T.C.
KIRIKKALE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

İNTERNET SUÇLARININ KİŞİSEL HAK VE ÖZGÜRLÜKLERE ETKİSİ

DOKTORA TEZİ

Hazırlayan
Erhan CAN

Danışman
Prof. Dr. Ahmet BİLGİN

Haziran–2017
KIRIKKALE

T.C.
KIRIKKALE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

İNTERNET SUÇLARININ KİŞİSEL HAK VE ÖZGÜRLÜKLERE ETKİSİ

DOKTORA TEZİ

Hazırlayan
Erhan CAN

Danışman
Prof. Dr. Ahmet BİLGİN

Haziran–2017
KIRIKKALE

KABUL-ONAY

Prof. Dr. Ahmet BİLGİN danışmanlığında Erhan CAN tarafından hazırlanan "İnternet Suçlarının Kişisel Hak ve Özgürlüklere Etkisi" adlı bu çalışma jürimiz tarafından Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim dalında Doktora tezi olarak kabul edilmiştir.

07/06/2017

(Tez Savunma Sınav Tarihi Yazılacak)

~~(İmza)~~

[Unvanı, Adı ve Soyadı] (Başkan)

Prof. Dr. Ahmet BİLGİN

[İmza]

[Unvanı, Adı ve Soyadı]

Prof. Dr. Doğan Soyaslan

[İmza]

[Unvanı, Adı ve Soyadı]

Prof. Dr. Ender Ethem ATAY

[İmza]

[Unvanı, Adı ve Soyadı]

Doç. Dr. Elif Sibel GALAE

Prof. Dr. Mehmet Emin BİLGE

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

.../.../20..

(Ünvan, Adı Soyadı)

Enstitü Müdürü

KİŞİSEL KABUL

Doktora Tezi olarak sunduğum "İnternet Suçlarının Kişisel Hak ve Özgürlüklere Etkisi" adlı çalışmanın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve faydalandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak faydalanılmış olduğunu beyan ederim.

07/06/2017

Erhan CAN

ÖNSÖZ

İnternet Suçlarının Kişisel Hak ve Özgürlüklere Etkisi adını taşıyan bu tez çalışmasında günümüzde her geçen gün hızla artan internet suçlarına zemin hazırlayan faktörlerin, suçun gelişiminin ve bağlı olduğu faktörlerin, internet suçlarının kişisel hak ve özgürlüklere nasıl sekte vurduğunun, bu ve benzeri suçların neden kamusal kapsamda değerlendirilmeleri gerektiğinin incelenmesi amaçlanmıştır.

İnternet yoluyla işlenen suçlara ilişkin bilgi ve bilinç oluşturma açısından son derece önem arz eden bir konuda çalışma yapmak için, beni yönlendiren, çalışmamın her aşamasında destek ve katkıları ile ufkumu açan, bu meşakkatli yolda her zaman yanımda olup yol gösteren, yardımları, fikirleri ve engin bilgisi sayesinde beni aydınlatan saygıdeğer hocam, danışmanım Prof. Dr. Ahmet BİLGİN'e, tez jürimde yer almalarından onur duyduğum değerli hocalarım Prof. Dr. Mehmet Emin BİLGE, Prof. Dr. Doğan SOYASLAN, Prof. Dr. Ender Ethem ATAY, Doç. Dr. Elif Sibel ÇAKAR'a, ayrıca çalışmamda verdikleri bilgilerle tezime katkı sağlayan internet suçları mağdurlarına da teşekkür etmeyi ödenmesi gereken zevkli bir borç telakki ediyorum.

Uzun soluklu doktora çalışmalarım boyunca beni hiçbir zaman yalnız bırakmayan, bu günlere gelmemde yegane varlık sebebim, yaşam ve ilham kaynağım Babacığım Bayram ve Anneciğim Şakire CAN, manevi desteğini üzerimden hiçbir zaman eksik etmeyen çok kıymetli ve sevgili eşimYeliz, canım oğlum Muhammed Türkkan ve canım kızım Neslişah Bengisu'ya sonsuz teşekkür ve şükranlarımı sunarım.

ÖZET

CAN, Erhan , "İnternet Suçlarının Kişisel Hak ve Özgürlüklere Etkisi", Doktora Tezi, Kırıkkale, 2017.

Hızlı bir şekilde gelişen teknoloji özellikle de bilişim teknolojileri her geçen gün yaşamın içinde daha fazla yer almaktadır. Sınırları ortadan kaldıran ve iletişim çağının kapısını aralayan bilişim sistemlerinin ve internetin karşısında hiçbir şekilde durulamamaktadır. Getirdiği birçok yararların yanı sıra bu sistemler ayni hızla gelişen bir takım olumsuzlukları da beraberinde getirmektedir.

Tüm bu olumsuzluklar içerisinde internet suçları belki de en önemli yeri tutmaktadır. Tez kapsamında özellikle günümüzün internet ve bilgi çağında giderek artan internet ve internet suçlarının kişisel hak ve özgürlüklere ve kişilik hakkının dokunulmazlığına ne ölçüde zarar verdiği incelenecek, internet suçlarının neden kamu hukuku kapsamında değerlendirilmeleri gerektiğine ışık tutulacaktır. Bu tezde günümüzde iyice artan internet suçlarına zemin hazırlayan faktörlerin, suçun gelişiminin ve bağlı olduğu faktörlerin, internet suçlarının kişisel hak ve özgürlüklere nasıl sekte vurduğunun ve bu ve benzeri suçların neden kamusal kapsamda değerlendirilmeleri gerektiğinin incelenmesi amaçlanmıştır.

Dört bölümden oluşan çalışmada internet suçlarında sıklıkla uygulanan yöntemler açıklanmakta, suçlu ve mağdur profillerine değinilerek bilişim suçlarının nasıl kolay ve hızlı bir şekilde işlenebileceği anlatılmaktadır. Ayrıca; bilgisayar, bilişim sistemleri ve internet kavramları ve bu suçlar ile mücadele amaçlı yapılan yasal düzenlemeler yer almaktadır. Tezin son bölümünde internet suçlarının mağduru olan insanlarla güncel ve arşiv bilgilerinden yola çıkılarak, anlatımsal söylev analizi metodu ve metafor analizi yöntemleri kullanılmıştır. Karşılaştırmalı istatistik yöntemi kullanılarak geçmişten günümüze internet suçlarının artış oranı incelenmiştir.

Anahtar Kelimeler: İnternet, Suç, İnternet Suçları, Bilişim Suçları, Siber Suçlar.

ABSTRACT

CAN, Erhan, “The Effect of The Internet Crimes on Personal Rights and Freedoms”, PhD Thesis, Kırıkkale, 2017.

Rapidly developing technology, in particular information technology is getting more and more involved every day. There is nothing to face with information system and internet which remove the limits and open the door of the communication age. In addition to the many benefits, these systems bring with developing negatives with it.

Internet crimes have perhaps the most important place within all these negatives. Within the scope of the thesis, it will be investigated how much internet and internet crimes which are increasing in today's internet and information era damages personal rights and freedoms and impunity of personality rights, and why internet crimes should be evaluated under public law. In this thesis, it is aimed to investigate the factors that make up the ground for internet crimes, crime development and related factors, how internet crimes have crashed against personal rights and freedoms and why these and similar crimes should be evaluated in public context.

In the study that consists of four parts describe methods that are frequently applied in internet crimes, and how criminal offenses can be handled easily and quickly by referring to criminal and victim profiles. Moreover, the study involves computer, information systems, internet concepts and legal regulations that designed to combat these crimes. In the last part of the thesis, narrative discourse analysis method and metaphor analysis methods are used with the help of internet crime that is taken from the current and archive information with the victims. The comparative statistical method was used to examine the rate of increase of past internet crimes.

Key words: Internet, Crime, Internet crimes, Information Crimes, Cyber Crimes.

SİMGELER VE KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
a.g.e	Adı geçen eser
AK	Avrupa Konseyi
AKSSS	Avrupa Konseyi Siber Suçlar Sözleşmesi
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Authority Net
AŞ	Anonim Şirket
ATM	Auto Telle Machine
BGB	Alman Medeni Kanunu
BM	Birleşmiş Milletler
BTK	Bilgi Teknolojileri Kurumu
CD	Compact Disc
CMK	Ceza Muhakemesi Kanunu
DARPA	Defence Advanced Research Project Agency
ETCK	Eski Türk Ceza Kanunu
F	F İstatistiği
FSEK	Fikir ve Sanat Eserleri Kanunu
HTTP	Hyper Text Transfer Protocol
IANA	İnternet Numara Kayıt Merkezi
ICANN	İnternet İdare ve Gelişim Merkezi
İEN	İnternet Erişim Noktası
İSS	İnternet Servis Sağlayıcıları
JANET	Joint Academic Network
MILNET	Military Network
n	Frekans
NCP	Network Control Program
NSFNET	National Science Foundation Network
ODTÜ	Orta Doğu Teknik Üniversitesi

ort.	Aritmetik Ortalama
p	Anlamlılık Değeri
RIR	Regional Internet Recording Center
RTÜK	Radyo Televizyon Üst Kurulu
SIM	Abone Kimlik Modülü
ss.	Standart Sapma
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
t	T istatistiği
TADOC	Turkish Academy Against Drug and Organised Crime
TBK	Türk Borçlar Kanunu
TBMM	Türkiye Büyük Millet Meclisi
TC	Türkiye Cumhuriyeti
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/İnternet Protocol,
TDK	Türk Dil Kurumu
TİB	Telekomünikasyon İletişim Başkanlığı
TMK	Türk Medeni Kanunu
TR-NET	Türkiye İnternet Proje Grubu
TTK	Türk Ticaret Kanunu
TTNet	Türk Telekom İnternet Hizmetleri
TURNET	Türkiye Ticari İnternet Ağı
TÜBİTAK	Türkiye Bilimsel ve Teknik Araştırma Kurumu
TÜVAKA	Türkiye Üniversiteler ve Araştırma Kurumları Ağı
ULAKNET	Ulusal Akademik Ağ
UYAP	Ulusal Yargı Ağı Projesi
www	World Wide Web
YCGK	Yargıtay Ceza Genel Kurulu
%	Yüzde
<	Küçüktür
>	Büyüktür

TABLOLAR / ŞEKİLLER

İÇİNDEKİLER

GİRİŞ

Tez kapsamında özellikle günümüzün internet ve bilgi çağında giderek artan internet ve internet suçlarının kişisel hak ve özgürlüklere ve kişilik hakkının dokunulmazlığına ne ölçüde zarar verdiği incelenecek, internet suçlarının neden kamu hukuku kapsamında değerlendirilmeleri gerektiğine ışık tutulacaktır.

Bu tezde günümüzde iyice artan internet suçlarına zemin hazırlayan faktörlerin, suçun gelişiminin ve bağlı olduğu faktörlerin, internet suçlarının kişisel hak ve özgürlüklere nasıl sekte vurduğunun ve bu ve benzeri suçların neden kamusal kapsamda değerlendirilmeleri gerektiğinin incelenmesi amaçlanmıştır.

Günümüz dünyasında internet hayatımızın olmazsa olmazı ve her bilgiye anında ulaşmamızı sağlayan büyük bir güç haline gelmiştir. Ancak internetin hayatımıza kattığı artılar yine aynı internetin potansiyel tehdit ve zararlarının görünürlüğünü azaltmıştır. Bugün, internet ve internet suçları kişisel özgürlüklere ve kişilik hakkının bütünlüğüne en çok zarar veren suçların başında gelir olmuştur. Bu sebeple kamu hukukuyla ilintili bu tezin kapsamında herhangi bir başka suçtan daha öncelikli olarak internet ve internet suçlarının ele alınması uygun görülmüştür.

İnsan topluluklarının bilişim teknolojilerine artan bağlılığı, gündelik yaşama paralel bir yaşam şeklinin oluşmasına neden olmuştur. Sürekli yeni keşiflerin olduğu dünyada kaçınılmaz olarak birçok sorun ortaya çıkmaktadır. Bu sorunlara zamanla yenileri eklenmekte, suçluyu bulma ve cezalandırma konusunda sıkıntılar ortaya çıkmaktadır.

Çalışma esnasında karşımıza çıkabilecek kayda değer en önemli problem ise internet suçlarının ve suçu işleyenlerin kimliklerinin tespitinin zorluğu ve oldukça sağlam ve maliyetli bir teknolojik altyapı gerektirmesi olacaktır.

Veriler toplanırken internet suçlarının mağduru olan insanlarla hem güncel röportajlar yapılacak, hem de bu insanlarla ilgili eskiden yapılmış olan röportajlar arşiv taraması yoluyla bulunup incelenecektir. Ayrıca internet suçlarını işleyip yakalanmış olan kişilerin ifade ve itirafları da incelenecektir. Bu kısımlar çalışmanın

sözel kısmını oluşturacaktır. Tezin sayısal kısmında ise internet suçlarının artış oranları karşılaştırma metoduyla incelenecektir.

