T.C.
ÇAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİMDALI

TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

TEZİ YAZAN
Damla ERMEYDAN

Tez Danışmanı : Doç. Dr. Murat KOÇ
Jüri Üyesi : Dr. Öğretim Üyesi Ahmet Korhan MASTI
Jüri Üyesi : Doç. Dr. Olgun DEĞİRMENCİ
(TOBB Ekonomi ve Teknik Üniversitesi)

YÜKSEK LİSANS TEZİ

MERSİN/HAZİRAN-2018

ONAY

T.C
ÇAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ' NE

20162020 numaralı öğrencimiz olan **Damla ERMEYDAN** tarafından hazırlanan **"Türk Ceza Kanunu'nda Bilişim Suçları"** başlıklı bu tez calısması jürilerimiz tarafından **oy birliği** ile **Kamu Hukuku** Anabilim Dalında **YÜKSEK LISANS TEZİ** olarak kabul edilmiştir.

(Enstitü Müdürlüğünde evrak aslı imzalıdır.)

Üniv. İçi - Tez Danışmanı - Jüri Başkanı: Doç. Dr. Murat KOÇ

(Enstitü Müdürlüğünde evrak aslı imzalıdır.)

Üniv. İçi - Jüri Üyesi: Dr.Öğr.Üyesi Ahmet Korhan MASTI

(Enstitü Müdürlüğünde evrak aslı imzalıdır.)

Üniv. Dışı - Jüri Üyesi: Doç. Dr. Olgun DEGIRMENCI
(TOBB Ekonomi ve Teknik Üniversitesi)

Yukarıdaki imzaların, adı geçen öğretim elemanlarına ait olduklarını onaylarım.

(Enstitü Müdürlüğünde evrak aslı imzalıdır.)

06 /06/ 2018

Doç. Dr. Murat KOÇ
Sosyal Bilimler Enstitüsü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirişlerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'ndaki hükümlere tabidir.

İTHAF

Sonsuz adalete ve yılmayanlara…

ETİK BEYANI

Çağ Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

• Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,

• Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,

• Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,

• Kullanılan verilerde ve ortaya çıkan sonuçlarda herhangi bir değişiklik yapmadığımı,

• Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

06/06/2018

Damla ERMEYDAN

TEŞEKKÜR

Tezin fikir aşamasından itibaren, her adımda engin bilgive tecrübesiyle yolumu aydınlatan değerli hocam Doç. Dr. Murat KOÇ'a, beni bugünlere taşıyan yolda karşılaştığım tüm zorluklarda, benden sevgisini ve desteğini esirgemeyen sevgili eşim Ahmet ERMEYDAN'a, anne kız saatlerimizi kısıtlamak zorunda kalmamı yaşından büyük bir anlayışla karşılayan biricik kızım Nehir ERMEYDAN'a ve bana olan sonsuz inanç ve destekleri için kıymetli ailelerimize çok teşekkür ederim.

ÖZET

TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

Damla ERMEYDAN

Yüksek Lisans Tezi, Kamu Hukuku Anabilim Dalı
Tez Danışmanı: Doç. Dr. Murat KOÇ
Haziran 2018, 121 sayfa

Çağımızın teknolojik gelişmelerinin bilişim sistemlerini, etkin, ucuz ve kolay erişilebilir suç aletleri haline getirdiğini söylemek mümkündür. Bu sistemlerin suç işlemeyi kolaylaştırıcı özellikleri terör örgütlerinin de dikkatini çekmiş ve birçok faaliyetlerinde bilişim sistemlerinden faydalanır hale gelmişlerdir. Bu kapsamda araştırmanın amacı, ceza hukuku açısından bilişim suçları konusunda gelişmiş ülkelerde ve Avrupa Birliğinde yapılan çalışmaların incelenmesi, 5237 Sayılı Türk Ceza Kanunu'nda yer alan düzenlemelerin kapsam ve yeterliliğinin değerlendirilmesi ile siber terör konusunda Türk ceza hukukunun eksiklik ve sorunlarına yönelik önerilerde bulunmaktır.

Çalışmanın ilk bölümde; bilişim suçlarının tanımı, tarihsel gelişimi, bilişim suçu fail ve mağdurlarının genel özellikleri, bilişim suçu işleme yöntemleri ile bilişim suçunun özel bir görünümü olarak siber terörün tanımı, özellikleri, hedefi ve tahrip gücü konularına değinilmiştir. İkinci bölümde ABD, Almanya, Fransa, İngiltere, Japonya, Çin ve Rusya gibi gelişmiş ülkelerin bilişim suçlarıyla mücadele konusunda yapmış oldukları hukuki düzenlemeler ve aldıkları önlemler ile bu suçları düzenleyen uluslararası tek belge olan "Avrupa Konseyi Siber Suç Sözleşmesi"nin hükümleri incelenmiş, Üçüncü bölümünde 5237 Sayılı Türk Ceza Kanunu'nda bilişim suçlarına ilişkin yapılan düzenlemeler üzerinde durulmuş, sonuç kısmında ise bütün bu inceleme ve analizlerin sonunda bilişim suçları ve siber terör tehdidine karşı hukuki anlamda daha etkin mücadele edebilmek için yapılması gereken düzenlemeler, alınması gereken tedbirler ve uygulanması gereken programlar sunulmuştur.

Anahtar Kelimeler: Bilişim Suçları, Siber Terör, Avrupa Konseyi Siber Suç Sözleşmesi, Türk Ceza Kanunu

ABSTRACT

CYBERCRIMES IN THE TURKISH CRIMINAL CODE

Damla ERMEYDAN

Master Thesis, Department of Public Law
Supervisor: Assoc. Prof. Dr. Murat KOÇ
June 2018, 121 pages

It is possible to say that the technological developments of our age make the information systems effective, cheap and easily accessible crime devices. The facilitating features of these systems have attracted the attention of terrorist organizations and they have benefited from their information systems in many activities. In this scope, the aim of the investigation is to examine the studies done in the developed countries and the European Union about information crimes in terms of criminal law, to evaluate the scope and adequacy of the regulations in the Turkish Criminal Code numbered 5237 and to make suggestions about the deficiencies and problems of Turkish criminal law in cyber terrorism.

In the first part of the study; the definition, characteristics, goal and destruction of cyber terror as a definition of information crime, historical development, general characteristics of information crime perpetrator and victims, information processing methods of crime and information as a special view of crime. In the second part, the legal regulations and measures taken by developed countries such as USA, Germany, France, UK, Japan, China and Russia to combat information crimes and the provisions of " Council of Europe Convention on Cybercrime " which is the only international document that regulates these crimes are examined. The Turkish Criminal Code numbered 5237 emphasized the regulations related to information crimes and in the conclusion of this analysis and analysis the necessary arrangements, measures to be taken and programs to be applied in order to deal more effectively with cybercrime and cyber terrorist threats were presented.

Keywords: Cybercrimes, Cyberterror, Council of Europe Convention on Cybercrime, Turkish Criminal Code

İÇİNDEKİLER

Sayfa No:

İKİNCİ BÖLÜM

KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SUÇLARI VE AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

ÜÇÜNCÜ BÖLÜM
5237 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

KISALTMALAR LİSTESİ

AB	**:** Avrupa Birliği
ABD	**:** Amerika Birleşik Devletleri
a.g.e.	**:** Adı geçen eser
a.g.m.	**:** Adı geçen makale
a.g.i.s	**:** Adı geçen internet sitesi
AKSSS	**:** Avrupa Konseyi Siber Suç Sözleşmesi
ARPA	**:** Advanced Research Project Agency (İleri Araştırma Projeleri Ajansı)
ARPANET	**:** Advanced Research Project Agency Network(İleri Araştırma Projeleri Ajansı Ağı)
b.	**:** Bent
Bkz.	**:** Bakınız
BM	**:** Birleşmiş Milletler
C.	**:** Cilt
E.	**:** Esas
EC	**:** European Commission
e.t.	**:** Erişim Tarihi
f.	**:** Fıkra
FBI	**:**Federal Bureau of Investigation (Federal Araştırma Bürosu)
IP	**:** Internet Protocol
K.	**:** Karar
m.	**:** Madde
NII	**:** The National Information Infrastructure
ODTÜ	**:** Orta Doğu Teknik Üniversitesi
s.	**:** Sayfa
S.	**:** Sayı
SSCB	**:** Sovyet Sosyalist Cumhuriyetler Birliği
TCK	**:** Türk Ceza Kanunu
TCKÖT	**:** Türk Ceza Kanunu Ön Tasarısı
TDK	**:** Türk Dil Kurumu
TÜBİTAK	**:** Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜİK	**:** Türkiye İstatistik Kurumu

UCM **:** Uluslararası Ceza Mahkemesi

YCGK **:** Yargıtay Ceza Genel Kurulu

YFCK **:** Yeni Fransız Ceza Kanunu

TABLOLAR LİSTESİ

Sayfa No:

ŞEKİLLER LİSTESİ

Sayfa No:

EKLER

Sayfa No:

GİRİŞ

Çağımızda bilim ve teknoloji alanında yaşanan süratli gelişme sonucunda, bilişim sistemleri hayatımızın her alanına girmiş, ekonomi, sağlık, eğitim, ulaşım, kültür ve sanat gibi pek çok alanda ihtiyaç duyduğumuz her türlü hizmeti internet aracılığıyla evlerimize kadar getirmiştir. Günümüz insanı, internete erişimi olan bilgisayar, android telefon gibi cihazlar vasıtasıyla birkaç tuşa dokunarak doktordan randevu alabilmekte, tatilini planlayabilmekte, bankacılık işlemlerini online olarak yapabilmekte, dünya genelinde her türlü habere dakika farkı ile ulaşabilmekte, daha da önemlisi ürettiği, duyduğu, gördüğü herhangi bir şeyi internete yükleyerek anında paylaşabilmektedir.

Bilişim teknolojisi, bilginin hızla aktarılmasını, ansiklopediler dolusu bilginin çok minik taşıma kartlarına sığacak kadar küçültülebilmesini, bilginin görsel ve işitsel olarak sunulabilmesini, aynı anda pek çok kişi ile paylaşılabilmesini sağlamıştır. Bu alanda yaşanan hızlı gelişim, her geçen gün bu imkanlardan faydalanmanın daha kolay ve ucuz hale gelmesine, bu da daha çok kişinin erişim sağlamasına yol açmaktadır. Bilgi, bilgi toplumunda güçtür, ama bu gücü kimin hangi amaçla kullanacağı bilinemez[1].

Erişim sağlayıcıların tamamının, bilişim sistemlerini iyi amaçlar için kullanması mümkün olmamaktadır. Bilgisayar ve internet teknolojisinin kamuya açıldığı 1970'li yıllardan itibaren bu sistemleri zarar vermek ya da haksız çıkar elde etmek niyetiyle kullanan kişiler aracılığıyla uluslararası metinlerde "siber suçlar", ulusal mevzuatımızda "bilişim suçları" olarak adlandırılan suç tipi ortaya çıkmıştır.

Bilişim teknolojisinde yaşanan hızlı gelişmeye paralel olarak bilişim suçları da zaman içinde çeşitlenerek artmış, bilişim suçluları suç işleme yöntemleri konusunda gittikçe uzmanlaşmış, suç trafiğinde yaşanan bu artış, yetkilileri önlem almaya itmiştir.

Bu tür suçlulukla mücadelede, bilişim suçlarını izleme, tanımlama ve yasal norm altına alma adımları bilişim hukukunu doğurmuş, ne yazık ki genel olarak tüm dünyada hukuki mevzuat bu süreci bir adım geriden takip etmek zorunda kalmıştır.

Bilişim hukuku çok yeni bir alan olmakla birlikte internet teknolojisinin yapısından dolayı bir çok hukuk dalı ile yakından ilişkilidir. Örneğin bilişim sistemleri içinde üretilen ya da bu sistemlere sonradan yüklenen ürün ve eserlere ilişkin ihlaller

[1] Haydar Çakmak ve Taner Altunok, **Suç Terör ve Savaş Üçgeninde Siber Dünya,** Barış Platin Kitabevi, Ankara, 2009, s. 12.

fikri mülkiyet hukukunun konusuna girerken; bilişim sistemleri kullanılarak işlenen hırsızlık, dolandırıcılık, kişisel verilere ilişkin suçlar ceza hukukunun; kamu kurum ve kuruluşlarında bilişim sistemlerinin kullanılmasına ilişkin ihlaller idare hukukunun; verilerin uluslararası kullanımından doğan sorunlar devletler hukukunun ve bilişim hukukundaki soruşturma, kovuşturma ve yargılama yöntemleri ise medeni usul hukuku ile ceza muhakemesi hukukunun kapsamına girmektedir.

Bahsedilen şekilde, oldukça fazla yer kaplayan bir alanın dokunduğu tüm hukuk dallarının tek bir çalışmada incelenmesi mümkün olamayacağından, inceleme temel olarak ceza hukuku sınırları içinde tutulmaya çalışılmış, gerekli olduğunda diğer hukuk dallarının ilgili konularına kısaca değinilmekle yetinilmiştir.

İnceleme sırasında genelden özele gidilerek tümden gelim yöntemi kullanılmış, bu kapsamda ilk olarak konuya ilişkin tanımlar, bilişim suçu ve suçluluğuna ilişkin özellikle işlenme yöntemleri, fail ve mağdur profili gibi konular hakkında genel bilgiler verilmiş, aynı başlık altında siber terör konusuna değinilmiştir.

Bilişim sistemlerinin anılan yapısı sadece kötü niyetli bireysel kullanıcıların değil, terör örgütlerinin de dikkatini çekmiş, teknolojiye bağlı olarak ortaya çıkan küreselleşme sonucunda evrimleşen terör örgütleri, faaliyetlerini daha etkin bir şekilde sürdürebilmek amacıyla bu sistemi aktif olarak kullanmaya başlamıştır.

Küresel bazda bilişim suçlarında yaşanan artışa paralel olarak, siber terör saldırılarında da artış meydana gelmektedir. Bu saldırılar kimi zaman bağımsız, kimi zaman da, karma savaş (hybrid war) sırasında destekleyici yan unsur olarak gerçekleştirilmektedir. Türkiye, sürekli olarak bilişim suçlarından etkilenmekle beraber zaman zaman da siber terör saldırılarının hedefi olmaktadır. Bu doğrultuda araştırmanın temel problemi; Türk Ceza Hukuku sisteminin, bilişim suçları ve siber terör saldırıları ile mücadelede yeterli olup olmadığıdır.

Hedefine ulaşmada hiçbir sınır tanımayan terör örgütleri, kriminolojideki "suçların fırsatları takip etmesi" ilkesinde olduğu gibi bilgi teknolojilerinin sunduğu imkanlardan faydalanarak, ülkelerarası suç trafiğini yönlendirmektedirler. [2] Bu bağlamda, bilişim teknolojilerini kendi amaçları için kullanmaya başlayan terör örgütlerinin, eylemlerini internet üzerinden gerçekleştirmeleri sonucunda siber terör kavramı ortaya çıkmıştır. Terör kavramı gibi siber terör kavramının da dünya genelinde kabul görmüş ortak bir tanımı yoktur.

[2] Mehmet Özcan, "Siber Terörizm ve Uluslararası Tehdit Boyutu", http://www.uiportal.net/siber-terorizm-ve-ulusal-guvenlige-tehdit-boyutu.html, 2011, e.t.: 01.12.2017

Siber terör saldırıları, sistemleri işleyemez hale getirmenin ya da istihbarat kayıpları oluşturmanın yanında, hedeflerine ciddi anlamda maddi zarar da vermektedirler. Bu bağlamda, hem uluslararası hukukta, hem de Türk Ceza Hukuku sisteminde siber suçlar ve siber terör saldırılarına ilişkin düzenlemelerin incelenmesi nedeniyle araştırmanın alanyazında nadir rastlanır nitelikte olduğu değerlendirilmektedir.

Çalışmanın devamında, karşılaştırmalı hukukta bilişim suçları incelenmiş, özellikle bu suçlara ilişkin ilk düzenlemeleri yapan, ABD, İngiltere, Almanya, Fransa gibi ülkeler ile bilişim suçlarının çokça işlendiği, Çin, Rusya, Japonya gibi ülkelerin mevzuatlarına bakılmıştır.

Yine bilişim suçu ile mücadelede uluslararası tek belge olan ve etkin düzenlemeler içeren Avrupa Konseyi Siber Suç Sözleşmesi hakkında genel bilgiler verilmiş, sözleşmenin ceza hukukuna ilişkin maddeleri yakından incelenmiştir.

Araştırmanın ana amacı, Türk Ceza Hukukunun bilişim suçlarıyla ilgili olarak, gelişmiş ülkelerin hukuk sistemleri ile karşılaştırılması ve elde edilen bulgular sonucunda tespit edilen eksiklik ve aksaklıkların ortaya konulmasıdır. Bunun yanında, 11 Eylül 2001'den günümüze, adından daha sık söz edilen siber terör kavramına yakından bakmak ve terör örgütlerinin siber uzayda gerçekleştirdikleri eylemlerle etkin şekilde mücadele edebilmek için, dünya genelinde hukuki açıdan alınan tedbirleri incelemek ve bu bilgiler ışığında çözüm önerileri sunmak da amaçlanmaktadır.

Araştırma, bilişim suçları, siber suç ve siber terör kavramları üzerine literatür taraması yöntemi ile yapılmıştır. Ulusal yazında, ağırlıklı olarak bilişim suçları üzerine eserler bulunması, ancak siber suç ve siber terör kavramları üzerine çok az eser bulunması, araştırmanın temel sınırlılığını oluşturmuştur.

Tüm bunlara ek olarak, siber suçlar ve siber terör kavramları üzerine ağırlıklı olarak yabancı yazından faydalanılması da ayrıca bir sınırlılıktır. Veri toplama aracı olarak basılı eserler ve internet kaynakları kullanılmıştır. Çok yeni bir alan olan bilişim hukukunun hızlı gelişen yapısı nedeniyle, uluslararası hukukta meydana gelen değişikliklerin takip edilmesinin zorluğu da başka bir sınırlılık oluşturmuş, araştırma yazıldığı tarihte var olan ve ulaşılabilen alan yazında mevcut verilerle sınırlı kalmıştır.

BİRİNCİ BÖLÜM

BİLİŞİM SUÇLARI

1.1. Genel Olarak Bilişim Suçları

Yaşadığımız çağda meydana gelen hızlı teknolojik gelişmelere bakıldığında, bilişim hukuku ya da bilişim suçları denildiğinde kapsam ve sınırlar itibariyle çok geniş bir alan akla gelmektedir. Bilişim sistemleriyle alakalı suçlar, *siber suçlar*, *bilgisayar suçu*, *elektronik suç*, *dijital suç* veya *ileri teknoloji suçları* şeklinde isimlendirilirken anlatılmak istenilen kavram genelde "bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçlar" olmaktadır.[3]. Tanımdan da anlaşılacağı üzere siber suçlar oldukça büyük bir alanı kapsamaktadır. Bu suçlar birçok farklı tür ve içerikte tasarlanabilmekte yani bildiğimiz anlamda geleneksel suçların bilişim teknolojisi ile farklı biçim ve yoğunlukta etkileşimi ile ortaya çıkmaktadırlar. Bu nedenle bu tür suçları irdelerken, çalışma boyunca ağırlıklı olarak *bilişim suçu*, uluslararası metinlerin gerektirdiği ölçüde de *siber suç* terimleri kullanılacaktır.

Bir suçla mücadele etmenin ilk aşamasının o suçu tanımak olduğu düşüncesinden hareketle, araştırmanın bu kısmında bilişim, bilgisayar ve internet kavramları üzerinde durularak, bilişim suçlarını işleme yöntemleri, bilişim suçunu meydana getiren şartlar ve bilişim suçu fail ve mağdurlarına ilişkin bulgular ile bilişim suçlarının özel görümü olarak siber terör değerlendirilecektir.

1.2. Bilişim Kavramının ve Bilişim Suçlarının Tanımı

21. Yüzyılda teknolojide, özellikle bilgisayar alanında yaşanan gelişmeler, insanoğlunun düşünmeye başladığı ilk yıllardan beri var olan bilgiyi, dijital ortamda veri haline getirmiş ve bu verilerin hızlı bir şekilde toplanmasını, işlenmesini ve iletilmesini sağlayarak, bilişim kavramının ortaya çıkmasına sebep olmuştur. Bilgisayarın ortaya çıkışı, gelişmesi ve kullanımının yaygınlaşmasıyla genel olarak toplum hayatında ve özellikle bilimin çeşitli dallarında adeta yeni bir çağ açılmış, bilişim sistemleri zamanla kendine özgü iletişim dilini yaratmıştır[4] Bilişim suçu adı

[3] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Üçüncü Basım, Seçkin Yayıncılık, 2009, s. 44.

[4] Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **Ankara Üniversitesi Siyasal Bilimler Dergisi**, C. 49, S. 3-4, Ankara, 1994, s. 149.

verilen suç tiplerinin, bilişim terörünün ve bilişim hukukunun oluşmasına neden olduğu değerlendirilmektedir.

Bilişim kavramı, Meydan Larousse Büyük Lugat'da bilginin, özellikle elektronik makineler aracılığıyla düzenli ve mantıklı biçimde işlenmesi bilimi olarak ifade edilmiştir[5]. Büyük Larousse'ta ise bilişim, insan bilgisinin, teknik, ekonomik ve sosyal alanlardaki iletişimin otomatik makinelerde akılcı olarak işlenmesini konu alan bilim olarak belirtilirken, bilişim sistemi ise, belli bir uygulama için kullanılan bilgiyi elde etme işleme ve aktarma olanaklarının tümü olarak tanımlanmaktadır[6]. Başka bir açıdan bilişim sistemi yöneticinin karar vermesi için gerekli bilgiyi değişik kaynaklardan toplayan, işleyen, saklayan ve veriyi raporlayan biçimsel bir bilgi sistemi olarak tanımlanabilir[7].

Etimolojik olarak Fransızca "İnformatique" kelimesinden Türkçeleştirilen ve "Enformatik" olarak da bilinen, bilişim; bilme ve haberleşmenin temeli olan bilginin rasyonel ve otomatik olarak işlenmesi şeklinde tarif edilmektedir[8].Daha genel bir tanım olarak ise bilişim; teknik, ekonomik, sosyal, hukuki alandaki bilginin bilişim sistemi içinde veriye dönüştürülerek, yüklenmiş program uyarına işlenmesi, saklanması, düzenlenmesi, değerlendirilmesi ve aktarılması [9] şeklinde ifade edilmektedir. Bu tanımlamalardan yola çıkarak ifade edildiğinde bilişim, her alandaki üretilmiş bilgileri içeren verilerin,bilişim sistemlerine yüklenebilecek biçimde toplanması,toplanan bu verilerin sistemde yazılı bulunan programa göre işlenmesi, depolanması, sınıflandırılması ve başka bilişim sistemlerine aktarılması ile ilgili bir bilim dalıdır.

Bilişim suçları ile ilgili olarak uluslararası alanda üzerinde uzlaşılan tek bir tanım oluşturulamamıştır. Sürekli gelişen teknoloji bilişim suçu faillerine yeni yeni imkanlar sunmakta, bu durumun bilişim suçlarının çerçevesini hızlı bir şekilde genişletmesi nedeniyle,net bir tanımlama yapmak zorlaşmaktadır.

Benzeri şekilde Avrupa Konseyi Siber Suç Sözleşmesinde de (AKSSS) bilişim suçlarının tanımının yapılmasından kaçınılmış, bunun yerine bilişim suçu kapsamına

---

5 "Bilişim", **Meydan Larousse Büyük Lugat ve Ansiklopedisi,** Meydan Yayınevi, (EK-2), İstanbul, 1992, s. 131

6 **Büyük Larousse Sözlük ve Ansiklopedisi** "Bilişim", Milliyet Gazetesi Yayınevi, İstanbul, 1994, s. 1646.

7 Mahmut Tekin Güleş ve Diğerleri, **Değişen Dünyada Teknoloji Yönetimi**, Damla Ofset, Konya, 2000, s. 83.

8 **Dictionnaire Larousse,** "Bilişim", Ansiklopedik Sözlük, İstanbul,1993, C.1, Milliyet Yayınları, 1993, s.370.

9 Olgun Değirmenci, "Bilişim Suçları", **Yayınlanmamış Yüksek Lisans Tezi,** Marmara Üniversitesi SBE, İstanbul, 2002, s.7.

gireceği öngörülen eylemler, suç olarak tek tek sayılmıştır. Buna göre AKSSS'nin ikinci bölümünde bilişim suçları; bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar; yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanımı, bilgisayarla bağlantılı suçlar; bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık içerikle bağlantılı suçlar; çocuk pornografisi olarak tanımlanmıştır.

Bilişim suçunu meydana getiren temel unsur klasik suç tiplerinde olduğu gibi hukuk kuralının ihlalidir. Ancak bilişim suçlarını, diğer suç tiplerinden ayıran en önemli özellik bu suçun işlenmesinde, bilişim sistemlerinin kullanılmasıdır. Bilişim kavramının genel tanımında yer alan işlemleri gerçekleştirebilecek tüm sistemlerin bilişim sistemleri olarak adlandırılabileceği düşünülürse, söz gelimi android mobil telefonlar, tabletler, akıllı ev sistemleri, android özelliklere sahip pos makineleri de bu şemsiye altında yer alacaktır. Ancak çalışmanın genel çerçevesi içerisinde bilişim sistemi olarak bilgisayar ve bilgisayar ağları kastedilecek, yeri geldikçe işlenen suç tiplerinin özelliklerinin gerektirdiği kadar diğer bilişim sistemlerine yer verilecektir.

Bilişim dünyasında gelecekte ne gibi gelişmelerin yaşanacağı, bilişim sistemlerinin ve bilişim suçlarının kapsamlarının ne kadar gelişeceği şu anda net olarak bilinmemekle birlikte, bilişim suçlarının yapısını daha iyi anlayabilmek için bu suç tipinin günümüze kadar geçirdiği evrimi incelemek faydalı olacaktır.

1.3. Bilişim Suçlarının Tarihsel Gelişimi

Bilginin, insanlığın avcılık ve toplayıcılıkla yaşamını sürdürdüğü ilk çağlarda çok az olduğu, ancak insanın gelişimi ile paralel olarak zamanla artan gelişen bir unsur olduğu varsayılmaktadır. Bilginin niceliğinde yaşanan bu artışın, bir süre sonra bilgiyi toplamak, sınıflandırmak, iletmek gibi ihtiyaçları doğurduğu düşünülmektedir. Buradan yola çıkarak,ihtiyaçlara cevap veren sistemler kurmayı ve bu sistemler aracılığıyla bilgiyi verimli bir şekilde işlemeyi başaran ulusların, daha ileri medeniyetler meydana getirerek tarihsel süreçte daha çok söz sahibi hale geldiği sonucuna varılabilir.

1870'ten sonra endüstri devrimi nitelik değiştirerek teknolojik devrime dönüşmüştür[10]. Teknolojide yaşanan gelişmeler bilgiyi hızla değişen ve bundan dolayı

[10] Durmuş Günay ve Ali Arıdıru, "Bilim ve Teknolojiye Yöneliş", **I. Teknoloji Kalite ve Üretim Sistemleri Kongresi**, 1999, Sakarya Kalite Derneği Adapazarı, s.22-34, https://www.researchgate.net/profile/Durmus_Gunay/publication/317662173_Bilim_ve_Teknolojiye_Yonelis/links/5947be17aca27242cda7604a/Bilim-ve-Teknolojiye-Yoenelis.pdf

takibi de zorlaşan bir biçime, "bilişim"e dönüştürmüştür. 21. yüzyılda insanlık Bilgi Toplumu, Bilişim Toplumu gibi çeşitli nitelendirmelerle belirtilen bir süreç yaşamaktadır. Teknolojik açıdan incelendiğinde bu süreçte; ilkel toplumu kesici taş aletleri, tarım toplumunu su değirmeni, sanayi toplumunu buhar makinesi ve bilişim toplumunu ise bilgisayar temsil etmektedir[11]. Gerçekten de günümüz insanının aldığı kararlara, attığı adımlara yön veren, günlük uğraşlarında ona eşlik eden, bu özellikleriyle yaşamını şekillendiren ana unsur bilişim sistemleri olmaktadır. Bilişim sistemlerinin temelinde ise bilgisayar ve bilgisayarları birbirine bağlayan internet ağı yer almaktadır.

Bilgisayarların en önemli özelliği, hem işlenecek verileri, hem de bunlara uygulanmak istenen işlemleri belleğinde tutmasıdır. Böylece sadece verilerin girilmesiyle, aygıtın kendisine daha önceden verilmiş komutları sorgulamaksızın yerine getirmesi sağlanmış olur[12]. Türk Dil Kurumuna ait sözlükte bilgisayar: Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç veya elektronik beyin olarak tanımlanmaktadır[13].

İngilizce "to compute =hesaplamak" kelimesinden türetilerek "computer" olarak isimlendirilen ve Türkçeye ismi bilgisayar olarak kazandırılmış cihazlar, kendilerine verilen elektronik emirleri sorgulamaksızın çok hızlı bir şekilde yerine getirirler[14]. Bilgisayar, aldığı bilgiye kendisine yüklenen program uyarınca işlem yapar, bu bilgileri sınıflandırır, birleştirir, depolar, çözümler, karşılaştırır, ayıklar ve iletir.

Kardaş'a göre bilgisayar, aritmetik ve mantık işlem dizileriyle oluşturulmuş programlara göre verileri otomatik olarak işleyen makinedir[15]. Yazıcıoğlu, bilgisayarı veri saklayabilen, depolayabilen ve bunları işleyebilen, depolanmış bir programı işletebilen ve işlem akışı ile sırasını otomatik olarak değiştirebilen bir aygıt olarak tanımlamıştır[16]. Bu bağlamda bilgisayarın, diğer programlanabilir makinelerden temel ayırt edici özelliği, verileri kapsamlı olarak işleyebilme, kullanabilme yeteneğidir.

---

[11] Çakmak ve Altunok, **a.g.e.** s. 12.

[12] "Bilim ve Teknoloji: Bilgisayar", **Thema Larousse,** Milliyet Gazetesi Yayınevi, İstanbul, 1993, s.456.

[13] **Türk Dil Kurumu Büyük Türkçe Sözlük,** "Bilgisayar", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5ab5225217f746.17587618 e.t.: 08.10.2017

[14] Levent Kurt, **Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Seçkin Yayınları Ankara, 2005, s. 29.

[15] Ümit KARDAŞ, "Bilişim Dünyası ve Hukuk", **Karizma Dergisi**, S. 13, 2003, s. 8.

[16] Recep Yılmaz Yazıcıoğlu **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle,** Alfa Basın Yayın Dağıtım, Bursa, 1997, s. 28.

Bilgisayarların birbiri ile iletişime geçmelerini sağlayan fiziki ortam ile bu ortamın fonksiyonunu gerçekleştirmesini sağlayan donanıma ise bilgisayar ağı denilmektedir[17]. Bu oluşumun çok daha kapsamlı hali olan internet ise,çok protokollü bir ağ olup birbirine bağlı bilgisayar ağ gruplarının tümü olarak da tanımlanabilir[18]. İnternetin kullanılmasıyla birlikte verilerin internet aracılığıyla bilgisayar ortamında toplanarak; sınıflandırılabilir, karşılaştırılabilir, seri bir şekilde aktarılabilir hale geldiğini, bu durumun da bilişim alanında yaşanan gelişmelerin hızını arttırdığını söylemek mümkündür.

İnternet gibi bir sistemin oluşturulabileceği fikrini ilk ortaya atan kişi, psikolog Joseph Carl Rebnett Licklider'dir[19]. Masachussets Teknoloji Enstitüsü'nde çalmaya başlayan Licklider, Ağustos 1962'de yazmaya başladığı "Galaktik Ağ" (Galactic Network) notlarında, herkesin veri ve programlara basit bir şekilde ulaşabildiği, birbiriyle bağlantılı bir bilgisayar kümesi hayal etmiştir[20]. Zamanla hayatımızın önemli bir parçası haline gelen internet, entegre bir yapıya sahip olup, her katılımla hızla büyümektedir[21].

İnternet, İngilizce "kendi aralarında bağlantılı ağlar anlamına gelen "interconnected networks" teriminin kısaltmasıdır[22]. İnternet kavramında yer alan net sözcüğü bilgisayar ağı anlamına gelir[23].İnternetin birden fazla haberleşme ağının (network) birlikte meydana getirdikleri; tüm bilgilerin bu ağa bağlı sistemler içinde aktarılabildiği bir ağ olduğu söylenebilir[24]. Başka bir tanıma göre ise, dünya üzerinde bulunan ağların veya bilgisayarların birbirine bağlanmasıyla oluşan, insan ve makine birliğini sağlayan, yeryüzündeki en büyük ağa internet denir[25].

İnternetin ortaya çıkışı, soğuk savaş döneminde Sovyet Sosyalist Cumhuriyetler Birliği'nin (SSCB) 1957'de Sputnik uydusunu uzaya göndermesiyle başlamıştır[26]. Bu olay Amerika Birleşik Devletleri (ABD)Savunma Teşkilatında büyük bir korku ve

---

17 Ahmet Caner Yenidünya ve Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.** Legal Yayıncılık, İstanbul, 2003, s. 34.
18 Şaban Cankat Taşkın, **Bilişim Suçları,** Beta Basım, İstanbul, 2008, s. 13.
19 Ali Osman Özdilek, **İnternet ve Hukuk**, Papatya Yayıncılık, Ankara, 2002, s. 18.
20 C. Bila, "Bireysel ve Kitlesel İletişim Aracı Olarak İnternet ve Toplumsal Etkileri", **Yayınlanmış Yüksek Lisans Tezi**, Gazi Üniversitesi SBE, Ankara, 2001, s. 18.
21 Kurt,**a.g.e.** s. 41.
22 Taşkın, **a.g.e.** s.13.
23 Hasan Sınar, **İnternet ve Ceza Hukuku**,Beta Yayınları, İstanbul, 2001, s. 21.
24 Ali Osman Özdilek, **İnternet ve Hukuk**, Papatya Yayıncılık, Ankara, 2002, s. 13.
25 Billy Baron ve Jill H. Ellsworth/Kevin M. Savetz. "The Internet Unleashed." **Technical Communication** 44.2, 1997, p. 4.
26 Taşkın, **a.g.e.** s. 13.

şaşkınlık yaratmış[27],savaş sırasında geleneksel haberleşme yollarının kullanılamayacağı bir durumda, ulusal komuta merkezinden balistik füze üslerine gerekli emirlerin verilebilmesini ve savaşta önemli emirlerin ulaştırılmasını sağlayacak bir haberleşme birimi olarak, İleri Araştırma Projeleri Ajansı (ARPA) kurulmuştur[28]. 1960'lı yıllarda dünyaya hükmetme yarışına girmiş iki süper gücün rekabeti sonucunda icat edilen internet, geçmişi yarım yüzyıldan daha az olan çok genç bir teknolojidir.

İlk etapta, Stanford Araştırma Enstitüsü, Utah Üniversitesi ve Kaliforniya Üniversitesinin Los Angeles ve Santa Barbara yerleşkelerinde bulunan dört bilgisayar birbirine bağlanarak İleri Araştırma Projeleri Ajansı Ağı (ARPANET)adlı askeri bilgisayar ağı oluşturulmuştur.

Devlet tekelinde olan ve askeri birimler tarafından idare edilen bu iletişim biçiminin idaresi, 1990'lı yılların başında çeşitli protokollerle sivillere devredilmiştir[29]. Ülkemizde ise, internet denilince akla ilk gelen kurum,Orta Doğu Teknik Üniversitesidir (ODTÜ). İlk defa 12 Nisan 1993 yılında, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından desteklenen bir projeye bağlı olarak, ODTÜ'de gerçekleştirilen bağlantının temel amacı, internetin akademik çevrede bilimsel veri alış verişi için kullanılmasıdır [30] . İlk kez ODTÜ'de bağlantısı gerçekleştirilen internetin Türkiye'de yaygın olarak kullanımı ise 2000'li yılları bulmuştur.

Bilgisayarlar aracılığıyla daha çok bilginin depolanıp işlenmesi, internet yoluyla işlenen verilerin hızlı bir şekilde iletilebilmesi, günlük toplumsal yaşamı değiştirdiği gibi bir çok sorunu da beraberinde getirmiştir. Çok miktarda verinin yüksek hızda iletildiği bilişim alanında yaşanan gelişmeler, bir yandan yeni hukuki yararlar meydana getirirken bir yandan da yeni ihlal sahaları oluşturmakta, bir nevi teknolojik devrim yaratmaktadır. Bilgisayar ve internet teknolojilerinin bir araya gelmesiyle ortaya çıkan güç,tüm dünya devletlerini aynı zamanda ve aynı oranda etkilememekle beraber, küreselleşmenin de etkisiyle neredeyse tüm dünya toplumlarına dokunmuştur. Bu devrimin etkisinde kalan bütün toplumlarda bir yandan aynı teknolojinin benzer

---

[27] Ian J. Lloyd, **Information Technology Law**, Third Edition, Butterworths, London, Edinburg, Dublin, 2000, p.8.

[28] Sınar, **a.g.e.** s. 22-23.

[29] Mehmet Nesip Öğün ve Adem KAYA, 'Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri Dergisi, S. 18, Ankara, 2013, s. 149. http://dergipark.gov.tr/download/article-file/84487

[30] Murat Volkan Dülger **Bilişim Suçları,** Seçkin Yayınları, Ankara, 2004, s. 61.

sonuçlar doğurması nedeniyle bir bütünleşme yaşanırken, diğer yandan her toplumun kendine özgü yapısı nedeniyle sorunlarda farklı yansımalar görülmektedir[31].

