m. 142/2-e), dolandırıcılık (TCK m. 158/1-f) olarak belirtilebilir. Bu aşamada çalışmamızın devamında TCK'da "Bilişim Alanında Suçlar" başlığı altında düzenlenen suçlar ele alınacaktır.

A. Bilişim Sistemine Girme Suçu

TCK Madde 243'te düzenlenmiş olup, buna göre;
"(1) Bir veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir. (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."[14]

Söz konusu kanunda yer verilen madde gerekçesinde bilişim sistemi, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma imkânı veren manyetik sistemler olarak tanımlanmış olup kanun koyucu bu düzenleme ile bilişim sisteminin güvenliğini koruma altına almış ve bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalmaya devam etme eylemine suç vasfı kazandırmıştır. Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi bulunmamaktadır. Sisteme, doğal olarak, haksız ve kasten girilmiş olması ile suç gerçekleşecektir.[15]

it is not clear whether the principle of consumer protection will be applied in all cases where the buyer is a consumer.

Bununla beraber alıcının tüketici olduğu her durumda tüketicinin korunması ilkesinin uygulanıp uygulanmayacağı da anlaşılamamaktadır.

FOOTNOTE

14 TPC art. 243.

15 TPC art. 243, Preamble.

DİPNOT

14 TCK m. 243.

15 TCK m. 243, Gerekçe.

PART 9

A Court of Appeal decision on this topic states: "Entering the complainant company's system is recognized as a crime under Article 244/1-3 of the TPC, which states to delete, alter, corrupt or bar access to data, prevent the functioning of a data processing system or render such useless, to introduce data into a system or send existing data to another place can not be executed and the act of entering the complainant company's system illegally and continuing to remian there should be accepted as a crime regulated in Article 243/1."[16]

The main factor in the crime of entering an informatics system illegally is "unlawfulness". The victim's permission to enter the system with his/her consent or sharing security information will change the criminal characteristic of the action.

B. Preventing the Functioning of a System and Deleting, Altering, or Corrupting Data

According to this crime regulated in Article 244 of the TPC:

Any person who prevents the functioning of a data processing system or renders such useless shall be subject to a penalty of imprisonment for a term of one to five years. (2) Any person who deletes, alters, corrupts, or bars access to data, or introduces data into a system or sends existing data to another place shall be subject to a penalty of imprisonment for a term of six months to three years. (3) Where this offence is committed in relation to a data processing system of a public institution or establishment, bank or institution of credit, then the penalty to be imposed shall be increased by one half. (4) Where a person obtains an unjust benefit for himself or another by committing the acts defined in the aforementioned paragraphs, and such acts do not constitute a separate offence, he shall be subject to a penalty of imprisonment from two years to six years and a judicial fine of up to five thousand days.[17]

This regulation turns acts that damage systems into a special crime. The subject of the crime is the physical existence of the vehicle and all other elements that ensure its functioning.[18] A crime occurs upon one of the optional actions in the legal definition taking place.

The crime of destroying or altering data in an information system takes place when data that the system user has recorded on the system is destroyed or changed. The crime of preventing the functioning of an information system occurs when a user is prevented from entering the relevant information system. The crime of corrupting an information system occurs when the operation of an information system is disrupted or it is ensured that the expected benefit from the system cannot be obtained.

In this decision, the Court of Appeal considered that blocking a user's access to their Facebook account by obtaining the user's password falls within the scope of this crime.[19] In another decision, it was ruled that the defendant, who illegally entered the complainant's e-mail account and blocked the complainant's access to it by creating a new password and then used the e-mail address, should be punished for the crime of "Preventing the Functioning of a System and Deleting, Alterating, or Corrupting Data".[20]

In another case, a complainant filed a lawsuit alleging that someone had blocked access to his Facebook account by accessing the account and changing his password. However, the complainant stated that he had then changed his password by answering the security question upon Facebook's notification and, as a result of the complainant's intervention, the other person could not log