Veriler anket, röportaj, arşiv taraması, betimsel ve ilişkisel tarama ve vaka analizi metotlarıyla toplanacaktır. Anket metodunda daha önce internet suçlarına karışmamış olan kişilerin internet suçlarını dışarıdan üçüncü bir göz olarak değerlendirmesi sağlanacaktır. Röportajlar yoluyla ise daha internet suçları mağdurlarının ve psikologların konuyla ilgili görüşlerine başvurulacaktır. Arşiv taraması ve vaka analizi metotlarıyla da basında yer alan internet suçlarına dair haber ve davalar incelenecektir.

Verilerin analizi sırasında kişilerin röportajlar sırasında söyledikleri anlatımsal söylev analizi metodu , metafor analizi yöntemleriyle ve IBM SPSS 21 paket programı aracılığıyla istatistiki test ve analizler uygulanarak incelenecektir. Geçmişten günümüze internet suçlarının artış oranı incelenirken karşılaştırmalı betimsel istatistik yöntemi kullanılacaktır.

Suça karışmış olan kişilerin geçmiş yaşantıları ve çocuklukları incelenecek, bu kişilerin ortak özellikleri saptanacaktır. Aynı şekilde suç mağdurlarıyla yapılan röportajlar sonrasında bu kişilerin en sık kullandığı kelimeler kodlanacak, bu kelimeler üzerinden kişilerin yaşadığı mağduriyet kişisel hak ve özgürlüklerle ilişkilendirilecektir. İnternet suçları sonucunda kişilerin hangi haklarının sabote edildiği saptanacak, bu alanlarda hangi hukuksal iyileştirmelerin yapılması gerektiği belirlenecektir. Suçlar incelenirken Yargıtay içtihatlarına da yer verilecektir.

Anlatımsal söylev analiz metodunda röportaj yapılan kişilerin en sık kullandıkları kelimelere göre çeşitli temel kategoriler belirlenir. Daha sonra bu kelimeler tezin konusuna hizmet eden, metafor adını verdiğimiz çeşitli ölçütlerle ilişkilendirilir. Örneğin bir kişi kendisini ‘çaresiz’ hissettiğinden sıklıkla bahsederse bu durum internet suçlarının kişinin ‘özgürlüğünü kısıtlıyor’ olduğuyla ilişkilendirilebilir ve ‘özgürlük kısıtlanması’ çalışma içerisinde incelenecek anahtar kavramlardan biri olarak belirlenip incelenir.

BİRİNCİ BÖLÜM

İNTERNET SUÇLARININ MAHİYETİ VE TARİHİ GELİŞİMİ

İnternet suçları konusuna giriş yapmadan önce, genel olarak internet ve internete dair kavramlarla ilgili genel bir alt yapı oluşturulması, internet suçlarının içeriğini, işlenme şekillerini ve kapsamının ne kadar büyük olduğunun anlaşılması bakımından faydalı olacaktır. Bu nedenle öncelikle internet kavramı ve internet kavramının ortaya çıkışından itibaren günümüze kadar ulaştığı noktadan söz edilecektir. İnternet konusunda gerekli bilgi altyapısının oluşturulması sonrasında internet suçlarının tanımı, tarihi gelişimi, yapısı, özellikleri ve internet suçlarının işlenme şekilleri üzerinde durulacaktır.

1.1. İNTERNET TANIMI VE TEMEL KAVRAMLAR

İnternet tanımı ve temel kavramlara geçmeden önce, bilgisayar tanımını yapmak hem daha doğru, hem de daha faydalı olacaktır. Çünkü bilgisayar kavramının anlamını bilmeden, bileşenleri hakkında fikir sahibi olmadan, internetin anlamı üzerinde yoğunlaşmak ve internetin suç ile bağlantısını kurmak zor olacaktır.

Buradan hareketle bilgisayar; insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler olarak tanımlanmaktadır. Başka bir deyişle bilgisayar; dış ortamdan aldığı verileri, üzerine yüklenen programlar aracılığıyla depolayan, işleyen, yeni sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan, veri iletişimini sağlayan makine olarak ifade edilmektedir. [1]

Bir başka tanım ise bilgisayarı; *"belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen masaüstü, dizüstü*

[1] Akarslan, Hüseyin, ***Bilişim Suçları***, Seçkin Yayınları, Ankara, 2012, s.28.

bilgisayarlar, cep telefonu ve benzeri tüm elektronik araçlar"[2] şeklinde betimlemektedir.

Teknoloji alanında yaşanan hızlı gelişme, bilginin paylaşımını etkileyerek çok önemli bir hale getirmiştir. Bu nedenle de, kişisel bilgisayarların birbiriyle bağlanması durumu ortaya çıkmış ve buna bilgisayar ağı adı verilmiştir. Başka bir ifadeyle, birbirine bağlı birden fazla bilgisayarın, sahip olduğu kaynakları paylaşmak üzere meydana getirdiği yapı bilgisayar ağı olarak adlandırılmaktadır. Bilgisayar ağları, tüm dünyaya yayılmış durumdaki bilgisayarları kapsamakta, bu bilgisayarlar arasındaki bağlantı da, genellikle kablo yardımıyla sağlanmaktadır. Ancak kablo bağlantısı kurulamayan durumlarda mikro dalgalar ve uydu sistemleri aracılığıyla ağ içi iletişim kurmak mümkün olmaktadır. Ağ içi iletişim sağlayan bilgisayar ağları, bilginin diğer bilgisayarlara iletimini sağlamakta, bilgisayarlar arasında sanal bir bilgi ortamı oluşturmaktadır. İşte oluşan bu sanal bilgi ortamı, bilgisayar ağlarının birbiriyle bağlantıya geçmesi sonucu ortaya çıkan iletişim ağı, internettir.[3]

Ağların ağı olarak da adlandırılan internet, *"international*" ve *"network"* kelimesinin bir araya gelmesinden oluşmaktadır. [4] İnternet kelimesinde yer alan ''net'' sözcüğü, bilgisayar ağını ifade etmektedir. Milyonlarca bilgisayarın bu ağ sistemi ile birbiriyle iletişim kurması ve bilgi aktarımında bulunması neticesinde, bugün bilgiye ulaşımın en kolay, hızlı ve pratik ulaşmanın şekli internet aracılığıyla yapılmaktadır. Bir başka deyişle internet, "*bilgisayar ağlarının(network) aralarında bağlantı kurmalarıyla oluşan ve bu şekilde küresel olarak gelişen toplumsal, kültürel, ticari, eğlendirici küresel bir kitle iletişim sistemidir."*[5]

İnternet; dünya üzerine yayılmış milyonlarla ifade edilen sayıdaki bilgisayarların birbirine bağlanması ile oluşan ağların, yine birbirlerine bağlanması ile oluşan çok geniş yapıdaki bir ağdır. [6]

---

[2] Dülger, Murat Volkan – Modoğlu, Gözde, ***Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri İle İnternet ve İletişim Hukuku Uygulama Rehberi***, Avrupa Birliği ve Avrupa Konseyi Ortak Yayını, Ankara, 2014, s. 25.

[3] Turhan, Oğuz***, Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar),*** Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi, Ankara, 2006, s. 4.

[4] Yenidünya, Ahmet Caner-Değirmenci, Olgun, ***Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,*** Legal Yayıncılık, İstanbul, 2003, s. 36.

[5] Avcı, Artun, ***Türkiye'de İnternet ve İfade Özgürlüğü***, İstanbul, Legal, 2013, s.27.

[6] Erkan, Boğaç – Songür, Murat, ***Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü***, Hacettepe-Taş Yayıncılık, 1999, s. 282.

Bir başka kaynakta internet; birden fazla haberleşme ağının birlikte meydana getirdikleri, tüm bilgilerin paylaşıldığı ve bilgisayarlar arasında karşılıklı olarak iletildiği bir ağ olarak ifade edilmektedir. [7]

Bu nedenle de çağımızın en önemli iletişim aracı olma özelliğini taşıyan internet; hızla gelişmekte, günlük yaşamın hemen hemen her alanında çok yönlü kullanım ve bilgi aktarımı gerçekleştirmektedir. Söz konusu gelişimin neden olduğu yaygınlık, tüm dünyadaki kullanıcı sayısının artması sonucunu doğurmanın yanında, internetin kullanıldığı faaliyet alanlarının da hızla artmasını sağlamakta, böylece internet, yaşamın vazgeçilmez bir parçası haline getirme yolunda ilerlemektedir.[8]

İnternetin ortaya çıkması, ABD ile SSCB arasındaki Soğuk Savaş dönemine rastlamaktadır. "Birçok keşif ve icatlarda olduğu gibi internetin de ortaya çıkışı bir krizin yaşandığı döneme rast gelmiştir. ABD'nin Rusya, Vietnam ve Küba ile soğuk-sıcak savaşlardan ve nükleer tehditlerden dolayı bilgiye problemsiz ulaşma ve iletişim kurma ihtiyacı bu süreci hızlandırmış ve başka bir deyişle vesile olmuştur".[9]

İnternetin fikirsel olarak temeli, ABD Savunma Bakanlığı'nın muhtemel bir savaş durumunda herhangi bir iletişim kopma tehlikesinin yaşanmayacağı bir iletişim ağı oluşturma arzusuna dayanmaktadır. Bu bağlamda internet, ilk olarak 1960'ların başında, askeri ve bilimsel alanda, bilgisayarların desteği aracılığıyla bilgi paylaşımı ve bilgi ağının muhtemel olması fikri karşısında, ABD Savunma Bakanlığının bir projesi ile ortaya çıkmıştır.[10] Bu proje, Amerikan Federal Hükümeti Savunma Bakanlığı'nın araştırma ve geliştirme kolu olan "Savunma İleri Düzey Araştırma Projeleri Kurumu (DARPA-Defence Advanced Research Project Agency)" tarafından oluşturulmuş, dört farklı kentteki dört büyük bilgisayar arasında bilgi alışverişi sağlanmıştır.[11]

---

[7] Özdilek, Ali Osman, ***İnternet ve Hukuk***, Papatya Yayıncılık, Ankara, 2002, s. 13.

[8] Yalçın, Filiz, ***İnternet Pazarlamasında Müşteri Memnuniyeti: Günün Fırsatları Üzerine Bir Uygulama***, Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2012, s.3.

[9] Haşıloğlu, Selçuk Burak, ***Elektronik Posta İle Pazarlama***, Beta Basım Yayın Dağıtım, İstanbul, 2007, s. 19.

[10] Leiner, M. Berry at al., "A Brief History of the Internet", ***ACM SIGCOMM Computer Communication Review***, Volume 39, Number 5, October 2009, (Erişim) http://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf, 10 Kasım 2016, s.23.

[11] İçel, Kayıhan ve Ünver, Yener, ***Kitle İletişim Hukuku***, Beta Basım Yayın Dağıtım, İstanbul, 2012, s. 427.