Ne yazık bilişim teknolojisi her zaman insanlığın iyiliğine hizmet etmemiş, bu teknolojinin getirdiği kolaylıklar haksız menfaat elde etmek isteyen insanlar tarafından da kullanılmıştır. Günümüzde yaygın olarak işlenen bilişim suçları, teknolojik gelişmelere paralel olarak çeşitli aşamalardan geçerek bugünlerine ulaşmıştır. İlk olarak 1970'lerde "Captain Crunch" lakabıyla anılan Draper, bedava uzak telefon görüşmesi yapabilmek için bir yol bulunca daha sonra "phreakers" olarak anılacak olan telefon hackerları ortaya çıkmıştır. Preaking olarak adlandırılan bu işlem telefon şirketlerinin güvenlik sistemlerini kırmak olarak bilinmesine rağmen daha çok, telefon sisteminin çalışmasının öğrenilmesi ve sistemin kişilerin ekonomik çıkarları doğrultusunda işletilmesi anlamına gelmektedir[32].

Amerika'da Telefon hatlarının bu şekilde yasa dışı kullanımı, telefon şirketlerini harekete geçirmiş ve bilişim suçlarını ilgilendiren yasaların yapılmasınaneden olmuştur. Bilgisayarların gelişmesiyle telefon hackerları bu teknolojiyi suç eğilimleri doğrultusunda kullanmaya başlamış ve ilk bilişim suçları ortaya çıkmıştır. 1980'lerde bu işe merak salan phreaker ve hackerlar her türlü sisteme girmeye başlamışlardır[33].

Bir başka bilişim suçu işleme yöntemi olan "hacking" ise 1981 yılında Texas A&M Üniversitesi öğrencisi olan Joe Dellinger'ın Aplle II bilgisayarları için kendisini kopyalayabilen bir program yazmasıyla ve bu programın kendisini geometrik olarak kopyalayabileceğini, bu yolla da bilgisayar sistemlerine zarar verebileceğini keşfetmesiyle ortaya çıkmıştır[34]. Günümüz bilgisayarlarının ataları denilebilecek ilk kişisel bilgisayarlar, renkli bir ekran üzerinde imleçle çeşitli pencerelere tıklanılması yerine, koyu renkli bir ekrana çeşitli program kodlarının yazılması yoluyla çalıştığından, sıradan bir kullanıcının bile program yazmayı öğrenmesini gerektirmekteydi. Bu durumun, zamanla gençler arasında kod öğrenerek program yazma rekabetine sebep olduğu ve bilişim suçlarının ortaya çıkmasının ve yaygınlaşmasının önemli bir nedeni olduğu değerlendirilmektedir.

---

[31] Atasoy, F. "Kültürler Üzerinde Bilişim Devriminin Etkileri", **Modern Türklük Araştırmaları Dergisi**, S. 4 (2), s. 168. http://mtad.humanity.ankara.edu.tr/IV-2_Haziran/27_MTAD_4-2_FAtasoy_163-178.pdf

[32] Santosh Rajagopalan, "A Study of Security Problems Associated with the Telephone Network." Oregon State University, Department of Electrical and Computer Engineering http://www.tucops.info/tucops3/phreak/general/r2.pdf , 2000 e.t.:27.10.2017

[33] Ç. Gümüş, "Bilişim Suçları İle Mücadelede Polisin Eğitimi", **Yayımlanmamış Doktora Tezi**, Fırat Üniversitesi SBE, Elazığ, 2008, s. 43-44.

[34] Kurt, **a.g.e.** s. 55.

Günümüzde, bilişim alanındaki gelişmelere paralel olarak, çok farklı suç işleme şekilleri ortaya çıkmıştır. Teknolojinin sunduğu imkanlar, suç işleme saikiyle hareket eden insanlara yeni suç kapıları aralamıştır[35]. Bu kapsamda, bilişim suçlarının işlenme şekillerini ana hatlarıyla incelemenin yararlı olacağı düşünülmektedir.

1.4. Bilişim Suçu İşleme Yöntemleri

Bilişim suçlarının işlenmesinde araç olarak bilgisayar, internet ve çeşitli yazılımların kullanılması nedeniyle, bu suçların neler olduklarının anlaşılması, kapsam ve sınırlarının çizilebilmesi için bir miktar teknik bilgiye ihtiyaç duyulmaktadır. Bu nedenle, bilişim suçlarının işlenmesinde kullanılan temel yöntemlerin bilinmesinin suçun net olarak ortaya konulması açısından önemli olduğu kanısına varılmaktadır.

Genel olarak bilişim suçlarına bakıldığında temel olarak iki şekilde işlendiği görülmektedir. Bunlardan ilki bilişim sistemlerine karşı suçlar, diğeri bilişim sistemleri kullanılarak işlenen suçlar şeklindedir.[36] Bilişim sistemlerine karşı suçlarda hedef, bilişim sistemi içinde muhafaza edilen bilgidir. Bilişim dünyasında veri olarak da adlandırılan bu bilgilere karşı, her türlü haksız erişim, bozma, değiştirme, taşıma, yok etme eylemi bu suç tipini oluşturabilmektedir. Bilişim sistemleri kullanılarak gerçekleştirilen suçlarda ise bilişim sistemleri bir hedef değil failin hedefine ulaşmasını kolaylaştıran bir araçtır. Bilişim sistemleri kullanılarak işlenen hırsızlık ve dolandırıcılık suçları bu grup suçlara örnek olarak verilebilir.

Teknolojik gelişmelere paralel olarak sürekli yenilenen bilişim dünyasında, bilişim suçlarının işlenme şekilleri de çeşitlilik göstermektedir. Bu açıdan bilişim suçlarının işlenme yöntemlerinin tamamının incelenmesi mümkün olmamaktadır. Bu nedenle araştırmanın bu bölümünde alan yazında en çok değinildiği tespit edilen;çöpe dalma, gizlice dinleme, veri aldatmacası, Truva atı, tarama, süper darbe, salam tekniği, sistem güvenliğinin kırılıp içeri girilmesi, gizli kapılar, ağ solucanları, bilgisayar virüsleri, mantık bombaları, istem dışı alınan e-postalar, oltalama, web sayfası hırsızlığı ve web sayfası yönlendirme ile hukuka aykırı içerik sunma teknikleri üzerinde durulacaktır.

---

[35] Kurt, **a.g.e.** s. 60.

[36] Aydın, Emin Doğan. **Bilişim Suçları Ve Hukukuna Giriş**. Doruk Yayınları, 1992, s. 27.

1.4.1. Çöpe Dalma (Scavenging)

Kullanıcı tarafından bilgisayarda yapılan işlemlerin masaüstünde bulunan çöpe atılmasıyla verilerin silindiği değerlendirilir, ancak bilgisayarın çalışma mantığı bu şekilde işlememektedir. Bilgisayara kaydettiğimiz veriler ancak kaydolundukları manyetik bant üzerindeki yerlerinin üzerine yeni bilgiler işlenmesi yolu ile silinebilmektedir.

Bu yöntemde, bilişim sisteminde gerçekleştirilen işlemler sonucunda kullanıcı tarafından silindiği düşünülen ancak hafızada kalmaya devam eden bu bilgiler, kullanıcının bilgisi dışında, fail tarafından depolanmaktadır. Bu yöntemin temeli, bilgisayar diskine kaydolan verinin manyetik bant üzerinde yaptığı izlerin kaybolmaması, silinmemesi ilkesine dayanmaktadır[37]. Burada temel amaç bilgisayarın hafızasında (bellek) bulunan ve artık kullanılmayacağı için silinmiş bulunan bilgileri tekrar geri getirerek kullanmaktır. Bu yöntem programlama bilgisine ve internet ağına gerek duymaktadır.

1.4.2. Gizlice Dinleme (Sniffing)

Veri aktarımı için bilişim sistemlerinin kullandığı ağlara fail tarafından yetkisiz erişim sağlanarak mağdurun veri akışının izlenmesi yöntemidir[38]. Bu yöntemde temel amaç, bilgisayarlar arasında iletişim halindeki veriye erişmektir. Veri akışına engel olunmadan, alınmak istenen verinin bir kopyası, ağı sniffing yapan kişinin bilgisayarına gizlice yönlendirilir. Sniffer yazılımları vasıtasıyla bilgiler gizlice toplanarak, internet üzerinden, kullanıcının bilgisi dışında başka bir bilişim sistemine aktarmaktadırlar.

1.4.3. Veri Aldatmacası (Data Diddling)

Veri aldatmacası yöntemi, uygulanmasının çok basit olması nedeniyle, bilişim suçları alanında yaygın olarak uygulanan bir tekniktir. Bu yöntemde belgelerin tahrif edilmesi, değiştirilmesi, kartlara ek karakter kaydı, bazı kayıtların iptali gibi

---

[37] Yazıcıoğlu, **a.g.e.** s. 113.

[38] Hemraj Saini/ Shankar Rao Yerra/T. C. Panda. "Cyber-crimes and Their İmpacts: A Review." **International Journal of Engineering Research and Applications** C. 2. S. 2, 2012 s. 203. https://s3.amazonaws.com/academia.edu.documents/38524184/10.1.1.417.1369.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523809470&Signature=fvF%2BX60JPk1c5JsryZfpguq25Uk%3D&response-content-disposition=inline%3B%20filename%3DCyber-Crimes_and_their_Impacts_A_Review.pdf

aldatmacaları içermektedir.[39]Bilişim sistemlerine yetkisiz erişim sağlanarak, depolanmış bilgiler üzerinde değişiklik yapılmasını kapsamaktadır.

Veri aldatmacası yönteminin yaygın kullanımı nedeniyle,bu suça yönelik davaların konusunun,bankaların kayıtları, bordrolar, envanterler, kredi kayıtları, okul transkriptleri, telefon şifresi yapılandırmaları ve hemen hemen tüm diğer veri işleme uygulamaları olduğu söylenebilir[40].

1.4.4. Truva Atı (Troyan Horse)

Adını Aka'ların, Truva'lıları aldatarak yenmek için yapmış oldukları Truva atından alan bu yöntem efsanedeki at ile aynı mantıkla çalışmaktadır. Truva Atı masum görünüşlü ancak gizli bazı fonksiyonlar içeren bir programdır. Bir Truva Atı sayesinde fail, işletim sisteminin açıklarından yararlanarak bütün sisteme hakim olabilmektedir.[41] Truva Atı bilgisayarın sabit diskine kaydedildikten sonra düzenli çalışan programlarla birlikte işlemeye başlar. Görünürde çalışan programın, aslında Truva Atı programını gizleyen bir alt program olduğu kullanıcı tarafından bilinmemektedir[42]. Truva atı yazılımları da, diğer birçok zararlı yazılımda olduğu gibi, kullanıcıların ilgisini çeken ücretsiz basit yazılımlar üzerine yerleştirilerek bilgisayarlara yüklenmesi sağlanmaktadır.

1.4.5. Tarama (Scanning)

İnternet ortamında temel mantık, tıpkı telefonlarda olduğu gibi her bilgisayarın internete bağlandığı bir hat numarasının yani Internet Protocol (IP) numarasının olmasıdır. Tarama yönteminde program,bir IP numarasından başlayarakrastlantısal arama yapmaktadır. Rastgele sayıların bir araya getirilmesiyle oluşturulan IP kodlarıyla yapılan aramaya olumlu sinyal gelmesi halinde, aranan IP numarasına sahip bilgisayara erişim sağlanmış olur.

Bu programlar sayesinde, IP numarası bilinmeyen herhangi bir bilgisayarın IP adresi çok kısa sürelerde bulunabileceği gibi, hangi dosyanın arandığı belirtilmek

---

39 D. Emin Aydın, **Bilişim Suçları ve Hukukuna Giriş**,Doruk Yayınları, Ankara, 1992, **s**. 48

40 Michel E. Kabay "A Brief History Of Computer Crime: An İntroduction For Students". School of graduate studies, 2008.http://www.mekabay.com/overviews/history.pdf e.t.: 09.10.2017

41 Değirmenci, 2002, s. 79

42 Eric J Sinrod ve P. Reilly William, "Cyber-crimes: A Practical Approach To The Application Of Federal Computer Crime Laws." **Santa Clara Computer and High Tech. *LJ*** 16 (2000): 177. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.tr/&httpsredir=1&article=1258&context=chtlj

suretiyle, sabit diskler üzerinde araştırmada bulunulması da mümkündür[43] Tarama programının tamamen rastlantısal IP kodları üzerinden çalışan, kötücül bir yazılım olduğu ifade edilebilir.

1.4.6. Süper Darbe (Super Zapping)

Süper Darbe (super zapping) yazılımları, bilgisayarların hırsızlığa karşı mevcut güvenlik programlarının denetimi ya da programların kendilerinden kaynaklanan sebeplerden çalışamaz hale gelen bilgisayar sistemlerinin, yeniden işler hale getirilmesi için kullanılırlar.[44]Bu yazılımlar bütün güvenlik önlemlerini aşarak sistemin işleyişine etki edebilen programlardır. Tüm güvenlik kontrollerinden geçtiğinden, yanlış amaçlarla kullanıldığında çok tehlikeli olabilmektedir. Yani sistemde büyük tahribatlar yapmak bilişim suçu faili için çok geniş olanaklar sağlamaktadır.

Amerikan Bankası müşterilerinden birinin, hesabındaki paranın azaldığını fark etmesi üzerine ortaya çıkan bir olayda, ABD‟de bir banka görevlisi, sistemde meydana gelen bir hatayı düzeltmek için usulüne uygun olarak süper darbe programını kullanmış ve işlem sırasında herhangi bir kontrolün olmadığını fark edince, arkadaşlarının hesaplarına yüklüce para transfer etmiştir [45] .Bilişim suçlularının, sadece bilişim sistemlerine hasar vermekle kalmayıp, yüksek miktarlarda maddi zarara sebep oldukları, faillerin ise eylemleri sonucunda haksız kazanç elde ettikleri ifade edilebilir.

1.4.7. Salam Tekniği (Salami Techniques)

Bu teknik “bozuklukları topla” isimli eski bir aldatmacaya dayanmaktadır. Banka hesaplarında virgülden sonraki ondalık rakamların son iki rakamlarının saldırganın belirlediği banka hesabına aktarılarak burada birikmesi şeklinde çalışır[46]. Transfer edilen meblağ çok küçük olmasına rağmen, çok sayıda ki hesaptan para toplanması nedeniyle, sonuç olarak fail açısından çok büyük miktarda haksız kazanç elde edilmiş olur. Genel olarak bu tekniğin icrası için Truva Atı programları kullanılmaktadır.[47]

---

[43] Değirmenci, s. 83.
[44] Kurt, **a.g.e.** s. 66
[45] Yazıcıoğlu, **a.g.e.** s. 156.
[46] Kabay, **a.g.e.** s. 24.
[47] Değirmenci, s. 84

1.4.8. Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking)

Hacking günümüzde bilgisayar sistemlerine yetkisiz erişim sağlanması [48] eylemine karşılık olarak kullanılmakta iken hacker terimi ise eylemi gerçekleştiren kişiye verilen addır. Hacking eylemi, internet üzerinden gerçekleştirilen bir tür ihlaldir. Bilgisayar ağlarında bulunan güvenlik açıklarının tespit edilerek bilgisayara ya da ağ sistemine yetkisiz erişim sağlanmasıdır [49]. Bu şekilde erişim sağlandıktan sonra hackerfark edilene kadar sistem içinde dilediği bilgiye ulaşabilmekte ve sisteme her şekilde etki edebilmektedir.

Hackerlar kendilerini yetenekli kişilerden oluşan elit bir topluluğun üyesi olarak düşünmektedirler ve bu düşünceyle bilgi ve tecrübelerini çeşitli forum ve sohbet odalarında diğer hackerlarla paylaşmaktadırlar. Örneğin her yaz Amerika, Nevada, Las Vegas'ta Geleneksel Def Con Bilgisayar Yeraltı Meclisi[50] bu amaçla toplanmaktadır. Bu toplantılara katılan fail profili, bilişim suçu işlemeyi yasal bir eylem olarak gören, kendi bilgi ve tecrübeleriyle gurur duyan ve bunu paylaşmak için organizasyonlar oluşturan bireyler, şeklinde çizilebilir.

1.4.9. Gizli Kapılar (Trap Doors)

Tuzak kapıları olarak da isimlendirilen gizli kapılar, yazılımcı tarafından, yazılımın içine bilinçli bir şekilde gizli olarak yerleştirilen bir virüs yazılımıdır. Tuzak kapısının fonksiyonu, kendisini programlayan kişinin sistemin içine, normal sistem koruyucularını aşarak sızmasını sağlamaktır[51].Gizli kapıların bizzat yazılımcının kendisi tarafından konulduğu için herhangi bir kullanıcı tarafından fark edilmesinin mümkün olmadığı, ancak yaşanan sorunlar nedeniyle yazılım üzerinde inceleme yapan uzmanlar aracılığıyla tespit edilebileceği değerlendirilmektedir.

---

[48] S. M. Furnell ve Matthew J. Warren. "Computer Hacking And Cyber Terrorism: The Real Threats in The New Millennium?." **Computers and Security** S. 18.1 1999, s. 29. https://s3.amazonaws.com/academia.edu.documents/50731522/10.1016_S0167-40489980006-6.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523809536&Signature=JKkhs9yP9zmK3Eh%2Bt%2FwztoWbSr0%3D&response-content-disposition=inline%3B%20filename%3DComputer_Hacking_and_Cyber_Terrorism_The.pdf

[49] Joe Grand and July Friday, "Advanced Hardware Hacking Techniques." Defcon 12. 2004, http://grandideastudio.com/wp-content/uploads/advanced_hardware_hacking_slides.pdf e.t.: 11.10.2017

[50] E. J. Sinroad ve W. P Reilly, "Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws", **Santa Clara High Technology Law Journal.** S. 16 (2) 2000, s. 182.

[51] Kurt, **a.g.e.** s. 67.

1.4.10. Ağ Solucanları (Network Worms)

Solucanlar otomatik olarak kendilerini bir bilgisayardan diğerine kopyalayabilen, bir kez sisteme girdikten sonra kendi başına ilerleyebilen ve kendisini çok sayıda çoğaltabilen programlardır. Bu şekilde ağ kapasitesini meşgul ederek internet hızını yavaşlatabilir ve internet ağlarının kilitlenmesine sebep olabilirler. Ağ solucanları, genellikle iyi oluşturulmamış güvenlik duvarını aşarak bilişim sistemine girmekte ve eylemlerine başlamaktadırlar[52]. Ağ solucanı ya bir virüs gibi davranarak yazılıma zarar vermekte ya da sisteme bir Truva Atı bırakmaktadır.[53]

Solucan programı bilgisayara yüklendiğinde, eğer yapabilirse, bulaşabileceği internet alanlarını arayan bir programı başlatmaktadır.Solucanın yüklediği bu programın başlayabilmesi için, herhangi bir kullanıcının işlem yapmasına ihtiyacı olmamaktadır[54].Bu bilgiler ışığında ağ solucanlarının, kullanıcıdan bağımsız çalışmaları nedeniyle, virüslerden daha etkili programlar olduğu kanısına varılabilir.

1.4.11. Bilgisayar Virüsleri

Bilgisayar virüsleri ençok bilinen bilişim suçu türüdür. Bilgisayar virüsü, kendisini uygulama programlarına ekleyerek sisteme dahil olmakta ve sonrasında ciddi hasarlar vermektedir. Virüsler kendilerini çoğaltabilen, kopyalarını çeşitli yollarla başka bilişim sistemlerine ulaştırarak bu sistemleri etkileyen yazılımlardır[55]. Burada failin amacı bir şeyler çalmak değil, sadece sisteme ya da dosyalara zarar vermektir. Fiil bu yönü ile vandalizmle karşılaştırılabilir[56]. Virüsler ile solucanlar karşılaştırıldığında, virüslerin aktif hale gelebilmek için kullanıcı tarafından çalıştırılmaya ihtiyaç duyması, solucanların ise kendi kendilerini aktif hale getirebilmeleri nedeniyle, solucanların virüslerden daha etkili yazılımlar olduğu söylenebilir.

---

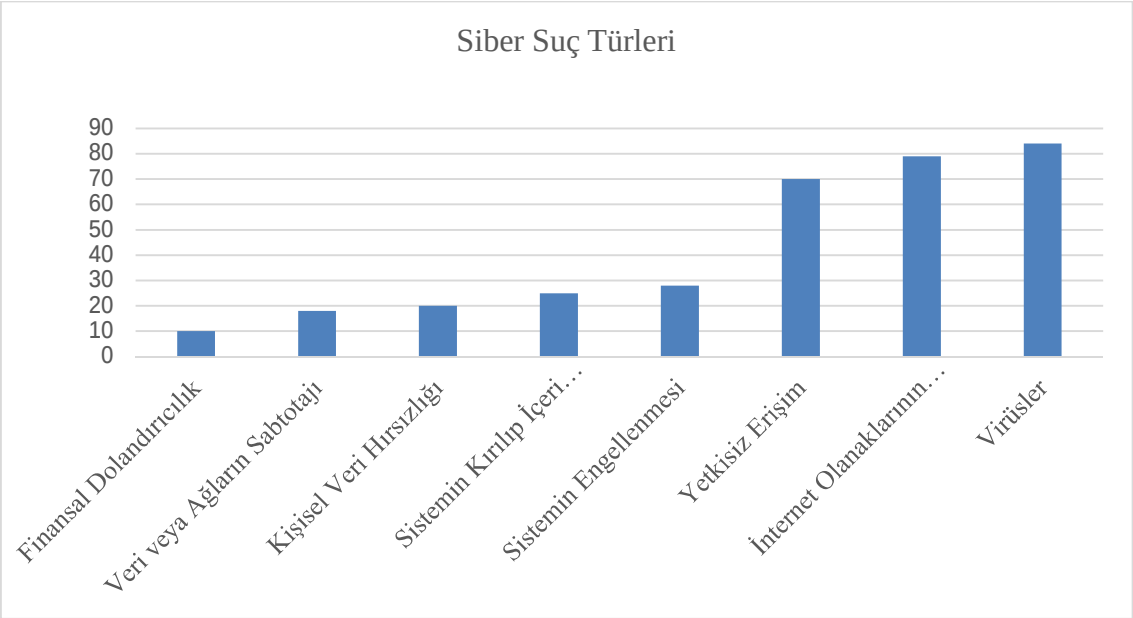
52 Esra Yaycı, "Bilişim Suçları", **Yayınlanmış Yüksek Lisans Tezi**, Gazi Üniversitesi SBE, Ankara, 2007, s. 35.

53 Değirmenci 2002, s. 87.

54 Ali Osman Özdilek, "Kurtlar ve Zombiler : Worm'ların ve Ddos Ataklarının Hukuki İncelemesi", http://www.hukukcu.com/bilimsel/kitaplar/wormlarhukuki.htm 2003, e.t.:11.11.2017.

55 Değirmenci, 2002, s.88.

56 Stanley Kratchman, Jacob Lawrence Smith, and Murphy Smith, **"The Perpetration and Prevention of Cybercrime**s. https://www.researchgate.net/profile/Murphy_Smith/publication/228301055_The_Perpetration_and_Prevention_of_Cybercrimes/links/56df253d08ae9b93f79a8de7.pdf 2008, s. 3, e.t.: 01.11.2017



*Şekil 1.*2000 yılında dünya genelinde siber suç tiplerinin kullanım oranı

Kaynak: İrfan, 2011.

Çeviri: D. Ermeydan

Dünya genelini baz alan istatistiki verilere göre, bilişim suçu işlemekte kullanılan yöntemler içinde en çok kullanılan yöntemin, bilgisayar virüsleri olduğu Şekil 1'de yer alan verilerden de anlaşılmaktadır..

1.4.12. Mantık Bombaları (Logic Bombs)

Mantık bombaları, zarar verme amacıyla yazılan kodların en basit örneğidir. Genellikle daha büyük bir programa gömülmüş bağımsız kod parçaları şeklindedirler[57]. Bu nedenle ilk bakışta fark edilmeleri mümkün olmaz. Bilişim sistemleri içinde uzun bir süre zarar verici herhangi bir işlem yapmaksızın bulunabilirler, ancak daha önceden programlanmış oldukları koşullar oluştuğunda ya da belirli bir sürenin sonuna gelindiğinde zarar verici sonuçlar meydana getirebilmektedirler.

Bu konuda verilebilecek en güzel örnek ülkemizde 1999 yılında görülen ve oldukça zarar veren Çernobil Virüsü olup programın yazılımı gereği, bilgisayarın belleğinde beklemekte ve her ayın 26'sında zarar verici eylemlerini

[57] Klaus Brunnstein "From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour" **22nd National Information Systems Security Conference,** July 23, 1999 http://www.bilisimogretmeni.com/genel/hacker-cracker-phreaker-nedir-nasil-calisirlar.html e.t.: 30.10.2017

gerçekleştirmektedirler[58]. Mantık bombalarının harekete geçmek için belirli bir hareket ya da tarih beklemesi nedeniyle bilinen anlamda saatli bomba ya da mayın düzeneği gibi çalıştığını söylemek mümkündür.

1.4.13. İstem Dışı Alınan E- Postalar (Spam)

Spam, genellikle sayısız alıcıya topluca gönderilen istenmeyen veya önemsiz e-postadır, genellikle eczacılık ürünleri veya pornografi ile ilgilidir. Spam e-postası, kimlik avı e-postaları veya kötü amaçlı yazılım göndermek için de kullanılır[59]. Spam adı verilen e-postaları, e-posta kutularına gönderen kişi ise "spammer" olarak adlandırılmaktadır. Spammer adı verilen kişiler oluşturdukları veritabanlarını satarak haksız kazanç elde etmektedirler.

Spam e-postaları daha çok bir ticari ürünün reklamının yapılması ya da pazarlanmasında büyük kitlelere ulaşmak için kullanılmaktadır[60]. İdeolojik, pornografik ve her türlü ticari duyuru yapmak isteyen kişiler, spam e-postaları sayesinde geniş kitlelere ulaşabilmektedirler[61]. Spam e-postaları, kullanıcıları en çok rahatsız eden yazılımlar arasında yer almaktadır.

1.4.14. Oltalama (Phishing Attacks)

Oltalama saldırısı (phishing attact), potansiyel kurbanları kandırmak, aldatarak tuzağa düşürmek için tasarlanmış e-postaların internet kullanıcılarına gönderilmesine dayanır[62].Bu teknikte kullanıcılara, tanınmış bir firmadan geliyormuş izlenimi verilmiş, cevap için postanın içindeki bağlantılı siteye geçilmesini talep eden e-postalar gönderilmektedir. Ancak verilen talimat uygulandığında erişilen site, dolandırıcılar veya istihbarat birimleri tarafından hazırlanmış ve gerçeğini taklit eden sahte bir internet sitesi olmaktadır[63] . Böylece, kullanıcılar tarafından siteye verilen her türlü gizli bilgi doğrudan dolandırıcıların eline geçmektedir.

---

58 Dülger, **a.g.e.** s. 75.
59 Kabay, **a.g.e.** s. 51-52.
60 Değirmenci, **a.g.e.** s. 98
61 Özdilek, **a.g.e.** s. 153.
62 Min Wu, Robert C. Miller and Simson L. Garfinkel. "Do Security Toolbars Actually Prevent Phishing Attacks?." **Proceedings of the SIGCHI conference on Human Factors in computing systems.** ACM, http://cs.union.edu/~fernandc/srs200/readings/SecurityToolbars.pdf. 2006. s. 601 e.t.: 03.11.2017
63 Gökhan Bayraktar, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, Yeniyüzyıl Yayınları, İstanbul, 2015, s. 91.

1.4.15. Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme

Bu suç tipi bir web sayfasına ulaşmak isteyen kullanıcının, ulaşmak istediği web sayfasına benzer şekilde hazırlanmış başka bir sayfaya yönlendirilmesi ve bu sayfada işlem yapmak isteyen kişinin kendiliğinden verdiği kullanıcı adı ve şifresine ulaşmak olarak tanımlanmaktadır[64]. Bilişim sistemleri aracığıyla işlenen dolandırıcılık suçu yaygın olarak bu yöntemle işlenmektedir.

Başka bir web sayfası yönlendirme tekniği ise "typing error hijacking" (yanlış yazanları kaçırma) olarak adlandırılan bir tekniktir. Bu teknikte hacker yaygın olarak bilinen yanlışları göz önüne alarak bu yanlışları yapan kullanıcıları kendi sayfasına yönlendirir[65]. Örneğin; www.xbank.com.tr gibi gerçek bir site adresinin kullanıcılarını www.x.bank.com.tr şeklinde yanıltarak şifrelerini bu site adresine yazmalarından faydalanmak tipik bir yanlış yazılanları kaçırma yöntemidir.

1.4.16. Hukuka Aykırı İçerik Sunma

Irkçı, ayrımcı, şiddeti teşvik eden ya da kişilik haklarına tecavüz eden içerikler gibi hukuka aykırı içeriklerin bilişim sistemlerinde bulundurularak veri iletim ağları aracılığıyla diğer kullanıcıların erişimine sunulması çok karşılaşılan bir bilişim suçudur[66]. Kişi farklı özellikleri nedeniyle bilişim sistemleri üzerinden hedef alındığından, nefret suçlarının işlenmesinde bu yöntem yaygın olarak kullanılmaktadır.

1.5. Bilişim Suçunun Özel Bir Görünümü Olarak Siber Terör

Günümüzde bilişim sistemlerinin sadece büyük banka veya şirketlerde değil, hastanelerde, okullarda, havaalanlarında, askeri tesislerde ve daha pek çok yerde kullanıldığı, bu tesislere yapılacak herhangi bir saldırının büyük zararlara yol açacağı ifade edilebilir.

Bilişim teknolojilerinden en çok faydalanan ülkelerin başında gelen ABD'de Amerikan Ulusal Bilgi Altyapısı (The National Information Infrastructure- NII) üzerinde hackerlar, teröristler veya yabancı hükümetlerden gelen saldırılara karşı

---

64 Kurt, **a.g.e.** s. 73.

65 Ali Sırımcıyan, "Domain Hırsızları", **CHIP Dergisi**, S. 3, Doğan Burda Dergi Yayıncılık, İstanbul, 2000, s. 164.

66 Bahaddin Alaca, "Ülkemizde Bilişim Suçları ve İnternetin Bu Suça Etkisi", Yayınlanmamış **Yüksek Lisans Tezi**, Ankara Üniversitesi SBE, Ankara, 2008, s. 71.

önleyici mekanizmalar geliştirilmeye çalışılmaktadır. Savunma bakanlığı NII üzerinde oluşabilecek bir zayıf kanalın sonuçlarının çok ağır olacağını belirtmiştir[67].

Bu kapsamda bilişim suçlarının evrimleşmesinde ulaştığı son nokta siber terördür. Bilişim suçlarının incelendiği çalışmanın bu bölümünde,11 Eylül 2001 yılında ABD'de Savunma Bakanlığı ve ikiz kulelere yapılan saldırının ardından her geçen gün daha sık telaffuz edilen "siber terör" kavramına değinilmeden geçilmesi mümkün görünmemektedir.

1.5.1. Siber Terörün Tanımı

Siber terörün tanımını yapabilmek için önce terör ve terörizm kavramlarının tanımının ortaya konulması yani adların adlarının tanımlanması oldukça önemlidir. Bu açıdan, Türk Dil Kurumunun sözlüğüne göre terör, yıldırı[68], terörizm, yıldırıcılık[69] anlamlarına gelmektedir. Kelime olarak Latince terrere'den gelen terör sözcüğünün korkutmak, dehşete düşürmek, korkutup kaçırmak, caydırmak gibi anlamları vardır[70].

Meydan Larousse Büyük Lugat'ta altüst edici ve felce uğratıcı aşırı korku, bir toplumda bir grubun halkın direnişini kırmak için yarattığı ortak korku, geniş anlamda ulusal veya uluslararası düzeni değiştirmek amacıyla, bu düzenlerin yasal saymadığı araç ve taktiklerin kullanımını öngören bir eylem türü[71] olarak yer alan terörizm, Temel Britannica ansiklopedisinde, bireylerin grupların ya da devletin siyasal bir amaçla başka kişi ve gruplara karşı giriştiği, savaş dışı istemli şiddet eylemleri [72] olarak tanımlanmıştır.

Bu tanımların yanında daha pek çok kaynakta çeşitli tanımları bulunmasına rağmen tüm dünya tarafından kabul edilen ve üzerinde uzlaşılmış bir terör tanımı yapmak imkansız görünmektedir. Ancak bu durum, terörün kişiden kişiye.şarta ya da coğrafi bölgeye göre değişen bir olay olduğu anlamına gelmemelidir. Burada temel

---

67 Çakmak ve Altunok, **a.g.e.** s. 102.

68 **Türk Dil Kurumu Türkçe Sözlük.** "Terör", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5ab6381a5e60b4.85280559 e.t.: 01.11.2017

69 **Türk Dil Kurumu Türkçe Sözlük,** "Terörizm", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5ab6379a845038.04036206 e.t.: 02.11.2017

70 Paul Wilkinson, **Political Terrorism**, NewYork, 1974, s. 9.

71 **"Terör"**, Meydan Larousse Büyük Lugat, s. 844,

72 **"Terör"**, Temel Britannica, s. 189.

sorunun terörün kapsamının ve sınırlarının belirlenmesinden kaynaklanan zorluklar olduğunu söylemek yanlış olmayacaktır.

Buna rağmen ele alınan bütün tanımlarda ortak noktanın şiddet kullanmak olduğunu söylemek mümkündür. Etimolojik olarak şiddet kavramı Arapça kökenli olup; sertlik, sert ve katı davranış, kaba kuvvet kullanma anlamını taşır[73]. Ancak olağan yani adi şiddet ile terörizm içindeki şiddet arasında bazı farklılıklar bulunmaktadır. Adi şiddette maksat, genel olarak şiddetin yöneldiği varlığa zarar vermek iken, terörizmde şiddet, şiddet kullananların kişisel menfaatlerinden veya ihtilaflarından kaynaklanan motivasyonlardan doğmaz[74].

Buradan da anlaşılacağı üzere şiddet hareketinde, hedef belirli bir kişi yada gruba zarar vermek iken terörün araç olarak kullandığı şiddette, amaç birilerine zarar vermek değil, birilerine zarar vererek toplumun geri kalanına (korku, panik, yıldırma, güvensizlik gibi) çeşitli alt mesajlar vermektir. Tüm bunlara ek olarak terör ve terörizm kavramları arasında anlamsal olarak bir fark olmadığını belirtmek yerinde olacaktır.

Siber terörizm kavramı ise, ilk olarak 1980 yılında Güvenlik ve İstihbarat Enstitüsü (Institute for Security and Intelligence – ISI) araştırmacılarından Barry Collin tarafından kullanılmıştır. Collin'e göre modern dönemin iki önemli korkusu olan, teknolojik araçlardan mahrum kalmak endişesi ile bilgisayar teknolojilerine olan güvensizlik duygusunun birleşiminden siber terörizm korkusu oluşmuştur.[75]Tanımda psikolojik bir durum olarak kendisini gösteren siber terör kavramının, günümüzde soyut bir durum olmaktan çıkıp günlük yaşamımızı etkileyen bir tehdit haline gelmekte olduğunu söylemek mümkündür.

Küreselleşme nedeniyle ülkeler arasında mal, insan ve sermaye hareketleri artmış, terör örgütleri teknolojik kolaylıklardan ve sivil toplum örgütleri gibi uluslararası alanın yeni aktörlerinden yararlanma imkanı bulmuştur[76].Yaşanan bu gelişmeler terör örgütlerini elini güçlendirmekle kalmamış, internetin merkezi kontrolden uzak olması, sınırlama olmaması, herkesin ulaşımına açık olması, hızlı bilgi

---

[73] Necmettin Özerkmen, "Terör, Terörizm ve Terörün Küreselleşmesi." **Polis ve Sosyal Bilimler Dergisi** S.2.1 Ankara, 2004, s. 248.

[74] Yayla, **a.g.m.** s. 340.

[75] Barry C. Collin, "The Future Of Cyberterrorism: Where The Physical And Virtual Worlds Converge." **Crime and Justice International** S. 13, 1997, s. 14-18.

[76] Fikret Birdişli, Teori ve Pratikte Uluslararası Güvenlik Kavram- Teori- Uygulama, Üçüncü Basım, Seçkin Yayıncılık Ankara. 2017, s. 249.

akışı sağlaması, ucuz ve kolay erişilebilir olması, çoklu ortam sağlaması, anonimlik özelliği ve medyanın yoğun ilgisi, terör örgütlerini internet kullanımına itmiştir[77].

Karşılaştırmalı hukukta tek başına siber terörizm başlığı altında bir yasa bulunmamakta, ancak gelişmiş ülkelerin terörizm yasalarında bu kavrama da yer verdikleri görülmektedir. Türk hukuk mevzuatında siber teröre ilişkin özel bir yasa bulunmamakla beraber Terörle Mücadele Kanunun 1'inci maddesinde[78] terörün tanımı yapılmış, aynı kanunun 4'üncü maddesinde ise Türk Ceza Kanunu'nun (TCK) 243'üncü maddesinde sayılan "Bilişim Sistemine Girme" suçu ile 244'üncü maddesinde sayılan "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme" suçlarının 1'inci maddede terör olarak sayılan amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlenmesi halinde terör suçu olarak değerlendirileceği hükme bağlanmıştır.

Buna göre; TCK'nın 10'uncu bölümünde "Bilişim Alanında Suçlar" başlığı altında yer alan 243 ve 244. Maddelerde sayılan bilişim suçlarının terör faaliyetlerinde bulunmak amacıyla kurulmuş bir terör örgütü tarafından gerçekleştirilmesi halinde eylemin bilişim suçu değil terör suçu kapsamına gireceği belirtilerek bilişim suçları ile terör kavramlarının buluşturulduğu ve siber terör tehdidine karşı yürürlüğe konulduğu ifade edilebilir.