FOOTNOTE

16 Penal Department no.8 of the Court of Appeal, T. 24.6.2014, E. 2013/1777, K. 2014/16144.

17 TPC art. 244.

18 TPC art. 244, Preamble.

19 Penal Department no.8 of the Court of Appeal, D. 1.11.2013, E. 2012/33557, K. 2013/25987.

20 Penal Department no.8 of the Court of Appeal, D. 23.6.2014, E. 2013/771, K. 2014/15833.

Yargıtay bir kararında; "Şikayetçi şirketin sistemine hukuka aykırı olarak girerek sistemin işleyişini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme şeklindeki TCK'nın 244/1-3.madde ve fıkralarında yazılı hallerin gerçekleşmemesi nedeniyle, anılan maddenin 4.fıkrasının uygulanamayacağı, şikayetçi şirkete ait sisteme hukuka aykırı olarak girme ve orada kalmaya devam etme şeklindeki eylemin TCK'nın 243/1. madde ve fıkrasında düzenlenen suçu oluşturacağının gözetilmesi" gerektiğine karar vermiştir.[16]

Bilişim sistemine hukuka aykırı girme suçunun oluşumu için temel etken "hukuka aykırılık" olup, mağdurun rızası ile sisteme giriş izni vermesi veya güvenlik bilgilerini paylaşması söz konusu eylemi suç vasfından çıkaracaktır.

B. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu

TCK madde 244'de düzenlenen bu suça göre;

"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur." şeklinde düzenlenmiştir.[17]

Bu düzenleme ile sistemlere yönelik zarar fiilleri özel bir suç haline getirilmiştir. Suçun konusunu aracın fiziki varlığı ve işlemesini sağlayan bütün diğer unsurlar oluşturmaktadır.[18] Kanuni tanımdaki seçimlik hareketlerden birinin gerçekleşmesi ile suç oluşmaktadır.

Bilişim sistemindeki verileri yok etme veya değiştirme suçu; sistem kullanıcısı kişinin sistem üzerinde kaydettiği verileri yok etme veya verilerin değiştirilmesi ile gerçekleşmektedir. Bilişim sisteminin işleyişini engelleme suçu; kişinin ilgili bilişim sistemine girmesinin engellenmesiyle gerçekleşir. Bilişim sistemini bozma suçu; bilişim sisteminin işleyişini bozma veya sistemden beklenen faydanın sağlanamamasını sağlama eylemleri ile oluşacaktır.

Yargıtay ilgili kararında facebook kullanıcısının şifresini ele geçirerek kullanıcının kendi hesabına erişimini engellemesini bu suç kapsamında değerlendirmiştir.[19] Bir başka kararında ise; şikayetçiye ait mail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın TCK md.244/2 uyarınca "bilişim sistemini engelleme, erişilmez kılma, bozma, verileri yok etme veya değiştirme" suçundan cezalandırılması gerektiğine hükmetmiştir.[20]

Diğer bir olayda ise şikayetçinin facebook hesabına erişim sağlanıp şifresinin değiştirilmesi suretiyle hesaba erişiminin engellendiği iddiasıyla dava açılmıştır. Ancak şikayetçinin facebookun bildirimi üzerine güvenlik sorusunu cevaplayarak kendi şifresini değiştirdiğini beyan etmesi ve şikayetçinin müdahalesi sonucu diğer kişinin sisteme girişinin sonuçlanamaması nedeniyle bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme eylemlerinin gerçekleşmediğinin anlaşılması sonucunda, sanığın eyleminin

DİPNOT

16 Yargıtay 8. Ceza Dairesi, T. 24.6.2014, E. 2013/1777, K. 2014/16144.

17 TCK m. 244.

18 TCK m. 244, Gerekçe.

19 Yargıtay 8. Ceza Dairesi, T. 1.11.2013, E. 2012/33557, K. 2013/25987.

20 Yargıtay 8. Ceza Dairesi, T. 23.6.2014, E. 2013/771, K. 2014/15833.

PART 9

into the system and the actions of destroying, changing, or rendering the data in the information system inaccessible, inserting data into the system, and sending the existing data elsewhere did not ocur and it was consequently accepted that whether or not the defendant's action constituted the crime of attempting to enter the information system should be discussed at this point.[21]