Bilgisayarların birbirine bağlanması fikri ilk olarak 1962'de, ABD'de Masachusettes Teknoloji Enstitüsü'nden J. Licklider tarafından ortaya atılmıştır. Licklider'in, önermiş olduğu yapı ARPA (Advanced Research Projects Agency), DARPA (Defence Advanced Research Project Agency) tarafından daha da ileri düzeye getirilmiştir. Bu yapı daha sonra ARPANET (Advanced Research Projects Authority Net) adını almıştır.[12] 1969 yılında ABD Savunma Bakanlığı, bir takım projeleri destekleme amacıyla ARPANET isimli Paket Anahtarlamalı Ağı oluşturmaya başlamıştır. ARPANET, ABD'de bulunan yükseköğretim ve araştırma kurumlarının farklı tipteki bilgisayarlarını kapsayarak daha da büyümüştür.[13]

ARPA'nın geliştirdiği internet, bir bakıma Soğuk Savaş döneminde ABD'nin SSCB'nin önüne geçme çabasının bir neticesi olduğunu da söylemek mümkündür. ARPA' ya bağlı bulunan bilgisayarların aynı tip ve özelliklere sahip olmamaları nedeniyle ortaya çıkan sorunların çözülmesi için iletişim, TCP/IP (Transmission Control Protocol/İnternet Protokolü) adlı bir protokole uygun şekilde sağlanmaya başlamıştır. Bu bağlamda ilk veri transferi, 1969 yılında Kaliforniya ve Utah'ta bulunan dört ayrı bilgisayar arasında gerçekleşmiştir. Bir sonraki aşamada da, dört bilgisayar arasında bulunan ağ sistemi geliştirilerek, ARPANET isimli askeri bir ağ kurulmuştur. 1973'de TCP/IP protokolü ARPANET' te NCP (Network Control Program) protokolünün yerini almıştır. Temeli İnternet Protokolü (IP) oluşturmakta ve makinenin adres bilgisini içermektedir. TCP (Transmission Control Protocol) büyük mesajları paketlere bölmekte ve paketler TCP tarafından birleştirilmektedir. Alıcı uçta ise TCP zarfları açılarak orijinal mesaj tekrar oluşturulmaktadır. [14]

ARPANET sistemi, elektronik posta ve ağ haberleri gibi servislerin belirli bir istikrara kavuşmasını sağlamıştır. 1980 yılında Amerikan ordusu, faaliyetlerini yeni kurduğu MILNET (Military Network) ağına taşıyarak, ARPANET'i tamamen sivil kullanıma bırakmıştır. Aynı yıllarda ABD'nin yanı sıra İngiltere ve Japonya gibi ülkelerde de yeni ağ sistemleri kurulması amacıyla çeşitli çalışmalar yapılmış, 1984 yılında İngiltere'de kurulan JANET (Joint Academic Network), ABD dışında

[12] Börteçin, Ege, "Nasıl Çalışıyor?", ***Bilim ve Teknik Dergisi***, Ekim 2013, s.67.
[13] Leiner, a.g.e., s. 24.
[14] Kalkota ve Whinston, 1996, akt., Karaçetin, Murat, ***İnternet Üzerinden Alışverişe Yönelik Tutumlar: Bir Araştırma***, Yayımlanmamış Yüksek Lisans Tezi, T.C. Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü, Burdur, 2015, s. 9.

kurulan ilk ağ sistemi olarak ortaya çıkmıştır.[15] Bilinen haliyle internetin sivil kullanıma açılabilmesi ise, Yüksek Kapasiteli Bilgi İşlem Kanunu (High Performance Computing)'nun kabul edilişi ile gerçekleştirilmiştir. ARPANET'in ağ üzerindeki tüm yönetim haklarını NSFNET (National Science Foundation Network)'e devretmesiyle, bugünkü bilinen internet ağı ortaya çıkmıştır.[16]

1986 yılında, NSFNET'in kurulması, internet açısından bir dönüm noktası haline gelmiş, 1989 yılında World Wide Web (WWW) ve 1990 yılında en temel dosya transfer protokolü olan HTTP'nin geliştirilmesi, ARPANET'in ortadan kaldırılmasına yol açmıştır. Bütün ağ sisteminin bir tek yapı üzerinde birleştirilmesi ve internetin kişisel kullanıma açılmasıyla birçok bilgisayar kullanıcısı bu şekilde tek bir ağa bağlanmış ve internet kullanımı yaygınlaşmıştır. [17]

"Türkiye'de ise internet, varsayılan ilk geniş alan bilgisayar ağı 1986 yılında üniversitelerin önderliğinde TÜVAKA - Türkiye Üniversiteler ve Araştırma Kurumları Ağı- ismi ile kurulmuştur. Teknolojik gelişmeler karşısında yetersiz kalan bu ağın geliştirilmesi için, Orta Doğu Teknik Üniversitesi (ODTÜ) ve Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından yeni ağ teknolojilerinin kullanılması gerektiği öngörüsü ile ortak bir proje Türkiye İnternet Proje Grubu (TR-NET) başlatılmıştır.TR-NET adını alan proje çalışmaları sonucunda, Türkiye'de ilk internet bağlantısı, 12 Nisan 1993 tarihinde 64 Kbps hızında yapılmıştır. Bu tarihten itibaren 12 Nisan, Türkiye için internetin doğum günü olarak kabul edilmiş ve her yıl Nisan ayının ikinci haftası "internet haftası" olarak kutlanmaktadır. İnternete ilk yıllarında sadece TÜBİTAK ve üniversitelerin kullanımına izin verilen ODTÜ ve Ege üniversiteleri üzerinden bağlanılabiliyordu. Bu süreç içerisinde İnternet ağı akademik kesimin egemenliği altındaydı. Ancak akademik kesimin egemenliği çok uzun sürmedi. 1995 yılımdan sonra çevirmeli hatlar (dial-up) ve X25 ile hem de kiralık hatlarla önemli sayıda kamu kurumu, şirket ve kişinin bağlantısı sağlandı".[18]

Bu üniversiteleri Ekim 1995'de Bilkent Üniversitesi, Kasım 1995'de Boğaziçi Üniversitesi ve Şubat 1996'da İstanbul Teknik Üniversitesi'nin internet bağlantıları gerçekleşmiştir. Ağustos 1996'ya ulaşıldığında, "TURNET" (Türkiye Ticari İnternet Ağı) çalışmaya başlamış, onu 1997 yılında, akademik kuruluşların İnternet

---

[15] Demir, Esra Peker, ***İnternet Aracılığı ile Kişilik Haklarına Saldırı***, Yayınlanmamış Yüksek Lisans Tezi, T.C. İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, 2014, s. 28.

[16] Yalçın, a. g. e., s. 5

[17] Oğuz, Habip, ***İnternet Ortamında Kişilik Haklarının İhlali ve Korunması***, Adalet Yayın Evi, Ankara, 2012, s.27

[18] Uslu, Tolga***, İnternet Güvenliği ve Risk Yönetimi***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2007, s.19.

bağlantısını sağlayan "ULAKNET" (Ulusal Akademik Ağ) izlemiştir. Böylece üniversiteler öncesine göre daha hızlı bir yapıyla birbirlerine bağlanarak, İnternet kullanır hâle gelmişlerdir. 1999 yılında ticari ağ altyapısında büyük değişiklikler gerçekleşir ve "TURNET"in yerini TTNet (Türk Telekom İnternet Hizmetleri) adındaki yeni bir oluşum almıştır. 2000'lere ulaşıldığında ticari kullanıcılar TTNet, akademik kuruluşlar ve ilgili birimler de ULAKNET üzerinden her iki bağlantı arasında gerçekleşen yüksek hızlı bağlantıya sahip İnternet erişimine sahip olmuşlardır.[19]

Şu anda Türkiye'nin İnternet çıkışını sağlayan merkezler üç grupta toplanabilir:[20]

- Üniversiteler ve akademik kuruluşların İnternet bağlantı çıkışları
- Genellikle ticari kuruluşların ve İnternet Servis Sağlayıcılarının (İSS) yararlandığı TTNET çıkışları
- Diğer bazı özel şirketlerin ve servis sağlayıcıların, TTNET ile yaptıkları İnternet Erişim Noktası (İEN) anlaşması sonrasında kullandıkları firma bazlı doğrudan yurtdışı İnternet çıkışları

1.2. İNTERNETİN YAPISAL UNSURLARI

Teknoloji alanında yaşanan hızlı değişime ayak uydurmaya çalışan Türkiye, bunda büyük ölçüde başarılı olmuştur. İnternet kullanımı ile bağlantı sıklığı konusunda yapılan araştırmalar da bunu destekler niteliktedir. İnternet artık yaşamın her alanında varlığını hissettirmekte ve özelde insan genelde toplum yaşamını çepeçevre sarmaya devam etmektedir. Gelecek yıllarda internetin yaşamın içinde daha başka boyutlarıyla karşımıza çıkma ihtimali de yüksek görünmektedir. Bugünün şartlarında internetle bilgi aktarımını ve paylaşımının sorunsuz bir biçimde uygulanabilmesi, çeşitli kurallara uyulması ile orantılıdır. Bu kurallar, "TCP/IP Protokolü" (Transmission Control Protocol/Internet Protocol) olarak adlandırılmaktadır. Ayrıca internetin yapısal unsurları arasında World Wide Web (www), intranet ve exranet bulunmaktadır. İnternetin yapısal unsurları başlığı altında bu üç unsur üzerinde durulacaktır.

[19] Milli Eğitim Bakanlığı. (2011). ***Bilişim Teknolojileri İnternet ve E-Posta Yönetim.*** Ankara, 2011, s. 6.
[20] Milli Eğitim Bakanlığı. (2013). ***Bilgisayarla İletişim***. Ankara, 2013, s.7.

1.2.1. TCP/IP (Transmission Control Protocol / Internet Protocol)

TCP/IP, bilgisayarlarla veri iletim-alım üniteleri arasında organizasyonu temin eden, bu şekilde bir yerden başka bir yere veri aktarımına imkân sağlayan birçok veri iletişim protokolüne verilen genel addır. TCP/IP protokolleri, birden çok bilgisayar arası veri aktarımının kurallarını ortaya koymaktadır. TCP/ IP, dört katmanlı (uygulama, ulaşım, yönlendirme ve fiziksel katmanı) bir yapıya sahip olan internet ağ mimarisinin protokol kümelerine verilen addır. [21] TCP/IP protokolü; dünya üzerindeki milyonlarca bilgisayarın ve yerel ağların birbirleri ile iletişim kurmalarını sağlayan ortak bir anlaşma dili olarak tanımlanabilir.[22]

TCP (İletim Kontrol Protokolü), iletilerin doğru yere ulaştırılması görevini gerçekleştirir. Bu protokolle; hem yerel hem de geniş alan ağları üzerinde, uçtan uca eş düzeyli birimler arasında bağlantı sağlarlar. Küçük ağlarda TCP katmanının hemen hemen tüm işi üstlendiği görülmekle birlikte, büyük ve karmaşık ağlarda IP katmanı en önemli görevi üstlenmektedir. TCP katmanına gelen bilgi, segmentlere ayrıldıktan sonra IP katmanına yollanır. [23] TCP bir üst katmandan gelen veriyi önce uygun büyüklükteki parçalara ayırır ve her bir parça önüne kendi başlığını ekleyerek ve bir altında bulunan IP'ye gönderir; o da gelen veriyi IP başlığı ekleyerek karşı sisteme iletilmesi için fiziksel katmana gönderir. [24]

IP (İnternet Protokol) ise, farklı bağlantı yolları ve ağlar üzerinden münferit paketlerin iletimini ve yönlendirilmesini sağlayan temel protokoldür. IP katmanı, kendisine gelen TCP segmentinin içinde ne olduğuyla ilgilenmeksizin, sadece kendisine verilen bilgiyi ilgili IP adresine yollamak amacındadır. IP katmanının görevi, bu segment için ulaşılmak istenen rotaya gidecek bir yol bulmaktır. [25] Bir başka deyişle bu protokoller, iletişim halinde olan birçok bilgisayarın oluşturduğu bir ağda bulunan çeşitli yapıya sahip bilgisayarların iletişim kurmaları için meydana gelen bir anlaşma dilidir. IP adresi, internete erişiminde kullanıcının tanımlanmasını sağlayan, sekiz adet dört hanelik numaralardan oluşmaktadır. İnternet bağlantısı, internet sağlayıcısının ISDN kartları aracılığıyla sağlanmaktadır. Bu bağlamda,

[21] Yenidünya ve Değirmenci, **a. g. e.** , s. 39
[22] Sınar, Hasan, ***İnternet ve Ceza Hukuku***, İstanbul, 2001, s.24
[23] Özen, Muharrem, Baştürk, İhsan, ***Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku***, Adalet Yayınevi, Ankara, 2011, s. 19
[24] Çölkesen, Rıfat, ***Network, TCP/IP ve Unix El Kitabı***, 3. Baskı, Papatya Yayıncılık, İstanbul, 2002, s. 62
[25] Özen ve Baştürk, **a. g. e.**, s.19

internet bağlantısı yapılan her cihazın bir IP numarası bulunmaktadır. Bu şekilde, IP numaralarından internet abonesinin kişisel bilgi ve konum bilgilerini bulunduran abone bilgilerine ulaşılabilmektedir. TCP/IP protokolünü oluşturma gereksinimi, birbirinden farklı donanım ve yazılımları kullanan cihazların birbirleri ile iletişiminin zorunlu olmasından kaynaklanmaktadır.[26]

TCP/IP protokollerine örnek olarak, internet üzerindeki bilgisayarlar arasında dosya alma/gönderme protokolü (FTP-File Transfer Protocol), elektronik posta iletişim protokolü (SMTP-Simple Mail Transfer Protocol), TELNET protokolü (internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen "login" protokolü) verilebilir. Adını sıkça duyduğumuz web ortamında birbirine bağlanmış farklı türden objelerin iletilmesini sağlayan protokol ise Hyper Text Transfer Protocol (HTTP) olarak adlandırılmaktadır. [27]

1.2.2. World Wide Web (www)

Geliştirilen çeşitli internet araçlarından, birçok internet hizmetini birleştiren bir araç olması ile ön plana çıkan World-Wide-Web (www); yazı, resim, film, canlandırma, ses gibi farklı formatta olan bilgilerin göz atıcı (browser) kullanılarak ulaşıldığı internet ortamıdır. İnternet kullanıcılarının en çok kullandığı platformdur.[28]

Günlük hayatın neredeyse bir parçası olan world wide web'de, veri transferi http (Hyper Text Transfer Protocol) kullanılarak sağlanmaktadır. Web, dünyanın her yerindeki yüz binlerce sunucuda kayıtlı, milyarlarca dosyadan oluşan bir bütündür ve kullanıcı açısından bakıldığında web, milyarlarca bilgi ve yayının yer aldığı çok geniş kapsamlı bir kütüphane, mal ve hizmetlerin sunulduğu açık bir pazardır.