İngiltere, 2000 tarihli Terörizm Yasasında siber terörizmi; hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlere izinsiz erişim sağlamak veya bu sistemleri bozmak olarak tanımlanmaktadır (United Kingdom Terrorism Act Of 2000)[79].

ABD Federal Araştırma Bürosu (Federal Bureau of Investigation-FBI) ise siber terörizmi; etnik gruplar ya da gizli ajanlar tarafından yapılan önceden tasarlanmış, siyasi amaçlı, savaş dışı hedeflere karşı şiddetle sonuçlanan, bilgisayar sistemleri, bilgisayar programları ve verilerine yöneltilen saldırılardır şeklinde tanımlamıştır[80]. Siber terörün

---

[77] Gabriel Weimann, "Terror On The Internet: The New Arena, The New Challenges", **US Institute of Peace Press.**2006, s. 3. https://www.researchgate.net/profile/Gabriel_Weimann/publication/238077713_Terror_on_the_Internet_The_New_Arena_The_New_Challenges/links/0f31753872b79cea95000000/Terror-on-the-Internet-The-New-Arena-The-New-Challenges.pdf e.t.: 03.11.2017

[78] Terörle Mücadele Kanununu http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf Erişim Tarihi 20.06.2018

[79] Mehmet Özcan, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu" UİPortal.net. http://www.uiportal.net/siber-terorizm-ve-ulusal-guvenlige-tehdit-boyutu.html. e.t: 23.11.2017.

[80] Mudawi Mukhtar Elmusharaf, "Cyber Terrorism- A new kind of terrorism", **Computer Crime Resourch Center**, 2004, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism/, e.t.: 25.11.2017

temel amacının yazılım kodlarını kullanarak, bilgi ve hizmet akışında yıkıma neden olmak, bu suretle halkta korku ve panik yaratarak kişilerin yönetime olan desteğini yok etmek olduğu ifade edilebilir.

Daha kapsamlı şekilde siber terörizm, bilişim sistemlerinin kullanılması yoluyla, ülkelerin kamu düzenlerinin ve çıkarlarının tahrip edilmesini amaçlayan, kişisel ve politik olarak motive olmuş, amaçlı eylem ve etkinliklerdir[81].

Denning ise siber terörü meydana getirdiği zarar açısından değerlendirmiş ve bir saldırının siber terör olarak adlandırılabilmesi için kişilere ya da mala karşı şiddetle sonuçlanması, ya da en azından korku yaratacak kadar zarar verici olması gerektiğini beyan etmiştir[82]. Meydana gelen zarara örnek olarak ölümle ya da yaralanma ile sonuçlanan saldırılar, patlamalar, uçak kazaları, su kirlenmeleri veya ciddi ekonomik kayıplarla sonuçlanan kritik altyapı sistemlerine karşı saldırılar verilebilir.[83]

Tüm bu tanımları bir araya getirdiğimizde, siber terörizmin terör örgütleri tarafından, siyasi veya ideolojik sebeplerle, kritik bilişim sistemlerine yönelik olarak bilişim aygıtları ile yapılan, klasik bir terör eylemine eşdeğer sonuçlar yaratan, her türlü saldırılar olduğu ifade edilebilir.

1.5.2. Siber Terörün Özellikleri

Siber suçlar, araç olarak bilgi sistemlerini kullanmak veya bilgi sistemlerine karşı kanundışı eylemler iken, siber terörizm de doğrudan bilişim sistemlerini çökertmeyi hedef almayan, aksine etkileyici sonuçlar doğuracak politik mesajlar vermek adına bilişim sistemlerinin kullanıldığı eylemler söz konusudur[84].Bu eylemlerin

---

81 Kevin C. Desouza ve Tobin Hensgen, "Semiotic Emergent Framework to Address the Reality of Cyberterrorism". **Technological Forecasting and Social Change** 2003, S. 70, s. 386 https://www.researchgate.net/profile/Kevin_Desouza/publication/223035624_A_Semiotic_Emergent_Framework_to_Address_the_Reality_of_Cyber_Terrorism/links/59e5d5560f7e9b0e1ab25345/A-Semiotic-Emergent-Framework-to-Address-the-Reality-of-Cyber-Terrorism.pdf e.t.: 03.11.2017

82 Dorothy E. Denning, "Cyberterrorism", **Calhoun Institutional Archive of the Naval Postgraduate Schooll, 2000, s. 1.** https://calhoun.nps.edu/bitstream/handle/10945/55351/Denning_Dorothy_2000_cyberterrorism.pdf?sequence=1 e.t.: 05.11.2017

83 Denning, s. 1

84 Erhan Akyazı, Necmi Emel Dilmen ve Tolga Kara, "Toplumsal ve Ekonomik Etkileri Bağlamında Bilişim Çağının Yeni Tehdidi: Siberterör." Türkiye Bilişim Derneği, **2. İstanbul Bilişim Kongresi,** 3-4 Haziran 2008, İstanbul, s.33. https://www.researchgate.net/profile/Necmi_Dilmen/publication/228582062_TOPLUMSAL_VE_EKONOMIK_ETKILERI_BAGLAMINDA_BILISIM_CAGININ_YENI_TEHDIDI_SIBERTEROR/links/5527a0020cf229e6d63630e2/TOPLUMSAL-VE-EKONOMIK-ETKILERI-BAGLAMINDA-BILISIM-CAGININ-YENI-TEHDIDI-SIBERTEROeR.pdf e.t.: 09.11.2017

siyasi amaçlarla yapılması nedeniyle her halükarda mağdurun devlet olduğunu söylemek mümkündür.

2008 yılında Güney Osetya Savaşı esnasında Rusya Federasyonu'nun Gürcistan'a yaptığı siber taarruzlarla hem Gürcistan halkını hem de dünya kamuoyunu psikolojik olarak etki altına alması ve sonuçta, Gürcistan hükümetinin siyasi olarak zor durumda kalması.[85], bilişim aygıtlarının politik amaçlarla kullanımına çarpıcı bir örnek teşkil etmektedir.

Ayrıca, internet aracılığıyla terör örgütünün propagandasının yapılması, eleman sağlanması, örgüt yararına dolandırıcılık yapılması, bomba yapımı, silahlı saldırı gibi eğitimler verilmesi, siber terör olarak değerlendirilebilecektir.[86]. Siber teröristlerin kurgulamış oldukları eylemlerini gerçekleştirmek için sadece internete erişimi olan bir bilgisayara ya da mobil telefona sahip olmaları yeterli olabilmektedir. Bu kapsamda siber terör, işleniş biçimi açısından siber suç, amaç ve sonuçları bakımından ise terör suçu özelliği taşımaktadır[87]. Ancak siber terör açısından sanal dünyada gerçekleştirilen eylemlerin etkilerinin gerçek dünyada somut bir biçimde görüldüğü ve çok yıkıcı olabildiği ifade edilebilir.

Joshua Green, "The Myth Of Cyberterrorism" başlığı taşıyan makalesinde; teröristler tarafından bilgisayar kullanılarak öldürülen insanların olmadığı gibi, terör örgütlerinin bilişim sistemlerini kullanarak yıkıcı bir saldırıda bulunduğuna dair kanıt olmadığını[88] ifade ederek, siber terör kavramının abartıldığını belirtmiştir.

Başka bir açıdan bakıldığında Denning'in deyişiyle geleceğin teröristleri bilgisayar klavyesiyle bir bombanın yaratacağı etkiden fazlasını yaratacaktır[89]. İnternet üzerinden hemen her türlü hizmetin yapıldığı günümüzde, sızmaların önüne geçmek çok zor olduğu gibi kritik tesislere verilen zararın can kaybına yol açmayacağının garantisi de bulunmamaktadır. Bu gibi faaliyetler, terörist örgütler tarafından,gerçekleştirilmeleri daha kolay ve emniyetli olduğundan daha çok tercih edilen yöntemler haline gelebilecektir.

---

85 Bayraktar, **a.g.e.** s. 16.

86 Gizem Özkışlalı, "Küreselleşme, İnternet ve Terörizmin Değişen Yüzü: Siber Terörizm", **Yayımlanmış Yüksek Lisans Tezi** . Hacettepe SBE, Ankara 2008, s. 71 https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=UPP_Zu9isEmWGFXFCBYasWZZPKrSaJUj7N8CJG3RcnZ2MKtGrRQIVjX3Ibazmb3H

87 Bayraktar, **a.g.e.** s. 77.

88 Joshua Green, "The Myth of Cyberterrorism." **Washington Monthly** S. 34, 2002, s. 2. http://werzit.com/intel/regions/cyber/articles/archives/Myth%20of%20Cyberterrorism.pdf e.t.: 10.11.2017

89 Denning, **a.g.m.** s. 70.

Siber suçlarda olduğu gibi bilgisayar ve bilgisayar sistemlerinin, araç veya hedef olarak kullanılması siber terörizm kapsamında değerlendirilebilir. Fakat siber suçlarla siber terörizmi birbirinden ayıran temel etken, eylemin siyasal bir sebeple işlenmesi gerçeği, yani suçun terörden ayrıldığı noktada ortaya çıkmaktadır[90]. Bu noktada siber suç olarak da adlandırılan bilişim suçları ile siber terörü meydana getiren unsurların incelenmesi yerinde olacaktır.

Tablo 1.

Siber Suç ve Siber Terör Arasındaki Farklar

Eylem	**Siber Suç**	**Siber Terör**
Niteliği	Doğrudan	Sembolik
Şiddeti	Az Yoğun	Yoğun
Motivasyonu	Kişisel Kazanç	Siyasi
Failleri	· Bireyler · Organize Suç Örgütleri · Anonim	· Terörist Örgütler · Hangi örgüt olduğu tahmin edilebilir
Hedefleri	Kazanç sağlanacak hedefler	· Kritik tesisler · Güvenlik Birimleri · Hükümet temsilcilikleri
Kaynağı	Ülke içinden ya da dışından	Ülke içinden ya da dışından

Kaynak: Çakmak (2009)

Tablo 2'de de görüldüğü üzere her iki kavramın ortak yanlarının yanında, ayrışan pek çok özellikleri bulunmakta, en temel farklılığın ise motivasyondan kaynaklandığı görülmektedir. Suçun ya da terör saldırılarının siber ortamda gerçekleştirilmesi bu kavramlara yüklenen anlamlarda öze yönelik bir değişiklik yapmamaktadır. Ancak etkilerde asimetriye işaret etmektedir. Ne şekilde sınıflandırılırsa sınıflandırılsın, günümüzde siber ortam kötü maksatlarla kullanıma açıktır. Gerekli hukuki ve fiziksel tedbirler ise bu saldırıları geriden takip etmek zorunda kalmıştır[91].

Siber teröristlerin bilişim sistemlerini kullanarak baraj kapaklarını açabilecekleri, hava trafik kontrol sistemlerini ele geçirerek, uçak kazalarına neden

[90] Çakmak ve Altunok, **a.g.e.** s. 41.
[91] Çakmak ve Altunok, **a.g.e.** s. 50.

olabilecekleri bu ve benzeri şekillerde kitlesel ölümlere yol açabilecekleri öngörülmektedir.[92]Bu kapsamda siber tehditlerin asli hedefi; ülkelerin can damarları olan kritik altyapılardır. Kritik altyapılar ise; bir ülkede ekonomi ve sosyal hayatın sağlıklı bir şekilde işlemesi için ciddi öneme sahip olan fiziksel ve sayısal sistemler olarak tanımlanmaktadır.[93]Tablo 3'te de görüldüğü üzere kritik altyapıların nitelikleri ve kapsamları ülkeden ülkeye farklılık göstermektedir.

Tablo 2.

ABD, AB ve Japonya'daki Kritik Altyapılar

ABD	AB	JAPONYA
Su	Su	Su
Sağlık	Sağlık	Sağlık
Bilgi ve Telekomünikasyon	Bilgi ve İletişim	Telekomünikasyon
Bankacılık ve Finans	Finans	Finans
Hükümet	Kamu Düzeni ve Güvenlik	Kamu Yönetimi
Posta ve Nakliye	Ulaşım	Demiryolu
Enerji	Enerji	Elektrik
Tarım ve Gıda	Gıda	Gaz
Savunma Sanayii	Uzay Araştırmaları	Sivil Havacılık
Acil Hizmetler	Sivil Yönetim	Lojistik
Kimyasal Materyaller	KBRN Endüstrileri	

Kaynak: Bayraktar (2015)

Toplumlar bilişim sistemlerinden faydalanma kapasiteleri ile doğru orantılı olarak siber saldırı riskine maruz kalmaktadırlar. İronik bir biçimde siber tehditlerden etkilenmesi en muhtemel ülkelerin dijital anlamda teknolojiyi en fazla kullanan ve alt yapı örüntüsünde bu sisteme en çok yer veren ülkeler olduğu görülmektedir.

1.5.3. Dünya'da ve Türkiye'de Siber Terör

İnternetin icadından günümüze kadar geçen kısa sürede, siber terörün sadece teoride kalmadığı görülmektedir. Terör örgütlerinin bilişim sistemleri ile olan ilişkisine

[92] Bayraktar, **a.g.e.** s. 18-19.

[93] Mehmet Kara ve Soner Çelikkol, "Kritik Altyapılar: Elektrik, üretim ve Dağıtım Sistemleri, SCADA Güvenliği", **4. Ağ ve Bilgi Güvenliği Sempozyumu** (4), Kocaeli, s. 1. http://www.emo.org.tr/ekler/2afc6bfb6139e85_ek.pdf e.t.: 20.11.2017

en çarpıcı örnek; ABD'nin Irak'ı işgali sonrası, terör örgütleri tarafından kaçırılan rehinelere ait infaz görüntülerinin, internet yoluyla tüm dünyaya servis edilmesi bu şekilde örgütün taraftar toplayıcı ve caydırıcı yönde propagandasının yapılmasıdır.

Terör örgütleri protesto amaçlı olarak devletlere ait internet sitelerini spam adı verilen e-postalarla meşgul ederek kullanılamaz hale getirebilmektedirler. Şubat 2001'de California elektrik hizmetleri sağlayıcısına (ISO) yapılan siber saldırılar sonucunda 11 gün elektrik bağlantısının kesilmesi, Nisan 2001'de Çin'deki bir Hacker grubu tarafından ABD ve Çin arasındaki havayolu uyuşmazlığı nedeniyle 1200 ABD web sitesi sistem dışı bırakılması,[94] bu saldırılar sonucu Beyaz Saray, ABD Hava Kuvvetleri ve Enerji Departmanının zarar görmesi örnek olarak verilebilir. Yapılan saldırılarda insan hayatı tehlikeye girmemiş ancak bilişim sistemlerine verilen zarar sonucunda kamu hizmeti alamayan çok sayıda kişinin mağdur olduğu görülmektedir.

2010 yılında İran'ın nükleer tesislerini hedef alan Stuxnet yazılımlı[95] siber taarruz ise; belli bir ekonomik değere yönelik olarak geliştirilmiş bir siber silahın ne kadar etkili olabileceğinin boyutlarının anlaşılması açısından verilebilecek en güzel örnektir.[96]Kullanılan bu yazılımın tesisi işletmekte kullanılan bilişim sistemlerine zarar vermesi nedeniyle tesis işlemez hale gelmiş ve büyük ekonomik zarar ortaya çıkmıştır.

Tam anlamıyla siber terör olayı olmasa da 11 Eylül 2001 tarihli saldırı Pentagon'un güvenlik şifrelerinin kırılması, hava radar sistemlerinin devre dışı bırakılması ve düşen uçakların pilotlarından kaçırılma sinyalleri alınamaması gibi unsurlar [97] nedeniyle yoğun şekilde teknoloji kullanılan bir terör olayı olarak nitelendirilebilir.

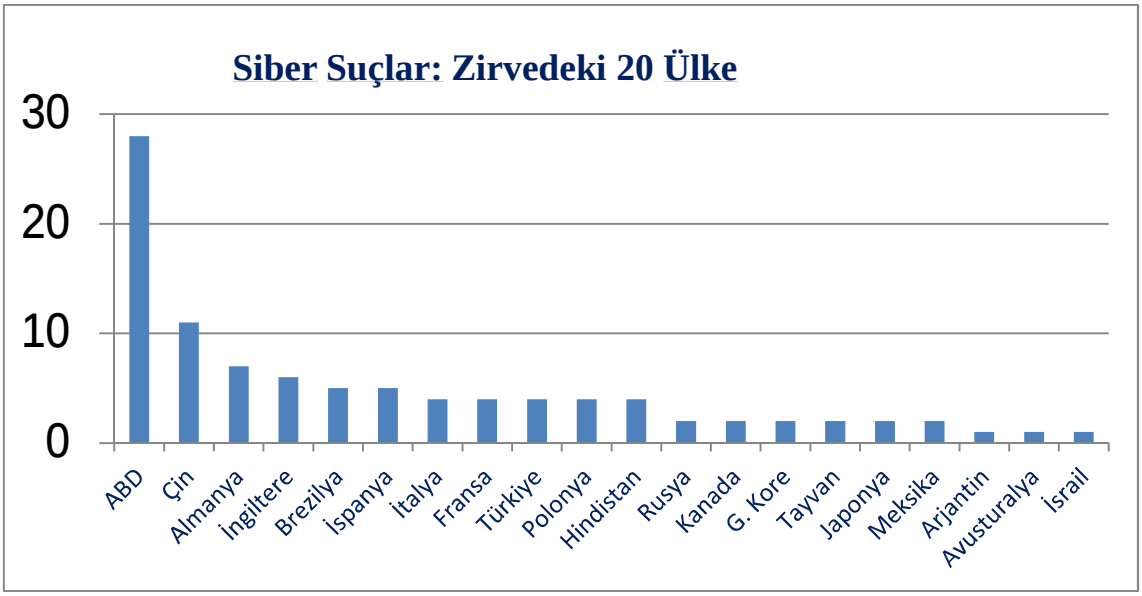
İnternetin terörist amaçlarla kullanımı sadece gelişmiş ülkeleri tehdit eden bir durum olmayıp bilişim alt yapılarını giderek daha fazla alanda kullanan ülkemiz de siber terörden etkilenmiştir. 1999 yılında İstanbul Emniyeti tarafından IBDA-C terör örgütüne yönelik olarak düzenlenen operasyonda, terör örgütüne ait web sitesinde hedef listesi oluşturarak militanların yönlendirildiği, "bomba yapımı ve bombalama, silah atış bilgisi, polis takibi, polis sorgusu, kırsalda yön tayini ve ilkyardım" konularında örgüt

---

94 Öğün ve Kaya, s. 162-163.
95 Öğün ve Kaya, s. 162-163.
96 Bayraktar, **a.g.e.** s. 16.
97 Tezcan Özkan, "Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi", **Yayınlanmış Yüksek Lisans Tezi**, Anadolu Üniversitesi SBE,Eskişehir, 2006, **s.** 83 http://www.ibrarian.net/navon/paper/NTERNET_S_TELER_NE_Y_NEL_K_B_R__ER_K_ANAL_Z.pdf?paperid=17691465

mensuplarının bilgilendirildiği ortaya çıkarılmıştır.[98] İnternet imkanlarının sınır aşan yapısı nedeniyle siber terörün, sadece sosyal ve ekonomik refah seviyesi yüksek Batı toplumları için değil aynı zamanda ülkemiz gibi gelişmekte olan ülkeler için de tehlike arz ettiğini söylemek mümkündür.

Yine konuyla bağlantılı olarak belli bir terör örgütü ile kesin ilişkisi tespit edilemediği için siber terör kapsamında değerlendirilemese de, 2011 yılında gümrük sistemlerinin çökmesi sonucu yaşanan uzun kuyruklar ile Atatürk havalimanında yolcu akışı ve hava trafiğinde aksamalara sebep olan virüs programı[99] hedefin kamuya ait varlıklar olması, mevcut düzende aksamalara neden olarak toplumun huzurunu bozucu etki yapması gibi nedeniyle siber tehdit şemsiyesi altında değerlendirilmektedir.



*Şekil 2.*Siber suçlar: zirvedeki 20 ülke

Kaynak: Symantec, 2015

Çeviri: D.Ermeydan

Symantec tarafından 2015 yılı itibariyle siber suçların en yoğun şekilde yaşandığı 20 ülkeye ait liste yayınlanmış olup şekil 2'de gösterildiği üzere ilk sırada ABD bulunurken, Türkiye dokuzuncu sırada yer almaktadır.[100] Türkiye'nin siber suçları yaratma ve yine bu suçlara maruz kalma oranının dünya sıralamasına göre oldukça yüksek olduğu görülmektedir.

---

98 Özcan, **a.g.m.** 2003

99 Öğün ve Kaya, s. 162-163.

100 İsmail Saygılı, h4cktimes, 2015https://h4cktimes.com/arastirma-ve-analiz/siber-suc-cografyasi-2014te-neler-yasandi.html, e.t: 30.11.2017

Bu kapsamda siber alan, uluslararası ilişkilerde güncel meselelerin yer aldığı kara, deniz, hava sahasına dördüncü bir alan olarak eklenmiş, 2016 tarihli Varşova Zirvesi'nde NATO tarafından operasyonel bir alan olarak resmen tanınmıştır[101]. Buradan yola çıkarak, cephe kavramının mekansal bir olgu olmaktan çıkarak siber alanın önemli bir savaş cephesi haline geldiğini söylemek mümkündür[102].

Siber terörün asıl yıkıcı etkileri, hybrid (karma) ya da asimetrik savaş olarak da adlandırılan savaş yöntemiyle ortaya çıkmaktadır. Bu, siber alanın icadıyla birlikte ortaya çıkan siber çatışmaları da içeren bir savaş türüdür[103]. Harekat sırasında tali güç olarak kullanılan siber saldırılar rakibin temel fonksiyonlarını zayıflatarak, güç dengelerini bozmaktadır.

İsrail'in 2007 yılında Suriye'ye yönelik olarak icra ettiği "Operation Orchard" harekatı(meyve bahçesi operasyonu) esnasında, Suriye radarlarına karşı kullandığı siber kabiliyetlerle siber savaşların klasik bir savaşla paralel olarak icra edildiği görülmüştür.[104] Savaş harekatını destekleyici bir unsur olarak ortaya çıkan siber saldırılar, hedefin bilişim sistemlerini etkisiz hale getirerek, onu savunma ve saldırı gücünden yoksun bırakmak, bilişim sistemlerine sızarak istihbarat edinmek, kritik alt yapılarına saldırarak panik yaratmak ve zarar vermek gibi işlevleri yerine getirerek, savaşın seyrini değiştirebilen önemli bir silah haline gelmektedir.

Rusya Federasyonunun, 2007 yılında, Avrupa'da e-devlet uygulamasına geçen öncü ülkelerden biri olan Estonya'ya yaptığı siber taarruzlar, dünyada bir ülkeye yönelik yapılan devletler arası ilk sistematik siber savaş olarak tarihe geçmiştir[105].

Savaşların ve yıkımın başrolü oynadığı dünya tarihine bakıldığında, keşif ve icatların muharebelerde düşmanı mağlup etmek için etkin şekilde kullanıldığı görülmektedir. Buradan yola çıkarak insanoğlunun en yeni ve en büyük keşfi olan bilişim teknolojisinin de gelecekte meydana gelecek savaşlarda ölüm ve yıkımı arttırmak için daha yoğun şekilde kullanılacağını tahmin etmek hiç de zor olmamaktadır.

Ülkelerin konuya yaklaşımlarının terör kavramına yaklaşımlarıyla paralellik gösterdiğini, tıpkı terör gibi siber teröre karşı da tüm dünya ülkeleri tarafından net bir

---

[101] "Varşova Zirvesi Sonuç Bildirgesi" https://www.nato.int/cps/en/natohq/official_texts_133169.htm e.t.: 27.11.2017

[102] Bayraktar, s. 132.

[103] Ali Poyraz Gürson ve Çağatay Fehmi Göker, "Turkey-Russia Relations After The Cold War Era And The Middle East Policies." **Advances in Social Sciences Research Journal** S. 4.5, 2017, s.24 http://scholarpublishing.org/index.php/ASSRJ/article/download/2823/1670

[104] Bayraktar, **a.g.e.** s. 16.

[105] Bayraktar, **a.g.e.** s. 17.

tanım, tavır ve işbirliği geliştirilemediğini söylemek bu noktada yanlış olmayacaktır. Siber dünyadaki tehditlerin eyleme dönüşmüş halleri siber suç, siber terör ve siber savaş olarak ifade edilebilir.

Söz konusu kavramlarla ilgili hukuki düzenlemelere bakıldığında, siber suçlarla ilgili düzenlemeler mevcutken, siber terörle ilgili gerekli hukuki düzenlemelerin uluslararası alanda işbirliğini sağlayıcı ve bağlayıcı şekilde var olmadığı görülmektedir.

Siber terörizmle mücadelenin en önemli boyutu, hukuki alt yapısının hazırlanmasıdır. Zira gelişmiş ülkelerin ulusal mevzuatlarında, özel bir siber terör yasası bulunmamakla birlikte, suçun işlendiği yerin tespiti, suçluların iadesi, savaş sırasında insanlığa karşı kullanımı noktasında, faillerin ve savaş suçlarından yargılanmasının düzenlenmesi gibi hususlarda herhangi bir bulguya rastlanmamıştır.

Araştırmanın bu noktasında, siber terör saldırısına maruz kalan bir ülke açısından uluslararası mevzuat bağlamında iki görüş bulunduğu görülmüştür. Bunlardan ilki BM Sözleşmesinin 51. Maddesine[106] yer alan meşru müdafaa hakkının kullanımına ilişkindir.[107]

BM Sözleşmesi 51. Madde uyarınca silahlı saldırı ile karşı karşıya kalan bir ülke BM Güvenlik Konseyi gerekli önlemleri alıncaya dek kendisini korumak için gerekli önlemleri alarak müdahale etmek hakkına sahiptir. Buradan yola çıkarak siber terör saldırısına maruz kalan ve kritik alt yapıları tehlike altında bulunan bir ülkenin bu maddeye dayanarak saldırıya müdahale etmek için gerekli önlemleri alması mümkün görünmektedir. Ancak saldırının silahlı olması zorunluluğu noktasından bakıldığında, siber terör saldırısının silahlı bir saldırı olarak nitelendirilip nitelendirilemeyeceği ya da hangi durumlarda silahlı saldırı olarak değerlendirilebileceği tartışma konusudur.

İkinci görüş ise Roma Statüsü'nün 7. maddesinde[108]insanlığa karşı suçlar başlığı altında sayılan *"herhangi bir sivil nüfusa karşı yaygın veya sistematik bir saldırının parçası olarak işlenen öldürme, toplu yok etme, köleleştirme…"* eylemleri ile ilgilidir.

Buna göre madde de belirleyici iki ön koşul olan "eylemin sivil nüfusa karşı yapılması" "eylemin yaygın veya sistematik bir saldırının parçası olması" koşullarının

---

[106] **BM Antlaşması** https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf e.t.: 25.11.2017

[107] Can Kasapoğlu, "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında" **EDAM Siber Politikalar Kağıtları Serisi,** 2017, s. 8. http://edam.org.tr/wp-content/uploads/2017/10/sibersavas_tr_rbs_logo.pdf e.t.: 25.11.2017

[108] **Roma Statüsü** http://sorular.rightsagenda.org/Uploads/UCM%20MEV/Roma%20Stat%C3%BCs%C3%BC.pdf e.t.: 27.11.2017

varlığı halinde terör suçlarının insanlığa karşı suç olarak kabul edilen eylemler kapsamında değerlendirilebileceği ve yargılama yetkisinin Uluslararası Ceza Mahkemesi tarafından yapılabileceği şeklindedir.[109]

Terörün alt başlığı olması nedeniyle yine "eylemin sivil nüfusa karşı yapılması" "eylemin yaygın veya sistematik bir saldırının parçası olması" koşullarını taşıması şartıyla siber terörün de aynı kapsamda değerlendirilmesi gerektiği düşünülmektedir. Kaldı ki insanlığa karşı suçların; uluslararası toplumu bir bütün olarak ilgilendiren çok ciddi suçlar olduğu ve kamu düzenini bozan siber terör suçlarının, özellikle karma bir savaşta yardımcı unsur olarak kullanılması halinde, burada "öldürme" ve 'toplu yok etme' olarak sayılan suçlara vücut verebileceği değerlendirilmektedir.

Tüm bunlara ek olarak 31 Mayıs – 11 Haziran 2010 tarihleri arasında düzenlenen Roma Statüsünü Gözden Geçirme Konferansında alınan 6 Sayılı Karar ile saldırı suçunun tanımı yapılmış olup karar kapsamında, Statü'nün 5/2 maddesi mülga olmuş ve Statü'ye 8 bis, 15 bis ve 15 ter maddeleri eklenmiştir[110].

Roma Statüsüne eklenen 8 bis maddesinin 1'inci fıkrasında "saldırı suçu" unsurlarıyla birlikte tanımlanmış olup buna göre bir devletin siyasi veya askeri eylemlerini etkili biçimde kontrol edebilme veya yönetebilme konumunda bulunan bir kimse tarafından, Birleşmiş Milletler Şartı'nı açıkça ihlal eden bir saldırı fiilinin planlanması, hazırlanması, başlatılması veya icrası olarak tanımlanmıştır[111].

Bu maddeye göre saldırı suçunu devletin siyasi ve askeri eylemlerini etkili biçimde kontrol edebilme yetkisine ve gücüne sahip kimse tarafından işlenebilecek bir suçtur.

Aynı maddenin 2/a bendine göre ise "saldırı fiili", bir devletin silahlı kuvvetlerince, bir diğer devletin topraklarına yönelik olarak yapılan istila veya taarruz ya da ne kadar geçici olsa da, bu tür bir istila veya taarruzdan kaynaklanan herhangi bir askeri işgal veya kuvvet kullanarak başka bir devletin topraklarının tümünün ya da bir

---

[109] Gürkan Doğan "Uluslararası Ceza Mahkemesi ve Terör Suçları Açmazı: Çözüm Açısından Bir Değerlendirme." **Güvenlik Stratejileri Dergisi** S. 15, 2012, s.55. http://dergipark.ulakbim.gov.tr/guvenlikstrtj/article/view/5000098878 e.t.: 23,11,2017

[110] Uğur Bayıllıoğlu , "Uluslararası Ceza Mahkemesinin Yargı Yetkisi Açısından Saldırı Suçuna İlişkin Kampala Düzenlemeleri", Uluslararası Hukuk ve Politika, Cilt:9, Sayı: 33, s. 61

[111] Nergiz Emir, "Uluslararası Ceza Mahkemesi'nin Yargı Yetkisi Bakımından Saldırı Suçu" http://andhd.dergi.anadolu.edu.tr/yonetim/icerik/makaleler/27-published.pdf. e.t: 20.06.2018

bölümünün ilhakı savaş ilan edilmiş olup olmamasına bakılmaksızın saldırı olarak tanımlanmaktadır.[112]

Siber savaşın pek çok örneğinin uluslararası ilişkilerin ortak bir unsuru haline gelmesi göz önüne alındığında bu kavramın da 8bis maddesi kapsamında "saldırı fiili" olarak sayılan bentlere dahil edilmesi yerinde olacaktır[113].

Devletler arası savaş sırasında siber savaş tekniklerinin "saldırı fiili" kapsamına dahil edilmesinin, Uluslararası Ceza Mahkemesinin görev kapsamını genişleterek, bu tarz eylemler sonucunda meydana gelebilecek zararların sorumlularının yargılanabilmesini, böylece siber savaş sırasında işlenen suçların cezasız kalmasının önüne geçilebileceği ifade edilebilir.

1.6. Bilişim Sistemlerinin Suç Yaratıcı Etkisi

Teknolojide meydana gelen gelişmelerin, maliyetlerin azalmasına, maliyetlerin azalmasının da daha çok kişinin bilişim sistemlerinin kullanıcısı haline gelmesine yol açtığı düşünülmektedir. Bilişim suçlarının ortaya çıkmasında bilişim sistemlerinin yaygın şekilde kullanımı önemli bir etkendir.

Bilgisayarın, bilişim suçlarının işlenmesini kolaylaştırıcı yönleri, verilen komutları hiçbir sorgulamaya tabi tutmadan uygulaması nedeniyle, mantık dışı ve dolandırıcılık içeren komutları fark edememesi, para transferini (EFT) çok uzak mesafelerde, çok kısa sürelerde ve çok büyük miktarlarda yapabilmesi ve suçların anonim şekilde işlenmesine olanak tanıması olarak düşünülebilir[114].

İnternetin belirli bir merkezinin olmayışı, başka bir deyişle internetin tam anlamıyla bir "özgürlükler alanı" oluşu, birtakım hukuki sorunları beraberinde getirmektedir. Öte yandan, internetin merkezi bir denetime tabi tutulması da, bireylerin haberleşme hürriyetine, özel yaşamına müdahale olabileceği için tartışma konusu olabilmektedir[115].İnternet faaliyetlerinin denetlenmesinde yaşanan zorluklar nedeniyle hukuka aykırı bir fiil, siber uzay da denilen internet ortamında fark edilmedenrahatlıkla işlenebilmektedir [116] .Bu perspektiften bakıldığında internetin, siber uzayda gerçekleştirilen fiillerin kontrol edilmesinde yaşanılan zorluklar nedeniyle, özgürlük

---

[112] Emir, **a.g.i.s.**

[113] David Scheffer, "The Missing Pieces in Article 8 bis (Agression) of the Rome Statute", http://www.harvardilj.org/2017/04/the-missing-pieces-in-article-8-bis-aggression-of-the-rome-statute/ e.t.:20.06.2018

[114] Mustafa T. Yücel, "Bilişim Suçları", **Ankara Barosu Dergisi**, S. 49 (4), Ankara, 1992, s.505.

[115] Taşkın, **a.g.e.** s. 15.

[116] Karagülmez, **a.g.e.** s. 301.

güvenlik dengesini sağlamayı zorlaştıran bir yapıya sahip olduğu sonucuna varılmaktadır.

Bilgisayar sistemlerin büyük miktarda bilgiyi tutabilecek kapasitede olması ve bilgi-işlem sırasında yapılan hatalar, bilişim suçu faillerine fırsat yaratmaktadır. Bilişim sistemlerinin diğer bir suç yaratıcı unsuru ise, bu sistemlerde işlenen suçlarda mağdurun belli olmaması, suçun sisteme karşı işlenmesidir. Bu durum ise failin tespitinde sorunlarla karşılaşılmasına neden olmaktadır[117].

Güncel bilgiler ışığında değerlendirildiğinde, bilişim sistemlerinde bilgilerin manyetik ortamlarda saklanmasının, geride hiçbir iz bırakmadan bu bilgilerde değişiklik yapılmasına neden olduğu ifade edilebilir. Buna ek olarak verilerin disket, compact disk (CD), data traveler gibi taşıma kolaylığı olan cihazlara kopyalanarak bilişim sistemi dışına çıkartılabilmesi bilişim sistemlerinin hedef çekiciliğini arttıran unsurlar arasında sayılabilir.

Tüm bunlara ek olarak internetin güvenilir bir kullanıcı grubuna hizmet edeceğinin düşünülmesi nedeniyle, IP paketleri içerisindeki bilgilerin orijinal halinin korunmasına yönelik hiçbir şifreleme önlemi alınmamıştır. Dolayısıyla, ileri seviyede bilgi sahibi bir kullanıcı IP paketleri içerisindeki bilgileri istediği gibi değiştirebilmektedir[118]. Bilişim suçlarının bu sistemler hakkında teknik bilgi sahibi olunmasını gerektiren bir suç türü olduğu söylenebilir. Bilgili olma şartı, bir yandan bu nitelikte kişilerin fazla olmaması nedeniyle uç etki gösterirken, diğer yandan suç yaratıcı unsur olarak ortaya çıkmaktadır[119].

Demirbaş'a göre, bilişim suçlarında bilinmeyen alan oldukça geniş olup, suçların büyük kısmı beyaz yaka suçlarına ilişkin özellikler göstermektedir[120]. Taşkın ise, bilgisayarın pek çok eve girdiği ve internetin oldukça yaygınlaştığı günümüzde bilişim suçlarının sadece uzmanların tekelinde bir suç tipi olarak görülmemesi gerektiği görüşünü savunmaktadır[121]. Şu halde fail bakımından "işin uzmanı olma" geçerli bir ölçüt olarak değerlendirilemeyecektir.

---

[117] Emin Doğan Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları", **Marmara İletişim Dergisi**, Sayı 1, İstanbul, 1992, s. 20. http://dspace.marmara.edu.tr/bitstream/handle/11424/2788/5000011620-5000018676-1-PB%20(1).pdf?sequence=1

[118] Gökhan Bayraktar, **Siber Savaş ve Ulusal Güvenlik Stratejisi**, Yeni Yüzyıl Yayınları, İstanbul, 2015, s. 100.

[119] Aydın, s. 18.

[120] Timur Demirbaş, **Kriminoloji**, Altıncı Basım, Seçkin Yayıncılık. Ankara, 2016, s. 300.

[121] Şaban Cankat Taşkın, **Bilişim Suçları,** Beta Yayınları, Bursa, 2008, s. 11.