C. Misuse of Bank or Credit cards

According to this crime regulated in Article 245 of the TPC:

Any person who secures a benefit for himself, or another, by acquiring or retaining (by any means), the bank or credit card of another person; or using, or allowing to be used, such a card without the consent of the card holder or the residual owner shall be sentenced to a penalty of imprisonment for a term of three to six years and a judicial fine of up to five thousand days. (2) Any person who produces, sells, transfers, purchases or receives a counterfeit bank or credit card which relates to the bank account of another shall be sentenced to a penalty of imprisonment for a term of three to seven years and judicial fine of up to ten thousand days. (3) Any person who secures a benefit for himself or another by using a counterfeit or falsified bank or credit card shall be sentenced to a penalty of imprisonment for a term of four to eight years and a judicial fine of up to five thousand days, provided such act does not constitute a separate offence. (4) Where an offence described in paragraph one concerns a loss to: a) a spouse of a marriage where such spouse has not been subject to a court decree of separation, b) a direct-antecedent or direct-descendent, direct in-law, adoptive parent or adopted child; or c) a sibling residing in the same dwelling. no penalty shall be imposed on the person who is related in such a way.[22]

The crime of Misuse of Bank or Credit cards can be committed in three different ways: misuse of real bank or credit cards belonging to another person (TPC Art .245/1), production, sale, transfer, purchase, or receiving a counterfeit bank or credit card (TPC Art .245/2), securing benefit for him or herself or another by using a counterfeit or falsified bank or credit card (TPC Art. 245/3).

In the crime of misuse of a real bank or credit card belonging to someone else, the main point is of providing benefit to him or herself or someone else by using or making usable a bank or credit card without the owner's consent. Since the definition of the criminal is regulated as "the person who seized or possessed the card in any way whatsoever" even if the card is stolen, found, or seized with the permission of the card holder, the crime will be committed provided that the card is used without permission and an unlawful benefit is obtained as a result of the action.[23]

In the act of producing, selling, transferring, buying, or accepting a counterfeit debit or credit card, the debit or credit card must be counterfeited and there must be an interest between an existing real account. Within the scope of this act, if there is no account with which the card is linked, it will not constitute the occurrence of a crime. Because the legislator does not seek any conditions to the benefit from the committing of this crime, it is regulated that the formation of the crime would be completed with the realization of one of the optional actions.

FOOTNOTE

21 Penal Department no.8 of the Court of Appeal E. 2016/11922 K. 2017/6655 T. 7.6.2017

22 TPC art. 245.

23 Ali Parlar, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2015.

bilişim sistemine girmeye teşebbüs suçunu oluşturup oluşturmayacağının tartışılması gerektiğini kabul etmiştir.[21]

C. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu

TCK m. 245'te düzenlenen bu suça göre;

"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır. (3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. (4) Birinci fıkrada yer alan suçun;a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz. Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."[22]

Banka veya kredi kartlarının kötüye kullanılması suçu; başkasına ait gerçek bir banka veya kredi kartının kötüye kullanılması (TCK md.245/1), sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek (TCK md.245/2), sahte bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak (TCK md.245/3) şeklinde üç farklı şekilde işlenmesi mümkündür.

Başkasına ait gerçek bir banka veya kredi kartının kötüye kullanılması suçunda asıl olan, kişinin, banka veya kredi kartının sahibinin rızası hilafına kullanılması veya kullandırtılmasıyla kendisine veya başkasına yarar sağlamasıdır. Suç tanımında her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse denildiğinden, kartın çalıntı, buluntu ya da kart sahibinin izni ile ele geçirilmesi söz konusu olsa bile izni olmadan kullanılması ve eylemlerin sonucunda hukuka aykırı yarar sağlanması ile suç gerçekleşecektir.[23]

Sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek eyleminde, banka veya kredi kartının sahte olarak üretilmeli ve var olan gerçek bir hesap arasında ilgi bulunmalıdır. İşbu fiil kapsamında kartın bağlantılı olduğu bir hesap olmaması durumunda suçun oluşmasından söz edilemeyecektir. Zira kanun koyucu bu suçun oluşumu için yarar sağlama koşulu aramamış, seçimlik hareketlerden birinin gerçekleşmesi ile suçun oluşumunun tamamlanacağını düzenlemiştir.