Web'de hyperlink aracılığıyla sunucularda bulunan bir dosya üzerinden başka bir dosya çağrılabileceği gibi, bir sunucuda bulunmayan ancak kullanıcının bilgisayarında kayıtlı olan bir dosyadan da, internet sunucusunda yüklü olan bir dosya çağrılabilmektedir. "Hyperlink (hypertextlink), bir internet ağı bağlantısında,

---

[26] Bayram, Mehmet Hanefi, ***Avrupa Birliği ve İnternet Hukuku***, Seçkin Yayınları, Ankara, 2011, s.41- 42.

[27] Avşar, Zakir - Öngören, Gürsel, ***Bilişim Hukuku***, Türkiye Bankalar Birliği Yayın, İstanbul, no:270, 2010, s. 32.

[28] Yaycı, Esra, ***Bilişim Suçları***, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2007, s. 15

bir dokümanın diğer dokümanı direkt izlemesi için referans olan, öncülük eden üst bir yapı, bağlantıdır.” [29]

1.2.3. Intranet ve Extranet

İntranet, komünikasyon ve haberleşme üzerine kurgulanmış, işletme içinde bulunan özel ağ ya da web şeklinde ifade edilebilir. İntranetin ortaya çıkış nedeni, işletme içi bilgi ve bilgi işlem sığasını paylaşmaktır. İntranetin amacı, tüm web niteliklerini temin etmenin yanında, kullanıcılarına erişim iznini belirli düzeylerde vererek, hangi kullanıcının nereye ve nasıl erişebileceğini denetlemektir.

Extranet ise, güçlü bir yetki kontrolü ve kimlik denetimi ile iş ortakları ya da müşteriler arasında bilgi akışına internet üzerinden izin veren bir ağdır yani extranet kurum içi uygulamaları, kurumdan kuruma veya kurumdan tüketiciye aktarmak için kurulan ağdır. Bu bağlantı özellikle iş ortaklarını kendi intranet alanlarına girmelerine izin veren şirketler tarafından kullanılır. Extranet çok sayıdaki organizasyonların iletişimini sağlayan genişletilmiş bir intranet ağıdır. Bu organizasyonların iç personelleri, müşterileri, tedarikçi firmaları ve stratejik ortakları, bağlantısız kapalı kullanıcı grupları halinde extranet yardımıyla birbirlerine bağlanabilirler.[30]

1.3. İNTERNETİN İŞLEYİŞİ

İnternetin kitle iletişim araçlarının en günceli olarak bütün dünyada yaygınlaşması sonucu internet, yeni bir sektörün doğmasına neden olmuştur. İnternetin her geçen gün artan işlevlerini yerine getirebilmesi işte sektör olarak internetteki konular tarafından sağlanmaktadır.[31] İnternetin hukuki konularını; internet servis sağlayıcıları (Internet Service Provider), internet erişim sağlayıcıları (Internet Access Provider), internet içerik sağlayıcıları (Internet Content Provider), sunucu(server), vekil sunucu (proxy server), host ve Usenet işleteni oluşturmaktadır. Bu konuların irdelenmesi, sorumluluklarının sınırlarının ortaya konulması açısından önemli olduğundan burada tek tek incelenmeleri yoluna gidilecektir. [32]

[29] Özen ve Baştürk, **a. g. e**. , s. 24
[30] Oğuz, 2012, **a.g.e.** , s. 34
[31] Sınar, **a. g. e**. , s. 40
[32] Sırabaşı, akt., Oğuz, 2012, **a.g.e.** , s. 47

1.3.1. Telefon/Telekomünikasyon İdareleri

Kullanıcılarına bilgi iletişimi sağlayan bir sistem olan internette kullanılan kanallar, ülkelerin bu konu ile ilgili mevzuatları göz önünde bulundurularak, genelde ülkelerin yerel telefon / telekomünikasyon idareleri tarafından hizmet verilen telefon hatları aracılığıyla kullanılmaktadır. Yetkili idarelerin, gerekli olan komünikasyon alt yapısını, internet servis sağlayıcı merciine sunum işlevi, tamamen teknik özellik taşımakta olup, telefon / telekomünikasyon idaresinin bütün yetki ve mesuliyeti sadece komünikasyon alt yapısının tedariki ile sınırlanmıştır. Bu nedenle, telefon / telekomünikasyon idareleri, internet servis sağlayıcılarının kullanımına sunduğu bu komünikasyon hatları aracılığı ile uygulanan çeşitli servislerden hukuki olarak sorumlu tutulamamaktadır.

Bireysel ya da kurumsal kullanıcılara internet hizmeti sunan İnternet servis sağlayıcıları, "omurga" olarak adlandırılan bir sistem üzerinden internet hizmeti almaktadırlar.

Omurgaları basitçe tarif etmek gerekirse aynı anda birçok verinin iletilmesini sağlayan ana iletim hattıdır. Hemen hemen her ülkede o ülkenin omurga (backbone) yapısını oluşturan belli başlı kurumlar vardır. Ayrıca her ülkede yer alan omurgalar birbirleri ile bağlanarak internetin ana yapısını oluşturmaktadır. Temel olarak nasıl bir ağla internete bağlanılacağı ağların kendi sorunudur ancak eğer internete bağlanılmak isteniyorsa TCP/IP protokollerine uygun bir bağlantı kurulması gerekmektedir. [33]

İnternet hizmeti sunmayı amaçlayan internet servis sağlayıcıları, bu hizmetin sunulması için hukuki olarak yetkili olan telefon / telekomünikasyon idaresi ile anlaşma yoluna giderek, internet servisi için gerekli olan komünikasyon alt yapısını temin ederek, abonelerine hizmet sunmayı amaçlarlar.

Telefon / telekomünikasyon idareleri, mevcut telefon hatları içindeki özel hatları internet servis sağlayıcılarına, internet bağlantısı sunmaları için vermektedir. İnternet servis sağlayıcı olan işletmeler, bu servisi sunmak ve faaliyetlerine başlamak için bu hakkı elinde bulunduran telefon / telekomünikasyon idareleri ile aralarında

[33] Gözüşirin, Mesih, ***5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi***, T.C. Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2011, s. 22

bir kontrat imzalayarak, bu hatların kullanım hakkını elinde bulundurmalıdır. Türkiye'de internet servis sağlayıcılarına internet altyapısı hizmeti, Türk Telekom tarafından yönetilmektedir.

Türk Telekom AŞ'nin yerine getirdiği hizmet, kamu hizmeti olarak nitelendirilse de, internet servis sağlayıcıları ile Türk Telekom arasında akdedilen sözleşmeler idari nitelikte değildir. Bu sözleşmeler özel hukuk nitelikli abonman sözleşmeleri olarak kabul edilmektedir dolayısı ile de Türk Telekom ile internet servis sağlayıcıları arasında çıkan uyuşmazlıklar özel hukuk hükümlerine tabidir ve adli yargı mahkemelerinde görülür. [34]

1.3.2. İnternet Servis Sağlayıcıları (Internet Service Provider)

İnternet servis sağlayıcılar (İSS), kendilerine bağlı bulunan bilgisayar donanım ve lokal şebeke üzerinden kiraladığı hatlarla, internet kullanıcılarını lokal ve milletlerarası internet omurgalarına taşırlar. Diğer bir ifade ile internet servis sağlayıcıları, sahip oldukları bilgisayarları, abonelerinin internete erişimini sağlamak için hizmetine sunan gerçek veya tüzel kişiliklerdir.[35]

İnternet servis sağlayıcıları, internetin birincil derecede önemli unsurudur. Zira internet servis sağlayıcıları, internet kullanıcılarının internete bağlanmaları, internet aracılığıyla iletişim kurmaları ve internetin sunduğu olanakları kullanmalarını sağlayan bir aracı elemandır. İnternet servis sağlayıcıları, genelde bir ticari işletme olarak kurumsallaşmalarına karşı, ticari özellik taşımayan (kamu kurumları, öğrencilere internet hizmeti sunan okullar) kurumlar biçiminde de oluşabilmektedir. İnternet servis sağlayıcılarının sunduğu hizmetlerin içeriği, hizmetin verildiği kuruma göre farklılık gösterebilmektedir. İnternet servis sağlayıcıları, çeşitli ülkelerde çeşitli yapılarda hizmet verebilmektedir. İnternet erişimi sağlama hizmetinin yanında internet servis sağlayıcıları, sunucu (server) kiralama, alan adı işlemleri, sunucu barındırma ve içerik sağlama gibi hizmetler de sunmaktadır. [36]

[34] Oğuz, 2012, **a.g.e.**, s.48
[35] Sınar, **a.g.e.**, s. 41-42.
[36] Oğuz, 2012, **a.g.e.,** s. 49

1.3.3. İnternet Erişim Sağlayıcıları (Internet Access Provider)

İnternet erişim sağlayıcıları, yalnızca iki veya daha fazla içerik sağlayıcının komünikasyonu için elektronik bağlantı temin etmektedir. Bir başka deyişle, internet erişim sağlayıcıları, bizzat iletişim halinde bulunmamakta, ancak diğerlerinin iletişim halinde bulunmasına aracı olmaktadır. İnternet servis sağlayıcıları gibi, internet erişim sağlayıcıları da, direkt olarak internet bağlantısına sahiptir.[37] Ancak İSS, başkalarının bilgilerini kendilerine ait sunucularda saklayarak, bu bilgileri internet üzerinden erişilir hale getirmektedir. Bu nedenle internet erişim sağlayıcılarının böyle bir işlevi yoktur. Özetle, İSS, yalnızca erişim hizmeti sağlıyorsa, erişim sağlayıcısı olarak isimlendirilmektedir. İnternet erişim sağlayıcılarının bir diğer tanımı, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda yapılmıştır. Bu kanuna göre, internet erişim sağlayıcıları kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişilerdir. [38] Aynı kanunun 6. Maddesinde ise, erişim sağlayıcının yükümlülükleri belirtilmiştir.

Bu maddeye göre, erişim sağlayıcı; *"herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten, bu kanun hükümlerine uygun olarak haberdar edilmesi halinde ve teknik olarak engelleme imkânı bulunduğu ölçüde erişimi engellemekle, sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla, faaliyetine son vereceği tarihten en az üç ay önce durumu kuruma, içerik sağlayıcılarına ve müşterilerine bildirmek ve trafik bilgilerine ilişkin kayıtları yönetmelikte belirtilen esas ve usullere uygun olarak kuruma teslim etmekle yükümlüdür"*. [39]

Aynı maddenin, 2. Fıkrasında ise , *"Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir."* hükmü yer

[37] Güran, Sait, v.d., ***İnternet ve Hukuk Temel Metni***, İstanbul, 2002, s.614.

[38] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", ***Resmi Gazete***, Kanun No: 5651, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016, Madde 2/e.

[39] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", ***Resmi Gazete***, Kanun No: 5651, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016, Madde 6.

almaktadır.[40]Son fıkrada ise, 1. Fıkranın (b) ve (c) bentlerinde bulunan yükümlülüklerden birini karşılamayan erişim sağlayıcı hakkında, Başkanlığın para cezası uygulayacağını belirtmiştir. Bununla birlikte, 2007 tarih ve 26716 sayılı Resmi Gazetede yayımlanan ve 5651 sayılı kanun uyarınca çıkarılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik çıkarılmış, bu yönetmeliğin 8. Maddesinde de erişim sağlayıcılarına çeşitli yükümlülükler getirilmiştir.

1.3.4. İnternet İçerik Sağlayıcıları (Internet Content Provider)

Belli bir bilgiyi internet sahasına aktaran, bir başka ifadeyle internetteki bir sitenin içeriğini hazırlayan ve internete aktarılan bilgiyi üreten unsur olan internet içerik sağlayıcıları, çok uluslu işletmelerden kişilere kadar, kamu kuruluşlarından özel şirketlere kadar geniş bir alanda bulunmaktadır.[41] [42]

Bir internet sayfasının içeriğini düzenleyen veya internetten indirme (download) ile elde edilen bilgileri düzenleyip, internete yükleyenler de içeri sağlayıcı olarak adlandırılmaktadır.[43] İçerik sağlayıcı, kendisinin bilgi, eser veya verisini ağ üzerinde erişime açık bir şekilde bulundurabileceği gibi, kendisinin olmayan bir veriyi de erişime açık tutabilir. İnternette erişilebilen sunucular da içerik sağlayıcı olarak görev yapmaktadır. [44]

İçerik sağlayıcı, 5651 sayılı kanunun 2. Maddesinin f bendinde "*İnternet ortamı üzerinden kullanıcılarına sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişiler*" olarak ifade edilmektedir. Aynı kanunun 4.