Suçların çoğu kamuoyuna duyurulmamakta, tüzel kişilikler açısından sadece programların çalınması, banka ve benzeri kuruluşlarda bulunan otomatik para veya bilet veren makinelerin kötüye kullanılması gibi olaylar polise ihbar edilmektedir. Gerçek anlamda bilgisayar suçlarının polise bildirilme oranı son derece azdır[122] . Bilişim suçlarının tespitinde yaşanan zorlukların bir nedeni de suçların "köstebek" olarak adlandırılan kurum içi çalışanlar vasıtasıyla işlenmeleri, dolayısıyla takip edilememeleridir[123]. Bu suçlar, klasik yöntemlerle işlenen suçlara göre, daha ağır sonuçlar doğurmaktadır.

Bilişim sistemlerinin anılan özelliklerine bakarak, ciddi tedbirler alınmaması halinde gelecekte, bilişim suçu işleme yöntemlerinde ve bilişim suçu fail ve mağdur sayılarında hızlı bir artış olacağı öngörülebilir. Mali açıdan değerlendirildiğinde, her yıl bilişim suçlarının dünya ekonomisine verdiği zarar yaklaşık 1 trilyon dolar civarındadır[124].

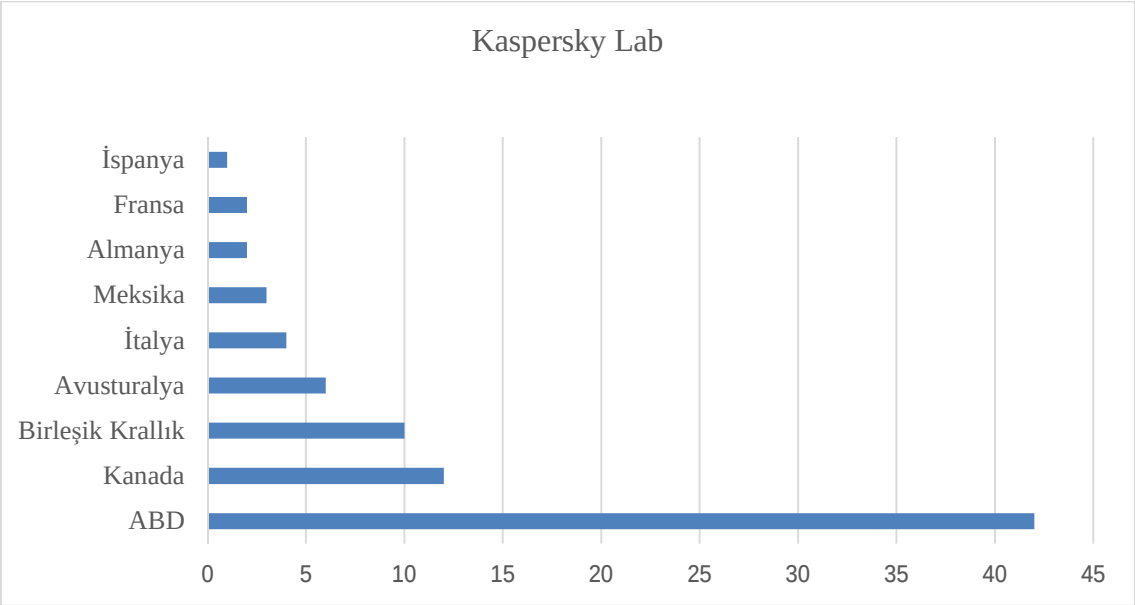
Bunun için öncelikle, bilişim suçlarının tanımının, internete bağlantısı olan akıllı telefon, tablet ve ev sistemleri gibi unsurları da kapsayacak şekilde yapılması gerekmektedir. Hukuki düzenlemelerde özgürlük güvenlik dengesinin hassas şekilde gözetilmesi de önemli bir başka konudur. Sanal dünyada işlenen suçların cezasız kalmaması için ülkesel bazda hızlı ve etkin yasa yapma sistemlerinin oluşturulması ve bu sistemlerin uluslararası alanda entegrasyonun sağlanmasının yararlı olacağı değerlendirilmektedir.

1.7. Bilişim Suçu Faillerinin Genel Özellikleri

Bilişim suçu faillerinin sayısı her geçen gün artmaktadır. Ancak faillerin teknik seviyelerindeki, hedeflerindeki, kullandıkları yöntemlerdeki farklılıklar nedeniyle hepsini aynı isimle etiketlemek mümkün değildir. Bilişim teknolojilerini suç işlemek maksadıyla kullanan bu kişiler çok geniş bir yelpazenin parçalarıdır. Şekil3'de görüleceği üzere bilişim suçlarından en fazla etkilenen ülkeler, bu sistemleri en uzun süredir ve en yaygın şekilde kullanan ülkelerdir.

---

[122] Demirbaş, **a.g.e.** s. 300.
[123] Hasan Dursun, 'Bilgisayar İle İlgili Suçlar", **Yargıtay Dergisi**, S. 24, Ankara, 1998, s. 337.
[124] Robert, K. Knake **Internet Governance in an Age of Cyber Insecurity.** No. 56. Council on Foreign Relations, 2010, s. 5 https://books.google.com.tr/books?hl=tr&lr=&id=FhuC1gIm_1AC&oi=fnd&pg=PR7&dq=Robert,+K.+Knake+Internet+Governance+in+an+Age+of+Cyber+Insecurity.+No.+56.+Council+on+Foreign+Relations,+2010,+s.+5+&ots=MXk2UeNIdJ&sig=mvh1nSgAIhquBh2f7ipXbtODIYQ&redir_esc=y#v=onepage&q&f=false



Şekil 3. Amerika ve Kuzey Avrupa ülkelerinin siber suçlardan etkilenme oranı

Kaynak:Namestnikov, 2012

Çeviri: D.Ermeydan

Görsel kaynaklara yönelik yapılan tarama sırasında, siber suçlara ilişkin araştırmaların, Şekil 3'te de ifade edildiği üzere bu suçlardan en çok etkilenen ülkeler olan ABD ve Avrupa ülkelerinde diğer ülkelere oranla daha yoğun olarak yapıldığı sonucuna varılmıştır. Bu nedenle bilişim suçu failleri ile ilgili yapılan araştırma sonuçları da daha çok bu ülkelerin verilerini yansıtmakla birlikte Demirbaş'a göre failler genelde 24 ila 33 yaşları arasındaki eğitimli ve genellikle erkeklerdir[125].

Bilişim suçu failleri normal insanlara göre daha uyanık, sabırsız, maceraperest ve teknolojik iddialaşma içinde bulunan kişiler olup; para kazanmaktan çok, kendi yeteneklerini ispatlamak arzusu taşıyan bir yapıya sahiptirler. Bir başka tespite göre ise failler para elde etmekten çok kendi yeteneklerini ispatlama arzusundaki kişilerdir[126].Örneğin, Birinci Körfez Savaşı sırasında Hollandalı bir grup genç Pentagon bilgisayarına sızarak ABD savaş operasyonları ile ilgili hassas bilgileri kopyalamışlardır.[127] Başlangıçta failleri bu tür suça iten sebebin kişinin zekasını ve yeteneklerini ispatlama isteği olduğu söylenebilir.

Failler çeşitli açılardan değerlendirildiğinde, sosyal anlamda başarılı, teknik bilgi seviyeleri yüksek ve işyerlerinde değerleri yeterince anlaşılamadığı duygusuna kapılmış

[125] Demirbaş, **a.g.e.** s. 301

[126] Yazıcıoğlu, **a.g.e.** s. 104.

[127] David L.Carter ve Andra J. Katz. "Computer Crime: An Emerging Challenge For Law Enforcement." **FBI L. Enforcement Bull.** S. 65, 1996, s. 1.

gençlerdir[128].Psikolojik olarak hak ettikleri destek ve ilgiyi göremedikleri inancıyla "kendilerine yapılan haksızlıkları, veriler üzerinde oynamak, ya da elektronik hilelerle elde ettikleri menfaatler vasıtasıyla dengelediklerine inanan bu kişiler, fiillerini şirket veya banka gibi tüzel kişiliklere karşı gerçekleştirdikleri için, bu fiillerin somut mağdurları bulunmadığı, dolayısıyla kimseye zarar vermedikleri inancıyla, psikolojik yönden suçluluk duygusu taşımamaktadırlar[129]. Bilişim suçu failinin amacı da klasik suçlu amacından farklıdır. Genel olarak amaç bir yarar sağlamak ya da zarar vermek olmayıp yeteneklerini sergilemektir [130].

Suçluların bir çoğu, bazen kişi ya da kurumların itibar kaybetmemek için ihbar etmeyeceklerinden bazen de bu eylemlerini karşılayacak ceza normunun bulunmaması nedeniyle işledikleri suçun cezasız kalacağına güvenerek hareket etmektedirler [131]. ABD'de yönetici ve programcılar arasında bilgisayar kullanımıyla ilgili davranışlar üzerinde yapılan bir anket çalışmasında, rakip şirkette çalışan arkadaşına çalıştığı şirketten elde ettiği bir programı verip kullanmasını sağlamak, izinsiz olarak bir programı başka bir tanesi ile değiştirmek veya başka bir çalışanla program takas etmek, gibi bazı hukuka aykırı eylemlerin programcılar tarafından hukuka aykırı olarak kabul edilmediği ortaya çıkmıştır[132].

Tüm bunlara ek olarak, Almanya ve Amerika'daki faillerin çalışma hayatları boyunca sıkça iş değiştirdikleri tespit edilmiştir [133]. Bilişim suçluları, eylemleri sonucunda bilişim sistemlerinin güvenliği konusunun önem kazandığı ve ilerleme sağlandığı, böylece toplumu ileri taşıyarak önemli bir görevi yerine getirdiklerini düşünmektedirler. Bilişim suçu faillerini, suç işlemeye yönelten nedenler arasında; işten çıkarılma veya işteki çeşitli hoşnutsuzluklar sebebiyle intikam alma duygusu, ekonomik nedenler, bilgisayarı aşabilme duygusu, rekabet duygusu sayılabilir[134]

Bilişim suçu faillerinin belirtilen özelliklerle sınırlanmasının mümkün olmadığı, çalışmalarda belirtilen fail profilinin çok dışında uç örneklerin de bulunmasının muhtemel olduğu, ancak saha çalışmalarında temel alınan verilerde, görülme sıklığının sonucu etkileyen en önemli etmen olması nedeniyle, genelleme yapıldığı görülmüştür.

---

[128] Demirbaş, **a.g.e.** s. 301.
[129] Demirbaş, **a.g.e.** s. 301.
[130] Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **Ankara Üniversitesi Siyasal Bilimler Dergisi**, S. 49, Ankara, 1994, s. 158.
[131] Demirbaş, **a.g.e.** s. 300.
[132] August Bequai, A Guide to Cyber Crime Investigationts. Computer And Security http://www.sciencedirect.com/science/article/pii/S016740489980056X(1998) e.t.: 03.11.2017
[133] Demirbaş, **a.g.e.** s. 301.
[134] Demirbaş, **a.g.e.** s. 302.

1.8. Bilişim Suçu Mağdurlarının Genel Özellikleri

Kriminoloji de "suçta siyah sayılar" olarak ifade edilen bilinmeyen alan bilişim suçlarında oldukça yüksek olup, %90-95'ler seviyesine ulaşmaktadır. Bunun nedeni, mağdurların kendilerini kamuoyundan saklamak istemeleridir[135]. Bilişim suçu failleri teknik bilgileri sayesinde bilişim sistemlerine yetkisiz erişim sağlayarak gerçek kişilere yönelik kişilik haklarını ya da özel hayatlarını ilgilendiren özel bilgilere ulaşabilmekte, tüzel kişilerin ürünlerinin içeriklerinden, stratejik planlarına, araştırma geliştirme (ar-ge) çalışmalarından, mali durumları ile ilgili ticari sırlarına kadar her türlü veriye erişebilmektedirler. Elbette ki anılan türden bilgiler hem gerçek kişiler hem de tüzel kişiler açısından toplumda duyulması istenilmeyecek türdedir. Bu bilgilerin internet ortamında sosyal medyada paylaşılması kişileri ve kurumları zor durumda bırakmakta, mağduriyetleri telafi edilemez boyutlara varmaktadır.

Gerçek kişiler açısından bakıldığında, bilişim suçu mağdurlarının çoğunluğunu kadınlar oluşturmaktadır. Bilişim suçlarının, kadınlar üzerinde erkeklerden çok daha fazla olumsuz etkisi vardır. Ne yazık ki kadınlar,dünya genelinde bu suçlardan erkeklere göre daha fazla etkilenmektedirler. Bilişim sistemleri aracılığıyla işlenen hakaret ve özel bilgilerin açıklanması nedeniyle mağdur olan kişilerin itibarları zedelenerek aşağılanmaları ve bazı koşullarda kriminolojideki anlamıyla damgalanmaları söz konusu olmaktadır.[136]

Çevrimiçi hizmet kullanan yetişkinlerin % 69'u bilişim suçu mağduru olmaktadır[137]. Bu tespit, bir internet kullanıcısının bilişim suçu mağduru olma riskinin büyüklüğünü ortaya koyması açısından oldukça önemlidir. Bunun yanında, bilişim suçu mağduru denildiğinde ilk akla gelen gerçek kişiler olmakta beraber, özellikle ekonomik amaçlarla işlenen bilişim suçu mağdurları büyük ticari şirketlerdir.

Amerika'da bilgisayar kullanılarak işlenen suçlara yönelik Donn B.Parker tarafından yapılan araştırmada; bankalar ile sigorta şirketlerinin diğer alanlardaki tüzel kişiliklere oranla daha yoğun olarak bilişim suçlarına maruz kaldıkları sonucuna

---

[135] Demirbaş, **a.g.e.** s. 302.

[136] Debarati Halder and Karuppannan Jaishankar **Cyber crime and the victimization of women: laws, rights and regulations**. Information Science Reference, Manonmaniam Sundaranar University Press, India, 2012.

[137] Christopher Hooper, Ben Martini, and Kim-Kwang Raymond Choo. "Cloud Computing And İts İmplications For Cybercrime İnvestigations İn Australia." **Computer Law & Security Review,** 29.2 2013, p. 152-163. http://search.ror.unisa.edu.au/record/UNISA_ALMA51109818270001831/media/digital/open/9915914119501831/12143169490001831/13143168750001831/pdf

varılmıştır[138] . Şirket yöneticileri, kolluğun şirketin iç işlerine karışarak kurumun işleyişi, sırları, planları konularında detaylı bilgi sahibi olmalarını istememeleri ve bu tür bir araştırmanın şirketin piyasalarda saygınlık kaybetmesine neden olacağına inanmaları nedeniyle mağduriyetlerini gizli tutmaktadırlar[139]. Bu durumun ise bilişim suçu faillerinin işledikleri suçun cezasız kalması sonucuna yol açtığı, böylece bu şirketlerin, daha çok fail için çekici birer hedef haline geldiği görülmektedir. Bazı şirketler, bilişim suçları sonucunda meydana gelen yıllık %5'e kadar olan zararları araştırma yapmaksızın olağan kabul etmektedirler[140]. Tüzel kişiliklerin bilişim suçları ile mücadele etmek yerine bu suçlar dolayısıyla oluşan mağduriyetlerini sineye çekmelerinin bir tür kartopu etkisi yarattığını ve mağduriyetlerini arttırdığını söylemek mümkündür.

Dünya genelinde bilişim suçlarıyla mücadelede, teknik önlemler alınmasının ve mevzuat anlamında hukuki düzenlenmeler yapılmasının, ulusların güvenlik politikaları açısından gittikçe daha çok önem verilen bir konu haline geldiği görülmektedir.

Bilişim suçlarına yönelik olarak yapılan araştırma sonucunda; bilişim suçlarına karşı koymanın ilk adımının, bilişim sistemlerini kullanan bireylerin bilişim sistemlerini kullanma etiği ve bu suçlardan korunma yöntemleri konularında eğitilmeleri olduğu söylenebilir. Zira güvenliği tehdit eden unsur bilişim sistemleri değil, bu sistemleri suç işleme saikiyle kullanan insan iradesidir.

Sanal alemde işlenen bilişim suçlarının cezasız kalmaması için ülkelerin ulusal mevzuatlarında bu suçlara ilişkin düzenlemeler yapmaları sorunun çözümünün önemli bir halkasını oluşturmaktadır. Ancak bu düzenlemeler yapılırken, özgürlük güvenlik dengesinin sağlanması konusunda özenli davranılması bir başka unsurdur. Bilişim sistemlerinin temeli olan internetin özgürlükçü yapısının,güvenliği sağlama konusunda hem olumlu hem de olumsuz etkileri ortaya çıkmaktadır.

---

[138] Johanna Granville, "The Dangers Of Cyber Crime And A Call For Proactive Solutions" **Australian Journal of Politics and History,** Vol. 49 Clemson University, 2003, s. 102.
[139] Demirbaş, **a.g.e.** s. 303.
[140] Demirbaş, **a.g.e.** s. 303.

İKİNCİ BÖLÜM

KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SUÇLARI VE AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

2.1. Karşılaştırmalı Hukukta Bilişim Suçları

Her ülkenin ekonomik durumu, teknolojik altyapısı, sosyolojik yapısı, internet kullanıcı sayısı ve profili birbirinden farklıdır. Bu durum, ülkeler bazında, bilişim suçlarının işlenme ve bilişim suçlarına maruz kalma sıklığını da farklılaştırmaktadır. Anılan etmenlere bağlı olarak ülkelerin,bilişim suçlarıyla mücadelede kararlılıkları ve etkili olma güçleri de farklılık göstermekle beraber, bilişim suçlarının tüm dünya ülkelerinin ortak sorunu haline geldiği ifade edilebilir. Dolayısıyla bilişim suçlarının niteliği, hızlı işlenebilmesi, uluslararası sonuçlar doğurması bu suçlarla ilgili yasal düzenlemeleri yapma ihtiyacını ortaya çıkarmıştır[141].

Karşılaştırmalı hukuk açısından bilişim suçları değerlendirilirken; hem ülkelerin kendi iç hukukları bazında bu alanda yürürlüğe konulan yasaların bulunduğu hem de Avrupa Konseyi Siber Suç Sözleşmesinde olduğu gibi uluslararası sözleşmeye imza atılması suretiyle, uluslararası anlamda uygulanan yasaların bulunduğu görülmektedir.

Bilişim suçlarına ilişkin düzenlemelere, ülkelerin kendi iç hukukları perspektifinden bakıldığındaysa Kıta Avrupası ve Anglo-Sakson hukuk sistemi olmak üzere iki tür hukuk sistemine göre normlar konulduğu ifade edilebilir.[142] Araştırmada yer alan ülkelerden İngiltere ve ABD'nin Anglo-Sakson hukuk sistemine göre, diğer ülkelerin ise Kıta Avrupası hukuk sistemine göre yasalar oluşturduğu görülmektedir.

Ülkeler açısından bir başka ayrım ise yönetim şekillerine göre ortaya çıkmaktadır. Örneğin ABD federe devletler topluluğu şeklinde örgütlendiğinden topluluğu oluşturan her devletin tıpkı diğer hukuk alanlarında olduğu gibi, bilişim hukuku alanında da kendine özgü federal yasalarının bulunduğu, bunun yanında üniter şekilde yönetilen, Almanya, Japonya, Fransa gibi ülkelerin ise tüm ülkeyi kapsayan bilişim hukukuna ilişkin yasaları bulunduğu değerlendirilmektedir.

---

[141] Ebru Altınok ve Ali Fatih Vural, "Bilişim Suçları" **Denetişim Dergisi,** 2011, http://dergipark.gov.tr/download/article-file/208853 e.t.: 10.11.2017

[142] Kemal Gözler, **"Genel Hukuk Bilgisi",** Yedinci Baskı,Ekin Basım Yayım Dağıtım, Bursa, 2008, s. 3-4 http://www.anayasa.gen.tr/ghb.pdf e.t.: 13.02.2018

Bilişim suçlarına ilişkin düzenlemelerin uluslararası alanda değerlendirilmesiyle ilgili olarak, bilinen ilk bilişim suçlarının 1970'li yıllarda ortaya çıktığı düşünülürse konunun uluslararası zemine taşınmasında çok zaman kaybedilmediği, ilk kez 1980'li yılların ortalarından itibaren BM Suçların Önlenmesi ve Suçluların Tretmanı Kongrelerinde bilişim suçlarıyla mücadelede çözüm arayışlarının gündeme geldiği görülmektedir.[143]1994 yılında BM Genel Kurulu'nun 1990 tarihli 45/121 sayılı kararına dayanılarak, bilgisayarlarla alakalı suçların önlenmesi ve denetimine dair elkitabı yayınlanmış, 2002 yılında, 56/121 sayılı bilişim teknolojilerinin suç işlemek amacıyla kötüye kullanılmasına karşı mücadele kararı alınmıştır. Daha sonraki yıllarda da, çeşitli Genel Kurul kararları ile siber suçlar meselesine değinilmiş, ayrıca, BM nezdinde, Siber suçlara dair Hükümetlerarası Uzmanlar Grubu da kurulmuş ve ilk toplantısını 2011'de yapmıştır[144].

Bu çalışmalara paralel olarak 1996 yılından itibaren Avrupa Topluluğu kapsamında konuya ilişkin çalışmalar Siber Suç Uzmanları Komitesinin kurulması ile ivme kazanmış, bu komitenin 1997 yılında başladığı çalışmalar sonucunda oluşturulan Avrupa Konseyi Siber Suç Sözleşmesi 23 Kasım 2001 tarihinde Budapeşte'de düzenlenen Siber Suçlar Uluslararası Siber Suçlar Konferansında imzaya sunulmuştur.[145] Avrupa Konseyi Siber Suç Sözleşmesine aralarında Türkiye'nin de bulunduğu pek çok ülke imza atmış olup, sözleşmenin uluslararası alanda siber suçlarla mücadelede dünya genelinde kabul gördüğünü ve bu haliyle misyonunu aştığını söylemek mümkündür.

Bilişim suçlarının neredeyse tüm dünya ülkelerinin sorunu haline gelmesi ve bu nedenle dünya genelinde bilişim alanında hukuki düzenlemelerin bulunması nedeniyle yer yüzünde mevcut tüm ülkelerin mevzuatlarının incelenmesi mümkün olmamış, araştırma kapsamına sınırlı sayıda ülke dahil edilebilmiştir. Kapsama dahil edilen ülkeler; bu suça yönelik ilk düzenlemelerin anavatanı olması nedeniyle ABD, Birleşmiş Milletler Güvenlik Konseyinin daimi beş üyesinden diğer dördü olan, Birleşik Krallık, Rusya, Çin Halk Cumhuriyeti ve Fransa ile yine bu alanda önemli yasal düzenlemeleri bulunması nedeniyle Almanya ve Japonya olmuştur.

---

[143] Sınar, s. 767.

[144] Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği" **Prof. Dr. Nur Centel'e Armağan**, 2013, s.1239 http://dergipark.gov.tr/download/issue-file/517 e.t. 15.11.2017

[145] Kurt, **a.g.e.** s. 88-89.

2.1.1. ABD ve Bilişim Suçları

Bilgisayarın anavatanı olan ABD bunun bir sonucu olarak bilişim suçlarıyla mücadeleyi başlatan ilk ülke olmuştur. Eyaletlerden oluşan bir birleşik devletler olduğu için her eyaletin kendine has kanunları bulunduğu gibi ayrıca tüm ülkeyi kapsayan kanuni düzenlemeler bulunmaktadır[146].

ABD' de bilişim suçları hem federal devlet, hem de eyalet kanunlarında yer almaktadır. Eyalet kanunlarının çok sayıda olması ve her eyaletin farklı bir mevzuatı olması nedeniyle eyalet kanunlarına değinilmemiş, bilişim suçları ile ilgili federal kanunlar Tablo 3'de gösterilmiştir.

Tablo 3.

Amerika Birleşik Devletlerinde Bilişim Suçlarına Yönelik Federal Kanunlar

ABD'de Bilişim Hukukuna Yönelik Federal Kanunlar		
1984 tarihli	Counterferit Access Device and Computer Fraud and Abuse Act	Bilgisayar Sahtekarlığı ve Bilgisayarın Kötüye Kullanılması Kanunu
1986 tarihli	Computer Fraud and Abuse Act	1984 tarihli kanuna üç yeni madde eklenmiştir.
1986 tarihli	Electronic Communications Privacy Act	Elektronik Haberleşme Gizlilik Yasası
1997 tarihli	Internet Gambling Prohibition Act	İnternette Kumarın Önlenmesi Yasası
1998 tarihli	Child Online Prevention Act	Çocukların Online Yayınlardan Korunması Yasası
2001 tarihli	USA Patriot Anti Terrorism Act	Anti Terörizm Yasası

Kaynak: Değirmenci (2003)

1984 tarihli kanun üç tip suç öngörmektedir. Birincisi, atom enerjisi, savunma veya dış politika konularında gizli bilgileri elde etmek ve bunları ABD aleyhine veya başka bir ülke yararına kullanmak amacıyla yetkisiz olarak bilgisayarlara girme eylemi, ikincisi finansal bilgiler elde etmek amacıyla gayri meşru şekilde bilgisayarlara

[146] Kurt, **a.g.e.** s. 99.

girilmesiveya bunların kullanılması, üçüncüsü hükümet tarafından kullanılan bilgisayarlardaki bilgilerin tahribi, değiştirilmesi veya yok edilmesi fiilleridir[147].

1986 tarihli Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı(Computer Fraud and Abuse Act) isimli kanun ise, bilişim suçlarına yönelik en temel kanundur. Bu kanununda bilişim suçları,öncelikle sistemin özelliği bakımından sınıflandırılmış, "koruma altındaki bilgisayar (protected computer)" kavramına yer verilmiştir. Koruma altındaki bilgisayar "finansal bir kurum ya da devlet kurumlarına münhasıran kullanılan veya bunlarca dolaylı olarak kullanılıp suç fiilinin bunları etkilediği veya ABD dışında da olsa eyaletler arası ya da uluslararası ticaret veya iletişim maksadıyla kullanılan bilgisayardır." Burada dikkat edilecek olursa bilişim sistemine karşı işlenen suçların cezalandırılmaya ve bilişim sistemlerinde korunan bilgilerin güvenliğinin sağlanarak, mağduriyetin önlenmeye çalışıldığı görülmektedir. Aynı kanunda öngörülen cezalar failin motivasyonuna göre de ayrılmaktadır, kişinin siyasi, ideolojik motivasyonla mı yoksa adi suç olarak da tanımlanan haksız çıkar elde etmek amaçlı mi hareket ettiği suçun mahiyeti ve cezanın tayini açısından önem taşımaktadır. Buna ek olarak yorum farklılığına sebebiyet vermemek maksadıyla bilgisayar, finansal kurum, zarar, kayıp gibi pek çok temel kavramın tanımlarına yer verilmiştir[148].

1984 ve 1986 tarihli kanunlara korunmaya çalışılan değerin, devletin önemli ve gizli bilgilerinin saklandığı ya da ülkenin kritik öneme haiz alt yapılarını işleten bilişim sistemleri olduğu anlaşılmaktadır. Bu sistemlere yönelik eylemlerin siber suçlardan çok siber terör eylemleri ile örtüşmesi nedeniyle anılan yasaların da aslında siber terör tehlikesine karşı yürürlüğe konulmuş oldukları ifade edilebilir.

Tüm bunların yanında Federal Temel Kanunda bilgisayarlar kullanılarak müstehcen nitelikte materyaller oluşturulması bunların eyaletler veya dış ticaret yoluyla nakledilmesi, küçüğün rızaen veya kandırılarak, cinsel içerikli bir görsel materyalde oynatılması ve bu materyalin nakledilmesi, küçüğe ait görüntülerin daha sonradan seksüel içerikli kullanılacağını bile bile nakledilmesi, çocuk pornografisi de suç olarak düzenlenmiştir[149].

---

[147] Yazıcıoğlu, **a.g.e.** s. 193.

[148] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", **Uluslararası Güvenlik ve Terörizm Dergisi,** Sayı 4, Ankara, 2013,s. 150-151. https://s3.amazonaws.com/academia.edu.documents/37825457/Siber_Suclar_ve_Turkiyenin_Siber_Guvenlik_Politikalari.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523810782&Signature=99Akwi3eBHCL8YuDaj3oyLjJW40%3D&response-content-disposition=inline%3B%20filename%3DSiber_Suclar_ve_Turkiyenin_Siber_Guvenli.pdf

[149] Hüseyin Çeken, "ABD'de İnternet Yoluyla İşlenen Suçlara İlişkin Düzenlemeler", **Askeri Adalet Dergisi**, S. 114, 2002, s. 74.

1986 tarihli Elektronik Haberleşme Gizliliği yasası ise genel anlamda kredi kurumları ile müşterileri arasında elektronik mali kaynakların kullanımı konusunda karşılıklı hak ve sorumlulukları düzenlerken aynı zamanda bilgisayarlara meşru olmayan usullerle girilmesi ve bu suretle kullanılmasına ilişkin eylemleri de suç haline getirmektedir. Kanun, bankamatik kartlarının gayri meşru kullanımını, sahtesinin yapımını, sahte, tahrif edilmiş veya hukuk dışı yollardan elde edilmiş ya da diğer eyaletler veya dış memleketlerde çalınmış bir kartın kullanımını da suç haline getirmektedir. Ayrıca hukuk dışı yollardan elde edilen kredi kartlarının çıkar amacıyla kullanılması ve bu tür kartların ticareti de yasaklanmıştır[150].

Konunun başında da belirtildiği gibi ABD'yi oluşturan devletlerin her birinde bunlardan ayrı bir kısım düzenlemeler bulunmaktadır. Eyalet yasaları federal yasalara göre daha ayrıntılı düzenlemeler içermektedir. Ayrıca tüm eyaletlerde de suç tanımlamasında bir paralellik bulunmamaktadır[151].

Bilişim suçlarından en çok etkilenen devletlerden biri olarak ABD'de konuya ilişkin her alanda yasal düzenlemeler yapılarak bu suçla etkin şekilde mücadele edilmeye çalışıldığı, ancak Roma Statüsünde olduğu gibi uluslararası sözleşmelere imza atmak hususunda isteksizlik politikasını Avrupa Konseyi Siber Suç Sözleşmesini imzalamak konusunda da sürdürdüğünü ifade etmek mümkündür.

Özellikle bilişim suçlarının en çok üretildiği ülkelerden biri olması nedeniyle ABD gibi çok gelişmiş bir devletin AKSSS'ye imza atmayarak bir anlamda bu şemsiye altında uluslararası işbirliğine katkı sağlamayı reddetmesinin bu suçla mücadelede oldukça büyük bir kayıp olduğu söylenebilir.

2.1.2. Almanya ve Bilişim Suçları

Alman Ceza hukuku (Strafgesetzbuch-StGB)Kıta Avrupası sisteminebağlı kalarak, bilişim alanında suçları Türk hukuk sisteminde olduğu gibi ayrı bir başlık altında ve özel bir bölümde ele almak yerine, ihlal edilen hukuki yararlara göre ilgili maddeler içinde düzenlemiştir[152] ,Örneğin bilgisayar ağına girerek bilişim sistemi içindeki bilgilere ulaşmak, bu bilgisayarlarla korunan sırra ulaşmak demek olduğundan bu suç sır aleyhine işlenen suçlar başlığı altında yer alır.

---

[150] Yazıcıoğlu, **a.g.e.** s. 191.
[151] Kurt, **a.g.e.** s. 101.
[152] Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.14, S.2, Ankara, 2010 s. 285. http://webftp.gazi.edu.tr/hukuk/dergi/14_2_10.pdf

Alman Ceza Kanunu'nun 11/3, 176, 176a, 184, 202a, 263a, 269, 271, 274/2, 303a, 303b, 303c maddeleri internet bilgisayar suçluluğu alanında özel olarak düzenlenmiş maddelerdir [153] Alman Ceza Kanunu hukuka aykırı olarak bilişim sistemlerine girmeyi suç oluşumu için yeterli görmemekte, verilerin ele geçirilmesi koşulunu da aramaktadır.

Yasa bu yönüyle AKSS 2. Maddesinde tanımlanan "yasadışı erişim" suçu ile tam olarak örtüşmemektedir. 2. Madde de yasadışı erişim suçunun oluşumu için bilişim sistemine haksız olarak erişim sağlamak yeterli görülmüşken, Alman Ceza Kanunu sadece yetkisiz erişimi yaptırım altına almamış olup eylem, kendisi veya üçüncü bir kişi yararına, kendisine ait olmayan, başkalarının girişine açık bulunmayan ve emniyete alınmış verilerin yetkisiz olarak ele geçirilmesi durumunda, suç haline gelmektedir[154].

Bunun dışında Almanya'da 13 Temmuz 1997 yılında kabul edilen Teleservisler Kanunu ile internet yayınlarından doğan ceza sorumluluğunun esasları belirlenmiştir. Bura göre internette yer alan içeriğin suç unsuru ihtiva etmesi durumunda içerik sağlayıcı genel hükümlere göre sorumlu kabul edilmektedir[155]Buna ek olarak Fikri Haklar Kanunu, Haksız Rekabet Kanunu, Telekomünikasyon Müşterilerin Korunmasına İlişkin Tüzük, Verilerin Korunması Hakkında Kanun da bilişim suçlarıyla ilgili hükümler barındırmaktadır[156].

Alman ceza hukukundaki bu düzenlemelerin, gerek kapsam, gerekse düzenleniş şekillerine yöneltilen bazı haklı eleştirilere rağmen, AB taleplerini, özellikle de Avrupa Konseyi Siber Suç Sözleşmesi'nden kaynaklanan yükümlülükleri gereğince karşıladıklarından şimdilik yeterli oldukları söylenebilir[157].

---

153 Schönke, 1996, s.354 Akt. Kurt, **a.g.e.** s, 106.
154 Yazıcıoğlu, **a.g.e.** s. 396.
155 Rüya Şamlı, "Türk ve Dünya Hukukunda Bilişim Suçları" (2010).. Akademik Bilişim. s.101. http://docplayer.biz.tr/3758191-Turk-ve-dunya-hukukunda-bilisim-suclari.html
156 Kurt, **a.g.e.** s. 106.
157 Erdağ, s. 300-301.

2.1.3. Fransa ve Bilişim Suçları

Fransa'da bilişim suçlarının sayısındaki artış genel olarak internet kullanıcı sayısının artması ve siber suçluların evrim geçirerek bireylerden uluslararası bağlantılı şebekelere dönüşmesi şeklinde yorumlanmaktadır[158].

Fransa'da bilişim suçları ayrı bir fasıl şeklinde düzenlenmeden önce bu tarz eylemler Fransız Ceza Kanunu'ndaki hırsızlık (m. 379), inancı kötüye kullanma, (m.408) ve dolandırıcılık (m. 405) gibi mal aleyhine işlenen bazı suçlarla karşılanmaya çalışılmaktaydı. 05 Ocak 1988 tarihinde 88-19 sayılı "relative a la fraude informatique" isimli kanunla ilk kez bilişim suçlarına ilişkin müstakil bir düzenleme yapılmıştır[159].

1 Mart 1994 tarihinden itibaren yürürlükte olan yeni Fransız Ceza Kanunu (YFCK)'nda ise bilişim suçlarına yönelik yeni suç tipleri oluşturulmuştur. Buna göre 226-16 ile 226-24 maddelerinde bilişim sistemleri aracılığıyla kişilik haklarına yapılan saldırılar düzenlenmiştir. YFCK'nın 277-3. maddesiyle küçüklerin resminin pornografik amaçla kullanılması, 277-24. maddesiyle ise küçükler tarafından erişilebilecek şiddet ya da pornografi içeren mesaj yayınlanması suç haline getirilmektedir[160].

765 Sayılı TCK'nın 2'nci Kitap 11'inci Bab'ında "Bilişim Alanında Suçlar" başlığı altında yer alan 525'inci madde Fransız sisteminden ilham alınarak hazırlandığından ve Yargıtay uygulamalarının tamamı bu güne kadar bu kanuna göre şekillendiğinden bilişim alanında suçlar açısından bu ülke düzenlemeleri bize mehaz (kaynak) olması nedeniyle oldukça önemlidir[161].

2.1.4. İngiltere ve Bilişim Suçları

Anglo-Sakson hukuk sistemini benimseyen İngiltere'de bu hukuk sisteminin genel özelliklerinden bağımsız olarak ABD'de olduğu gibi bilişim suçları ayrı bir kanun olarak düzenlenmiş ve aşağı yukarı aynı suç tipleri her iki ülke mevzuatında yer almıştır[162].

İngiltere'de Bilişim Suçları, 29.08.1990 tarihinde yürürlüğe giren 29.06.2000 tarihli 'Bilgisayarın Kötüye Kullanılması Yasası' (Computer Misuse Act) ile düzenleme

---

158 Avner Levin and Daria Ilkina. "International comparison of cyber crime." **Privacy and Cyber Crime Institute,** Ted Rogers School of Management, Ryerson University, 2013, s. 24. https://www.ryerson.ca/content/dam/tedrogersschool/privacy/AODAforms/Ryerson_International_Comparison_ofCyber_Crime_-March2013%20AODA.pdf

159 Yazıcıoğlu, **a.g.e.** s. 197.

160 Dülger, **a.g.e.** s.

161 Kurt, **a.g.e.** s. 104.

162 Kurt, **a.g.e.** s. 102.

altına alınmıştır[163]. Kanun 3 bölüm ve 18 kısımdan oluşmaktadır. Temel olarak bilgisayarlardaki veri ve programlara yetkisiz olarak girilmesi, başka suçların işlenmesini kolaylaştırmak veya yardımcı olmak amacıyla yetkisiz olarak bilgisayara girilmesi, bilgisayar program veya verilerinin yetkisiz olarak değiştirilmesi suçlarını düzenlemiştir[164].