DİPNOT

21 Yargıtay 8. Ceza Dairesi E. 2016/11922 K. 2017/6655 T. 7.6.2017

22 TCK m. 245.

23 Ali Parlar, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2015.

PART 9

In the crime of benefiting him or herself or someone else by using a fake bank or credit card, the use of only a fake bank or credit card is not sufficient for the occurrence of a crime, and, as a result, the perpetrator must benefit him or herself or someone else. In cases where the targeted benefit cannot be achieved, it can be easily stated that this crime, which is a crime of damage, remains at the stage of attempt. However, in order for the crime regulated within the scope of this paragraph to be punished, the action must not be another crime that requires a heavier penalty.

V. CONCLUSION

In the 21st century, the development rate of technology has increased exponentially resulting in a noticeable change in information systems. As a result of ongoing developments, the concept of cybercrime, which is defined as the types of crimes targeting information systems and data in these systems, has emerged. However, the diversification in using these systems contrary to their allocated purposes has led to the commitment of many types of cybercrime with different characteristics. As a result, many countries have focused on their own international regulations as well as their own domestic legal regulations. The legislator, too, is not indifferent to the changes the current age has brought and has created various types of crimes with cybercrime characteristics.

Additionally, there are some crimes regulated in the Crimes on Informatics section of the Turkish Penal Code as Access to a data processing system, hindrance or destruction of the system, deletion or alteration of data, improper use of bank or credit cards, and some other crimes have been deemed not as Crimes on Informatics but as having cybercrime characteristics as defamation, violation of communicational secrecy, tapping and recording of conversations between individuals, violation of privacy, recording of personal data, unlawful delivery or acquisition of data, theft, and qualified form of fraud in different articles.

Analysis of Turkish legislation shows regulation of different crimes. However, depending on the development of technology, it should be noted that continuity should be ensured in making additional legislation due to legal systems protecting themselves by preserving their dynamism at every point and are unable to remain independent from the developments of the era. The things to be done regarding cybercrime can be stated as making legislation in line with 21st century developments, ensuring more efficient execution of criminal proceedings, providing the technological infrastructure, and raising awareness of information system users.

Sahte bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçunda, sadece sahte banka veya kredi kartının kullanılması suçun oluşumu için yeterli olmayıp neticesinde failin kendisine veya başkasına fayda sağlaması gerekmektedir. Hedeflenen yararın sağlanamadığı bir dünyada zarar suçu olan bu suçun teşebbüs aşamasında kaldığı rahatlıkla söylenebilecektir. Ancak bu fıkra kapsamında düzenlenen suçun cezalandırılabilmesi için fiilin daha ağır bir cezayı gerektiren başka bir suça vücut vermemesi gerekmektedir.

V. SONUÇ

21. yüzyılla gelişim hızı katlanarak artan teknolojiyle birlikte bilişim sistemlerinde de gözle görülür seviyede değişim yaşanmıştır. Süregelen gelişmelerin bir sonucu olarak ise bilişim sistemlerini ve bu sistemlerdeki verileri hedef alan suç tipleri şeklinde tanımlanan siber suç kavramı hayatımıza girmiştir. Ancak söz konusu sistemlerin tahsis amaçlarına aykırı kullanımı noktasında meydana gelen çeşitlenme, farklı özellikler gösteren çok sayıda siber suç tipinin işlenmesine neden olmuştur. Bunun sonucunda, birçok ülke kendi iç hukuk düzenlemeleri yanında uluslararası regülasyon çalışmalarına yoğunlaşmıştır. Kanun koyucu ise çağın getirdiklerine kayıtsız kalmamış ve siber suç özelliği taşıyan çeşitli suç tipleri ihdas etmiştir.