---

[40] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", ***Resmi Gazete***, Kanun No: 5651, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016, Madde 6/2.

[41] Özel, Sibel, ***Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması***, Seçkin Yayınları, Ankara, 2004, s.157.

[42] Avşar, Zakir, Öngören, Gürsel, ***Bilişim Hukuku***, Türkiye Bankalar Birliği Yayınları, Yayın No:270, İstanbul, 2010, s. 120.

[43] Karagülmez, Ali, ***Bilişim Suçları ve Soruşturma Kovuşturma Evreleri***, Seçkin Yayınları, Ankara, 2011, s.321.

[44] Demir, Önder, " İnternet Servis Sağlayıcısının Cezai Sorumluluğu", ***İzmir Barosu Dergisi***, 2000, Sayı:3, s.3; Oğuz, **a.g.e.**, s. 52.

Maddesine göre içerik sağlayıcı, internette kullanıma sunduğu her türlü içerikten sorumludur.[45]

1.3.5. Sunucu (Server)

Dijital dataları, kapasiteleri miktarında depolayarak diğer bilgisayarlara hizmet sunan bilgisayar ya da programlar olan sunucular, internet servis sağlayıcıları tarafından, üstüne aldıkları hizmetleri yerine getirmek için kullanılırlar. Ana bilgisayar şeklinde de ele alınabilecek olan sunucu, bir ya da birden çok ağa bağlantı kurabilen bir cihazdır.[46]

İnternet servis sağlayıcıları, genellikle sunucu olarak görev görürler. Diğer yandan, sunucuların da aynı anda internet bağlantısı gerçekleştirme görevini yürütüyorsa, artık internet servis sağlayıcı konumunda olmaktadır.[47]

Özel ve kamuya ait kuruluşlar da kendilerine ait lokal sunucular kurup, kendilerinin bilgilerini depolayabilirler. Ancak, bilgisayarlarını sunucu olarak kullanacak olan kullanıcılar, bilgilerini internet ortamında kullanmak için, ya bizzat servis sağlayıcı hizmeti olarak görev görecek ya da başka bir internet servis sağlayıcısının sunduğu hizmetten faydalanacaktır.[48]

1.3.6. Vekil Sunucu (Proxy Server)

İnternet erişimi sırasında kullanılan bir ara sunucu olan ve erişim sırasında vekil görevi gören vekil sunucusu, kullanıcıdan aldığı bilgi alma isteğini gerçekleştirerek, neticeyi tekrar kullanıcıya iletir. Kullanıcının istediği bilgiler, vekil sunucunun önbelleğinde tutulur ve bir sonraki erişimde, kullanıcının istediği bilgiler direkt ilgili internet sayfasından değil, vekil sunucudan gelmektedir. [49]

Vekil sunucu, genel olarak iki amaç için kullanılmaktadır. Birinci amaç, bilgilerin önbellekte tutulması neticesinde erişimdeki hızdır ki, vekil sunucunun esas

---

[45] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", ***Resmi Gazete***, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016, Madde 2.

[46] Avşar ve Öngören**, a.g.e**., s.119.

[47] Özel, **a.g.e**., s. 157.

[48] Soysal, Tamer, "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları," ***TBB Dergisi***, 2005, s.310.

[49] Oğuz, 2012, **a.g.e**., s. 54.

fonksiyonu da budur. Diğer amaç ise, vekil sunucu ile internete erişilmişse, internete erişimde kullanılan IP adresi, vekil sunucuya bağlanan bilgisayarın IP adresi değil, vekil sunucunun IP adresidir. Fakat kullanıcının internette uyguladığı işlemler, suç özelliği taşıyorsa, bu nedenle vekil sunucu kullanılıyorsa, vekil sunucu hukuki süreç birkaç gün gecikmektedir. Çünkü anonim vekil sunucular bile genellikle, kendilerine bağlantı kurulan bilgisayarların kayıtlarını tutmaktadır.[50]

1.3.7. İnternet Yer Sağlayıcısı (Host)

İnternet ile erişim sağlanan dijital bir depo olan internet sağlayıcısı, sunuculardaki olduğu gibi içyapısında dijital dataları saklayan internet servis sağlayıcıları da host olarak adlandırılmaktadır.[51]

5651 sayılı kanuna göre yer sağlayıcı, hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilerdir.[52] (5651 sayılı kanun, 2/f)

Aynı kanunun 5. Maddesinde yer sağlayıcının yükümlülükleri belirtilmiştir. 5. Maddeye göre, yer sağlayıcı, yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü olmamakla birlikte, yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, bu Kanunun 8. ve 9. maddelerine göre haberdar edilmesi halinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür. (5651 Sayılı Kanun, m. 5)[53]

30.11.2007 tarih 26716 sayılı yönetmeliğin 7. maddesi ile yer sağlayıcıya iki yükümlülük daha getirilmiştir. 26716 sayılı yönetmeliğin 7/b maddesine göre, sunucu barındırma hizmeti dâhil, yer sağlamakla ilgili hizmetlerinde (a) bendindeki hükümlere uymakla, 7/c maddesine göre de yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdür.

---

[50] Oğuz, 2012, **a.g.e**., s. 54-55.
[51] Avşar ve Öngören, **a.g.e.**, s. 120.
[52] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", ***Resmi Gazete***, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016.
[53] "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", ***Resmi Gazete***, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016, Madde 6/2.

1.4. İNTERNETİN YÖNETİMİ

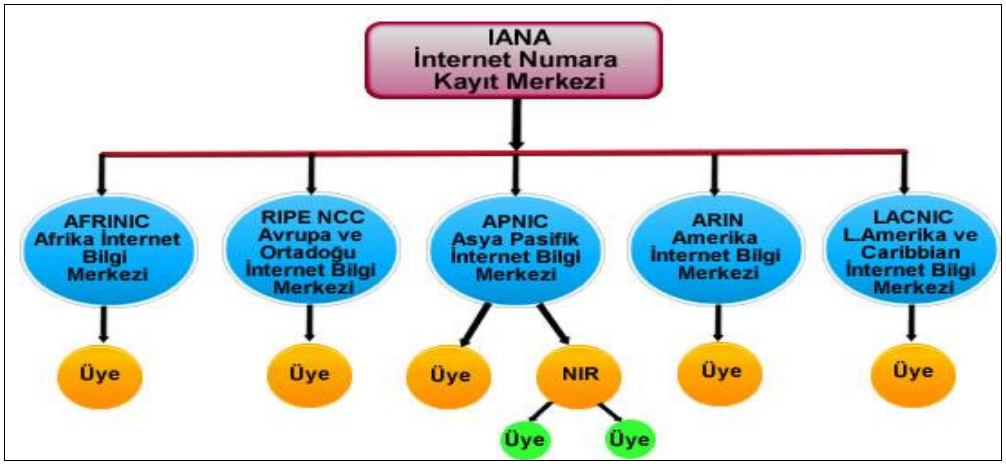
İnternetin küresel bir özellik taşıması, belli bir merkezi ve sınırı olmayan doğası, internetle ilgili problemler ve tartışma hususunda, ülkelerin tek başlarını etkin legal düzenlemelerin yapılmasına olanak vermemektedir. Bu bağlamda, devletlerin, teknoloji ve bilhassa küresel iletişim üzerindeki ilerlemeleri takip etmesi, kendi legal düzenlemeleri ve düşünce ve politika ortaya koyma şekillerine, bu sahada ulaşılan sonuçları da strüktürel olarak uyarlama ihtiyacının olduğu anlamına gelmektedir.

Modern IP tabanlı ağların idaresi günümüzde önem kazanan bir olgu olarak karşımıza çıkmaktadır. Her geçen gün internet ağına katılan yeni kullanıcılar, eklenen yen Ethernet anahtarları, cihazların takibi, idaresi, ağ trafiğinin denetlenmesi gibi her gün ortaya çıkan problemlerin çözümünde ağ yöneticilerinin kullanımına dair hazırlanan birçok yazılım bulunmaktadır. Fakat bunlar, yalnız belli bir vazifeyi gerçekleştirecek biçimde geliştirilmiştir.[54]

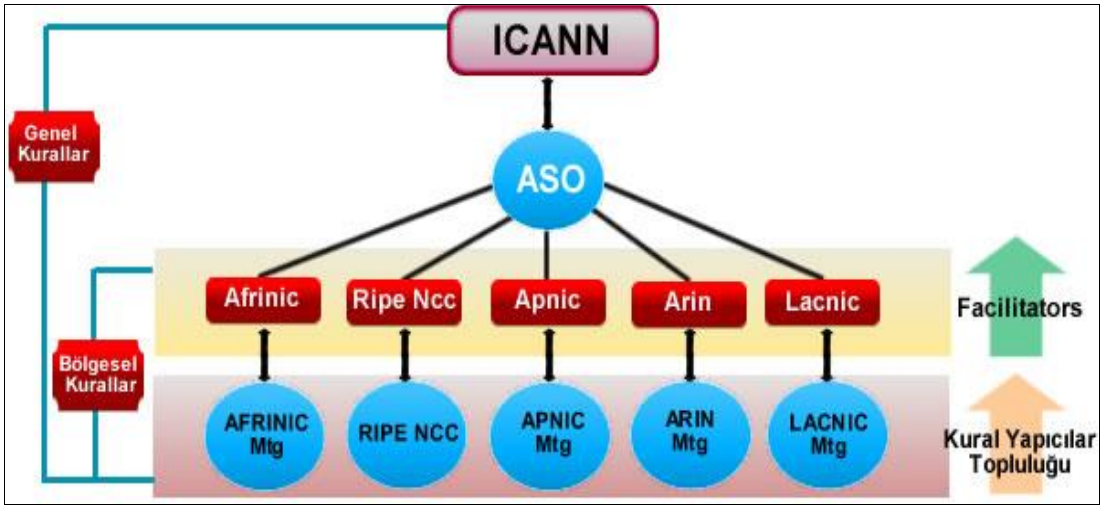
Ağ topolojisi tespit çalışmaları, internetin daha yaygın kullanımı ile artmaya başlamıştır. Ağ katmanı seviyesinde yapılan çalışmalar, genelde ana omurgaların yer aldığı geniş alan ağları ve ağ katmanı düzeyinde topoloji gösterimini amaçlamış, çoğu zaman yerel alan ağları ve bileşenlerine önem vermemiştir. Bu durum daha sonra, birçok üretici ve geliştiricinin çıkardığı çeşitli ürünlerle doldurulmaya çalışılmıştır. Günümüzde internetin tek ve belli bir sahibi bulunmamaktadır. İnternet trafiği küresel kurallar içinde, küresel işbirliğiyle gönüllü kuruluşlar tarafından yönetilmektedir. Ortaya çıkan bu kurallar ve kuruluşların yapısı, artan internet trafiğinin gereksinimleri tarafından belirlenmektedir. Bu nedenle, zamanla bu kuruluşların yapısı da gereksinimlere bağlı olarak değişmektedir. Bugün, internet idaresinde iki kurum bulunmaktadır. Bunlardan biri, internet numaralarının tahsisini idare eden IANA (İnternet Numara Kayıt Merkezi), diğeri de internet idare ve gelişme politikalarını tayin eden ICANN (İnternet İdare ve Gelişim Merkezi) kuruluşudur. Bu kuruluşların altında, dünyanın beş bölgesi için internet kaynaklarının ICANN tarafından belirlenen politikalar uyarınca idare eden RIR

[54] Alkan, Mustafa ve Canbay, Cafer, "İnternet Alan Adları Yönetimi, Mevcut Sorunlar ve Çözüm Önerileri", (Erişim) https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FArastirma_Raporlari%2FInternet_Alan_Adlari_Yonetimi_Mevcut_Sorunlar_ve_Cozum_Onerileri.pdf, 12 Aralık 2016, s. 4.