Ayrıca bu yasa 2006 yılında daha da genişletilmiş[165]aynı yıl, Polis ve Adalet Yasası (Police and Justice Act 2006) ile Computer Misuse Act'da yer alan suçlara eklemeler yapılmış ve bilgisayarların kötüye kullanıma ilişkin yeni suç tipleri düzenlenmiştir. Bunlara daha sonra 2007 tarihli Ağır Suçlar Yasası (Serious Crime Act 2007) ile yeni eklemeler de yapılmıştır[166].

Anılan yasaya ek olarak bilişim sistemleri suretiyle işlenen dolandırıcılık, sahtecilik, müstehcenlik, ekstrem pornografi, grooming gibi suçları da ilgili kanunlara derç etmiş, kişisel verilerin korunmasına ilişkin eylemleri de suç haline getirerek yasalaştırmıştır[167].

Bunların dışında İngiltere'nin, AKSSS'yi imzalamış taraf devlet olması nedeniyle, sözleşmenin yükümlülüklerini yerine getirmek amacıyla yasalarında bilişim suçlarına ilişkin çeşitli değişiklikler yapmıştır.İngiltere'nin ceza hukukunda bilişim alanına yönelik düzenlemeleri yaparken interneti, bu kapsamda sanal ağları dikkate aldığını, 5237 sayılı TCK'da ise temel alınan ölçütün internet ve sanal ağlar değil, bilişim sistemleri ve bu sistem içinde mevcut veriler olduğunu söylemek mümkündür.

2.1.5. Japonya ve Bilişim Suçları

Japonya 22.06.1987 tarihinde Ceza Hukuku Alanında Bazı Hükümler Değişiklik Yapılmasına İlişkin Kanun'la Japon Ceza Kanunu'na bilişim suçlarına ilişkin suç tiplerini dahil etmiştir[168].ABD ve İngiltere gibi ülkelerle paralel şekilde, erken yıllarda

---

[163] Dülger, **a.g.e.**.
[164] Yazıcıoğlu, **a.g.e.** s.194.
[165] Levin ve İlkina, **a.g.m.** s. 17-18.
[166] Murat Volkan Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması", **Türkiye Adalet Akademisi Dergisi,** Yıl:8, Sayı:31, 2017, s. 171
[167] Murat Volkan Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması", s. 246-247 www.taa.gov.tr/.../karsilastirmali-hukuk-baglaminda-birlesik-krallik-ingiltere-hukuku e.t.: 24.04.2018
[168] Oğuz Turhan, "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)" **Planlama Uzmanlığı Tezi** Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, 2006, s. 95http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf e.t.: 15.11.2017

bilişim suçlarına karşı tedbirler alan Japonya'nın, bu farkındalığının altında, hiç kuşkusuz teknolojik gelişmelerin merkezinde bulunması yatmaktadır.

İlerleyen yıllarda Japonya'da 13.02.2000 tarihinde yürürlüğe giren İnternete Haksız Girmenin Yasaklanması Hakkında Kanun ile ceza hukuku alanında önemli düzenlemeler getirilmiştir.[169]

Japonya 2001 yılında AKSSS'yi imzalayarak günümüze kadar sözleşme ile paralel düzenlemeleri ceza hukukuna geçirmiş, bilişim suçlarıyla mücadelede uluslararası işbirliği kapsamında ne kadar istekli olduğunu sergilemiştir.

2.1.6. Çin ve Bilişim Suçları

1994 yılında küresel internet ağına ilk kez bağlanan Çin, 2008 yılından itibaren dünyanın en büyük internet kullanıcısı olmuştur[170]. Zamanla internetten büyük gelir sağlanmasına karşın kamu İnternet kullanımı üzerinde sıkı kontrol sağlamaya ve artan bilişim suçlarla mücadele etmeye çalışılmıştır.

Çin, 1997, 2000, 2009 ve 2011 yıllarında Ceza Kanununda bilişim suçlarla mücadele edebilmek için bir takım iyileştirmelere gitmiştir. Kanunda geçen ana maddeler; 285a; ülke ilişkileri, ulusal güvenlik ve ileri seviye bilim ve teknoloji ile ilgili bilişim sistemleri sızma, 285b; bilgisayar verilerini elde etme ve bilişim sistemlerini kontrol etme, 285c; bilişim sistemlerini kontrol edebilecek program ve araç gereç sağlama, 286; sistemi arızalandıracak bilişim sistemlerine sabotajda bulunma konularında düzenlemeler ve cezai müeyyideleri belirlemektedir[171].

Bu düzenlemelere ek olarak 1997 tarihli "Bilgisayar Bilgilerinin Güvenliğini Koruma Kuralları", 2000 tarihli " Devlet Sırları için Uluslararası Bilgisayar Ağları Birliği İdaresi Yönetmeliği" ve " Devlet Komitesi Tarafından İnternet Güvenliğini Koruma Konusunda Yapılması Gerekenler Hakkında Karar "[172] bulunmaktadır.

Çin'deki mevcut yasal çerçeve yeterli olmayıp alınan kararlar tepkisel yasal düzenlemeler şeklindedir[173]. Çin devlet başkanı Xi Jinping Merkezi İnternet Güvenliği ve Bilişim Teknolojisi Yönetim Grubu toplantısında yapmış olduğu konuşmada "İki

---

169 Dülger, **a.g.e.** s.

170 Bin Liang ve Hong Lu. "Internet Development, Censorship, And Cyber Crimes İn China." **Journal of Contemporary Criminal Justice** 26.1 2010, s. 103-120.

171 Levin ve İlkina, **a.g.m.** s. 34.

172 Michael Yip, "An İnvestigation İnto Chinese Cybercrime And The Underground Economy İn Comparison With The West" **Doctoral Dissertation**, University of Southampton, 2010, https://eprints.soton.ac.uk/273136/1/dissertation_final.pdf e.t.: 17.11.2017

173 Man Qi, Yongquan Wang ve Rongsheng Xu, "Fighting Cybercrime: Legislation İn China". **International Journal of Electronic Security and Digital Forensics**, 2(2), 2009, s. 219-227.

Yüzyıl Hedefleri" çerçevesinde bir yasama planı belirleyerek internet üzerinden sağlanan bilgi akışına yönelik içerik yönetimini güçlendiren, kritik alt yapıların güvenliğini sağlayan nitelikte yasaların çıkartılmasının gerekliliğini vurgulamıştır[174].

Çin bugüne kadar siber suçlarla ilgili olarak herhangi bir uluslararası sözleşmeye taraf olmamıştır.

2.1.7. Rusya ve Bilişim Suçları

Rusya'da bilişim suçlarına yönelik olarak düzenlemeler 1998 yılından öncesine kadar bir düzenleme bulunmamaktayken bu tarihten itibaren Ceza Kanununa bilişim suçlarıyla ilgili maddeler derç etmiştir. Bilişim Suçlarıyla ilgili maddeler; bilişim sistemleri kullanılarak her türlü pornografik materyalin üretimi ve dağıtımı (242.m), verilere ve yazılımlara hukuka aykırı etkide bulunma (272.m), veri ve yazılımlara zarar verecek yazılımların üretilmesi ve yayınlanması (273.m), bilişim sistemlerine ilişkin kuralların ihlali (m274)[175] şeklindedir.

1997 yılında Washington'da G-8 ülkelerince yapılan Adalet ve İçişleri Bakanları toplantısında "Ulusal Temas Noktaları" oluşturulmasına karar verilmesi üzerine, Rusya İçişleri Bakanlığı bünyesinde "R dairesi" olarak adlandırılan bir temas noktası oluşturulmuştur. Bu bölüm, ülke içindeki güvenlik ve yargı organlarının diğer ülkelerdeki karşıtları ile doğrudan temas halinde bulunmakta ve uzmanları 24 saat kesintisiz çalışmaktadır[176].

2016 yılının ortalarında, Rusya, internet ve diğer elektronik iletişim üzerindeki devlet kontrolünü ciddi biçimde sıkılaştıran ulusal yasalarına birtakım değişiklikler getirerek esneklik sağlamayı amaçlamış, 2017 yılında Rusya Dışişleri Bakanlığı "Bilgi Suçuna Karşı Mücadelede İşbirliği Hakkında" konulu toplantı taslağını hazırlayarak

---

[174] Xi Jinping, "The Governance Of China" Çeviren; Foreign Languages, Press Co. Kaynak Yayınları, İstanbul, 2017, s. 242- 243 .

[175] Çığır İlbaş, "Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi", **Yüksek Lisans Tezi.**Başkent Üniversitesi FBE, 2009, s. 16. http://acikerisim.baskent.edu.tr:8080/bitstream/handle/11727/2287/00457.pdf?sequence=1&isAllowed=y

[176] Halil İbrahim Dilek, "Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri", **Yüksek Lisans Tezi**,Dicle Üniversitesi Sosyal Bilimleri Enstitüsü, 2007, s. 111-112. https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=ePX_SaJ0b35Gq45swKG3lNl3QYX9BP5t7qYcP3mDfEjkxbtXfxNMY8BOgKRcgs7l

Avusturya'nın Viyana kentinde düzenlenen bir konferansta BM uzmanlarına sunmuştur[177].

Rusya'nın bilişim suçlarıyla mücadele açısından özellikle, 32. Paragrafta yer alan çeşitli milletlere ait özel servislerin sınır ötesi erişimine ilişkin düzenlemeden dolayı, AKSSS'yi imzalamayı reddetmesi nedeniyle, bağlayıcı uluslararası sözleşmelere kuşkuyla yaklaştığını ifade etmek mümkündür.

İncelenen ülkeler bakımından bilişim suçlarıyla hukuki açıdan mücadele yöntemlerine bakıldığında, ülkelerin hukuk sistemlerine uygun şekilde özellikle ceza hukuku alanında çeşitli düzenlemeler yapıldığı, bu düzenlemelerin bilişim suçlarından etkilenme zaman ve oranlarıyla paralellik gösterdiği ifade edilebilir.

İngiltere, Fransa, Almanya gibi Avrupa ülkelerinin AKSSS'ye geniş katılım sağlarken, Çin, Rusya ve ABD gibi ülkelerin bu sözleşmeyi imzalayarak uluslararası işbirliğine katkıda bulunmak ve bazı yükümlülükler altına girmek konusunda isteksiz oldukları değerlendirilmektedir.

2.2. Avrupa Konseyi Siber Suç Sözleşmesi

Bilişim dünyasının sınır aşan yapısı nedeniyle geleneksel ceza hukuku kuralları siber uzay olanaklarının suç işlemek amacıyla kullanılmasını engellemeye yetmemektedir. İnternetin uzak mesafelerdeki bilişim sistemlerini birbirine bağlaması sonucunda "mesafe suçları" olarak nitelenen suçları daha fazla işlenebilir hale getirmiş, siber uzayda yaşanan hızlı gelişime ülkelerin mevzuatları yetişemez olmuştur.

Siber uzayda işlenen mesafe suçlarıyla uluslararası alanda mücadelede karşılaşılan hukuki güçlükleri incelediğimizde; ilk olarak yargılama yetkisi sorunu karşımıza çıkmaktadır.[178]Söz gelimi, bilişim suçunun faili, oturma odasında kahvesini yudumlayarak kendi bilgisayarından başka bir ülkede ki masum bir kullanıcının bilgisayarına bağlanıp, onun bilgisayarını daha başka bir ülkedeki sisteme zarar vermek için kullanabilmektedir. Burada görüleceği üzere fail, suç aleti ve mağdur dünyanın bambaşka köşelerinde bulunabilmektedir.

Bu noktada bilişim suçu failleriyle mücadele hususunda ülkelerin iç hukukları yetersiz kalmakta, işlenen suç açısından birden fazla ülkenin hukuku kendini yetkili

[177] Dado Ruvic, "**Russia Prepares New Un Anti-Cybercrime Convention – Report"** Reuters, 14 Nisan 1997 tarihli internet haberi, https://www.rt.com/politics/384728-russia-has-prepared-new-international/ e.t: 28.04.2017

[178] Bayraktar, **a.g.e.** s. 106.

saymaktadır. Böyle bir durumda suçun işlendiği yerin tespiti (locus delicti) ile aynı fiil nedeniyle bir kişinin yalnız bir kez yargılanması (non bis in idem) ilkelerinin uygulanmasında sorunlar çıkabilmektedir.[179]Bu suçun işlendiği saha olan siber alanın kesin bir tanımının yapılamamış olması, bu da ülkelerin sahip oldukları siber alanın sınırlarını çizmekte zorlanmalarına neden olmaktadır.[180]

Bilişim suçlarıyla mücadelede uluslararası alanda yaşanan diğer bir zorluk ise fiziksel arama ya da haberleşmenin dinlenmesi gibi yasal yetkilerin alınması için süreci başlatacak yeterli delilin toplanmasında yaşanmaktadır.[181] İnternetin her geçen daha fazla kullanıcı tarafından ve günden güne daha aktif bir şekilde kullanılması, failin izinin sürülmesini ya da suça ilişkin delil olabilecek bulguların elde edilmesini engellemektedir. 31 Aralık 2017 tarihi itibariyle dünya genelinde internet kullanımına ilişkin yapılan istatistik uyarınca toplam insan nüfusu 7,634,758,428 iken internet kullanıcısı sayısı 4,156,932,140'dır.[182]

Uluslararası alanda bu suçla mücadelede yaşanan bir başka güçlük ise, suçluların iadesinde ortaya çıkmaktadır. Bir failin elde edilebilmesi için suça konu olan eylemin, belli bir ceza eşiğini geçen ağır bir suç olması ve çifte suçluluk şartının aranması (eylemin talep eden ve talep edilen devlet kanunlarına göre suç olması) gerekmektedir.[183]Yaşanan teknolojik gelişmeler ve küreselleşmenin de etkisiyle, bilişim suçlarında ortaya çıkan artışın, ülkeleri hem ulusal hem de uluslararası anlamda önlemler almaya ittiği söylenebilir.

Yakın zamana kadar siber suçlarla mücadele konusunda uluslararası bir fikir birliğinden bahsetmek mümkün değilken, Avrupa Konseyi Siber Suçlar Sözleşmesinin kabulü ile aynı kaderi paylaşan toplumların harekete geçmesi için olumlu bir ahlaki iklim oluşmuştur[184].

---

[179] F. Pocar, "New Challenges For International Rules Against Cyber-Crime", **European journal on Criminal Policy and Research,** 2004,S.1, S. 24-39

[180] M. Gürkaynak ve A.A. İren "Reel Dünyada Sanal Açmaz: siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, S.2, s. 263-279

[181] R.G. Smith, P. Grabosky ve G. Urbas, "Cyber Criminals On Trial", **Cambridge Universty Press.** Australia, 2006.
https://www.researchgate.net/profile/Gregor_Urbas/publication/233023456_Cyber_Criminals_on_Trial/links/5407fbb60cf2c48563b891d6.pdf

[182] Internet World Stats, "World Internet Usage and Population Statistics", 2017 https://www.internetworldstats.com/stats.htm e.t: 04.04.2018

[183] Bayraktar, **a.g.e.** s. 107

[184] Roderic Broadhurst, "Developments in The Global Law Enforcement Of Cyber-Crime". **Policing: An International Journal of Police Strategies & Management,** 29(3), 408-433. (2006) http://eprints.qut.edu.au/3769/1/3769_1.pdf

2.2.1. Ana Hatlarıyla Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa'da bilişim suçları üzerine atılan ilk adım Avrupa Konseyi'nin 1976 yılında Strasburg'da düzenlediği Ekonomik Suçluların Kriminolojik Yönü konulu konferans olmuştur.[185] Ardından 1985 yılında bilgisayarlarla ilişkili suçların hukuku boyutunu tartışmak üzere bir toplantı yapılmış ve burada uluslararası yasaların getirdiği sorumluluklar çerçevesinde ulusal yasaların yapılmasını öngören 1989 tarihli Öneri kabul edilmiştir.[186]

Avrupa Topluluğu bünyesinde yapılan ikinci büyük düzenleme, Bakanlar Komitesi tarafından, 11 Eylül 1995 tarihinde kabul edilen ceza usul yasalarındaki soruşturma ve el koymaya yönelik hükümlerin bilişim teknolojilerinin getirdiği yeniliklere adaptasyonu ve uluslararası işbirliği konularında usul yasalarında yapılacak düzenlemelerdir. [187]Yine Avrupa Konseyi bünyesinde kurulan Avrupa Suç Sorunları Komitesi Kasım 1996'da siber suçlarla ilgilenecek bir uzmanlar komitesi kurmaya karar vermiş [188] bunun üzerine 1997 yılında Siber-Uzay Suçları Uzmanlar Komitesini kurularak 2001 yılında Budapeşte Sözleşmesi olarak da bilinen Siber Suçlar Sözleşmesi kabul edilmiştir[189].

Sözleşme, sadece Avrupa Konseyi üyeleri ile sınırlı olmayıp imzalamak isteyen diğer ülkelerin de hizmetindedir. 2014 yılı başı itibariyle bu sözleşme 55 ülke tarafından imzalanmış 41 ülke de onaylanmıştır. Bu devletlerden 17'si Avrupa Konseyine üye değildir[190].

Genel olarak bakıldığında; sözleşmenin üç temel amacının, cezai suçların ortak tanımlarını ortaya koymak, böylece ilgili mevzuatın ulusal düzeyde uyumlu hale getirilmesi, bilgi teknolojisi ortamına uyan ortak yetkileri tanımlamak, böylece ceza muhakemesi kurallarının yeknesaklaşmasını sağlamak ve hem klasik anlamda hem de çağın gereklerine uygun türden yeni uluslararası işbirliği türlerini belirleyerek

---

185 Stain Schjolberg, s. Computer-Related Offences,, Fransa, 2004, http://www.cybercrimelaw.net/documents/Strasbourg.pdf. e.t: 21.03.2018

186 Bayraktar, **a.g.e.** s. 109

187 Murat Önemli, "İnternet Suçlarıyla Mücadele Yöntemleri", **Yayınlanmış Yüksek Lisans Tezi**, Türkiye, Ortadoğu ve Amme İdaresi Enstitüsü, Ankara, 2004, s. 38

188 Kayıhan İçel "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası S.** 59.1-2, Ankara, 2001, s. 4.

189 Levin ve İlkina, **a.g.m.** s. 8.

190 Servet Yetim, "Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi",**Türkiye Adalet Akademisi Dergisi**, S. 17, 2014, s. 189. http://www.taa.gov.tr/indir/siber-suclar-yargilama-yetkisi-ve-yeni-bir-model-onerisi-bWFrYWxlfDE4MjEyLTQ1MWRkLWQ5ZWI5LWVkMTY0LnBkZnwzMjk/

devletlerin bu hükümleri hızlı bir şekilde uygulayabilmesini sağlamak [191] olduğu görülmektedir.

Günümüz itibariyle 55 ülke bu sözleşmeyi imzalamış, 30 ülke sözleşme maddelerini iç hukuka uyarlamıştır. Türkiye, Avrupa Konseyi Siber Suçlar sözleşmesini 2010 yılında imzalamış, 2014 yılında ise mecliste 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanunu onaylayarak sözleşmeye taraf olmuştur[192].

2.2.2. Avrupa Konseyi Siber Suç Sözleşmesinde Siber Suçlar

Avrupa Konseyi Siber Suçlar Sözleşmesi dört ana bölümden oluşmaktadır: Birinci bölümde, sözleşmede kullanılan terimler tanımlanmıştır. İkinci bölümde, ulusal düzeyde alınacak tedbirlere yer verilmiştir. Üçüncü bölümde uluslararası işbirliğinin çerçevesi çizilmiştir. Dördüncü bölümde ise, son hükümler başlığı altında sözleşmenin uygulanmasına dair birtakım usuli ve teknik hükümlere yer verilmektedir.

Sözleşmede, üzerinde anlaşılmış tek bir tanımı bulunmayan siber suç kavramını tanımlamak yerine, siber suç kapsamında değerlendirilebilecek temel suç tiplerinin tanımlanarak tek tek sayıldığı görülmektedir. Bu bağlamda siber suçlar:*"Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar", "Bilgisayarla bağlantılı suçlar", "İçerikle bağlantılı suçlar", "Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar"* ile *"Tali yükümlülükler ve yaptırımlar"* başlıkları altında sayılmıştır.

2.2.2.1. Bilgisayar Verilerinin ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Yönelik Suçlar

Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar;"Yasadışı Erişim" (m.2), "Yasadışı Araya Girme" (m.3), "Verilere Müdahale" (m.4), "Sisteme Müdahale" (m.5), "Cihazların Kötüye Kullanımı" (m.6) olarak tanımlanmıştır.

Sözleşmenin 2. Maddesinde[193]

[191] Broadhurst, s. 13.
[192] Yetim, s. 187.
[193] *AKSSS* http://www.bhd.org.tr/dokumanlar/Avrupa%20Konseyi%20Siber%20Suclar%20Sozlesmesi%20TR.docx e.t:: 20.12.2017

Her bir taraf devlet bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı gerekli önlemleri almalıdır. hükmü yer almıştır.

Yetkisiz erişim fiili, hak sahibi kullanıcının sistemi kullanmasını engelleyebileceği gibi verilerin bozulmasına, değiştirilmesine ya da yok edilmesine neden olabileceğinden, suçun ilk aşamasını oluşturan bu fiilin suç olarak düzenlenmesi önemli bir koruma sağlayabilecek niteliktedir[194]. Bu açıdan yetkisiz erişim fiilinin madde metninin lafzi yorumundan engelleme suçu olarak tasarlandığını söylemek mümkündür.

Sözleşmenin3.maddesinde;

Her bir taraf devlet kamuya açık olmayan elektromanyetik emisyon da dahil olmak üzere bilgisayarlar arasında gerçekleşen bir iletişimin arasına bilerek isteyerek ve haksız olarak arasına girmeyi kanununda suç olarak tanımlamalı ve diğer gerekli tüm önlemleri almalıdır. Taraf devlet bu suçun oluşmasını kötü niyet şartına bağlı kılabilir

hükmüne yer verilmiştir.[195]

Sözleşmenin bu maddesinde amacın bilişim sistemini korumaktan ziyade bilişim sistemleri arasında gerçekleşen veri haberleşmesinin mahremiyetinin koruması olduğu açıktır. Bu bakımdan Avrupa İnsan Hakları Sözleşmesinin 8. Maddesinde belirtilen kişilerin özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi ilkesinin telefon, belgegeçer, e-posta veya dosya iletimi şeklindeki bütün elektronik veri transferi biçimlerine uygulanmış halidir.[196]

Bu madde iletişimin gizliliğinin yanında iletişimin güvenliğinin korunmaya çalışıldığı açıktır. Günümüzde kullanıcıların internet üzerinden işlemlerini gerçekleştirirken zaman zaman kişisel ve mali bilgilerini aktardıkları göz önüne

[194] Özgür Eralp, 2017, "**Avrupa Konseyi Siber Suç Sözleşmesi Açıklayıcı Memorandum**", Paragraf 44 http://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ e.t.: 25.03.2018

[195] AKSSS ***a.g.i.s.*** e.t.: 20.12.2017

[196] Açıklayıcı Rapor, Paragraf 51.

alındığında araya giren kötü niyetli bir kullanıcının şantaj, tehdit, dolandırıcılık, sahtekarlık gibi pek çok suçu kolayca işleyebileceği değerlendirilmektedir.

Ayrıca cezai yükümlülüğün oluşabilmesi için araya girme eyleminin, kasıtlı olarak ve haksız biçimde gerçekleşmesi gerekmektedir. Özellikle yasal ve yetkili mercilerin yürüttükleri soruşturma kapsamında ve usulüne uygun olarak bu fiili gerçekleştirmesi suç teşkil etmemektedir.[197]

AKSSS 4. Maddesi "*veriye müdahale*" başlıklı olup birinci fıkrasında

> *Her bir taraf devlet, bir kimsenin bilgisayar verisine hakkı olmadığı halde, bilerek ve isteyerek zarar verme, silme, bozma, değiştirmeye ya da ortadan kaldırma fiilleri işlemesini suç olarak düzenlemek üzere gerekli kanuni düzenlemeyi yapmalı ve gerekli diğer önlemleri almalıdır* hükmü yer almaktadır.[198]

İkinci fıkrada ise "*Taraf devlet 1. paragrafta belirtilen durumun oluşmasını ciddi zarar oluşma olasılığına bağlı tutma hakkına sahiptir*."[199]ibaresi bulunmaktadır.

Maddede suçu oluşturan eylem tanımlanırken öncelikli şartın haksız şekilde yani erişim izni olmaksızın veriye ulaşmak olduğu, aynı zamanda bu eylemin bilerek ve isteyerek yani kasten işlenmesi gerektiği değerlendirilmektedir.

Ayrıca haksız fiilin, veriyi değiştirme, bozma, zarar verme, ortadan kaldırma ve silme şeklinde derecelendirildiği bu yolla suç teşkil edebilecek tüm eylemlerin madde kapsamına dahil edildiği görülmektedir.

Maddede sayılan eylemlerden "veriyi değiştirme", sistem içinde mevcut olan verinin içeriğinin ya da uzantısının değiştirilmesi, "veriyi bozma", değiştirmeden farklı olarak veriyi tahrip ederek kullanıcının veriden elde etmeyi beklediği faydayı elde etmesine imkan bırakmamak, "zarar verme", bozmanın bir adın ötesinde veriyi geri dönüşü imkansız şekilde hasara uğratmak, "veriyi ortadan kaldırmak"veriyi sistem içinde başka bir yere taşımak ya da başka bir sisteme aktarmak, "silme" ise veriyi geri dönüşü mümkün olmayacak şekilde yok etmek olarak ifade edilebilir.

AKSSS 5. madde[200]ile;

---

[197] Açıklayıcı Rapor, Paragraf 55.
[198] ***AKSSS a.g.i.s.*** e.t.: 20.12.2017
[194] ***AKSSS a.g.i.s.*** e.t.: 21.12.2017

Her bir taraf devlet veri yükleyerek, aktararak zarar vererek, silerek, bozarak, değiştirerek veya müdahale ederek bilgisayar sisteminin kullanımında hakkı olmadığı halde bilerek ve isteyerek bilgisayarın sisteminin çalışmasını sekteye uğratma fiilini ulusal kanununda suç olarak düzenlemeli ve gerekli diğer düzenlemeleri yapmalıdır şartını getirmiştir.

Sözleşme ile korunan hukuki değer bilgisayar ve iletişim sistemlerinin yetkili kullanıcılar tarafından amacına uygun şekilde kullanılabilmesi hakkıdır. [201]

Bilgisayar sisteminin işleyişinin kesintiye uğratılması aynı zamanda bu sistemden beklenilen faydanın sağlanmasının engellenmesi anlamına geldiği açıktır. Sözleşme eylemin suç teşkil edebilmesi için yetkili kullanıcının sistemi kullanmasını önemli ölçüde etkileyecek derecede engellenmesini öngörmekte, bunu belirleyecek hususları kararlaştırmayı ise taraf devletlere bırakmaktadır.[202]

Madde de doğrudan siber terör konusuna değinilmemiştir. Ancak haksız şekilde veri yüklemesi ya da aktarımı yoluyla zarar verme, silme, bozma, değiştirme veya müdahale yöntemleriyle bilişim sisteminin işleyişinin engellemesinin ülkelerin kritik alt yapı tesislerine yöneltmesi durumunda siber terörün de bu suç kapsamına gireceği değerlendirilmektedir[203].

AKSSS'nin Cihazları Kötüye Kullanma başlıklı 6. maddesine[204] göre taraflar, 2. ve 5. maddelerde yer alan eylemlerden herhangi birini gerçekleştirmek üzere tasarlanmış ya da dönüştürülmüş bir cihazın ya da bilgisayar sisteminin bir parçasını veya tamamını erişilebilir kılacak parola, erişim kodu ve benzer verilerin üretimi, satışı kullanımı amacıyla temini, ithali, dağıtımı ya da başka şekillerde ulaşılabilir hale getirilmesini suç olarak tanımlayacak gerekli yasal düzenlemeleri yapmalıdırlar.

Bu maddede sözleşmenin amaçlarından biri siber suçların işlenmesi için standart olarak üretilen cihaz ve programlardan farklı olarak suç işlemek amacıyla dönüştürülmüş veya üretilmiş cihaz veya programlara ihtiyaç duyulması nedeniyle oluşan karaborsayı yok ederek suçu önlemektir. [205]Böylece maddenin virüs, Truva atı, ağ solucanları gibi kötücül yazılımların üretim, kullanım ve dağıtımını da suç haline getirdiğini söylemek mümkündür.

---

[200] ***AKSSS a.g.i.s.*** e.t.: 22.12.2017
[201] Açıklayıcı Rapor, Paragraf 65.
[202] Açıklayıcı Rapor, Paragraf 66-67.
[203] Havuz, s. 150.
[204] ***AKSSS a.g.i.s.*** e.t.: 22.12.2017
[205] Açıklayıcı Rapor, Paragraf 71.

Bunlara ek olarak cihazların kötüye kullanımı suçunun oluşabilmesi için cihazı suç işleme amacıyla kullanma niyetinin bulunması gerekmektedir. Genel olarak satışa sunulan cihaz veya programların aynı zamanda suç işleme saikiyle de kullanılabilmesi nedeniyle madde iyi niyetli kullanıcıların bu araçlardan yararlanma hakkını korumak istemiştir. [206]

Metnin lafzi yorumundan da anlaşılabileceği üzere, yasa koyucu, suçun oluşumu için failde suç işleme niyetini aramaktadır. Ancak, muhakeme aşamasında yargılama makamlarının karşısına çıkan somut olayda, failde bu niyetin varlığının ya da yokluğunun ispatının, bilişim suçlarının yapısından kaynaklanan gerçek faile ve yeterli delile ulaşmada yaşanan güçlükler nedeniyle, kolay olmayacağı değerlendirilmektedir.

2.2.2.2. Bilgisayarlarla Bağlantılı Suçlar

Bilgisayarla bağlantılı suçlar iki madde halinde"Bilgisayarla Bağlantılı Sahtecilik" (m.7), "Bilgisayarla Bağlantılı Dolandırıcılık" (m.8)olarak tanımlanmıştır.

Sözleşmenin Bilgisayarla Bağlantılı Sahtecilik suçunu düzenleyen 7.maddesine göre[207]

> *Her bir Taraf devlet, bir hak olmaksızın kasıtlı olarak yapılan, açıkça okunabilir ve anlaşılabilir olup olmadığına bakmaksızın, yasal amaçlar için kullanılması ve ele alınması niyetiyle sahte veriler olarak sonuçlanan bilgisayar verilerinin girilmesi, değiştirilmesi, silinmesi veya yerlerinden kaldırılmasına yönelik fiilleri gerekli yasal ve benzeri önlemlerle iç hukukunda birer suç eylemi olarak ortaya koymalıdır.*

Maddeye ek olarak taraf devletin, bu suçun oluşumunu sahtekarlık veya benzeri bir kötü niyetin varlığı şartına bağlayabileceği de belirtilmiştir.

Madde içeriğinde verilerin izinsiz olarak değiştirilmesi ya da yeni verilerin yaratılması, doğrudan orijinal verilerin hukuki anlamda delil özelliğinin değiştirilmesi ile ilgilidir ve aldatmaya yöneliktir. [208] Buradan yola çıkarak dijital ortamda aldatmak amacıyla veriyi değiştirme, silme ya da yerinden kaldırma fiillerinin resmi bir işleme konu olması halinde somut bir resmi evrak üzerinde yapılan sahtecilik ile aynı sonuçları

[206] Açıklayıcı Rapor, paragraf 76.
[207] ***AKSSS a.g.i.s.*** e.t.: 22.12.2017
[208] Havuz, s. 152

doğuracağı söylenebilir. Burada korunan hukuki yarar hukuki işlemlere konu olabilecek nitelikteki elektronik veri güvenliğinin ve güvenilirliğinin korunmasıdır.[209]

Bu maddenin sözleşmenin 4. Maddesinde bulunan veriye müdahale suçu ile benzer olduğu ancak incelenmekte olan 7. Maddedeki manevi unsurun "yasal amaçlar için kullanılması ve ele alınması niyeti" olduğu göz önüne alınmalıdır.[210]Bu durumda failin eylemini başka amaçlarla gerçekleştirmesi halinde 7. Madde kapsamında "Bilgisayarla Bağlantılı Sahtekarlık" suçu yerine 4. Madde kapsamında "Veriye Müdahale" suçunun oluşacağı değerlendirilmektedir. Buradan yola çıkarak failin saikinin suçun türüne direkt olarak etki ettiğini söylemek mümkündür.

AKSSS'nin Bilgisayarla Bağlantılı Dolandırıcılık suçunu yaptırım altına alan 8. Maddesi ise[211]

> *Her bir Taraf devlet, bir hak olmaksızın kasıtlı olarak yapılan kendi veya başkasına ekonomik bir menfaat temin etmek kötü niyetiyle veya dolandırıcılık niyetiyle diğer bir kişinin mal kaybına sebep olan,*
> *a . her türlü bilgisayar veri girişi, değiştirilmesi, silinmesi ve yerinden kaldırılması,*
> *b . bir bilgisayar sisteminin çalışmasına yönelik her türlü müdahale fiillerini gerekli yasal ve benzeri önlemlerle iç hukukunda birer suç eylemi olarak ortaya koymalıdır* hükmünü içermektedir..

Madde içeriğinde temel olarak mal varlığını yasa dışı şekilde aktarmak için verilerin işlenip değerlendirilmesi sürecine yapılan yasadışı müdahale suç olarak düzenlemektedir.[212] Bankacılık işlemlerinin yoğun olarak internet ortamında yapıldığı günümüzde, birçok soyut mal varlığı sanal ortamda yönetilebilir olmuştur. Ekonomik çıkar elde etmek isteyen bilişim suçu failleri açısından veri akışı yoluyla transfer edilen yüksek meblağların hedef çekiciliğini arttırdığını söylemek mümkündür.

Yasalara uygun yaygın ticari eylemler, rekabet sayılabilecek faaliyetler madde kapsamına girmemektedir.[213] Bilgisayar bağlantılı dolandırıcılık suçunun oluşabilmesi

[209] Açıklayıcı Rapor, Paragraf 81
[210] Havuz, s. 153
[211] ***AKSSSa.g.i.s.*** e.t.: 22.12.2017
[212] Açıklayıcı Rapor, Paragraf 86.
[213] Açıklayıcı rapor, Paragraf 88-90.

için failin bir kişinin mal varlığında azalmaya yol açarak kendisi ya da bir başkası adına kazanç sağlaması gerekmektedir.

2.2.2.3. İçerikle İlişkili Suçlar

Sözleşmede, "İçerikle İlişkili Suçlar" başlığı altında sadece "Çocuk Pornografisiyle Bağlantılı Suçlar[214]" (m.9) sayılmıştır.

Yasa koyucu organlar tarafından genel pornografik görüntüler ile çocuk pornografisi arasında ayrıma gidildiği, görülmektedir; çocuk pornografisine karşı olan yasalar öncelikle bu görüntülerin oluşturulması sırasında gerçekleşen çocuk istismarı ile ilgilenmekte, ikincil olarak ise bu ürünlerin tüketilmesinin sonuçlarına eğilmektedir.[215]

AKSSS 9. Maddenin ilk fıkrasında çocuk pornografisi ile ilgili olarak her bir taraf devlete, *"haksız yere kasıtlı olarak bilgisayar sistemi vasıtasıyla,*

a .dağıtmak amacıyla çocuk pornografisi üretmek,

b. çocuk pornografisini temin edilebilir hale getirmek veya göstermek,

c. çocuk pornografisini aktarmak veya dağıtımını yapmak,

d. kendisi veya başkası için çocuk pornografisi temin etmek,

e. bir bilgisayar sisteminde veya bilgisayar veri depolama ortamında çocuk pornografisine sahip olmak

Fiillerinden sorumlu tutulması için gerekli kanuni düzenlemeyi yapmalı ve ihtiyaç duyulan önlemleri almalıdır" şeklinde yükümlülükler yüklemiştir.

Maddenin devamında, çocuk pornografisi; *"a) Bir küçüğün cinsel olarak kullanılmasını, b) Bir küçük gibi görünen kişinin cinsel olarak kullanılmasını,c) Bir küçüğü temsil eden gerçekçi bir imajın cinsel olarak kullanılmasını görsel olarak içeren pornografik materyaldir"* şeklinde tanımlanmıştır.

Son paragrafta "reşit olmayan kişi" terimi, BM Çocuk Hakları Konvansiyonundaki "çocuk" tanımına (m.1) uygun biçimde, *"18 yaşın altındaki herkestir"* şeklinde tanımlanmış olup, tarafların, *"16 yaşından az olmamak üzere daha düşük bir yaş sınırı"* getirmelerine izin verilmiştir. Burada söz edilen yaşın (gerçek ya

[214] ***AKSSS a.g.i.s.*** e.t.: 23.12.2017

[215] Murat Volkan Dülger, Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması, s. 180

da hayali) çocukların cinsel eylemlerde kullanılmasıyla ilgili olduğu ve cinsel ilişki için izin yaşından farklı olduğu göz önünde bulundurulmalıdır.[216]

Bu Sözleşme çocuk pornografisi suçunu üretimden bulundurmaya kadar tüm fiilleri kapsayacak şekilde tanımlayarak bu suçla etkin şekilde mücadele etmeyi amaçlamıştır. Maddede suç olarak tanımlanan eylemler, internet siteleri oluşturmak online bağlantılar kurmak veya hiper bağlantılar aracılığıyla gerçekleştirilebileceği gibi, bu malzemeler bir bilgisayar sisteminde ya da veri depolama araçlarında bulundurulabilir.[217]

Madde ayrıca suçun oluşmasını için çocuğun kullanılmasını şart koşmamış, animasyon programları yardımıyla yaratılan çocuk görüntüsünü ya da yetişkin bir kişinin görüntüsünün bilgisayar programları yardımıyla çocuk izlenimi verecek şekilde değiştirilmiş halini de suç kapsamında değerlendirmiştir. Maddenin amacı gerçek bir çocuğa zarar verilmese bile çocuğa kötü muameleye izin veren bir alt kültürün oluşmasını engellemektir.[218]

Ancak AKSSS 9. Madde kapsamına "çocuk erotizmi" dahil edilmediğinden, birçok ülkede bu konudaki yasal boşluktan yararlanılarak bu tür ürünlerin satılması suç olarak tanımlanmamıştır[219].