Başta Türk Ceza Kanunu'nda Bilişim Alanında İşlenen Suçlar başlığı altında bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka veya kredi kartlarının kötüye kullanılması suçlarının düzenlenmesinin yanı sıra "Bilişim Alanında İşlenen Suçlar" başlığı altında yer almamakla birlikte yine siber suç niteliği gösteren suçlar olarak hakaret, haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal, kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme, hırsızlık, dolandırıcılık suçları farklı maddelerde kendisine yer bulmuştur.

Mevzuatımıza bakıldığında farklı suçların düzenlendiği; ancak teknolojinin gelişimine bağlı olarak ek düzenlemelerin hali hazırda yapılmasında sürekliliğin sağlanması gerektiği belirtilmelidir. Zira hukuk sistemleri her çağda dinamizmini koruyarak kendilerini muhafaza etmiş ve bulundukları çağın gelişmelerinden bağımsız kalamamışlardır. Siber suçlarla ilgili olarak yapılması gerekenler ise 21. Yüzyılın getirilerine paralel olacak şekilde düzenlemelerin yapılması, suç takiplerinin daha etkin yürütülmesi için teknolojik alt yapının sağlanması ve bilişim sistemi kullanıcılarının bilinçlendirilmesi şeklinde belirtilebilir.

BIBLIOGRAPHY

İç İşleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", https://www.egm.gov.tr/siber/sibersucnedir (Access Date: 21.07.2020.)

CAHİT ALİUSTA, RECEP BENZER, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Vol:4, No:2, December 2018.

Türk Dil Kurumu, https://sozluk.gov.tr/ (Access Date: 20.07.2020.)

C. ÖZEL, (2002). Bilişim-İnternet Suçları. Access Date: 20.09.2011, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm 'dan nakleı; Ebru Altunok, Ali Fatih Vural, Bilişim Suçları, See also. https://dergipark.org.tr/tr/download/article-file/208853 Er. Access Date: 20.07.2020.

LEVENT KURT, Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, İstanbul, September 2005.

MURAT VOLKAN DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınları, Ankara, September 2015.

SÜLEYMAN YILMAZ & GÖKÇE FİLİZ ÇAVUŞOĞLU, Kişisel Verileri Koruma Hukuku, Yetkin Basımevi, Ankara, 2020.

OĞUZ TURHAN, "Bilgisayar Ağları ile İlgili Suçlar", Başbakanlık Devlet PlanlamaTeşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara, April 2006.

LEVENT KURT, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, İstanbul, 2005.

KAYNAKÇA

İç İşleri Bakanlığı, Emniyet Genel Müdürlüğü, Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", https://www.egm.gov.tr/siber/sibersucnedir (Erişim Tarihi, 21.07.2020.)

CAHİT ALİUSTA, RECEP BENZER, "Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin Dahil Olma Süreci", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Vol:4, No:2, Aralık 2018.

Türk Dil Kurumu, https://sozluk.gov.tr/ (Erişim Tarihi, 20.07.2020.)

C. ÖZEL, (2002). Bilişim-İnternet Suçları. Er. Tar. 20.09.2011, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm 'dan nakleı; Ebru Altunok, Ali Fatih Vural, Bilişim Suçları, Erişim için bkz. https://dergipark.org.tr/tr/download/article-file/208853 Er. Tar. 20.07.2020.

LEVENT KURT, Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, İstanbul, Eylül 2005.

MURAT VOLKAN DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yayınları, Ankara, Eylül 2015.

SÜLEYMAN YILMAZ / GÖKÇE FİLİZ ÇAVUŞOĞLU, Kişisel Verileri Koruma Hukuku, Yetkin Basımevi, Ankara, 2020.

OĞUZ TURHAN, "Bilgisayar Ağları ile İlgili Suçlar", Başbakanlık Devlet PlanlamaTeşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara, April 2006.

LEVENT KURT, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması Seçkin Yayınları, İstanbul, 2005.