(Bölgesel İnternet Kayıt Merkezi) isimli kuruluşlar bulunmaktadır. Ticari amaç sahibi olmayan ve hükümetlere bağlı olmayan birer sivil toplum kuruluşu olan bu merkezler, bu özelliklerinden başka, ICANN politikalarının oluşturulmasında rol oynamaktadırlar. Böylece, global olarak katılımcı ve demokratik bir internet idaresi oluşmaktadır.[55]



Şekil 1. IANA yönetim organizasyonu [56]



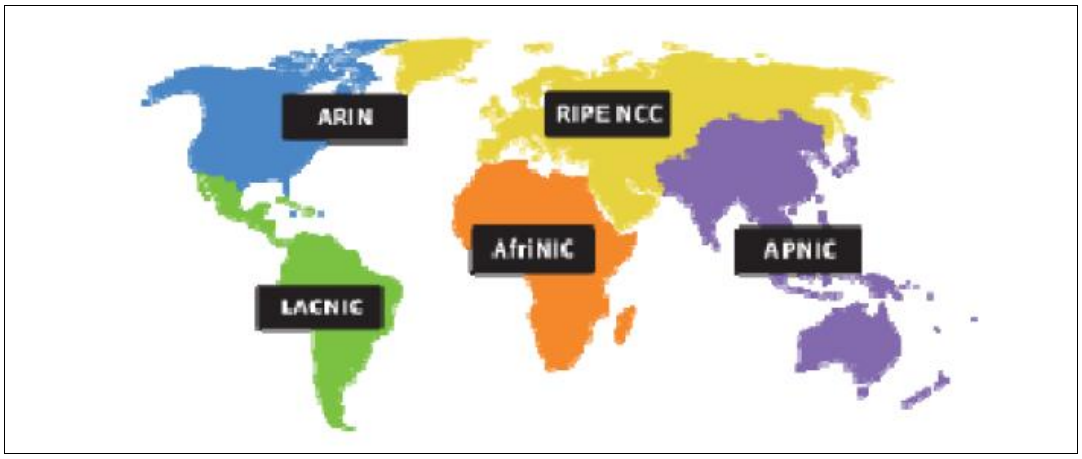
Şekil 2. ICANN yönetim organizasyonu [57]

[55] Soysal, Tamer, İnternet Alan Adları Sistemi ve Tahkim Kuruluşlarının UDRP Kurallarına Göre Verdikleri Kararlara Eleştirel Bir Yaklaşım-I**,** ***Sosyal Bilimler Enstitüsü Dergisi***, Sayı: 21, Yıl: 2006/2, 493-494.

[56] Çetin, Hakan, ***Türkiye'nin Otonom Sistem Seviyesinde İnternet Haritasının Çıkarımı ve İncelenmesi***, T.C. Muğla Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2009, s. 11

[57] Çetin, **a. g. e.** , s. 11

Bölgesel internet kaydı yönetimi, sorumluluk bölgelerinde bulunan internetin belli bir düzen içinde dağıtımı, kaydının yapılması işlemlerini uygulamaktadır. İnternet kayıt dağıtımı dünya üzerinde beş bölgeye ayrılmıştır. (Şekil 3)



Şekil 3. Bölgesel gösterim haritası [58]

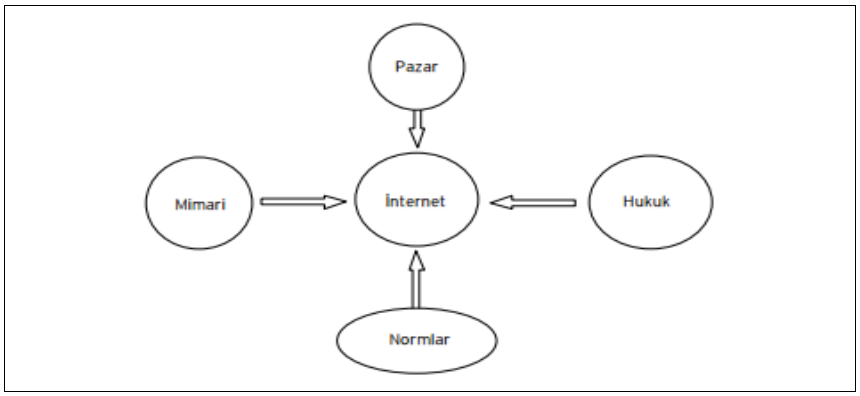
Dünya'da ARIN, LACNIC, RIPE NCC, APNIC ve AfriNIC olmak üzere beş tane bölgesel internet kayıt merkezi bulunmaktadır. ARIN, Kuzey Amerika, LACNIC Latin Amerika ve bazı adalar, RIPE NCC Avrupa, Orta Doğu ve Orta Asya, APNIC Asya Pasifik, AfriNIC Afrika bölgesini kapsayan ve kaydını tutan organizasyonlardır. Ancak bu alanlar, kesin sınırlara sahip değildir. Örnek olarak ARIN, bölgesel olarak Kuzey Amerika'yı kapsasa da, Güney Amerika ve Afrika'ya da hizmet vermektedir. Türkiye bu kayıt merkezlerinden RIPE NCC içindedir.

Lessing'e göre; günümüzde kendi kendini idare modeline bırakılmış olan internetin, tasarım, hukuk, piyasa yapısı ve sosyal kurallar sahası olmak üzere dört unsuru bulunmaktadır. Lessing, internete ait politikaları doğrudan ve dolaylı model olarak ikiye ayırmaktadır.[59]

İnternetin doğrudan düzenleme modelinde, siyaset yapıcılarının internet idaresinde doğrudan bir etkisinin bulunduğu farz edilmektedir. Günümüzde globalleşmenin önem kazanması ve çeşitli sınırların kaldırılması, internet üzerinde bu şekilde doğrudan idare modelinin olması güç bir durumdur. Doğrudan düzenleme modeli, internet üzerinde gitgide sınırlama ve sansürün oluşmasına neden olan bir

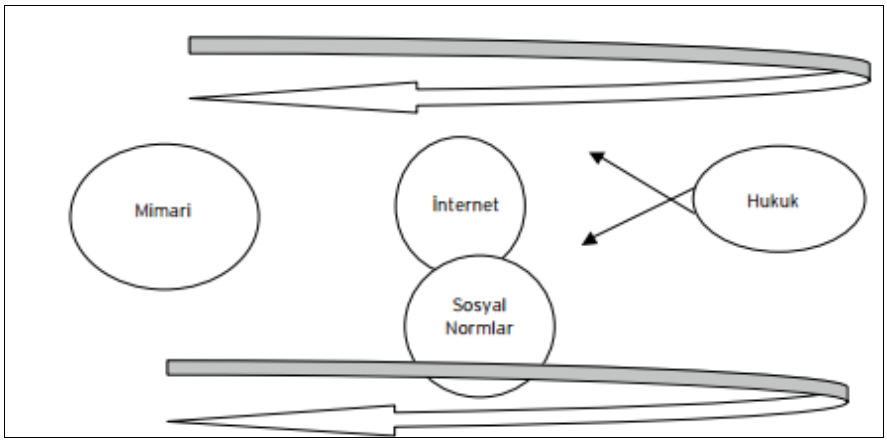
[58] Çetin, **a. g. e.** , s. 12
[59] Kaymas, Serhat, İnternet ve Ulusal Kamu Politikaları: İnternet Yönetiminde Türkiye için Alternatif Öneriler, **İletişim: Araştırmaları**, 5(2), 2007, (Erişim) http://dergiler.ankara.edu.tr/dergiler/23/1820/19198.pdf , 29.Eylül 2016, s. 123

modeldir. Her ne kadar bu modelin güç bir model olduğu görüşünde bulunulsa da, başta Çin olmak üzere bazı ülkelerin internet üzerindeki yönetim biçimi, anti-demokratik olarak değerlendirilse de, bu ülkelerdeki yönetim biçimi doğrudan düzenleme biçimine dayanmaktadır.[60]



Şekil 4. İnternetin doğrudan düzenleme Modeli [61]

İnternet düzenlemelerinde bulunan diğer bir model ise dolaylı internet yönetimi modelidir. Dolaylı internet yönetimi modelinde, internet düzenlemeleri bir dizi unsurun eş zamanlı olarak dolaylı bir şekilde gündeme alınmasıdır. Bu model daha çok Avrupa Birliği tarafından uygulanmaktadır. [62]



Şekil 5. İnternetin dolaylı olarak düzenlenmesi [63]

Çeşitli toplumlarda internetin gelişmesi hakkında çeşitli yaklaşımlar bulunmaktadır ve internetin etkinliği toplumlardan toplumlara farklılıklar

[60] Kaymas, **a. g. e. ,** s. 123.
[61] Cooke, 2007, akt., Kaymas, **a. g. e.** , s. 123
[62] Kaymas, **a. g. e**. , s. 124
[63] Cooke, 2007, akt., Kaymas, **a. g. e.** , s. 124

göstermektedir. İktisadi gelişmişlik, alt ve üst strüktür bağlamında, teknolojik donanım, kişisel haklara saygı, uluslararası alanda söz ve oy sahibi olma konularında, her ülke aynı seviyede değildir. Örnek olarak, Türkiye, internetle yaşamı daha gelişme aşamasındayken, bazı ülkeler, internet alanında çok daha ilerlemiş, internet erişimi ve kullanımının hızlanması gibi farklı konular üzerinde yoğunlaşmaktadır. Bunun doğal bir sebebi olarak, ülkelerin internetin çok taraflı yönetimine yaklaşım biçimi ve politika oluşturma sürecinin de farklı önceliklerle ortaya çıkmaktadır. [64]

Çok taraflı yönetim kavramının, internet ile ilgili çözümlemede, başta Batı Avrupa için uygun bir kavramdır. Bu, sadece teknolojinin doğası nedeniyle değil, aynı zamanda Batı Avrupa'nın siyasi ve toplumsal doğasından da kaynaklanmaktadır. Sonuç olarak internetin legal düzenlenişi ve internetteki sosyokültürel farklılıkların ve yaklaşımların hukuki olarak tanımlanışında, Batı Avrupa ülkelerinde çeşitli zorluklar bulunmaktadır. Avrupa Birliği üye ülkeleri seviyesinde, ortak bir Bilgi Toplumu Çağına uyum sağlansa da, ülkeler arasında kültürel, tarihi ve sosyo - politik farklılıklardan dolayı, Avrupa'deki çeşitli toplumlarında internetin gelişmesi ve yönetimi konusunda farklı yaklaşımların bulunduğu görülmektedir. Örnek olarak, Almanya'da internette ırkçılık hakkında yayınların yapılmasına çekinceli yaklaşılırken, İngiltere bu konuda daha sakin bir tutum takınmaktadır. Ancak, cinsellik konusunda İngiltere, toplumun sahip olduğu geleneksel ve katı tutum yansıtan politikalar izlemekte bir sakınca görmemektedir. [65]

Çok Katmanlı (Taraflı) Yaklaşım internet gibi yeni iletişim teknolojilerinin gelişimi ve bu teknolojinin merkezi olmayan ve küresel doğası, kuşkusuz Türkiye'yi de etkilemektedir, daha da etkileyecektir. Yukarıda da belirtildiği gibi, toplumların internet ve internet politikaları üzerinde farklı kaygıları ve çekinceleri vardır. İnternet yönetimi de her toplumun kendi kültürel, tarihi ve politik geçmişinin ve devlet gelişiminin doğal bir yansımasıdır. İnternet'in kendine has; merkezi olmayan ve küresel doğası, uluslararası ve uluslar üstü düzeydeki gelişmelerin ve anlamaların etkisi ve gücü nedeniyle, "etkin" kural koyma olgusu, tek bir devlet üzerinde sınırlanmayacaktır. [66]

---

[64] Akdeniz, Yaman, ***Çağdaş İnternet Yönetimi***, Nisan 2004, (Erişim) http://www.policy.hu/akdeniz/beyaz_kitap_sura.pdf, 12 Aralık 2016, s. 2.
[65] Akdeniz, **a. g. e.** , s. 2-3.
[66] Aynı, s.3.

Uluslar üstü ve milletlerarası ilerlemelerin devletlerin idaresindeki etkinliği göz ardı edilemez. İnternetle ilgili sorunlara ortak çözümler bulmak, kullanıcı güvenliğini artırmak, bilişim çağında güveni sağlamak için izlem ve politikaların uluslararası seviyede bir araya getirilmesi bir zorunluluk halini almıştır. İnternetin çoklu idaresi için uygulanan yöntemler, yerel seviyede normatif maddi şartlar ve süreç şartlarına bağlı olmalıdır. İnternetin çoklu idaresi, ifade hürriyeti ve gizlilik gibi kişisel hakları tartışılmaz değerler olarak kabul eden normatif çerçeve içinde ele alınmalıdır. Normatif maddi şartlar, Avrupa İnsan Hakları Sözleşmesi ve diğer uluslararası insan hakları sözleşmeleri ile tanınan ve korunan haklar ya da ifade hürriyeti, bilgiye erişim ve iletişim gizliği gibi haklardır. Bu esas sözleşmelerin gizliliği ve ifade hürriyetini uluslararası olarak koruması, bilhassa global iletişim ağı internetin özelliklerine de uygun düşmektedir.