Bilişim suçlarıyla uluslararası mücadelede bu sözleşme ile kayda değer gelişmeler elde edilmekle birlikte, henüz yolun çok başında olunduğu açıktır. Siber suçun üzerinde uzlaşılmış bir tanımının bulunmaması nedeniyle sözleşmede tanımı yapılmamış ancak içerik ve kapsamına yönelik suç tipleri belirlenerek ülkelerin ulusal hukuklarında çeşitli düzenlemeler yapmaları sağlanmıştır.

Avrupa Konseyi Siber Suç Sözleşmesi'nin işlerlik kazanması için dünya çapında katılımın arttırılması, gelişmiş ülkelerin hukuki, teknolojik, ekonomik anlamda her türlü yardımı gerçekleştirerek, gelişmekte olan ülkelerin de sözleşmeyi imzalamaya teşvik edilmesi gerekmektedir.

Sözleşmede yer alan maddeler, imzacı devletlerin bu suçlarla mücadelede ulusal mevzuatlarındaki eksikliklerini tamamlamalarına yardımcı olurken, aynı zamanda

---

[216] Füsun Sokullu Akıncı, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi." **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası** S.59.1-2, 2001, s. 33, 34.
http://dergipark.ulakbim.gov.tr/iuhfm/article/viewFile/1023004153/1023003747 e.t.: 11.04.2018

[217] Açıklayıcı Rapor, Paragraf 94-99.

[218] Havuz, s. 158

[219] Murat Volkan Dülger, "İnternet İletişimin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme", s. 1523.

imzacı olmayan devletlerin bilişim suçlarıyla mücadelede iç hukuklarını oluşturmalarında önemli bir referanstır.

Sözleşmede doğrudan siber terör konusuna değinilmemiş, ancak haksız şekilde veri yüklemesi ya da aktarımı yoluyla zarar verme, silme, bozma, değiştirme veya müdahale yöntemleriyle bilişim sisteminin işleyişinin engellemesi eylemlerinin ülkelerin kritik alt yapı tesislerine yöneltmesi durumunda siber terörün de bu suç kapsamına gireceği değerlendirilmektedir.

ÜÇÜNCÜ BÖLÜM

5237 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

3.1. Genel Olarak 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları

Türk hukuk mevzuatında bilişim suçları ilk olarak 765 sayılı Türk Ceza Kanunu'nun[220] "Bilişim Alanında Suçlar" başlıklı 525'inci maddesinde yer almıştır. Ardından 26.09.2004 tarihinde kabul edilen 5237 Sayılı Türk Ceza Kanunun Onuncu Bölümünde "Bilişim Suçları" başlığı altında özel olarak bilişim suçları düzenlenmiştir. 5237 sayılı TCK'da bilişim sistemleri aracılığıyla işlenmesi mümkün olan başkaca suçlar bulunmakla birlikte, başka kanunlarda da bilişim sistemlerine karşı suçların düzenlendiği görülmüştür.

AKSSS'de siber suçların tanımlanması yerine bu suç kapsamına giren eylemlerin madde madde sayılması sistemine paralel olarak, 5237 sayılı TCK'da da bilişim suçlarının tanımlaması yapılmamış, bunun yerine bilişim suçları başlığı altında maddeler halinde sayılmıştır.

Temel olarak, günümüz teknolojik imkanları çerçevesinde, TCK'da yer alan bir çok suç bilişim sistemleri aracılığıyla işlenebilir hale gelmiştir. Örneğin bir hastanenin bilişim sistemine yetkisiz erişim sağlanarak hasta kayıtlarına ulaşılması ve kimi hastaların ilaçlarının ya da ilaç dozlarının değiştirilmesi suretiyle TCK 81 ve 82'nci maddeler kapsamında "Kasten Öldürme" suçunun işlenmesi mümkün olabilecektir. Ancak TCK'da bulunan tüm suçların, bahsedilen şekilde bilişim sistemleri aracılığıyla işlenebilirliğinin incelenmesi, araştırmanın kapsamını oldukça genişleteceğinden araştırma doğrudan ve dolayısıyla bilişim suçları tasnifi uyarınca yürütülmüştür.

Türk Ceza Kanunu'nda bilişim suçları iki biçimde sınıflandırmaya tabi tutulmuştur a) Doğrudan Bilişim Suçları (Gerçek Bilişim Suçları) b) Dolayısıyla Bilişim Suçları (Bilişim Bağlantılı Suçlar)[221]. Doğrudan bilişim suçları, TCK'da "Bilişim Suçları" başlığı altında ayrıca sayılan suçlarını kapsarken, dolayısıyla bilişim suçları, TCK'da yer alan klasik suçların bilişim sistemleri kullanılarak işlenen şekillerini ifade etmektedir.

---

[220] 765 Sayılı Türk Ceza Kanunu, http://www.ceza-bb.adalet.gov.tr/mevzuat/765.htm e.t.: 02.04.2018

[221] Yargıtay Ceza Genel Kurulu E. 2009/11-193, K. 2009/268, 17.11.2009 http://www.turkhukuksitesi.com/serh.php?did=6165 e.t.: 24.04.2018

Araştırmanın bu bölümünde hem doğrudan bilişim suçları olan "*Bilişim Sistemine Girme*" (m.243), "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*" (m.244) ve "*Banka veya Kredi Kartlarının Kötüye Kullanılması*" (m.245) suçları hem de dolayısıyla bilişim suçları olarak nitelendirilebilecek "*Haberleşmenin Gizliliğini İhlal*" (m.132), "*Kişisel Verilerin Kaydedilmesi*" (m.135), "*Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme*" (m.136) ile "*Verilerin Yok Edilmemesi*" (m.138) suçları incelenecek, daha sonra "*Haberleşmenin Engellenmesi"* (m.124), "*Hakaret"* (m.125) " *Bilişim Sisteminin Kullanılması Yoluyla Hırsızlık"* (m.142/2.b.e), "*Bilişim Sisteminin Kullanılması Yoluyla Dolandırıcılık"* (m.158/1.b.f), "*Müstehcenlik"* (m.226) suçları üzerinde durulacaktır.

3.2. 5237 Sayılı Türk Ceza Kanununda Bilişim Alanında Suçlar

Bilişim suçları TCK'nın ikinci kitabında "Topluma Karşı Suçlar" başlığını taşıyan üçüncü kısmın "Bilişim Sistemlerine Karşı Suçlar" başlığını taşıyan Onuncu bölümünde düzenlenmiştir. Sırasıyla 243'üncü madde de düzenlenen "*Bilişim Sistemine Girme*", 244'üncü maddede de düzenlenen "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*" ve 245'inci madde de düzenlenen "*Banka veya Kredi Kartlarının Kötüye Kullanılması*" suçları bu başlık altında incelenecektir.

3.2.1. Bilişim Sistemine Girme Suçu

Bilişim sistemine girmek veya orada kalmaya devam etmek suçu daha önce 1997, 2000 ve 2003 Türk Ceza Kanunun Ön Tasarı (TCKÖT) metinlerinde düzenlenmiş ancak Türk ceza mevzuatında ilk kez 5237 Sayılı TCK'da ceza normu haline gelmiştir[222].

243. maddenin ilk fıkrasında[223] "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimse"* hakkında hapis cezasına hükmolunmaktadır.

Birçok bilişim suçunun gerçekleştirilmesinin ilk adımının bilişim sistemine girilmesi olduğu değerlendirildiğinde, yasa koyucunun bilişim sistemine girme suçu

[222] Ahmet Taşkın ve İbrahim Zengin "Ceza Hukuku El Kitabı" Eda Matbaası, Ankara, 2004, s. 35

[223] *TCK* http://mevzuat.basbakanlik.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=5237 e.t.: 03.04.2018

ile bir tür "engelleme suçu" yaratmak istediği görülmektedir.[224] Bilişim sistemine girme suçu failin hakkı olmaksızın bilişim sistemindeki dosyalara herhangi bir şekilde ulaşması ile gerçekleşmektedir. Bu basitçe bir kişinin bilgisayarını açarak ona ait dosyaları görmek şeklinde fiziki hareketlerle olabileceği gibi sanal ortamda bilişim sistemi kullanılarak gönderilen yazılımlar yoluyla mağdurun dosyalarına ulaşmak şeklinde de olabilir.

2. fıkra uyarınca [225] *ilk fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranında* indirime tabidir. Failin bedelini ödeyerek hukuka uygun olarak erişebileceği bir sisteme bedelini ödemeksizin girmesi ve sistemde kalması söz konusudur.

TDK Büyük Türkçe Sözlüğünde "bedel: (1) değer, fiyat, kıymet (2) bir şeyin yerini tutabilen karşılık" olarak tanımlanmaktadır.[226] Dolayısıyla madde metnindeki bedel ibaresini sadece "para" olarak değil, "karşılık" olarak anlamak gerektiği değerlendirilmektedir. Bu açıdan bakıldığında, kontör yükleyerek, abone olunarak, form ya da anket doldurarak erişilebilecek sistemlerin de madde kapsamında indirime tabi olacağını söylemek yerinde olacaktır.

Yasa koyucunun indirim sebebinin yerinde olup olmadığı konusunda doktrinde farklı görüşler mevcuttur.[227] Ancak yaygın olan görüş mağdurun bedel karşılığı başka kişilere bilişim sistemlerine erişim sağlatması nedeniyle sistemdeki verilerin önemli ekonomik hakları ya da manevi değerleri barındırmadığının öngörüldüğü şeklindedir.[228]

Eylem nedeniyle *sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına* hükmolunmaktadır (f. 3)[229]. Hacker olarak tabir edilen bilişim korsanlarının temel amacı bir bilişim sistemine yetkisiz erişim sağlayarak sistemde bulunan verileri kendi çıkarlarına uygun olarak çalmak ya da değiştirmektir. Eylemin artırım nedeni yapılmasının bilişim korsanları ile mücadelede oldukça etkili olacağı değerlendirilmektedir.[230]

---

[224] Recep Yılmaz Yazıcıoğlu, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim sistemine Girme Eylemi" 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara, 2009, s. 81 –Erdoğan Bilişim Sistemine Girme ve Kalma Suçu s. 1365

[225] TCK**a.g.i.s.**e.t.: 03.04.2018

[226] "Bedel" Türk Dil Kurumu Büyük Türkçe Sözlük, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5ad2118a21a0b1.92319868 e.t: 02.04.2018

[227] Erdoğan, s. 1399

[228] Yenidünya, s. 1040 – Erdoğan, s. 1399

[229] TCK**a.g.i.s.**e.t.: 03.04.2018

[230] Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu" s. 1367

4. fıkrada yer alan [231] "b*ir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlenmesine"* ilişkin hükmünün AKSSS 3. Maddesinde sayılan "Yasadışı Araya Girme" suçu ile eşdeğer olarak düzenlendiği görülmekle, bir sistemin kendi içinde veya diğer bilişim sistemleri ile gerçekleştirdiği veri nakillerini sisteme girmeksizin hukuka aykırı olarak izleyen kişi hakkında, bir yıldan üç yıla kadar hapis cezasına hükmolunmaktadır. Bilişim suçu işleme tekniklerinde ayrıntılı olarak anlatılan "sniffing" yönteminin tam olarak bu eylemi içerdiği değerlendirilmektedir[232].

3.2.1.1. Korunan Hukuki Yarar

Madde ile korunmak istenen hukuki değer karma nitelikte olup, *"toplum düzenini korumak, özel hayatın gizliliği, haberleşmenin gizliliği, kullanıcı ve sistem sahibinin menfaatleri, olası başka suçların işlenmesinin önlenmesi, bilişim sisteminin güvenliği"* olarak sayılabilir.[233]

Madde metnindeki "kimse" ifadesinden suçun failinin herkes olabileceği, konusunun bilişim sistemi olduğu değerlendirilmektedir. Ayrıca suçun oluşumu için bilişim sisteminin tamamına girilmesinin şart olmayıp sadece bir bölümüne erişim sağlanmasının da suçu meydana getireceği tanımdan anlaşılmaktadır.

Mağdurun zarar görmesi şart olmadığından suçun "tehlike suçu" olarak değerlendirilmesi gerekmektedir. [234] Madde gerekçesinde de suçun oluşumu için sisteme hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmesinin şart olmadığı açıklığa kavuşturulmuştur.

3.2.1.2. Suçun Maddi Unsuru

243 üncü maddenin birinci fıkrasının metni 24.03.2016 tarihinde yapılan değişiklikten önce "…hukuka aykırı olarak giren ve orada kalmaya devam eden"

---

http://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-12-ozel/3-kamu/6-yavuzerdogan.pdf e.t.: 02.04.2018

[231] *TCK MADDE 243 - (4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası il e cezalandırılır*.**a.g.i.s.**e.t.: 03.04.2018

[232] Bkz. Bilişim suçu işleme yöntemleri s.

[233] Erdoğan, s. 1370-1371

[234] Taşkın, **a.g.e.** s. 26

şeklinde iken 6698 sayılı Kanunun[235] 30 uncu maddesiyle, bu fıkrada yer alan "ve" ibaresi "veya" şeklinde değiştirilmiştir

Suçun seçimlik hareketli olup olmadığı konusunda iki farklı görüş bulunmaktadır. İlk görüş, bilişim sistemine girilmesi veya sistemde kalmaya devam edilmesi eylemlerinden birisinin yapılmasıyla suçun gerçekleşeceğinden bahisle suçu seçimlik hareketli bir suç olarak tanımlarken[236], diğer görüş, suçun maddi unsurunu bilişim sistemine girmek ve orada kalmaya devam etmek şeklinde kabul etmiş[237], suç madde metninde her ne kadar "haksız şekilde bilişim sistemine girme veya bilişim sisteminde kalma" olarak tanımlanmışsa da oluşması için icrai nitelikteki girme eylemi ile ihmali nitelikteki kalma eyleminin bir arada bulunması gerektiğini, sadece bilişim sistemine girmenin ise teşebbüs sayılacağını vurgulamıştır.[238]

Maddenin lafzi yorumundan "veya" ibaresinin yasal olmayan şekilde başka birine ait bilişim sistemine girmek eylemi ile yetkisiz erişim sağlanmış olan bilişim alanında kalmaya devam etmek fiillerinden birinin gerçekleşmesi halinde suçun oluşacağı anlaşılmaktadır. Ancak bilişim sisteminde haksız yere kalmaya devam edebilmenin ön koşulu öncelikle o bilişim sistemine yetkisiz erişim sağlamak yani girmek fiilinin gerçekleştirilmesidir. Bu noktada madde metninin 6698 sayılı kanundan önce "bilişim sistemine girmek ve kalmaya devam etmek" şeklinde olduğunu hatırlatmak yerinde olacaktır. Yasa koyucu suçun oluşumu için birbirini tamamlayan "girmek ve kalmaya devam etmek" eylemlerini "veya" ibaresiyle birbirinden ayırmak suretiyle bilişim sistemine yetkisiz olarak sadece "girmek" fiilini tek başına suç haline getirmek istediği değerlendirilmektedir.

Tüm bunların yanında TCK'nın "Konut dokunulmazlığının ihlali" [239] maddesinde ifade edildiği şekilde, yetkili makamların izni olmaksızın kişilerin özel mülkiyetine girmek mümkün olmadığı gibi, günümüzde kişilerin özel alanı haline gelen bilişim sistemine yetkisiz erişim sağlanması da kişinin özel mülkiyetine ya da

---

[235] 6698 sayılı Kişisel Verilerin Korunması Kanunu http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf Sayılı http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

[236] M. Volkan Dülger, "**Bilişim Suçları**" Seçkin Yayıncılık, Ankara, 2004, s. 217

[237] Serdar Havuz, Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği "Yayınlanmış Yüksek Lisans Tezi" Genel Kurmay Başkanlığı Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, Uluslararası İlişkiler Ana Bilim Dalı, İstanbul, 2007, s. 144

[238] Dülger, Bilişim Suçları s.217 – Taşkın Bilişim Suçları s.20

[239] TCK**a.g.i.s.**e.t.: 20.06.2018

şahsiyetine taciz olarak kabul edilmektedir.[240] Bu noktadan hareketle bilişim sistemine girilmesi eyleminin tek başına suçun oluşumu için yeterli olacağı, failin hakkı olmaksızın bilişim sistemindeki dosyalara herhangi bir şekilde ulaşması ile suçun meydana geleceği ifade edilebilir.

3.2.1.3. Suçun Manevi Unsuru

Suçun oluşumu için AKSSS 2. Madde *"Yetkisiz Erişim"* ile paralel bir şekilde kast unsuru aranmaktadır. Metinde özel bir saik belirtilmediğinden genel kast yoluyla işlenen bir suç olduğu değerlendirilmektedir[241]. Buradan yola çıkarak istemeden ya da yanlışlıkla bir bilişim sistemine yetkisiz olarak girmenin suç oluşturmayacağı değerlendirilebilir.

Bilişim suçu işleme yöntemleri başlığı altında incelendiği üzere günümüzde failler, sistemde bulunan güvenlik zafiyetlerini kullanarak (trap doors), sistemdeki boşlukları değerlendirilerek (phishing) ya da "virüs", "solucan", "Truva Atı" gibi güvenlik kırıcı çeşitli programlar kullanarak bilişim sistemlerine nüfuz edebilmektedirler. Failin eylemini hangi yollarla gerçekleştirebileceğinin madde metninde sayılmamasından, suçun oluşumuna herhangi bir sınırlama getirilmek istenilmediği değerlendirilmektedir.

Madde metninin AKSSS'nin 2. Maddesinde yer alan "Yasadışı Erişim" başlıklı suçuna paralel olarak düzenlendiği, ancak sözleşme metninde sisteme erişimin tek başına suç olarak kabul edildiği görülmektedir.

Maddeye benzer düzenlemeler Avustralya, Belçika, Şili, Çin Fransa, İsviçre, İngiltere, Singapur, İrlanda, ABD, Yunanistan, İsrail, Malta, Hollanda, Finlandiya, Kanada ve Malezya hukuklarında da mevcuttur[242].

3.2.2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

Bu maddede, verilerin ve bilişim sisteminin zarara uğratılması suçlarının düzenlendiği görülmektedir.

244/1. Madde uyarınca b*ir bilişim sisteminin işleyişinin engellenmesi veya bozulmasının* müeyyide altına alındığı görülmektedir.

---

[240] Erdoğan, Bilişim Sistemine Girme ve Kalma Suçu, s. 1364

[241] Erdoğan, s. 1404

[242] Şaban Cankat Taşkın, "Bilişim Hukuku Uluslararası Anlaşmazlıklar" **TBB Dergisi,** Sayı 85, 2009, s. 335 http://tbbdergisi.barobirlik.org.tr/m2009-85-571 e.t.: 24.04.2018

TDK Büyük Sözlükte "e*ngellemek" i*stek, gereksinim veya bir davranışın belli bir sonuca ulaşmasının önlenmesi, "*bozulma*" ise bir şeyin kendisinden beklenilen işi yapamayacak hale gelmesi şeklinde tanımlanmıştır[243]. Bu tanımlardan yola çıkarak sistemin "engellenmesi" eyleminden, sistemin programlandığı işi yapmasının önüne geçilmesi, çalışmasının sınırlandırılması, sistemin faaliyetinin hızının düşürülmesi ya da tamamiyle kilitlenmesi,"bozulma" kavramından ise sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi anlaşılmalıdır. [244] Engelleme veya bozma eylemlerinin bilişim sistemlerinin sadece yazılım kısmına karşı değil, ana kart üzerinde bulunan parçaların yerinden çıkartılması, kırılması gibi fiziki hareketlerle donanım kısmına karşı da gerçekleştirilmesi mümkündür.

Maddenin ikinci fıkrasında[245]b*ir 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* ifadesi ileverilere zarar vermenin suç olarak düzenlendiği görülmektedir.

Maddenin üçüncü fıkrasında[246]*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 ifadesi ile* hem bilişim sisteminin zarar görmesi sonucunu doğuran hem de sistemdeki verilerin zarar görmesi sonucunu doğuran eylemlerin ağırlaştırılmış hali düzenlenmiş, bir banka veya kredi tüzel kişiliğine ait bilişim sistemine karşı işlenmesi halinde verilecek cezada artırıma gidilmesi düzenlenmiştir.

Son fıkrada[247]ise *ilk üç fıkrada tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde"* cezalandırılması öngörülmüştür.

İlgili fıkrada kişinin eyleminin başka bir suç oluşturmaması halinde yaptırıma bağlanması bir ön koşul sunarak, eylemin başka bir madde ile norm altına alınması halinde öncelikle bu norma göre cezalandırılacağı bildirilmiştir. Bu açıdan fıkranın tali bir hüküm niteliğinde olduğu değerlendirilmektedir.

---

[243] **"Engelleme, Bozulma",** TDK Büyük Sözlük, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5ae40a83f00f60.52341302 e.t: 24.04.2018

[244] Kurt, **a.g.e.** s. 161.

[245] TCK**a.g.i.s.**e.t.: 03.04.2018

[246] TCK**a.g.i.s.**e.t.: 03.04.2018

[247] TCK**a.g.i.s.**e.t.: 03.04.2018*)*

3.2.2.1. Korunan Hukuki Yarar

Suçta korunan hukuki değere yönelik iki farklı görüş bulunmaktadır, bunlardan ilki, korunan hukuki değerin bilişim sisteminde bulunan veriler üzerindeki tasarruf yetkisi, olan kişinin bu verilere herhangi bir engel olmaksızın ulaşması şeklindeki yararıdır[248], ikinci görüşe göre ise ilk fıkrada bilişim sistemindeki verilerin malikinin mülkiyet hakkı, ikinci fıkrada verilerin zilyedinin dokunulmazlığı ile sistemde bulunan verilerin niteliğinin korunduğu yasal haklardır[249].

Madde metnindeki "kimse" ifadesinden suçun failinin herkes olabileceği anlaşılmaktadır. Ancak verilerin malikinin ve zilyedinin, veriler üzerindeki tasarruf hakkı nedeniyle, suça konu eylemleri gerçekleştirmeleri elbette ki suç teşkil etmeyecektir. Bu nedenle verilerin failin tespitinde bilişim sisteminin ya da sistemde bulunan verilerin sahibinin, zilyedinin ve zararı kimin meydana getirdiğinin önemi oldukça fazladır.[250]

3.2.2.2. Suçun Maddi Unsuru

Maddenin birinci fıkrasında bilişim sistemine zarar vermek suç olarak sayılmışken ikinci fıkrada verilere zarar vermenin suç olarak düzenlendiği görülmektedir. Dikkat edilirse verilerin zarar görmesi sonucunu doğuran tüm fiiller suç olarak sayılmaya çalışılmıştır[251]. Buradan yola çıkarak suçun serbest hareketli suçlar kapsamında olduğu değerlendirilmektedir.

Madde 244/2'de belirtilen hareketlerden biri de "verilere erişilmez kılmak" fiilidir. Verilere erişilmez kılmak kavramıyla ilgili üç farklı görüş bulunmaktadır. İlk görüşe göre,[252] bu eylemden verilerin maliki ya da zilyedinin ihtiyaç duyduğu ya da talep ettiği anda verilere erişiminin önüne geçilmesi anlaşılmalıdır. Buna göre verilerin silinmesi, verilerin içinde bulunduğu sistemin bozulması fiilleri bu kapsamda değerlendirilebilecektir.

---

[248] Murat Volkan Dülger, Seçkin Yayınları, Bilişim Suçları, Ankara, 2004, s. 231
[249] Levent Kurt, Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, Ankara, 2005 , s. 162.
[250] Murat Dülger, Bilişim Suçları, s. 232
[251] Kurt, **a.g.e.** s. 161.
[252] Dülger, Bilişim Suçları, s.237

İkinci görüşe göre,[253] verilere erişilmez kılınmasının, verilere erişimi sağlayan şifre, parola gibi anahtar bir sözcüğün değiştirilmesi yoluyla veriye ulaşımın engellenmesi olduğunu savunmaktadır.

Üçüncü görüş ise,[254] eyleminin, sistemde anahtar kelime bulunmadığı halde sisteme anahtar kelime yerleştirmekle de işlenebileceği yönündedir. Bu durumda, sonradan yerleştirilen anahtar kelime hakkında bilgisi bulunmayan yetkili kullanıcı sonuç olarak verilere erişemeyecektir.

3.2.2.3. Suçun Manevi Unsuru

Birinci ve ikinci fıkralarda failin sisteme ve verilere çeşitli yollarla zarar verme saikiyle hareket etmesi gerektiğinden, suçun manevi unsurun kast olduğu, taksirle işlenmesinin mümkün olmadığı görülmektedir.[255]

Maddenin ilk iki fıkrasının değerlendirmesinde kastın niteliği konusunda iki görüş ortaya çıkmaktadır. İlk görüşe göre,[256] birinci fıkrada failin kastı, ne şekilde olursa olsun sistemin işleyişini bozmak veya sisteme zarar vermektir. Oysa ikinci fıkrada fail sistemin bütününe zarar vermek yerine, yalnızca sistemdeki belli verilere ve belli uygulama yazılımlarına zarar vermek kastıyla hareket etmektedir. Bunun sonucu olarak da ikinci fıkranın yaptırımı daha hafif düzenlenmiştir.

İkinci görüşe göre ise,[257] ikinci fıkradaki suçun oluşması için, failin eyleminin bilişim sisteminin işleyişini engelleyecek boyutta olmaması gerekir. Maddede tanımlanan seçimlik hareketlerden herhangi birinin sonucunda sistemin işleyişi engellenmişse, artık TCK m. 244/1 uygulanacaktır.

Dördüncü fıkra metninde yer alan "işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının" ibaresinden failin özel kastının bulunması gerektiği düşünülmektedir.[258]

TCK'nın 244. Maddesi AKSSS'nin "Verilere Müdahale" başlıklı 4. Maddesi ile "Sisteme Müdahale" başlıklı 5. Maddesine paralel şekilde düzenlenmiştir.

Karşılaştırmalı hukukta ise, madde de sayılan eylemler Fransa, Almanya, Danimarka, Finlandiya, Avusturya, İtalya, İsveç Ceza Kanunlarında genel olarak bilişim

---

253 Kurt, **a.g.e.** s. 170
254 Taşkın, Bilişim Suçları, s. 48
255 Karagülmez, **a.g.e.** s. 190
256 Dülger, Bilişim Suçları, s. 236
257 Karagülmez, **a.g.e.** s. 190
258 Karagülmez, **a.g.e.** s. 190

sistemlerine karşı mala zarar verme suçu biçiminde tanımlanmışken, İngiltere ve İrlanda bu eylemleri ayrı bir kanunda düzenlemiştir[259].

3.2.3. Banka veya Kredi Kartlarının Kötüye Kullanılması

Banka veya kredi kartlarının kötüye kullanılması, işlenebilmesi için bilişim sistemine ihtiyaç duyulan bir suç olması nedeniyle, bilişim suçu türüdür. Maddede bir bilişim sistemine bağlı olarak çalışan ve bilişim temelli bir faaliyetin sonucu olarak fonksiyon ifa eden banka ve kredi kartlarıyla işlenen suçlar kastedilmektedir[260].

5464 sayılı Banka ve Kredi Kartları Kanunu'nun[261] 3'üncü maddesinde "*banka kartı*", mevduat hesabı veya özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kart olarak tanımlanmışken yine aynı kanunda "*kredi kartı*", nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarası olarak tanımlanmıştır.

Ekonomik hayat içinde banka veya kredi kartının kullanılmasında üç unsurun bir araya gelmesi gerekmektedir. Bunlardan ilki, kişiye kullanım amaçlı olarak kartı temin eden banka veya finans kurumu, ikincisi, banka veya kredi kartıyla alışveriş yapılmasına imkan sağlayan ticarethaneler, üçüncüsü ise, banka veya finans kurumundan kart sağlayarak alışveriş yapan kart hamili.

245. madde gerekçesinde, maddenin banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasının, bu yolla çıkar sağlanmasının, önlenmesi ve faillerin cezalandırılması amacıyla kaleme alındığı belirtilmiştir[262]. Banka kartı ile kredi kartı arasındaki en büyük farkın banka kartının sahibinin hesabında nakit bulunması halinde kartı kullanması, kredi kartı sahibinin ise hesabında nakit olmasa da bankanın kart sahibine sağladığı kredi hesabında bulanan parayı kullanması olduğu söylenebilir.

Maddenin ilk fıkrasında[263] *başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya*

---

[259] Taşkın, Bilişim Hukuku Uluslararası Anlaşmazlıklar, s. 343
[260] Kurt, **a.g.e.** s. 186.
[261] 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, **Resmi Gazete** http://www.resmigazete.gov.tr/eskiler/2006/03/20060301-1.htm e.t: 02.04.2018
[262] Kurt, **a.g.e.** s. 177
[263] TCK**a.g.i.s.**e.t.: 03.04.2018

kullandırtarak kendisine veya başkasına yarar sağlaması, eylemi hüküm altına alınmıştır.

Maddenin ikinci fıkrasında [264] "b*aşkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi"* hakkında cezaya hükmedilmesi şeklindeki düzenleme ile suçun meydana gelmesi için öncelikle başkasına ait bir banka hesabının bulunması sonra bu hesapla ilişkilendirilmiş sahte banka veya kredi kartı oluşturulması gerekmektedir.

İlişkilendirme kavramı banka hesabıyla "bağ kurmayı" ifade etmektedir. Ancak oluşturulan bu bağ hukuka aykırı niteliktedir.[265]"sahte olarak oluşturulan" ifadesinden kartın alınması sırasında gerçeğe aykırı, ya da başka bir kişiye ait bilgilerin verilerek sahte kart oluşturulması anlaşılmalıdır. [266] Ayrıca oluşturulan bu kartın üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi fiilleri de müeyyide altına alınmıştır.

Üçüncü fıkrada[267]"s*ahte olarak oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi hakkında, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde…"* hapis cezasına hükmedilmiştir.

Dördüncü fıkrada ise[268]özel bir cezasızlık sebebi düzenlenerek*"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..."* faile ceza verilmeyeceği hüküm altına alınmıştır.

3.2.3.1. Korunan Hukuki Yarar

Bu suç aslında hırsızlık, dolandırıcılık, güveni kötüye kullanmak ve sahtecilik suçlarının özelliklerini barındığından tüm su suçların koruduğu hukuki yarar bu suçun da hukuki yararı olacaktır. [269] Sırasıyla hırsızlık suçunda, zilyetlik, dolandırıcılık suçunda, üçüncü kişilerin iyi niyetleri, güveni kötüye kullanmada,

[264] TCK**a.g.i.s.**e.t.: 03.04.2018
[265] Karagülmez, **a.g.e.** s. 219
[266] Kurt, **a.g.e.** s. 187
[267] TCK**a.g.i.s.**e.t.: 03.04.2018
[268] TCK**a.g.i.s.**e.t.: 03.04.2018

[269] Kurt, **a.g.e.** s. 177

mülkiyet[270], sahtecilik suçunda ise belgelere olan güven duygusu hukuki yarar olarak korunmaktadır.[271]

İlk fıkra metninde yer alan "kimse" ifadesinden suçun failinin herkes olabileceği anlaşılmaktadır. Bu konuda TCK'nın 37'nci maddesi[272] uyarınca suçun faili olmak için mutlaka uzman olmak gerekmemektedir. Ayrıca suçu kendi çıkarı için işleyen kişinin yanında "kartı kullandırtarak kendisine yarar sağlayan kişi" de fail olarak sorumlu olmaktadır.

Mağdur, mal varlığında suç nedeniyle azalma olan kişi olmakla beraber, mağdurun herkes olması mümkündür. Aracı olarak görev yapan banka veya finans kurumlarının durumu ise ticari itibarlarının zarar görmesi nedeniyle "suçtan zarar gören" olarak ifade edilebilir. Sonuç olarak, TCK'nin 245'inci maddesinin ihlali ile en büyük mağdurların bankalar ve banka ve kredi kartı sahibi vatandaşlar olduğu sonucuna varılmaktadır.

3.2.3.2. Suçun Maddi Unsuru

Suçun oluşumu için failin serbest seçimlik hareketlerden birini gerçekleştirerek banka veya kredi kartını kullanmak suretiyle kendisi ya da başka biri adına çıkar elde etmesi yeterlidir. Eylem sonucunda failin yarar elde etmemesi durumunda suç da oluşmayacaktır[273]. Ancak elbette ki icraya ilişkin hareketler tamamlandıktan sonra failin elinde olmayan nedenlerden dolayı yararın sağlanamaması durumunda teşebbüs hükümleri saklı kalacaktır.[274]

3.2.3.3. Suçun Manevi Unsuru

Madde metninde yer alan "kendisine veya başkasına yarar sağlayan kişi" ifadesinin lafzi yorumundan failin eylemlerini gerçekleştirirken bunun hukuka aykırı olduğunu bilmesi gerekmemektedir. Rızası olmaksızın başka birinin banka kartının kullanılması ya da sahte kart üretilmesi durumunda ise eylemin hukuka aykırı olduğunun bilinmemesi mümkün değildir. Dolayısıyla failin bilerek ve isteyerek eylemi gerçekleştirme kastıyla hareket etmesi suçun oluşması için yeterlidir.

---

[270] Sulhi Dönmezer, "Ceza Hukuku Özel Kısım", Filiz Kitabevi, İstanbul, 1983, s. 283-385-427.
[271] Kurt, **a.g.e.** s. 178.
[272] TCK**a.g.i.s.**e.t.: 03.04.2018
[273] Dülger, 2004, s. 260
[274] Gözüşirin, s. 77

245. madde benzeri düzenlemelere, ABD, Hollanda, İsviçre ve Almanya kanunlarında da rastlanmaktadır. ABD'de[275] 1986 tarihli "Elektronik Haberleşme Gizliliği Kanunu" (Electronic Communication Privacy Act) ve "Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Kanunu" (Computer Fraud and Abuse Act) ile "Kredi Kartlarının Kötüye Kullanılmasının Önlenmesi Kanunu" (Credit Card Fraud Act); Hollanda'da 1 Mart 1993 tarihli Ceza Kanunu değişikliği,[276] İsviçre'de 01.01.1995 tarihli Ceza Kanunu değişikliği, Almanya'da[277] Ceza Kanunu'nun 226.b maddesi bu tür suçları düzenleyen karşılaştırmalı hukuk normlarına örnektir.

3.3. 5237 Sayılı Türk Ceza Kanununda Diğer Bilişim Suçları

Araştırmanın bu bölümünde 5237 Sayılı TKC'da bilişim suçlarıyla işlenmesi mümkün olan suç tipleri incelenecek olup, bu suç tiplerinin ortak özelliği, geleneksel suç tiplerinin bilişim sistemleri aracılığıyla işlenmiş hali olmalarıdır. Suçların işlenmesi esnasında bilişim sistemleri araç olarak kullanıldığı için, madde metninde pek çok kez suçun ağırlaşmış şekli olarak yer aldıkları görülmektedir.

İlk olarak 5237 sayılı TCK'nın dokuzuncu bölümünde Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında yer alan "*Haberleşmenin Gizliliğini İhlal*" (m.132), "*Kişisel Verilerin Kaydedilmesi*" (m.135), "*Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme*" (m.136) ile "*Verilerin Yok Edilmemesi*" (m.138) suçları incelenecek, daha sonra "*Haberleşmenin Engellenmesi"* (m.124), "*Hakaret"* (m.125) " *Bilişim Sisteminin Kullanılması YoluylaHırsızlık"* (m.142/2.b.e), "*Bilişim Sisteminin Kullanılması Yoluyla Dolandırıcılık"* (m.158/1.b.f), "*Müstehcenlik"* (m.226)suçları incelenecektir.

3.3.1. Haberleşmenin Gizliliğini İhlal

5237 sayılı TCK'nın 132. Maddesinde,[278] *"kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır"* hükmü ilekişiler arasındaki haberleşmenin gizliliğini ihlal eden kimsenin eylemi yaptırım altına alınmış,. *"bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse,*

[275] Karagülmez, **a.g.e.** s. 197
[276] Yazıcıoğlu, Bilgisayar Suçları, s. 174
[277] Ayşe Nuhoğlu, **'Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması** , *Analiz Basım Yayınevi, İstanbul* 2002, s. 254
[278] TCK**a.g.i.s.**e.t.: 03.04.2018

verilecek ceza bir kat artırılır" hükmü ile deihlalin içeriğin kaydı suretiyle gerçekleştirilmesi artırım sebebi olarak sayılmıştır.

Maddenin ikinci fıkrasında[279] ise kişiler arasındaki haberleşme içeriklerinin hukuka aykırı olarak ifşa edilmesi hüküm altına alınmış, ancak ifşanın aleni yapılması şartı getirilmemiştir.[280]

Ancak elbette ki yasal soruşturma kapsamında hukuka uygun olarak yetkili mercilerce yapılan haberleşmenin içeriğine dair tespitler CMK 135. Madde[281] uyarınca "b*ir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması"* koşullarının bulunması halinde *"…şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir"* biçimindeki düzenleme kapsamında icra edilen eylemler hukukauygunluk nedeni oluşturacaktır.