Bu bağlamda çoklu idare, yalnızca belirtilmiş olan değerler göz önünde bulundurarak uygulandığında legallik kazanabilir. Sonuç olarak, internetin iyi yönetişimi hakkında herkes tarafından kabul edilen standartların gelişimi, enternasyonal insan hakları standartları gibi düzgüsel şartlarla, milli, milletlerarası ve uluslar üstü seviyedeki internet idaresiyle ilgili siyasi girişimler ve amaçların örtüşmesi ile alakalıdır. Devletler tarafından yapılan düzenlemeler ve kanunlaştırma teşebbüsleri sırasında ya da işbirliğine dayalı düzenleme modelleri geliştirilirken, bu girişimler insan hakları ve düzgüsel değerler altında değerlendirilmelidir. Devletlerin yaptığı kanunlaştırmalar günümüzde dahi birçok durumda güçlü bir ihtimal ve gereklilik şeklinde algılansa da, internetle alakalı sorunlarda, hükümetçe yapılan düzenlemelere seçenek olabilecek düzenleme yöntemleri de dikkatle değerlendirilmelidir.

1.5. İNTERNET (BİLİŞİM) SUÇLARININ TANIMI

Suç, kanun koyucu tarafından içinde bulunduğu toplum için zarar verici ya da tehlikeli olduğu kabul edilen ve belirtilen faaliyet, hal ve harekettir. Suç, bir devletin hukuk kuralları içinde, yapıldığı takdirde cezai müeyyidesi olan eylemdir. İşlendiği takdirde, mağdura maddi ve / veya manevi hasar verecek nitelikte olan davranışların suç sayılabilmesi için, kanunda gösterilmiş olması ve cezai karşılığının bulunması

gereklidir. Bir faaliyetin suç sayılabilmesi için, suçta yasallık prensibinin zaruri bir neticesi olarak, işlenen faaliyetin kanunda belirtilen tarife uygun olması gereklidir.[67]

Bilgi işlem teknolojilerinin hızlı bir şekilde gelişim göstermesi ve buna orantılı olarak hayata olan etkisi gün geçtikçe artmaktadır. Bilgi işlem teknolojisinde gelişen artış ve gelişim etkisini olumlu gelişmelere olduğu kadar, suç dünyasına da yansıtmaktadır. Suç dünyasında bilişim teknolojilerinin ilk kez kullanıldığı zamanlardan beri bu alanda bir sınır çizmek, konuyu belli tartışma kalıplarına sığdırmak hep zor olmuştur. Ayrıca bilişim teknolojilerinin gelişmişliği ve kullanım yaygınlığı dünyanın farklı bölgelerinde ve farklı ülkelerinde değişkenlik göstermektedir. Bu ve benzeri sebeplerden dolayı evrensel bir "bilişim suçu" tanımı dahi yapılamamaktadır. [68]

Bilgi işlem teknolojilerinin kullanımının yaygınlaşması ile birlikte ceza hukukunda, bu sistemlerin kötüye kullanımına dair eylemlerin cezalandırılabilir olması ve kötüye kullanımının oluşturduğu sorunların çözümü veya çözüme ait yaklaşım sonucu bu konuyla ilgili birçok tanım yapılmış ve bu tanımları ifade etmek için birçok terim kullanılmıştır. Bu şekilde, bilişim ve bilgisayar sistemi ile işlenen suçlar ile ilgili bilgisayar suçları, bilgisayar suçluluğu, bilişim suçları, internet suçları ve siber suçlar terimleri kullanılmaktadır.[69]

İnternet suçlarının tanımı ve tasnifi hakkında herkesçe kabul edilen bir tanım ve birlik bulunmamaktadır. Teknolojinin gelişmesi ile beraber, bilişim suçlarının kullanıldığı alan ve cihazlar ve işlenme şekillerinin de değişmesi, tek bir bilişim suçu tanımını yapmayı zorlaştırmaktadır. İnternet ve bilişimin özellikle hukuk alanında birçok davranış şekilleri ile birlikte yeni sorunları da beraberinde getirmektedir. Türkiye'de teknoloji yoluyla işlenen suçlar genel olarak "bilişim suçu" ya da "internet suçu" olarak adlandırılmaktadır. Bu nedenle internet suçu ve bilişim suçu bir bütün olarak görülmüş ve çalışma süresince de her iki kavram yer yer kullanılma yoluna gidilmiştir. Bununla birlikte, birçok ülkede olduğu gibi Türkiye'de de bilişim suçunun tanımı yapılmamış, bunun yerine bilişim alanında suç olarak değerlendirilen davranışların tanımları yapılmıştır.

---

[67] Hafızoğulları, Zeki – Güngör, Devrim, "Türk Ceza Hukukunda Suçların Tasnifi", ***TBB Dergisi***, Sayı 69, 2007, s. 21-50.

[68] Akarslan, Hüseyin, ***Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı***, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2011, s. 12

[69] Ketizmen, Muammer, ***Türk Ceza Hukukunda Bilişim Suçları***, Yayımlanmamış Doktora Tezi, T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 45

Her şeyden önce bilişim, kavram olarak, bilgisayar kavramına göre daha geniş bir anlam taşıması nedeniyle ve günlük yaşamda kullanılan cep telefonu vb. gibi çoğu elektronik aletin bilgisayar olmadığı, ancak birer bilişim sistemi olduğu dikkate alındığında, elektronik aletler yoluyla işlenen bütün suçların bilgisayar suçu olarak adlandırılmaması gerektiği uygun bulunmuştur. Bilişim, bilgisayara göre daha genel bir alanı ve bir üst kavramı ifade etmektedir. Temel olarak bilişim suçları, "*bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenilen suçlardır."* [70]

Bilişim suçları genel olarak elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde silinmesi, değiştirilmesi veya bu tür kayıtlara girilmesi olarak tanımlanabilir.[71]

Bilişim suçlarına ilişkin ittifak edilen bir tarif yoksa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu (AET) Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır."[72] Bu bağlamda, Avrupa Ekonomik Topluluğu'nun tavsiye kararında verilen tanıma göre, bilişim suçlarının çeşitli şekillerde işlenebildiği, suçun farklı görünüş şekillerinin değişik özellikler bulundurduğu belirtilmiştir. AET bir tavsiye kararında bu suçları beşe ayırmıştır. Bunlar,[73]

- Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,
- Bir sahtekârlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

[70] Dilek, Halil İbrahim, ***Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri***, T.C. Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2007, s. 4

[71] Tunçbilek, Burak, *Bilişim Suçları ve Üniversite Lisans* ***Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri***, Gazi Üniversitesi Bilişim Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2012, s. 5.

[72] Kurt, Levent, ***Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulaması,*** Seçkin Yayınları, Ankara, 2005a, s. 50.

[73] Özel, Cevat, ***Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı***, Yeşim Atamer (Ed.), İnternet ve Hukuk, İstanbul, Bilgi Üniversitesi Yayınları No: 51, 2004, s. 342.

- Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,
- Ticari anlamda yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,
- Bilgisayar sistemi sorumlusunun izni dışında konulmuş olan emniyet tedbirlerini aşmak suretiyle sisteme kasten girerek müdahalede bulunmaktır.

Bir diğer ifadeyle bilişim suçları, "*dolandırıcılık yapmak için bilerek bilgisayar veri ya da programlarına girmek, onları bozmak, silmek, yok etmek*" şeklinde tanımlanmış ve suçun unsurlarında dolandırıcılık yapma amaç ve suçu işleyenin bir çıkar elde etmesi aranmıştır.

Literatürde bilişim ve bilgisayarın farklı anlamlara geldiği ve bilgisayar suçu ile bilişim suçunun farklı anlamlar ifade ettiğini savunan yazarlar da bulunmaktadır. Yazıcıoğlu'na göre, "*bilişimle bilgisayar ve bilgisayar suçu ile bilişim suçu birbirinden farklı anlamlara sahiptir. Pratikte ise bilgisayarın en yaygın bilişim aracı olması nedeniyle bilişim suçları yerine bilgisayar suçları kavramının kullanıldığını söylemektedir.*"[74]

Yenidünya ve Değirmenci'ye göre; "*bilişim terimi, bilgisayara göre, daha geniş bir alanı kapsayıp bir üst kavramdır. Bilgisayar verilerin depo edilmesi, saklanması, islenmesi ve yeniden değerlendirilmesi faaliyetlerini, diğer bir anlatımla veri-işlemi tek basına gerçekleştirebilmektedir. Bilişim ise, hem verilerin islenmesini hem de verilerin aktarımını kapsar. Bilişim sistemlerinin en yaygın kullanılan unsurunun bilgisayarlar olması, "bilgisayar suçu" teriminin yaygınlık kazanmasına neden olmuştur. Bu açıklama doğrultusunda yazarlar bilişim suçu terimini kullanmayı uygun bulduklarını belirtmektedirler."* [75]

Tanım ve terim zenginliği yanında bu alanda ortaya çıkan ihlallerin cezalandırılabilmesine ilişkin suçlar esas alınarak, bilgisayarın ya da bilişim sisteminin suçun maddi konusu ya da suçta kullanılan araç olması gibi hususlar esas alınarak birçok sınıflandırma yapılması kapsam sorunlarını da beraberinde getirmiştir.[76]

---

[74] Yazıcıoğlu, Yılmaz, ***Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları ile***, 1997, s. 131

[75] Yenidünya ve Değirmenci, **a. g. e.** , s. 31

[76] Ketizmen, **a. g. e.** , s. 45

Bu suçlarda yapılan sınıflandırmaların büyük bir kısmı, söz konusu suçların klasik suçlardaki biçimine dayanmaktadır. Öncelikle, bilgisayar suçun / suçlunun hedefi olabileceği gibi (bilgisayar donanımı veya yazılımlarının çalınması gibi) bilgisayarın kendisi de suçun konusu olabilir. Yani, burada bilgisayar, suçun fiziki yapısı, kaynağı veya nedenidir; çeşitli şekillerde zarar verme söz konusu olabilir. Ek olarak, bilgisayar klasik suçları daha karmaşık şekilde işlemek için suçta araç olarak kullanılabilir. [77]

Konuyu ifade için kullanılan terimler arasındaki farklılık (yani terim sorunu) bir sonrakinin bir öncekine oranla konunun özünü veya kriminolojik yanını veyahut sistematiğini daha iyi anlattığı, daha çok kapsadığı iddiasından kaynaklanmaktadır. Tercih edilen terimin önemiyse asla küçümsenmemelidir, zira her biri konunun boyutunu değiştirdiği gibi, konuya gösterilmesi gereken yaklaşımın belirlenmesinde de önemli bir rol oynamaktadır. [78]

Bilişim ortamındaki suçları beş ayrı grup altında toplayan yaklaşımlar da vardır.[79]

- Bilgisayar sistem veya ağlarına hakkı olmadan girmek,
- Hak sahibinin rızası olmadan bilgisayar veri ve programlarına zarar vermek, bilgisayar veri ve programlarını silmek, bozmak, tahrip etmek ve elde etmek,
- Bilgisayarların işlemesini veya telekomünikasyon sistemini engellemek amacıyla bilgisayar veri ve sistemlerini tahrip etmek, veri yüklemek, değiştirmek, silmek veya elde etmek,
- Hukuk dışı olarak iletişime müdahale etmek,
- Menfaat temin etmek için ticari sırları izin almadan veya hukuken bir hak olmaksızın ifşa etmek veya tevzi etmek veya kullanmaktır.

Hangi eylemlerin bilişim suçu kapsamına gireceği, hukuki sistemin başlıca sorunudur. Bu sorunun çözümünde, bilişim suçlarının yapısının tam anlamıyla ortaya konulamaması, en temel sorun olarak karşımıza çıkmaktadır.

---

[77] Avşar ve Öngören, **a. g. e.** , s. 123
[78] Yazıcıoğlu, **a. g. e.** , s. 130
[79] Kurt, 2005a, **a. g. e.** , s. 69

Dar anlamda bilişim suçları, bilişim sisteminin güvenliğini veya veri işlemini hedef alan eylemlerdir. Geniş anlamda siber suçlar ise bilişim sistemi ve ağı marifetiyle veya bu sistem veya ağda gerçekleşen herhangi hukuk dışı eylemlerdir. [80]

Sadece bilişim ortamında işlenebilen, klasik suçlar arasında sayılmayan, bilgisayar ve internete özgü suçlar dar anlamda suçlardır. Bu suçlar, daha önce hiç görülmeyen ve bilinmeyen, bilgisayarın icadı ve yaygınlaşması sonucu ortaya çıkan, internetin yaygınlaşmasıyla da işlenmeleri kolaylaşan ve artan suçlardır. Bu suçları ortadan kaldırmak veya bir çerçeve içinde sınırlandırmak mümkün değildir. Her geçen gün çok değişik yöntemler kullanılarak bu suçlar çoğaltılmaktadır. Bu suçlara yetkisiz erişim (hacking)i verilere yönelik suçlar, bilişim ağlarına yönelik suçlar ve sanal tecavüz verilmiştir. [81]

Literatürde teknoloji yoluyla işlenen suçlar için birçok kavramın kullanıldığı göz önünde bulundurulduğunda, bu kadar geniş bir sahada, bilişim suçu ile bilişim yoluyla işlenen suç kavramlarında bir ayrıma gidilmesine olanak vermemektedir. Fakat uygulamada, bu çeşit bir ayrım bulunmaktadır ve yapılan bu tanımlamaların, yapılan ayrımın içeriğine aykırı olmaması gereklidir. Bilişim sahasında işlenen suçların tanımlamaları yapılırken, suç oluşturacak davranışların hem teknolojik hem de hukuki yönleriyle ele alınması bu sorunu ortadan kaldıracaktır. Türk hukukunda, bilhassa terimsel olarak bilişim suçu veya bilgisayar suçu terimleri kullanılmakta ve bu iki terim arasında anlam ve kapsam olarak farklılık oluşturulmaktadır. Bahsedilen farklılık, bilişim ve bilgisayar terimlerinin farklılığı durumundan doğmaktadır. Bu terimler arasında yapılan ayrım neticesinde, bilişim suçu teriminin, bilgisayar suçlarını da kapsayan geniş bir alana sahip olduğu belirtilmektedir.