Maddenin üçüncü fıkrasında[282] ise"k*endisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden…"* kişinin eylemi yaptırım altına alınmış olup bu kez suçun oluşumu için aleniyet şartı aranmaktadır. Suç genel kastla işlenebilir, takibi şikayete bağlıdır ve aleniyet suçun zorunlu unsurudur.[283]

Fıkranın devamında yer alan "i*fşa edilen bu verilerin basın ve yayın yoluyla yayımlanması…"* ibaresinde yer alan basın ve yayın kapsamına internette girmektedir. Suçun oluşumu için zarar aranmamakta dolayısıyla suç tehlike suçu olarak tasnif edilmektedir.[284]

3.3.1.1. Korunan Hukuki Yarar

Bu madde ile kişiler arasındaki haberleşme özgürlüğü ve haberleşmenin gizliğinin korunması amaçlanmıştır.[285]Maddenin ilk iki fıkrasına göre herkes, suçun faili ve mağduru olabilecek iken üçüncü fıkrada yer alan düzenleme uyarınca mağdur herkes olabilirken, fail haberleşmenin tarafların dışındaki biri olacaktır.

---

[279] TCK**a.g.i.s.**e.t.: 03.04.2018
[280] Taşkın, s. 93
[281] CMK http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5271&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=5271 e.t.: 03.04.2018
[282] TCK**a.g.i.s.**e.t.: 03.04.2018
[283] Taşkın, **a.g.e.** s. 94
[284] Taşkın, **a.g.e.** s. 94
[285] Ali Karagülmez, s. (2011) Bilişim Suçları Ve Soruşturma-Kovuşturma Evreleri, 3. Baskı, Seçkin Yayınları, Ankara, s. 339

3.3.1.2. Suçun Maddi Unsuru

Failin haberleşmenin gizliliğini ihlal etmesi yeterli olup, ihlalin nasıl gerçekleşebileceği tek tek sayılmamıştır, benzeri şekilde cezai müeyyidenin artırımı için kaydın yapılması yeterli olup, kaydın ne şekilde yapılması gerektiği madde de tanımlanmayarak serbestli hareketli hale getirilmiştir.

3.3.1.3. Suçun Manevi Unsuru

Suçun oluşumu için failde genel kast aranmaktadır[286] taksirle işlenmesi mümkün değildir, dolayısıyla failin bilerek ve isteyerek eylemi gerçekleştirmesi suçun oluşumu için yeterli olmaktadır.

3.3.2. Özel Hayatın Gizliliğini İhlal

5237 sayılı TCK'nın 134. Maddesinde[287], *"kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası"* ileyaptırıma bağlanmış, "*gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi"* artırım sebebi olarak sayılmıştır.

Özel hayatın gizliliği T.C. Anayasasının "Kişinin Hakları ve Ödevleri" başlıklı ikinci bölümünün 20. Maddesinde[288] yer alan temel haklardan biridir. Buna göre "*herkesözel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz."*

Maddenin ikinci fıkrasında[289] ise "k*işilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimsenin"* eylemi yaptırım altına alınmış, ifşanın basın ve yayın yolu ile de yapılabileceği belirtilmiştir. Suç, genel kast yolu ile işlenebilir, takibi şikayete bağlıdır, ilgilinin rızası, kanun hükmünün icrası, yasal mercilerce kanuna dayanılarak yapılan teknik izleme tedbiri ise hukuka uygunluk nedenlerini oluşturur.[290]

---

[286] Taşkın, **a.g.e.** s. 93
[287] TCK**a.g.i.s.**e.t.: 03.04.2018
[288] *T.C. ANAYASASI - MADDE 20 A.* ***Özel Hayatın Gizliliği*** http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.2709&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=2709 e.t.: 20.04.2018
[289] TCK**a.g.i.s.**e.t.: 03.04.2018
[290] Taşkın, **a.g.e.** s. 96.

3.3.2.1. Korunan Hukuki Yarar

Suçla korunan hukuki yarar, kişinin özel yaşamı ve bu yaşamın gizli alanı, suçun maddi unsuru özel hayatın gizliliğinin ihlalidir.[291] Çağımızın teknolojik olanakları sayesinde kişilerin hayatının topluma kapalı kısmına ait gizli ve özel bilgilerin dinlenmesi, kaydedilmesi, değiştirilmesi, silinmesi, hatta ortadan kaldırılması mümkün olmaktadır[292].

Suçun faili ve mağduru herkes olabilir. Ancak mağdur açısından her somut olayda mağdurun ve olayın kendi iç dinamikleri göz önünde bulunarak karar verilmesi gerekmektedir.[293] Mağdurun konumuna göre, sözgelimi sıradan bir vatandaş için elzem sonuçlar doğurabilecek bir ihlal şöhret olmuş biri için doğurmazken, sıradan bir kişi için bilinmesinde sakınca olmayan bir husus göz önünde bulunan bir sanatçı için büyük zararlar doğuran bir ihlal olabilmektedir.

3.3.2.2. Suçun Maddi Unsuru

İhlalin ne şekilde olması gerektiği madde de sayılmamıştır, yani suç serbest hareketli olup oluşumu için ihlalin gerçekleşmesi yeterlidir. Ancak ihlal edilen içeriğin kaydedilmesi ağırlaştırıcı neden olarak öngörülmüştür.

3.3.2.3. Suçun Manevi Unsuru

Suç genel kast ile işlenebilecek olup, kanun koyucu suçun oluşumu için özel kast aramamıştır. Suçun kasten işlenmesi arandığından taksirle işlenmesi mümkün olmamaktadır.

3.3.3. Kişisel Verilerin Kaydedilmesi

5237 sayılı TCK'nın 135. Maddesinde[294], hukuka aykırı olarak kişisel verilerin kaydedilmesi fiili yaptırım altına alınmıştır.

T.C. Anayasasının "Kişinin Hakları ve Ödevleri" başlıklı ikinci bölümünün 20. Maddesi ek fıkrasına göre[295] kişisel verilerin korunmasını talep etme hakkı; "*kişinin*

---

[291] Taşkın, **a.g.e.** s. 95

[292] Sevil Yıldız, "*Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi"*. **Doktora Tezi Özeti**. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 620. dergisosyalbil.selcuk.edu.tr/susbed/article/download/507/489 e.t.: 24.04.2018

[293] Ali Karagülmez, Bilişim Suçları Ve Soruşturma-Kovuşturma Evreleri s. 347

[294] TCK**a.g.i.s.**e.t.: 03.04.2018

[295] *T.C. ANAYASASI* - TCK**a.g.i.s.**e.t.: 04.04.2018 *i*

kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi…" kapsamaktadır. Aynı maddeye göre " *kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."*

Konuyla ilgili Avrupa Birliği tarafından, 24/10/1995 tarihinde 95/46/EC sayılı "Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi" kabul edilerek kişisel verilerin korunmasına ilişkin temel ilkeler ortaya konulmuş[296], 2002 yılında ise "Elektronik İletişim Sektöründe Kişisel Verilerin İşlenmesi ve Mahremiyetin Korunması"na ilişkin 2002/58/EC sayılı direktif kabul edilerek bilişim teknolojilerinin hızla gelişmesi karşısında yönergenin yetersiz kalması önlenmeye çalışılmıştır.[297]

Ayrıca maddenin ikinci fıkrasıyla[298]"k*işisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda…"*verilecek cezada yarı oranında artırım öngörülmüştür.

3.3.3.1. Korunan Hukuki Yarar

Kişisel Verilerin Korunması Kanunu'na göre[299]*kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi",* k*işisel verilerin işlenmesi* ise kişisel verilerin "*otomatik, yarı otomatik veya herhangi bir veri kayıt sisteminin parçası olan otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, ulaşılabilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi"* işlemleriniifade etmektedir. Buna göre suçta korunan hukuki yarar, kişinin özel hayatı ve buna ilişkin verilerdir.

---

[296] Oğuz Habip, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum." ***Uyuşmazlık Mahkemesi Dergisi*** 2013,C.3, S.3, s. 9 file:///C:/Users/Lenovo/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/5000145743-5000233431-1-PB.pdf e.t.: 21.04.2018

[297] Karagülmez, **a.g.e.** s. 229

[298] TCK**a.g.i.s.**e.t.: 04.04.2018

[299] *6698 sayılı Kişisel Verilerin Korunması Kanunu MADDE 3 – Tanımlar http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf*

3.3.3.2. Suçun Maddi Unsuru

Metindeki eylemin kişisel verilerin hukuka aykırı olarak bilişim sistemine yüklenmesi şeklinde tanımlanabilmesi mümkündür.[300] Hastanelerin hastalarına ilişkin, sigorta şirketlerinin müşterilerine ilişkin, ticari şirketlerin reklam, pazarlama ve satışlarına yönelik olarak kişilerin, sağlıklarına, ekonomik durumlarına, siyasi veya felsefi yönelimlerine ilişkin bilgileri toplamaları söz konusudur.

Anılan verilerin kişilerin haberi olmaksızın, onayları alınmaksızın kaydedilmesi durumunda kişisel verilerin kaydedilmesi suçunun oluşacağı değerlendirilmektedir. Zira madde gerekçesinde de, kişilere ait özel ve gizli bilgilerden oluşan kişisel verilerin amaçları dışında kullanılması ya da yetkisi olmayan veya kötü niyetli üçüncü şahısların eline geçerek hukuka aykırı olarak yararlanılması nedeniyle hakkında bilgi toplanan kişilerin büyük zararlara uğrayabildikleri, bu nedenle kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınmasının suç olarak düzenlendiği ifade edilmiştir.[301]

Ancak elbette ki kanuni düzenlemeler nedeniyle ya da yetkili bir merciin emri[302] uyarınca örneğin bir suçun önlenmesi amacıyla emniyet ve istihbarat tedbirleri uyarınca yapılan kayıtlar hukuka aykırılığı ortadan kaldırdığından suç oluşmayacaktır.

Buna ek olarak 5271 sayılı CMK'nın 134. Maddesinde[303] *"bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır"* düzenlemesinde olduğu gibi kanunun verdiği yetkiye dayanarak kişisel verilerin kayda alınmasının da hukuka uygunluk nedeni oluşturacağı değerlendirilmektedir.

3.3.3.3. Suçun Manevi Unsuru

Bu suç kasten işlenebilmekte, failin kastının hukuka aykırılığı da kapsaması gerekmektedir. Kişisel verilerin sahibinin rızası en temel hukuka uygunluk nedeni olup, rıza varsa suçun oluşması mümkün olmayacaktır. Ancak kişinin rızasını fiilin gerçekleştiği anda açık ya da üstü kapalı olarak belli etmesi gerekmektedir[304].

---

[300] Taşkın, **a.g.e.** s. 97.
[301] Karagülmez, **a.g.e.** s. 228.
[302] B. Zakir Avşar ve Gürsel Öngören, **Bilişim Hukuku,** Türkiye Bankalar Birliği Yayınları, İstanbul, 2010, s. 155.
[303] CMK **a.g.i.s.** e.t.: 04.04.2018
[304] Karagülmez, **a.g.e.** s. 232

3.3.4. Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme

5237 sayılı TCK'nın 136. Maddesinde[305], kişisel verilerin hukuka aykırı olarak bir başkasına verilmesi, yayılması veya gele geçirilmesi fiili norm altına alınmıştır.

Bu suç en yaygın şekilde bilişim alanında kimlik hırsızlığı yöntemi ile müşterilerin isim, nüfus bilgileri, sosyal güvenlik numaraları, kredi kartı bilgileri gibi bilgilerinin elde edilerek haksız kazanç elde edilmesi şeklinde işlenmektedir.[306]

3.3.4.1. Korunan Hukuki Yarar

Bu suç türü ile korunan hukuki yarar özel hayatın gizliliğidir. Her iki madde de yer alan suçun mağduru, suçun konusunun "kişisel veriler" olması nedeniyle gerçek kişiler iken fail herkes olabilecektir.[307]

3.3.4.2. Suçun Maddi Unsuru

Bu suç tipi seçimlik hareketli olup madde de belirtilen eylemlerin herhangi birinin veya bir kaçının gerçekleştirilmesiyle suç islenmiş olacak ve faile tek bir suçun cezası verilecektir.

Metinde yer alan "verme" fiilinin yanında kullanılan "yayma" fiili, vermenin yayma düzeyine ulaşmayan seviyede bir paylaşım olduğunu anlatmaktadır.[308] Buradan yola çıkarak kişisel veriyi yayma eyleminin başkasına verme eyleminden daha fazla kişiyle paylaşımı ifade ettiği söylenebilir. Anılan türde bir fotoğraf ya da videonun, internet ortamında bir web sitesinde paylaşılması ile veri sayısız kişiye yayılmış olmaktadır.

Ele geçirme fiili ise bir çok farklı şekilde olabilirken, en yaygın yöntem, bilişim sistemine yetkisiz erişim sağlayarak verilere ulaşmak şeklinde olmaktadır.[309]

3.3.4.3. Suçun Manevi Unsuru

Burada da hukuka aykırılık bir ön şart olduğundan suç ancak kastla işlenebilmektedir. Kişinin rızası, kanunun yerine getirilmesi, yetkili organın emrine uyma, meşru müdafaa, ıztırar ve bir hakkın kullanılması varsa bu suç oluşmayacaktır[310].

---

[305] TCK**a.g.i.s.**e.t.: 04.04.2018
[306] Karagülmez, **a.g.e.** s. 233
[307] Karagülmez, **a.g.e.** s. 236
[308] Karagülmez, **a.g.e.** s. 235
[309] Karagülmez, **a.g.e.** s. 235

3.3.5. Verilerin Yok Edilmemesi

5237 sayılı TCK'nın 138. Maddesine göre[311], "kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmemesi…" eylemi norm altına alınmış olup, ikinci fıkrada "suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması …" ve bu verinin yok edilmemesi durumunda verilecek cezada bir katı oranında artırım öngörülmüştür.

Madde kapsamına yalnızca devlete ait kurumlar tarafından tutulan kişisel veriler değil, aynı zamanda hukuka uygun olarak veri kaydı yapan özel kuruluşlar da girmektedir. [312] Yok etme veriyi geri getirilemeyecek şekilde tamamen ortadan kaldırmayı ifade etmektedir.

Suçun oluşması için temel olarak iki koşulun gerçekleşmesi gerekmektedir. Bunlardan ilki, kaydedilmiş kişisel verilerin kaydedilme süresinin yasa da belirlenmiş olması, yani sistemdeki kişisel verinin yok edilmesi gereken yasal bir son tarih olmasıdır.[313] Kanunda anılan verilerin sistemde tutulacağı sürenin açık ve anlaşılabilir biçimde yazılmış olması gerektiği değerlendirilmektedir. İkinci olarak ise verilerin sistem içinde yok edilmemesi gerekmektedir. Burada sözü edilen sistem bilişim suçları açısından bilişim sistemini, bilişim suçları dışında ise verinin muhafaza edildiği yeri işaret etmektedir[314].

3.3.5.1. Korunan Hukuki Yarar

Madde suçun unsurları açısından 135, 136 ve 137. Maddeler ile paralellik arz etmektedir, benzer şekilde korunmak istenen hukuki yarar özel hayatın gizliliği olup suçun konusu kişisel verilerdir. Suçun faili yasal olarak kaydedilmiş veriyi süresi dolmasına rağmen sistem içinde yok etmeyen kişidir. Bu kişi bir kamu görevlisi olabileceği gibi yasal yollarla kişisel verileri kaydeden özel kuruluşlarda çalışan bir kişi de olabilecektir. Mağdur açısından genel anlamda, kamu hakları zarar görmektedir.[315] Bu bağlamda kişisel verileri yok edilmeyen kişinin de muhakeme esnasında katılan olabileceği değerlendirilmektedir.

---

[310] Avşar ve Öngören, s. 156.
[311] TCK**a.g.i.s.**e.t.: 05.04.2018
[312] Karagülmez, **a.g.e.** s. 237
[313] Karagülmez, **a.g.e.** s. 238
[314] Karagülmez, **a.g.e.** s. 238-239
[315] Karagülmez, **a.g.e.** s. 239

3.3.5.2. Suçun Maddi Unsuru

Suçu oluşturan eylem veriyi yok etmemek olduğundan, ihmali hareketlerle işlenebilen bir suç türüdür. Kanunda imha süresi belirlenmiş bir verinin süresi dolduğunda imha edilmemesi, hükmün ihlal edeceğinden, suç kamu düzenine ilişkindir ve mağdurun rızası hukuka uygunluk nedeni oluşturmamaktadır.[316]

3.3.5.3. Suçun Manevi Unsuru

5237 sayılı kanunun 139. Maddesine göre[317]; kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme, verileri hukuka aykırı olarak ele geçirme, verileri yok etmeme suçları şikayete bağlı değil iken, haberleşmenin gizliliğini ihlal, kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması, özel hayatın gizliliğini ihlal suçları şikayete tabidir.

Ayrıca 5237 sayılı kanunun Dokuzuncu Bölümünde yer alan *"Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar"* başlığı altında yer alan suçların işlenmesi dolayısıyla tüzel kişiler açısından güvenlik tedbirlerine hükmolunabilmektedir (m.140)[318]

3.3.6. Hakaret

5237 sayılı TCK'nın sekizinci bölümünde "Şerefe Karşı Suçlar" başlığı altında yer alan *"Hakaret"* suçu (m.125)[319]araştırmanın kapsamı bakımından bilişim sistemi aracılığıyla gerçekleştirildiği durumlar açısından ele alınacaktır.

Maddenin ikinci fıkrasına göre, kişinin onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnadı veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldırı fiilleri, *"mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde"*üç aydan iki yıla kadar hapis veya adli para cezasına hükmolunacaktır.

Konuyla ilgili olarak Yargıtay'ın 04.03.2014 Tarih 2013/1791 Esas 2014/4946 Karar sayılı hükmünde[320]katılana ait e-posta ve facebook hesaplarının şifresini ele geçirerek hesaba erişimi engelleyen ve burada bulunan özel fotoğraflarını açtığı yeni bir

[316] Karagülmez, **a.g.e.** s. 239
[317]TCK**a.g.i.s.**e.t.: 05.04.2018
[318]TCK**a.g.i.s.**e.t.: 05.04.2018
[319]TCK**a.g.i.s.**e.t.: 05.04.2018
[320] Uyap Mevzuat Sistemi

facebook adresinde sergileyen ve *"Bandırma o...su Gizem A...'ı tanıyanlar buraya" "Bandırma'nın o..nu iyi tanıyın"* şeklinde yazılar yazansanığın, eyleminin *T.C.K..nun 244/2 ve 125/2. madde yollamasıyla 125/1. maddesi uyarınca hakaret suçundan cezalandırılması*gerektiği şeklindeki kararı uyarınca sosyal medya üzerinden yapılan hakaret ve sövme kapsamında değerlendirilebilecek paylaşımlar, 125.madde 2. fıkranın konusu olacaktır.

Maddenin dördüncü fıkrasında, hakaretin alenen yapılması cezada artırım sebebi olarak düzenlenmiştir. İnternetin tüm dünyada izlenebilir oluşu nedeniyle, bir web sayfası üzerinden yapılan video, fotoğraf, yazı gibi veri paylaşımının aleniyet unsuru taşıdığı ifade edilebilir.[321]

3.3.7. Bilişim Sisteminin Kullanılması Yoluyla Hırsızlık

"Hırsızlık" suçu (m.141) [322] temel olarak 5237 sayılı TCK'nın onuncu bölümünde "Malvarlığına Karşı Suçlar" başlığı altında düzenlenmiş olup, konumuz açısından "*Nitelikli Hırsızlık*" (m.142) suçunun bir türü olan bilişim sistemi aracılığıyla gerçekleştirilmesi hali üzerinde durulacaktır.

Madde metninde "Zilyedinin rızası olmadan başkasına ait taşınır bir malın, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alınması" olarak tanımlananhırsızlık suçunun bilişim sistemleri kullanılarak gerçekleştirilmesi durumunda verilecek cezada TCK 142/2- e bendi uyarıncaartırım öngörülmektedir. Çünkü fail burada, bilişim sisteminin kendisine sağladığı kolaylıktan yararlanmakta ve yakalanma riskini azaltmaktadır.[323]

Suçun oluşumu açısından, kişinin üzerinde bulunan paranın fiili olarak çalınması eylemi ile söz gelimi, bankada bir hesapta bulunan parasının bilişim sistemi aracılığıyla başka bir kaynağa aktarılması arasında, verilen zarar ve mağduriyet açısından bir fark bulunmadığı açıktır. Bilişim sistemlerinin güvenle kullanılması, aynı anda hızlı ve kolayca birçok kişiye ulaşılması ve bu tür suçların işlenmesinde faile kolaylık sağlaması nedeniyle nitelikli hal sayılmıştır.[324]İlk eylemde failin kendisini açık etme riski daha fazla iken, suçun bilişim sistemleri yoluyla işlenen şeklinde, sistemin yapısından kaynaklanan zorluklar nedeniyle failin bulunması daha zor olmaktadır.

---

[321] Taşkın, **a.g.e.** s. 116
[322]TCK**a.g.i.s.**e.t.: 05.04.2018
[323] Taşkın, **a.g.e.** s. 116.
[324] YCGK, 02.04.2013 tarih ve 2012/15-1293 Esas 2013/111 karar sayılı kararı, http://www.baltaci.av.tr/bilisim-sistemleri-araciligi-ile-nitelikli-dolandiricilik e.t 20.04.2018

Suçun konusu malvarlığı iken bilişim sistemleri suçta araç olarak kullanılmaktadır.[325]

3.3.8. Bilişim Sisteminin Kullanılması Yoluyla Dolandırıcılık

5237 sayılı TCK'nın 157. Maddesinde *"Dolandırıcılık"* suçunun *"hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kişinin kendisine veya başkasına yarar sağlaması"* şeklinde genel tanımı yapılmış olup [326] *"Nitelikli Dolandırıcılık*" (m.158) suçunun bir türü olan bilişim sistemi aracılığıyla gerçekleştirilmesi hali üzerinde durulacaktır.

TCK 158/1-f bendine göre [327] dolandırıcılık suçunun "b*ilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması"* suretiyle gerçekleştirilmesi durumunda cezada artırım öngörülmektedir.

Madde gerekçesinde de "bilişim sistemlerinin ya da banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır" açıklamalarına yer verilmekle, bu bentte, bilişim sistemleri ile banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık olmak üzere birden fazla nitelikli hal kabul edildiği görülmektedir. [328]

Burada hırsızlığın nitelikli halindeki düzenleme ile paralel bir yapı gözlenmektedir. Dolayısıyla eylemin bilişim sistemleri yoluyla işlenmesi fail açısından avantaj sağlayacağından eylemin nitelikli hal olarak düzenlenerek cezanın ağırlaştırılmasının caydırıcılık açısından isabetli olduğu değerlendirilmektedir.

Bilişim sisteminin kullanılarak bir insanın aldatılması, yani dolandırılması halinde bu bendin uygulanması mümkündür. Bilişim sisteminden yararlanılarak çıkar sağlanmışsa bilişim suçu veya bilişim sistemi kullanılmak suretiyle hırsızlık suçunun oluşması sözkonusu olacaktır[329].

Suçun konusu malvarlığı iken bilişim sistemleri suçta araç olarak kullanılmaktadır.[330]

---

[325] Taşkın, **a.g.e.** s. 117
[326] TCK**a.g.i.s.**e.t.: 05.04.2018 .
[327] TCK**a.g.i.s.**e.t.: 03.04.2018
[328] YCGK, 02.04.2013 tarih ve 2012/15-1293 Esas 2013/111 karar sayılı kararı, http://www.baltaci.av.tr/bilisim-sistemleri-araciligi-ile-nitelikli-dolandiricilik e.t.:20.04.2018
[329] YCGK, 02.04.2013 tarih ve 2012/15-1293 Esas 2013/111 karar sayılı kararı, http://www.baltaci.av.tr/bilisim-sistemleri-araciligi-ile-nitelikli-dolandiricilik e.t.: 20.04.2018
[330] Taşkın, **a.g.e.** s. 117

3.3.9. Müstehcenlik

Müstehcenlik suçu 5237 Sayılı TCK'nın "Topluma Karşı Suçlar" başlığı taşıyan yedinci bölümünde yer almaktadır. 226. Maddenin birinci fıkrasında müstehcenlik kavramının tanımın yapılmadığı ancak müstehcenlik suçunun failinin ayrıntılı olarak tanımlandığı görülmektedir

Buna göre müstehcenlik suçunun faili:

a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,
b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,
c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,
d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,
e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,
f) Bu ürünlerin reklamını yapan kişidir[331].

Madde metninde öncelikli olarak çocuğun müstehcen olduğuna kanaat edilen içeriklerden her şekilde korunmasının amaçlandığı, bu bakımdan AKSSS'nin 9. Maddesinde yer alan *"Çocuk Pornografisiyle Bağlantılı Suçlar"*ile paralel yapıda düzenlendiği görülmektedir.

AKSSS 9. Madde 2. Fıkra da "çocuk pornografisi" terimi, reşit olmayan şahsın cinsel içerikli eylemlerde bulunması, reşit olmayan şahıs görüntüsüne haiz kişinin cinsel içerikli eylemlerde bulunması, reşit olmayan şahsın cinsel içerikli eylemlerde bulunmasını betimleyen gerçekçi görüntüler olarak ayrıntılı tanımlanmışken, 226. Madde metninde müstehcenlik kavramının tanımlanmamasından, takdirin yasa uygulayıcılarına bırakıldığı değerlendirilmektedir.

"Müstehcen" kelimesi Arapça "Hücnet" kelimesinden türemiş olup sözlüklerde; "soysuzluk, karışıklık, bayağılık, aşağılık, kötü davranış" olarak tarif edilmektedir.[332]

[331] TCK**a.g.i.s.**e.t.: 05.04.2018
[332] Cevat ÖZEL, "Müstehcenlik Kavramı", http://archive.li/mWYit#selection-259.0-275.137 e.t: 20.06.2018

Müstehcenlik TDK Büyük Sözlükte[333] "açık, saçık, edebe aykırı, yakışıksız" olarak tanımlanmaktadır ancak neyin açık saçık ya da yakışıksız olacağı kişiden kişiye değişen, göreceli bir kavramdır. Bu tanımdan hareketle müstehcenlik kavramının çekirdeğinde ahlak kavramının yer aldığı söylenebilir. Genel ahlak Anayasa Mahkemesinin 1963/128 esas ve 1964/8 sayılı kararında tarif edilmiş olup, "belli bir zamanda, belli bir toplumun büyük çoğunluğunca benimsenmiş, kolayca anlaşılan ahlak kurallarının bütünü olduğu belirtilmiştir.[334]

Buradan yola çıkarak müstehcenlik kavramı ile yakından ilişki halinde bulunan ahlak kavramının da net bir tanımının yapılamadığı söylemek yanlış olmayacaktır. Hangi eylemin ahlaki hangisinin gayri ahlaki ya da müstehcen olduğu konusunda kişilerde farklı kanaatlerin meydana gelebileceğini, bu durumun müstehcenlikle ilgili kanun maddesinin somut olaya uygulanması sırasında hakimin takdir yetkisini oldukça genişlettiğini söylemek mümkündür.

Müstehcenliğin tespiti hususunda hakimin kişisel kanaatinin somut olayın takdirinde bu derece önemli rol oynamasının "eşit suça eşit ceza" ilkesine aykırılık teşkil edebileceği[335] ifade edilebilir. Karışıklıklara neden olmamak için AKSSS ve ABD'de olduğu gibi hangi eylemlerin pornografik hangi eylemlerin müstehcen sayıldığının belirtilmesi, yasadaki müstehcen kavramının sınırlarının ve içeriğinin açıkça belirtilerek pornografik olarak değiştirilmesi yerinde olacaktır.[336]

Müstehcenlik suçunun benzeri düzenlemelere karşılaştırmalı hukukta da rastlanmaktadır. ABD Çocukların Online Yayınlardan Korunması Yasası (Child Online Prevention Act), Çocuk Pornografisinin Önlenmesi Yasası (Child Pornografy Prevention Act), İngiltere'de Müstehcen Yayınlar Yasası (Obscene Publications Act)[337]özel olarak bu fiilleri düzenlemekte iken, Almanya, Fransa, Rusya gibi diğer ülkeler de bu tür eylemleri ceza kanunlarında suç olarak yaptırım altına almış bulunmaktadırlar.

İncelenen konu bakımından TCK m.226/1 metninde belirtilen suçun oluşabilmesi için bir bilişim sisteminde bulunan müstehcen verinin bu sistem kullanılarak çocuğa izlettirilmesi, dinlettirilmesi ya da müstehcenlik içeren verinin

---

[333] "**Müstehcenlik**", TDK Büyük Sözlük, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5adb60af0059f1.03945727 e.t.: 20.04.2018

[334] Özel, Müstehcenlik, **a.g.i.s**

[335] Taşkın, **a.g.e.** s. 123

[336] Murat Volkan Dülger, "İnternet İletişimin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme", **İstanbul Barosu Dergisi**, C.81, S.2007/4, s. 1522.

[337] Taşkın, **a.g.e.** s. 119.

çocuğun erişebileceği şekilde bulundurulması gerekmektedir. Bu durumda suç, çocuğa müstehcen veriyi izlettirmek, dinlettirmek şeklinde icrai hareketlerle işlenebileceği gibi müstehcen verilere çocuğun ulaşımını engelleyecek tedbirleri almama şeklinde ihmali hareketlerle de işlenebilecektir.[338]

Türkiye İstatistik Kurumu (TÜİK) 2016 verilerine göre ülkemizde internet erişim imkanı bulunan hane sayısı %76,3 olarak tespit edilmiştir, bu yaklaşık olarak on haneden sekizinin internet tüketicisi olduğu anlamına gelmekte iken 16-74 yaş grubu aralığında bilgisayar ve internet kullanım oranları sırasıyla %54,9 ve 61,2 olarak belirlenmiştir. İnternet erişimli cep telefonu kullanma oranı ise %96,9 olmuştur[339]. Bu noktadan hareketle, evinde internet paketi bulunan ve çocukları internete erişim sağlayan ebeveynlerin, çocukların müstehcen verilere erişimini engelleyecek çocuk filtresi yüklemek gibi, önlemler almamaları halinde bu suçun faili haline gelmeleri olasıdır.

Genel olarak maddenin değerlendirilmesinde, manevi unsuru genel kasttır, suçun faili herkes olabilecekken mağduru çocuklardır, seçimlik hareketli bir suçtur, kasten işlenmesi mümkündür, aleniyet şartı aranmamaktadır, aleniyet suçun oluşumunda seçimlik şarttır.[340]

Maddenin 2. fıkrasında "müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır düzenlenmesi yer almaktadır. Özellikle "yayınlayan" ifadesinin kapsamına internet yayınlarının da girmekte olduğu düşünülürse suçun kapsamının fazlaca genişletildiği değerlendirilebilir.[341] İnternet kullanıcılarının neredeyse yarısının internetteki pornografik görüntülerin tüketicisi oldukları[342] düşünüldüğünde, müstehcenlik kavramının kapsamının dar yorumlanmasının doğabilecek mağduriyetlerin önüne geçilmesi açısından önemi ortaya çıkmaktadır.

---

338 Taşkın, s. 129.

339 "Hane Halkı Bilişim Teknolojileri Kullanım Araştırması", Türkiye İstatistik Kurumu, 2016 http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779 e.t.: 20.04.2018

340 Taşkın, s. 130

341 Taşkın s. 122.

342 Wall, Cybercrimes, Crime and the İnternet. Routledge, 2003, s. 6 https://books.google.com.tr/books?hl=tr&lr=&id=6CqCAgAAQBAJ&oi=fnd&pg=PP1&dq=Wall,+Cybercrimes,+Crime+and+the+%C4%B0nternet+&ots=OSD2nfuFTJ&sig=HHxmyUzBEZB27IsJHyfckq1Bpc4&redir_esc=y#v=onepage&q=Wall%2C%20Cybercrimes%2C%20Crime%20and%20the%20%C4%B0nternet&f=false e.t.: 20.04.2018

Bu noktadan hareketle müstehcenliğe ilişkin kanun maddesinin uygulanması sırasında, müstehcen olarak düşünülen materyallerin yayılması ve çocukların müstehcen görüntülere konu olması ya da maruz kalmasının önüne geçilmesi ile yetişkinlerin cinsel özgürlüklerine getirilen kısıtlamanın boyutu arasında hassas bir denge kurulmasının oldukça önemli olduğu sonucuna varılabilmektedir.

Maddenin 3. Fıkrasında yer alan *"müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır"* hükmü, tam olarak AKSSS 9. Maddenin 2. Fıkrasında sayılan çocuk pornografisini karşılar niteliktedir. Burada çocuk olarak kastedilenin, TCK'nın 6. Maddesi (b) fıkrasında yer alan "henüz onsekiz yaşını doldurmamış kişi" olduğu açıktır.

Buna ek olarak AKSSS 9. Madde metninde suçun oluşması için çocuğun kullanılması şart koşulmamış animasyon programları ile yaratılan çocuk görüntüsü yada yetişkin bir kişinin görüntüsünün çeşitli bilgisayar programları ile çocuk izlenimi verecek şekilde değiştirilerek pornografik malzemeye konu edilmesi de yasa kapsamına alınmış olup, müstehcenliğe ilişkin madde kapsamında "temsili çocuk görüntüsü" deyiminden bu hususların kastedildiği düşünülmektedir.

Fıkranın devamında *"bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır"* hükmü yer almaktadır.

Çocuklara ilişkin müstehcenlik bakımından Yargıtay 5.CD, 01.10.2007 tarih ve 2007-9856 E; 2007-6957 K. sayılı son kararında[343] özetle *"...Çocuk pornografisi ve hayvanlarla yapılan cinsel davranışlara ilişkin çok sayıda resim ve video kaydını bilgisayar sistemi vasıtasıyla temin edip bilgisayarda sistematik bir şekilde depolama ve bulundurma fiili kişisel amaçlı dahi olsa 5237 sayılı TCK'nın 44. maddesi yollamasıyla 226/3. maddesindeki suçu oluşturur."* demiştir.

Dördüncü fıkra Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi" hakkındaki ceza hükümlerini içermektedir.

[343] Yargıtay Kararları Dergisi, Şubat 2008, s. 337.

Metinde sayılan davranışlardan, *"doğal olmayan yoldan yapılan cinsel ilişki"* kavramının muğlak kalmasından dolayı, burada kastedilen davranışların tam olarak ne olduğunun açıkça belirtilmesi gerekmektedir.[344] Zira bu durum hukukun temel ilkelerinden olan kanunilik ilkesine ters düşmektedir. Örneğin eşcinsel ilişki bazı kişiler için normal bir cinsel yönelim olarak değerlendirilirken bazı kişilere göre doğal olmayan bir ilişki türü olabilmektedir.

Fıkrada ayrıca anılan yazı, görüntü veya seslerin depolanması veya bulundurulması da norm altına alınmıştır. Bu durumda, kişinin kişisel bilgisayarında bu tür materyallerin bulunması da cezalandırma sebebi olabileceğinden devlet eliyle kişinin bilgisayarına, dolayısıyla yaşamının gizli alanına müdahale edilebilecektir.[345] Depolamak, bulundurmaktan farklı olarak, nicelik olarak daha çok ürünü çağrıştırmaktadır ancak depolamak[346] ayrıca, bir bellek cihazına veriyi yerleştirmek veya saklamak anlamında da kullanılabilmektedir.

Bilişim suçlarının özünde teknik bir konu olması, faillerinin genel olarak alanında eğitimli kişiler olması, bu suçlara yönelik oluşan sektörün sürekli gelişmesi konuyla etkin bir şekilde mücadele edilmesini önlemektedir. Bu nedenle yargılamaya konu olan ve içtihatlara yansıyan suç, fail ve mağdur bilgileri de ne yazık ki suçun boyutunu tam olarak yansıtmamaktadır.

---

344 Taşkın, **a.g.e.** s. 125

345 Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, Gözden Geçirilmiş 6. Baskı, Yetkin Yayınevi, Ankara, 2006 s. 464,

346 "**Depolamak**", TDK Büyük Sözlük, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5adb7a7dbfc949.60272403 e.t.: 20.04.2018

SONUÇ

Bilişim suçları sürekli gelişmekte ve değişmekte olan yapısıyla mevcut ceza hukuku sistemlerine adeta meydan okumaktadır. Gelişmiş ülkelerde 1970'li yıllardan itibaren başlayan bilişim suçları ile mücadele süreci ne yazık ki ülkemiz açısından 1991 yılında 765 Sayılı TCK'ya "…bilgileri otomatik işleme tabi tutan sistem" ibaresinin eklenmesi ile başlanmıştır.

Bilişim suçlarının sınıraşan yapısı nedeniyle ülkelerin ulusal mevzuatlarında düzenleme yapmaları yanında uluslararası işbirliği de önem arz etmektedir. Konuya ilişkin AKSSS'nin imzaya açılması tek başına yeterli olmamakla birlikte oldukça sevindirici bir gelişme olmuştur. AKSSS, bir yandan ülkelerin iç hukuklarında bilişim suçlarına yönelik etkili yasalar oluşturmalarına referans teşkil ederken, diğer yandan, internet kaynaklı mesafe suçlarında yaşanan artış nedeniyle, yetki ve çifte cezalandırılabilirlik konularında ortaya çıkan uluslararası sorunlara çözüm getirmiştir.

Türk ulusal mevzuatında bilişim suçları açısından özellikle AKSSS'nin imzalanması ve iç hukukta sözleşme hükümleri ile paralel normlara yer verilmesi ile etkili adımlar atılmıştır. Ancak bilişim sistemlerinin teknik yapısından kaynaklanan zorluklar nedeniyle suçlularla etkin şekilde mücadele edilmesinde özellikle delil elde edilmesi, mevcut delillerin saklanması ve yargılama aşamasında doğru şekilde değerlendirilmesi konularında zorluklar yaşanmaktadır.

TCK'da bilişim sistemleri yoluyla işlenmesi mümkün olan suç tipleri kapsamında incelenen müstehcenlik suçu (m.226) açısından hangi tür eylem ve davranışlarının müstehcen olduğunun kanunda net olarak tanımlanmamıştır. Eşitlik ve adalet ilkeleri çerçevesinde eşit suça eşit ceza uygulanabilmesi açısından tanımın netleştirilmesi önem arz etmektedir.

Aynı maddenin dördüncü fıkrasında "doğal olmayan yoldan cinsel ilişki" kavramının tam olarak hangi tür eylemleri ifade ettiğinin kanunilik ilkesi gereğince açıklanarak, ceza muhakemesi sırasında hukuk normunun somut olaya uygulanması konusunda yaşanacak güçlüklerin önüne geçilebileceği değerlendirilmektedir.

Yine TCK 226.maddesi 4.f. yer alan "depolamak" kavramı hem sayıca fazla olan bir şeyleri toplayarak bir araya getirmek ve saklamak hem de taşınabilir bellek ya da hard disk gibi bilişim sistemleri unsurları içinde toplamak gibi anlamları olması nedeniyle kavram karmaşası oluşturmaktadır.

Bilişim suçları açısından TCK'nın dokuzuncu bölümünde Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında incelenen suçlar ile ihlal edilen hakların niteliği itibariyle, yasaların etkin şekilde uygulanması, düzenlemelerin ulusal bazda kalmayıp, uluslararası işbirliğinin güçlendirilmesi gerekmektedir.

Siber terör konusunda tıpkı terör konusunda olduğu gibi üzerinde uzlaşılan bir tanım yapılamadığından dünya çapında buna ilişkin özel bir mevzuat bulunmamaktadır. Bu açıdan ulusal mevzuatımız da benzeri şekilde özel bir yasal düzenleme mevcut değildir.

Siber terör tehdidinin bir ülkeye karşı kullanılması şeklinde ortaya çıkan ve insanlığa karşı ciddi bir suç sayılan siber savaş ve siber terör suçları konusunda Roma Statüsü'nün usul hükümlerinde yapılacak bir takım değişiklikler Uluslararası Ceza Mahkemesi'nin (UCM) görevli ve yetkili hale getirilmesinin mümkün olduğu değerlendirilmektedir.

Önlem almanın tedavi olmaktan daha iyi olduğu noktasından hareketle öncelikle bir ulusal eylem planı hazırlanarak idari ve yasal düzenlemelerin yeni koşullara göre yeniden yapılandırılması yoluna gidilmeli, siyasal, bürokratik ve akademik kadroların etkin katılımı sağlanmalıdır.

Bir suçla mücadele edilebilmesi için önce eylemin yasalarla suç olarak tanımlanması gerekmektedir. Var olan mevzuat bilişim suçlarının gerisinde kalmaktadır. Bu nedenle olumlu ve olumsuz etkileri tüm boyutlarıyla düşünülerek etkili bir suç politikası kapsamında mevzuat üretilmesi, üretilen mevzuatın ise tutarlı şekilde uygulanması önem arz etmektedir.

Bilişim suçlarıyla mücadele atılacak adımlar hiç kuşkusuz tek tek kullanıcı bireylerin bu suç türüne karşı önleyici tedbirleri alma ve siber etik (sanal alamde davranış kuralları) konularında eğitilmesi ile başlamaktadır. Özellikle bilişim dünyasının yaygın kullanıcısı olan gençlerin yaşları itibariyle içinde bulundukları psikolojik durum nedeniyle yaşadıkları sanal alem - gerçek dünya çatışmasının ortadan kaldırılarak, bu bireylerin internet ortamında gerçekleştirdikleri haksız fiillerin gerçek dünyada somut zararlar meydana getirdiği hususunda bilinçlendirilmesi,bilişim suçu failliğinin önüne geçilmesi konusunda oldukça önemli olmaktadır.

Diğer yandan, büyük sermayeli ticari kuruluşlar, bilişim suçu mağduru olduklarının duyulması durumunda itibarlarının zedeleneceğini düşünerek, yetkili mercilere başvurmakta tereddüt yaşamakta bu suçlar nedeniyle meydana gelen ekonomik zararları karşılamak üzere bütçelerinden pay ayırmayı tercih etmektedirler.

Mali zararla sonuçlanan birçok bilişim suçu bu nedenle, soruşturmaya uğramamaktadır. Yetkili makamlara başvurama konusunda pasif davranılması bilişim suçu faillerine delilleri yok etme, kimliklerini gizleme ve yeni eylemlere kalkışma konularında için zaman ve olanak kazandıracaktır. Anılan nedenlerle ister gerçek ister tüzel kişi olsun, tüm bilişim suçu mağdurlarının zaman kaybetmeksizin soruşturma makamlarına başvurusu teşvik edilmelidir.

Bilişim sistemlerinin tüketicisi olan ülkemiz, ne yazık ki bu sistemlerin üretilmesi aşamasında bir varlık gösterememekte, sektörde hem yazılım hem donanım teknolojisi açısından nitelikli işgücü açığı bulunmaktadır. Bu nedenle bilişim alanında yetkin personelin yetiştirilmesi, ülkemizin tüketici konumundan üretici konumuna geçmesi teknoloji ile evrilen yeni dünya düzeninde var olabilmesi açısından önem arz etmektedir.

Son olarak bilişim suçlarıyla mücadeleye yönelik mevzuat oluşturulurken ve uygulanırken, internetin özgürlükçü yapısı göz önünde tutularak, özgürlük - güvenlik dengesinin sağlanması ve korunması konusunda sağduyulu davranılması büyük önem taşımaktadır.

KAYNAKÇA

AKINCI, Füsun Sokullu; "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi." **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası** S.59.1-2, 2001http://dergipark.ulakbim.gov.tr/iuhfm/article/viewFile/1023004153/1023003747

AKYAZI, Erhan, DİLMEN Necmi ve KARA Emel; Tolga "Toplumsal ve Ekonomik Etkileri Bağlamında Bilişim Çağının Yeni Tehdidi: Siberterör." Türkiye Bilişim Derneği, **2. İstanbul Bilişim Kongresi,** İstanbul, 3-4 Haziran 2008 https://www.researchgate.net/profile/Necmi_Dilmen/publication/228582062_TOPLUMSAL_VE_EKONOMIK_ETKILERI_BAGLAMINDA_BILISIM_CAGININ_YENI_TEHDIDI_SIBERTEROR/links/5527a0020cf229e6d63630e2/TOPLUMSAL-VE-EKONOMIK-ETKILERI-BAGLAMINDA-BILISIM-CAGININ-YENI-TEHDIDI-SIBERTEROeR.pdf

ALACA, Bahaddin; "Ülkemizde Bilişim Suçları ve İnternetin Bu Suça Etkisi", Yayınlanmamış **Yüksek Lisans Tezi**, Ankara Üniversitesi SBE, Ankara, 2008

ALTINOK, Ebru ve VURAL, Ali Fatih, "Bilişim Suçları" **Denetişim Dergisi,** 2011, http://dergipark.gov.tr/download/article-file/208853

ATASOY, F. "Kültürler Üzerinde Bilişim Devriminin Etkileri", **Modern Türklük Araştırmaları Dergisi**, S. 4 (2) http://mtad.humanity.ankara.edu.tr/IV-2_Haziran/27_MTAD_4-2_FAtasoy_163-178.pdf

AVŞAR, B. Zakir ve ÖNGÖREN Gürsel, **Bilişim Hukuku,** Türkiye Bankalar Birliği Yayınları, İstanbul, 2010, s. 155.

AYDIN, Emin Doğan, "Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları", **Marmara İletişim Dergisi**, Sayı 1, İstanbul, 1992, s. 20. http://dspace.marmara.edu.tr/bitstream/handle/11424/2788/5000011620-5000018676-1-PB%20(1).pdf?sequence=1

_____, **Bilişim Suçları ve Hukukuna Giriş**,Doruk Yayınları, Ankara, 1992

BARON Billy, ELLSWORTH Jill H. ve SAVETZ Kevin M. "The Internet Unleashed." **Technical Communication** 44.2, 1997

BAYILLIOĞLU Uğur; "**Uluslararası Ceza Mahkemesinin Yargı Yetkisi Açısından Saldırı Suçuna İlişkin Kampala Düzenlemeleri**", Uluslararası Hukuk ve Politika, Cilt:9, Sayı: 33.

BAYRAKTAR, Gökhan; **Siber Savaş ve Ulusal Güvenlik Stratejisi**, Yeniyüzyıl Yayınları, İstanbul, 2015

BECENİ, Yasin; "**Türk Hukukunda Bilişim Suçlarının Tasnif Şekilleri**", Bilişim ve Hukuk, Ankara Barosu Hukuk Kurultayı, 03-07 Ocak 2006, Ankara, s. 90

BEYHAN, Cem; "Türkiye'de Bilişim Suçları ve Mücadele Yöntemleri", **Polis Bilimleri Dergisi**, , S.4 Ankara, 2002

BEQUAİ, August; A Guide to Cyber Crime Investigationts. Computer And Security http://www.sciencedirect.com/science/article/pii/S016740489980056X(1998)

BİLA, C. "Bireysel ve Kitlesel İletişim Aracı Olarak İnternet ve Toplumsal Etkileri", **Yayınlanmış Yüksek Lisans Tezi**, Gazi Üniversitesi SBE, Ankara, 2001

BİRDİŞLİ, Fikret, Teori ve Pratikte Uluslararası Güvenlik Kavram- Teori- Uygulama, Üçüncü Basım, Seçkin Yayıncılık Ankara. 2017

BROADHURST, Roderic "Developments in The Global Law Enforcement Of Cyber-Crime". **Policing: An International Journal of Police Strategies & Management,** 29(3), 408-433. (2006) http://eprints.qut.edu.au/3769/1/3769_1.pdf

BRUNNSTEİN, Klaus; "From AntiVirus to AntiMalware Software and Beyond: Another Approach to the Protection of Customers from Dysfunctional System Behaviour" **22nd National Information Systems Security Conference,** July 23, 1999 http://www.bilisimogretmeni.com/genel/hacker-cracker-phreaker-nedir-nasil-calisirlar.html

Büyük Larousse Sözlük ve Ansiklopedisi Milliyet Gazetesi Yayınevi, İstanbul, 1994

CARTER, David L. ve KATZ Andra J.. "Computer Crime: An Emerging Challenge For Law Enforcement." **FBI L. Enforcement Bull.** S. 65, 1996

COLLIN, Barry C. "The Future Of Cyberterrorism: Where The Physical And Virtual Worlds Converge." **Crime and Justice International** S. 13, 1997

ÇAKMAK, Haydar ve ALTUNOK, Taner; **Suç Terör ve Savaş Üçgeninde Siber Dünya,** Barış Platin Kitabevi, Ankara, 2009

ÇEKEN, Hüseyin, "ABD'de İnternet Yoluyla İşlenen Suçlara İlişkin Düzenlemeler", **Askeri Adalet Dergisi**, S. 114, 2002

DEĞİRMENCİ, Olgun; "Bilişim Suçları", **Yayınlanmamış Yüksek Lisans Tezi,** Marmara Üniversitesi SBE, İstanbul, 2002

DEMİRBAŞ, Timur, **Kriminoloji**, Altıncı Basım, Seçkin Yayıncılık. Ankara, 2016

DENNİNG, Dorothy E. “Cyberterrorism”, **Calhoun Institutional Archive of the Naval Postgraduate Schooll, 2000, s. 1.** https://calhoun.nps.edu/bitstream/handle/10945/55351/Denning_Dorothy_2000_cyberterrorism.pdf?sequence=1

DESOUZA Kevin C. ve HENSGEN Tobin, “Semiotic Emergent Framework to Address the Reality of Cyberterrorism”. **Technological Forecasting and Social Change** 2003, S. 70 https://www.researchgate.net/profile/Kevin_Desouza/publication/223035624_A_Semiotic_Emergent_Framework_to_Address_the_Reality_of_Cyber_Terrorism/links/59e5d5560f7e9b0e1ab25345/A-Semiotic-Emergent-Framework-to-Address-the-Reality-of-Cyber-Terrorism.pdf

DİLEK, Halil İbrahim, “Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri”, **Yüksek Lisans Tezi**,Dicle Üniversitesi Sosyal Bilimleri Enstitüsü, 2007 https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=ePX_SaJ0b35Gq45swKG3lNl3QYX9BP5t7qYcP3mDfEjkxbtXfxNMY8BOgKRcgs7l

DOĞAN, Gürkan; "Uluslararası Ceza Mahkemesi ve Terör Suçları Açmazı: Çözüm Açısından Bir Değerlendirme." **Güvenlik Stratejileri Dergisi** S. 15, 2012 http://dergipark.ulakbim.gov.tr/guvenlikstrtj/article/view/5000098878

DÖNMEZER, Sulhi, “Ceza Hukuku Özel Kısım”, Filiz Kitabevi, İstanbul, 1983

DURSUN, Hasan, ‘Bilgisayar İle İlgili Suçlar”, **Yargıtay Dergisi**, S. 24, Ankara, 1998

DÜLGER, Murat Volkan; **Bilişim Suçları,** Seçkin Yayınları, Ankara, 2004

_____; “Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı Ve Uygulaması”, **Türkiye Adalet Akademisi Dergisi,** Yıl:8, Sayı:31, 2017 www.taa.gov.tr/.../karsilastirmali-hukuk-baglaminda-birlesik-krallik-ingiltere-hukuku

_____; “İnternet İletişimin Engellenmesinin Hukuksal Açıdan Değerlendirilmesi ve 5651 Sayılı Yasayla Getirilen Düzenleme”, **İstanbul Barosu Dergisi**, C.81, S.2007/4

Dictionnaire Larousse, Ansiklopedik Sözlük, İstanbul,1993, C.1, Milliyet Yayınları, 1993

EMİR, Nergiz, “Uluslararası Ceza Mahkemesi’nin Yargı Yetkisi Bakımından Saldırı Suçu” http://andhd.dergi.anadolu.edu.tr/yonetim/icerik/makaleler/27-published.pdf.

ELMUSHARAF, Mudawi Mukhtar; “Cyber Terrorism- A new kind of terrorism”, **Computer Crime Resourch Center**, 2004, http://www.crime-research.org/articles/Cyber_Terrorism_new_kind_Terrorism

ERALP, Özgür, 2017, “**Avrupa Konseyi Siber Suç Sözleşmesi Açıklayıcı Memorandum**”, Paragraf 44 http://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/

ERDAĞ, Ali İhsan; “Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.14, S.2, Ankara, 2010

ERDOĞAN, Yavuz; “Bilişim Sistemine Girme ve Kalma Suçu” s. 1367 http://hukuk.deu.edu.tr/dosyalar/dergiler/dergimiz-12-ozel/3-kamu/6-yavuzerdogan.pdf

ERSOY, Yüksel, “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”, **Ankara Üniversitesi Siyasal Bilimler Dergisi**, S. 49, Ankara, 1994 http://webftp.gazi.edu.tr/hukuk/dergi/14_2_10.pdf

FURNELL S. M. ve WARREN Matthew J.. "Computer Hacking And Cyber Terrorism: The Real Threats İn The New Millennium?." **Computers and Security** S. 18.1 1999, s. 29. https://s3.amazonaws.com/academia.edu.documents/50731522/10.1016_S0167-40489980006-6.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523809536&Signature=JKkhs9yP9zmK3Eh%2Bt%2FwztoWbSr0%3D&response-content-disposition=inline%3B%20filename%3DComputer_Hacking_and_Cyber_Terrorism_The.pdf

GÖZLER, Kemal, **“Genel Hukuk Bilgisi”,** Yedinci Baskı,Ekin Basım Yayım Dağıtım, Bursa, 2008, s. 3-4 http://www.anayasa.gen.tr/ghb.pdf e.t.: 13.02.2018

GRAND, Joe and Friday July, "Advanced Hardware Hacking Techniques." Defcon 12. 2004, http://grandideastudio.com/wp-content/uploads/advanced_hardware_hacking_ slides.pdf

GRANVİLLE, Johanna, “The Dangers Of Cyber Crime And A Call For Proactive Solutions” **Australian Journal of Politics and History,** Vol. 49 Clemson University, 2003, s. 102.

GREEN, Joshua, "The Myth of Cyberterrorism." **Washington Monthly** S. 34, 2002, s. 2.http://werzit.com/intel/regions/cyber/articles/archives/Myth%20of%20Cyberterrorism.pdf

GÜLEŞ, Mahmut Tekin, GÜLEŞ, Hasan K. ve BURGE Tom; **Değişen Dünyada Teknoloji Yönetimi**, Damla Ofset, Konya, 2000, s. 83.

GÜNAY, Durmuş ve ARIDIRU Ali, "Bilim ve Teknolojiye Yöneliş", **I. Teknoloji Kalite ve Üretim Sistemleri Kongresi**, 1999, Sakarya Kalite Derneği Adapazarı, s.22-34, https://www.researchgate.net/profile/Durmus_Gunay/publication/317662173_Bilim_ve_Teknolojiye_Yonelis/links/5947be17aca27242cda7604a/Bilim-ve-Teknolojiye-Yoenelis.pdf

GÜRSON, Ali Poyraz ve GÖKER Çağatay Fehmi, "Turkey-Russia Relations After The Cold War Era And The Middle East Policies." **Advances in Social Sciences Research Journal** S. 4.5, 2017, s.24 http://scholarpublishing.org/index.php/ASSRJ/article/download/2823/1670

GÜMÜŞ, Ç. "Bilişim Suçları İle Mücadelede Polisin Eğitimi", **Yayımlanmamış Doktora Tezi**, Fırat Üniversitesi SBE, Elazığ, 2008, s. 43-44.

GÜRKAYNAK, M. ve İREN A.A. "Reel Dünyada Sanal Açmaz: siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, S.2, s. 263-279

HABİP, Oğuz; "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum." ***Uyuşmazlık Mahkemesi Dergisi*** 2013,C.3, S.3, s. 9 file:///C:/Users/Lenovo/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/5000145743-5000233431-1-PB.pdf

HALDER, Debarati and JAİSHANKAR Karuppannan; **Cyber crime and the victimization of women: laws, rights and regulations**. Information Science Reference, Manonmaniam Sundaranar University Press, India, 2012.

"Hane Halkı Bilişim Teknolojileri Kullanım Araştırması", Türkiye İstatistik Kurumu, 2016 http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779

HAVUZ, Serdar; Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği "Yayınlanmış Yüksek Lisans Tezi" Genel Kurmay Başkanlığı Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, Uluslararası İlişkiler Ana Bilim Dalı, İstanbul, 2007

HEKİM, Hakan ve BAŞIBÜYÜK Oğuzhan; “Siber Suçlar ve Türkiye’nin Siber Güvenlik Politikaları”, **Uluslararası Güvenlik ve Terörizm Dergisi,** Sayı 4, Ankara, 2013,s. 150-151. https://s3.amazonaws.com/academia.edu.documents/37825457/Siber_Suclar_ve_Turkiyenin_Siber_Guvenlik_Politikalari.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523810782&Signature=99Akwi3eBHCL8YuDaj3oyLjJW40%3D&response-content-disposition=inline%3B%20filename%3DSiber_Suclar_ve_Turkiyenin_Siber_Guvenli.pdf

HOOPER, Christopher, MARTİNİ Ben, and CHOO Kim-Kwang Raymond. "Cloud Computing And İts İmplications For Cybercrime İnvestigations İn Australia." **Computer Law & Security Review,** 29.2 2013, p. 152-163. http://search.ror.unisa.edu.au/record/UNISA_ALMA51109818270001831/media/digital/open/9915914119501831/12143169490001831/13143168750001831/pdf

Internet World Stats, “World Internet Usage and Population Statistics”, 2017 https://www.internetworldstats.com/stats.htm e.t:

İÇEL, Kayıhan; "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası S.** 59.1-2, Ankara, 2001

İLBAŞ, Çığır, “Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi”, **Yüksek Lisans Tezi.**Başkent Üniversitesi FBE, 2009, s. 16. http://acikerisim.baskent.edu.tr:8080/bitstream/handle/11727/2287/00457.pdf?sequence=1&isAllowed=y

JİNPİNG, Xi, “The Governance Of China” Çeviren; Foreign Languages, Press Co. Kaynak Yayınları, İstanbul, 2017

KABAY, Michel E. “A Brief History Of Computer Crime: An İntroduction For Students”. School of graduate studies, 2008.http://www.mekabay.com/overviews/history.pdf

KASAPOĞLU, Can, “Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında” **EDAM Siber Politikalar Kağıtları Serisi,** 2017, s. 8. http://edam.org.tr/wp-content/uploads/2017/10/sibersavas_tr_rbs_logo.pdf

KARA, Mehmet ve ÇELİKKOL Soner, "Kritik Altyapılar: Elektrik, üretim ve Dağıtım Sistemleri, SCADA Güvenliği", **4. Ağ ve Bilgi Güvenliği Sempozyumu** (4), Kocaeli http://www.emo.org.tr/ekler/2afc6bfb6139e85_ek.pdf

KARAGÜLMEZ, Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Üçüncü Basım, Seçkin Yayıncılık, 2009.

KARDAŞ, Ümit, "Bilişim Dünyası ve Hukuk", **Karizma Dergisi**, S. 13, 2003, s. 8.

KNAKE, Robert, K. **Internet Governance in an Age of Cyber Insecurity.** No. 56. Council on Foreign Relations, 2010 https://books.google.com.tr/books?hl=tr&lr=&id=FhuC1gIm_1AC&oi=fnd&pg=PR7&dq=Robert,+K.+Knake+Internet+Governance+in+an+Age+of+Cyber+Insecurity.+No.+56.+Council+on+Foreign+Relations,+2010,+s.+5+&ots=MXk2UeNIdJ&sig=mvh1nSgAIhquBh2f7ipXbtODIYQ&redir_esc=y#v=onepage&q&f=false

KRATCHMAN, Stanley, SMİTH Jacob Lawrence, and SMİTH Murphy, **"The Perpetration and Prevention of Cybercrime**s. https://www.researchgate.net/profile/Murphy_Smith/publication/228301055_The_Perpetration_and_Prevention_of_Cybercrimes/links/56df253d08ae9b93f79a8de7.pdf 2008

KURT, Levent, **Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Seçkin Yayınları Ankara, 2005

_____; Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, Ankara, 2005

LEVİN, Avner and ILKİNA Daria. "International comparison of cyber crime." **Privacy and Cyber Crime Institute,** Ted Rogers School of Management, Ryerson University, 2013, s. 24. https://www.ryerson.ca/content/dam/tedrogersschool/privacy/AODAforms/Ryerson_International_Comparison_ofCyber_Crime_-March2013%20AODA.pdf

LİANG, Bin ve LU Hong. "Internet Development, Censorship, And Cyber Crimes İn China." **Journal of Contemporary Criminal Justice** 26.1 2010

LLOYD, Ian J. **Information Technology Law**, Third Edition, Butterworths, London, Edinburg, Dublin, 2000, p.8.

Meydan Larousse Büyük Lugat ve Ansiklopedisi, Meydan Yayınevi, (EK-2), İstanbul, 1992

NUHOĞLU, Ayşe, **'Ceza Hukukunda Kredi Kartlarının Kötüye Kullanılması** , *Analiz Basım Yayınevi, İstanbul* 2002

ÖĞÜN, Mehmet Nesip ve Adem KAYA, 'Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", Güvenlik Stratejileri Dergisi, S. 18, Ankara, 2013http://dergipark.gov.tr/download/article-file/84487

ÖNOK, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği" **Prof. Dr. Nur Centel'e Armağan**, 2013, s.1239 http://dergipark.gov.tr/download/issue-file/517

ÖZCAN, Mehmet, "Siber Terörizm ve Uluslararası Tehdit Boyutu", http://www.uiportal.net/siber-terorizm-ve-ulusal-guvenlige-tehdit-boyutu.html, 2011

ÖZERKMEN, Necmettin, "Terör, Terörizm ve Terörün Küreselleşmesi." **Polis ve Sosyal Bilimler Dergisi** S.2.1 Ankara, 2004, s. 248.

ÖZDİLEK, Ali Osman, **İnternet ve Hukuk**, Papatya Yayıncılık, Ankara, 2002

_____, "Kurtlar ve Zombiler : Worm'ların ve Ddos Ataklarının Hukuki İncelemesi", 2003 http://www.hukukcu.com/bilimsel/kitaplar/wormlarhukuki.htm

ÖZKAN, Tezcan, "Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi", **Yayınlanmış Yüksek Lisans Tezi**, Anadolu Üniversitesi SBE,Eskişehir, 2006, **s.** 83 http://www.ibrarian.net/navon/paper/NTERNET_S_TELER_NE_Y_NEL_K_B_R__ER_K_ANAL_Z.pdf?paperid=17691465

ÖZKIŞLALI, Gizem "Küreselleşme, İnternet ve Terörizmin Değişen Yüzü: Siber Terörizm", **Yayımlanmış Yüksek Lisans Tezi** . Hacettepe SBE, Ankara 2008, s. 71 https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=UPP_Zu9isEmWGFXFCBYasWZZPKrSaJUj7N8CJG3RcnZ2MKtGrRQIVjX3Ibazmb3H

ÖNEMLİ, Murat, "İnternet Suçlarıyla Mücadele Yöntemleri", **Yayınlanmış Yüksek Lisans Tezi**, Türkiye, Ortadoğu ve Amme İdaresi Enstitüsü, Ankara, 2004, s. 38

POCAR, F., "New Challenges For International Rules Against Cyber-Crime", **European journal on Criminal Policy and Research,** 2004,S.1, S. 24-39

Qİ Man, WANG Yongquan ve XU Rongsheng, "Fighting Cybercrime: Legislation İn China". **International Journal of Electronic Security and Digital Forensics**, 2(2), 2009

RAJAGOPALAN, Santosh; "A Study of Security Problems Associated with the Telephone Network." Oregon State University, Department of Electrical and Computer Engineeringhttp://www.tucops.info/tucops3/phreak/general/r2.pdf , 2000

RUVİC, Dado, "**Russia Prepares New Un Anti-Cybercrime Convention – Report"** Reuters, 14 Nisan 1997 tarihli internet haberi, https://www.rt.com/politics/384728-russia-has-prepared-new-international/

SAYGILI, İsmail, h4cktimes, 2015 https://h4cktimes.com/arastirma-ve-analiz/siber-suc-cografyasi-2014te-neler-yasandi.html,

SAİNİ, Hemraj / YERRA Shankar Rao / PANDA T. C.. "Cyber-crimes and Their İmpacts: A Review." **International Journal of Engineering Research and Applications** C. 2. S. 2, 2012 s. 203. https://s3.amazonaws.com/academia.edu.documents/38524184/10.1.1.417.1369.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1523809470&Signature=fvF%2BX60JPk1c5JsryZfpguq25Uk%3D&response-content-disposition=inline%3B%20filename%3DCyber-Crimes_and_their_Impacts_A_Review.pdf

SCHEFFER, David, "The Missing Pieces in Article 8 bis (Agression) of the Rome Statute" http://www.harvardilj.org/2017/04/the-missing-pieces-in-article-8-bis-aggression-of-the-rome-statute/ e.t.:20.06.2018

SCHJOLBERG, Stain, s. Computer-Related Offences,, Fransa, 2004, http://www.cybercrimelaw.net/documents/Strasbourg.pdf

SCHÖNKE, A. 1996, s.354 Akt. Kurt, s, 106.

SINAR, Hasan, **İnternet ve Ceza Hukuku**,Beta Yayınları, İstanbul, 2001, s. 21.

SIRIMCIYAN, Ali "Domain Hırsızları", **CHIP Dergisi**, S. 3, Doğan Burda Dergi Yayıncılık, İstanbul, 2000, s. 164.

SINROD, Eric J ve WİLLİAM P. Reilly, "Cyber-crimes: A Practical Approach To The Application Of Federal Computer Crime Laws." **Santa Clara Computer and High Tech. *LJ*** 16 (2000): 177. https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.tr/&httpsredir=1&article=1258&context=chtlj

SMİTH, R.G., GRABOSKY P. ve URBAS G., "Cyber Criminals On Trial", **Cambridge Universty Press.** Australia, 2006. https://www.researchgate.net/profile/Gregor_Urbas/publication/233023456_Cyber_Criminals_on_Trial/links/5407fbb60cf2c48563b891d6.pdf

SOYASLAN, Doğan, **Ceza Hukuku Özel Hükümler**, Gözden Geçirilmiş 6. Baskı, Yetkin Yayınevi, Ankara, 2006 s. 464,

ŞAMLI, Rüya, "Türk ve Dünya Hukukunda Bilişim Suçları" (2010).. Akademik Bilişim. s.101.http://docplayer.biz.tr/3758191-Turk-ve-dunya-hukukunda-bilisim-suclari.html

TAŞKIN Şaban Cankat, **Bilişim Suçları,** Beta Basım, İstanbul, 2008

_____, "Bilişim Hukuku Uluslararası Anlaşmazlıklar" **TBB Dergisi,** Sayı 85, 2009, s. 335 http://tbbdergisi.barobirlik.org.tr/m2009-85-571

TAŞKIN, Ahmet ve ZENGİN İbrahim "Ceza Hukuku El Kitabı" Eda Matbaası, Ankara, 2004 Temel Britannica, s. 189.

Thema Larousse, Milliyet Gazetesi Yayınevi, İstanbul, 1993, s.456.

TURHAN, Oğuz, "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)" **Planlama Uzmanlığı Tezi** Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, 2006, s. 95http://www.bilgitoplumu.gov.tr/wp-content/uploads/2015/01/Bilgisayar_Aglari_ile_ilgili_Suclar_OguzTurhan.pdf

Türk Dil Kurumu Büyük Türkçe Sözlük
http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5ab5225217f746.17587618 e.t.: 08.10.2017

"Varşova Zirvesi Sonuç Bildirgesi" https://www.nato.int/cps/en/natohq/official_texts_133169.htm

YAYCI, Esra, "Bilişim Suçları", **Yayınlanmış Yüksek Lisans Tezi**, Gazi Üniversitesi SBE, Ankara, 2007

YAZICIOĞLU, Recep Yılmaz **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle,** Alfa Basın Yayın Dağıtım, Bursa, 1997

_____, "Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim sistemine Girme Eylemi" 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara, 2009, s. 81

Yargıtay Kararları Dergisi, Şubat 2008, s. 337.

YCGK, 02.04.2013 tarih ve 2012/15-1293 Esas 2013/111 karar sayılı kararı, http://www.baltaci.av.tr/bilisim-sistemleri-araciligi-ile-nitelikli-dolandiricilik

YCGK,. 2009/11-193, K. 2009/268, 17.11.2009 http://www.turkhukuksitesi.com/serh.php?did=6165

YENİDÜNYA, Ahmet Caner ve DEĞİRMENCİ, Olgun **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.** Legal Yayıncılık, İstanbul, 2003

YETİM, Servet, "Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi",**Türkiye Adalet Akademisi Dergisi**, S. 17, 2014, s. 189.http://www.taa.gov.tr/indir/siber-suclar-yargilama-yetkisi-ve-yeni-bir-model-onerisi-bWFrYWxlfDE4MjEyLTQ1MWRkLWQ5ZWI5LWVkMTY0LnBkZnwzMjk/

YILDIZ, Sevil, *"Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi"*. **Doktora Tezi Özeti**. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 620.

dergisosyalbil.selcuk.edu.tr/susbed/article/download/507/489 e.t.: 24.04.2018

YİP, Michael, "An İnvestigation İnto Chinese Cybercrime And The Underground Economy İn Comparison With The West" **Doctoral Dissertation**, University of Southampton, 2010, https://eprints.soton.ac.uk/273136/1/dissertation_final.pdf

YÜCEL, Mustafa T. "Bilişim Suçları", **Ankara Barosu Dergisi**, S. 49 (4), Ankara, 1992, s.505.

WALL, Cybercrimes, Crime and the İnternet. Routledge, 2003, s. 6 https://books.google.com.tr/books?hl=tr&lr=&id=6CqCAgAAQBAJ&oi=fnd&pg=PP1&dq=Wall,+Cybercrimes,+Crime+and+the+%C4%B0nternet+&ots=OSD2nfuFTJ&sig=HHxmyUzBEZB27IsJHyfckq1Bpc4&redir_esc=y#v=onepage&q=Wall%2C%20Cybercrimes%2C%20Crime%20and%20the%20%C4%B0nternet&f=false

WEIMANN,Gabriel"Terror On The Internet: The New Arena, The New Challenges", **US Institute of Peace Press.**2006, s. 3.https://www.researchgate.net/profile/Gabriel_Weimann/publication/238077713_Terror_on_the_Internet_The_New_Arena_The_New_Challenges/links/0f31753872b79cea95000000/Terror-on-the-Internet-The-New-Arena-The-New-Challenges.pdf

WILKINSON, Paul, **Political Terrorism**, NewYork, 1974, s. 9.

WU Min, MİLLER Robert C. and GARFİNKEL Simson L.. "Do Security Toolbars Actually Prevent Phishing Attacks?." **Proceedings of the SIGCHI conference on Human Factors in computing systems.** ACM, http://cs.union.edu/~fernandc/srs200/readings/SecurityToolbars.pdf

KANUNLAR

Avrupa Konseyi Siber Suç Sözleşmesi

http://www.bhd.org.tr/dokumanlar/Avrupa%20Konseyi%20Siber%20Suclar%20Sozlesmesi%20TR.docx

Birleşmiş Milletler Antlaşması,

https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/3-30.pdf

Ceza Muhakemesi Kanunu

http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5271&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=5271

Roma Statüsü

http://sorular.rightsagenda.org/Uploads/UCM%20MEV/Roma%20Stat%C3%BCs%C3%BC.pdf

T.C. Anayasası

http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.2709&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=2709

765 Sayılı Türk Ceza Kanunu, http://www.ceza-bb.adalet.gov.tr/mevzuat/765.htm

3713 Sayılı Terörle Mücadele Kanunu,

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf

5237 Sayılı Türk Ceza Kanunu,

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu, **Resmi Gazete**

http://www.resmigazete.gov.tr/eskiler/2006/03/20060301-1.htm

6698 sayılı Kişisel Verilerin Korunması Kanunu

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

EKLER

EK-1: Etik Kurulu Onay Belgesi

T.C.
ÇAĞ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
TEZ / ARAŞTIRMA / ANKET / ÇALIŞMA İZNİ / ETİK KURULU İZİNİ TALEP FORMU VE ONAY TUTANAK FORMU

ÖĞRENCİ BİLGİLERİ	
T.C. NOSU	13029914652
ADI VE SOYADI	Damla ERVEYDAN
ÖĞRENCİ NO	20162020
TEL. NO.' LARI	0 555 613 55 48
E - MAİL ADRESLERİ	damlaerveydan@gmail.com
ANA BİLİM DALI	Kamu Hukuku
PROGRAM ADI	Kamu Hukuku
BİLİM DALININ ADI	Kamu Hukuku
HANGİ AŞAMADA OLDUĞU (DERS / TEZ)	TEZ
İSTEKDE BULUNDUĞU DÖNEME AİT DÖNEMLİK KAYDININ YAPILIP-YAPILMADIĞI	........../.............................. DÖNEMİ KAYDINI YENİLEDİM.
ARAŞTIRMA/ANKET/ÇALIŞMA TALEBİ İLE İLGİLİ BİLGİLER	
TEZİN KONUSU	Türk Ceza Kanunu'nda Bilişim Suçları
TEZİN AMACI	Türk Hukuk Mevzuatını bilişim suçları açısından incelemek
TEZİN TÜRKÇE ÖZETİ	Bilişim suçlarının tanımı, tarihsel gelişimi, bilişim suçu fail ve mağdurlarının genel özellikleri, bilişim suçu işleme yöntemleri ile bilişim suçunun özel bir görünümü olarak siber terörün tanımı, özellikleri, hedefi ve tehdit gücü konularına değinilmiştir. İkinci bölümde ABD, Almanya, Fransa, İngiltere, Japonya, Çin ve Rusya gibi gelişmiş ülkelerin bilişim suçlarıyla mücadele konusunda yapmış oldukları hukuki düzenlemeler ve [illegible] örnekler ile bu suçları düzenleyen uluslararası tek belge olan "Avrupa Konseyi Siber Suç Sözleşmesi" nin hükümleri incelenmiş, Üçüncü bölümünde 5237 Sayılı Türk Ceza Kanunu'nda bilişim suçlarına ilişkin yapılan düzenlemeler üzerinde durulmuş, sonuç kısmında ise bütün bu inceleme ve analizlerin sonunda bilişim suçları ve siber terör tehdidine karşı hukuki anlamda daha etkin mücadele edilebilmek için yapılması gereken düzenlemeler, alınması gereken tedbirler ve uygulanması gereken programlar sunulmuştur.
ARAŞTIRMA YAPILACAK OLAN SEKTÖRLER / KURUMLARIN ADLARI	
[illegible]	
[illegible]	
[illegible]	

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı- Soyadı **:** Damla ERMEYDAN
Doğum Tarihi ve Yeri **:** 04.06.1978/ ANKARA
İletişim E- mail **:** damlaermeydan@gmail.com

EĞİTİM

2016- Tez Aşaması **:** Çağ Üniversitesi/ Kamu Hukuku - Yüksek Lisans (Mersin)
2011- 2014 **:** Çukurova Üniversitesi-Hukuk Fakültesi (Adana)

YABANCI DİL

İngilizce **:** Okuma, yazma ve konuşma iyi düzey

İŞ TECRÜBESİ

2004- … **:** DEVLET MEMURU