Ceza Hukukunun temel normları arasında yer alan, suç da ve ceza da kanunilik ilkesi, aynı şekilde ceza kanunlarında "kıyas" yapılamaması ilkesi gereği, "söz konusu teknolojinin sınır tanımaz tabiatı, iç hukuk düzenlemelerini yetersiz bırakmakta, hukukçuları zaman ve mekân kavramını yeniden sorgulamaya itmektedir." [82]

765 Sayılı TCK'nin 525a vd. ve TCK'nin 243, 244 ve 245. maddelerinde düzenlendiği şekliyle, suçun konusunun ya da suçta kullanılan aracın tespitinden

[80] Avşar ve Öngören, **a. g. e.** , s. 124
[81] Aynı.
[82] Akıncı, Hatice – Alıç, Emre A. ve Er Cüneyt, "Türk Ceza Kanunu ve Bilişim Suçları", ***İnternet ve Hukuk***, Ed. Yeşim Atamer, Bilgi Üniversitesi Yayınları, İstanbul, No: 51, 2004, s. 159.

önce bilişim suçu ile neyin anlaşılması gerektiğinin tespiti gerekmektedir. Türk Hukukunda bilişim ya da bilgisayar suçları, bilişim sistemi, bilgileri otomatik işleme tabi tutan sistem ve bilgisayar terimlerinin anlam ve kapsamı belirlenmek suretiyle tanımlanmaktadır. Bu doğrultuda, bilişim ve bilgisayarın anlamlarından yola çıkılarak ve ayrıca bilişim sistemi olarak değerlendirilen araç ve aygıtlar ve de bilgisayar arasındaki farklar da esas alınarak bilişim ya da bilgisayar suçu tanımları yapılmaktadır. Aynı şekilde söz konusu suçların sınıflandırılmasında da suçta kullanılan araç ya da suçun maddi konusu olan bilgisayar ya da bilişim sistemi esas alınmaktadır. [83]

Bilişim sisteminin kullanılmasının yaygın hale gelmesi, bilhassa ağırlıkla bilgisayar sistemlerinin kullanılması, bilgisayar sistemlerinin kullanılmasındaki amaç ve kullanım yerine göre yasal sorunlara sebep olabilmektedir. Ceza hukuku açısından ortaya çıkan sorunlar, suç unsurundan ortaya çıkabileceği gibi, cezalandırma bakımından daha önce suç olarak düzenlenmeyen bir eylemin, suç oluşturması ve suç haline getirilmesinin gerekli olup olmaması hakkında ortaya çıkmaktadır. Kısaca, suç ve cezada yasallık ilkesi uyarınca var olan suç unsurlarının, bu eylemleri kapsayıp kapsamadığı veya bu tür eylemlere dair yeni suçların düzenlenmesi, sorunun esas noktasını oluşturmaktadır.[84]

Suçun, hukuki açısı bakımından bunun anlamı, ortaya çıkan yeni eylemler durumunda, mevcut bulunan çeşitli kanunlar ile korunan hukuki değerlerin, yeni eylemler karşısında korunmasına dair yöntemlerin saptanmasıdır.

1.6. TARİHİ GELİŞİMİ

Bilişim suçlarının ortaya çıkması, bilgisayarların yaygın biçimde kullanımıyla başlamıştır. Bilişim suçlarının işlenme oranının artması ve bu nedenle bilhassa ceza hukuku bakımından düzenleme yapılması gereksiniminin belirmesi de, internetin ortaya çıkması ve bunun, bireylerin kullanımına sunulmasıyla gerçekleşmiştir. Teknolojinin gelişmesi, insanların hayatını her geçen gün daha da kolaylaştırmaktadır. Bilişim ve iletişim teknolojilerindeki gelişmeler, günümüzde

[83] Ketizmen, **a. g. e**. , s. 48

[84] Uğur, Hüsamettin, "Suçta ve Cezada Kanunîlik İlkesi ve Anayasa Mahkemesi Kararları Karşısında Yaptırımsız Kalan Bazı Suçlar", ***TBB Dergisi***, 91, 2010, (Erişim) http://tbbdergisi.barobirlik.org.tr/m2010-91-662, 12 Aralık 2016, s. 302.

insanlık için önemli bir değişim ve devrim olarak kabul edilmektedir. Bu bağlamda eğitimden eğlenceye, ticaretten alışverişe, birçok sahada geleneksel anlayışı değiştirmiş, insanlara yeni bir anlayış, yeni bir yaşam tarzı kazandırmıştır. Olumlu gelişmelerle birlikte, bu gelişimlerin bir sonucu olarak, yeni suç tipleri ortaya çıkmış, suça meyilli olan bireyler, insanların hizmetine sunulan gelişmeleri kullanarak bilişim suçlarını ortaya koymuşlardır. Günümüzde, bilişim kavramı yalnızca insanların yaşamlarını kolaylaştıran bir unsur olmaktan çıkmış, aynı zamanda kişilerin güvenliğini tehdit eden ve suç ile birlikte anılan bir araç olmuştur.

Bu bağlamda her yenilik, yeni hukuki çıkarlar oluşturmakla birlikte yeni ihlal alanlarını da birlikte getirmektedir. "*Bilişim suçlarının her geçen gün yeni işlenme şekillerinin ortaya çıkması gerek kamu gerekse özel hukuk açısından birçok sorunu da beraberinde getirmiştir.*[85]

Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır.[86] Dülger de, ABD'de kimi kişilerin sistemde yer alan boşluklardan yararlanarak, telefon konuşmalarını bedava yapmalarını, bilişim suçunun başlangıcı olarak belirtmektedir.[87] Son yıllar içinde bilişim suçları, bilgisayar programcılarından, bilgisayar üreticilerine, bilgisayar kullanıcılarından, hukukçulara kadar tüm bilişim uzmanları ve kullanıcılarını kapsayan geniş bir sahaya yayılmaktadır.

1981 yılında Condor rumuzlu Mitnick isimli şahıs, Pasific Bell anahtarlama istasyonuna ait verileri çalmakla suçlanmış, 1982 yılında Kuzey Amerika Hava Savunma Komutanlığı bilgisayarına girmiş, ayrıca Kaliforniya'daki tüm telefon anahtarlama merkezlerine erişerek, Manhattan'daki üç adet merkezi telefon şirketinin geçici olarak kontrolünü ele geçirmiştir. 1988'de Mitnick, MCI ve Digital Equipment şirketlerinin güvenlik çalışanlarının elektronik postalarını ele geçirmiştir. Bunun üzerine Digital Equipmant, Mitnick'i bilgisayar işlemlerine 4 milyon Amerikan Doları zarar vermekle ve 1 milyon Amerikan Doları değerindeki yazılımı çalmakla suçlamış ve yargılama neticesinde Mitnick 1 yıl hapse mahkûm edilmiştir. Yine 1993 yılında Mitnick, California Motorlu Araçlar Departmanı'nın veri tabanlarından

[85] Kurt, 2005a, **a. g. e.** , s. 28
[86] Aynı.
[87] Dülger, Murat Volkan, ***Bilişim Suçları,*** Ankara, Seçkin Yayınları, 2004, s. 54

sürücü belgelerini çalmakla suçlanmıştır. 1994 yılının ilk günü ise Mitnick, San Diego Supercomputer Center'da bulunan Tsutomu Shimomura'nın sistemine girmiştir. Bunun üzerine Shimomura da, Mitnick'in tutuklandığı 1995 yılına kadar internet üzerinden Mitnick'i kovalamıştır. Ve neticede Mitnick, yargılanarak suçlu bulunmuştur. [88]

1981 yılında AET'nin düzenlediği '' Bilgisayarlaşan Toplumda İhlaller '' adlı toplantıda belirlenmiş olan tanımlar, bugün de geçerliliğini korumaktadır. 1985 yılında Avrupa Topluluğu Suç Problemleri Komitesi, kendi yapısı altında bilişim suçları sahasında çalışmalar yapılması ve üye devletlere tavsiyelerde bulunması için bir alt komisyon oluşturulmuştur. Aynı yıl, Milano'da düzenlenen Birleşmiş Milletler Toplantısında, bilgisayar suçlarının sonuçları görüşülmüştür. 1988 yılında, Birleşmiş Milletler bünyesinde bilişim suçları ile ilgili bir toplantı yapılmış, bu toplantıda komisyon tarafından yapılan 3 yıllık bir çalışmaya ilişkin üye devletlere tavsiye kararlarında bulunmuştur. Topluluğun 1989 yılında yapmış olduğu ve "*Bilgisayarla ilgili Suçlar üzerine Uzman Raporu"* adlı bildiride, toplantıda alınan kararlar özetle bilgisayar sahtekârlığı ve bilgisayar dolandırıcılığını da içine alan elektronik suçlarla mücadele için etkili yasal önlemler alınmasını önermektedir. [89]

1990 yılında Küba'da yapılan Birleşmiş Milletlerin Toplantısında bilişim suçlarının hızlı bir artış içinde olduğu, bu suçların çözümünün zorlukları, bilişim suçlarının işlenmesinin normal suçlara göre daha kolay olması ve ekonomik zararları da göz önünde bulunduran çeşitli kararlar üye devletlere sunulmuştur.

1990'ların başında internetin bireysel kullanımının başlaması ve bireylerin kendi bilgisayarlarına sahip olmaları sebebiyle bilişim suçlarında bir artış yaşanmıştır. Günümüzde internet, bilişim suçlarının işlenmesinde en etkili araç olarak karşımıza çıkmaktadır. İnternet yalnızca internetin iyi yanlarını kullananlara değil, aynı zamanda kötü yanlarını kullananlara da bu anlamda eşit durmaktadır. Bilişim suçları sahasında, günümüze kadar yapılan en etkin yasal düzenleme 2001 yılında Avrupa Konseyi tarafından yapılan Avrupa Konseyi Siber Suçlar Sözleşmesidir.

[88] Özdilek, 2002, **a. g. e.** , s. 27
[89] Gözüşirin, **a.g.e.** , s. 29.

1.7. ÖZELLİKLERİ

Yüzlerce yıldır işlenen hırsızlık, öldürme, yaralama, gasp gibi klasik suçların yanında bilişim suçu, görece daha yeni bir kavram olarak karşımıza çıkmaktadır. Bu sebeple, bilişim suçları klasik suçlarla az da olsa bir benzerlik gösterse de, genel olarak klasik suçlarla arasında farklılıklar bulunmaktadır. Bilişim suçlarının sınırlarını çizmek ve kapsamını belirlemek, klasik suçlara göre zordur. Teknolojik gelişmeler ve yaygın duruma gelmesi, bu durumu daha da zor duruma sokmaktadır. Devamlı olarak değişim gösteren ve hızla artan bir suç türü olan bilişim suçları ile mücadele etmeyi daha da zorlaştırmaktadır.

Bilişim suçları, bilhassa bilgisayar ve internet kullanımının artmasıyla birlikte ortaya çıkmış, tanım ve yapısı bakımından tam bir uzlaşmaya gidilmemiştir. Bilhassa bilişim suçlarının, çok geniş bir yelpazeye yayılması, klasik ceza hukukunu bir takım çıkmaza sokmuştur. Bunun en temel sebebi, "*bilişim suçlarının yapısının durağan olmaması, bir başka deyişle dinamik bir yapıya sahip olmasıdır ve bu sahada yapılan düzenlemelerin, gelişen teknolojiyle birlikte yeni çıkan suçların işlenme şekillerinin hukuka aykırı bir eylem olarak hükmedilmesi gerekmesidir."* [90]

Bilişim suçlarının yapısal olarak kendine ait özelliklerinin başında, suçun işlendiği saha önemlidir. Bilişimin olmadığı bir sahada, bilişim suçundan bahsedilemeyecektir. Bununla birlikte, bilişim suçunun işlenebilir olması için gerekli olan bilişim sahasının temel unsurları üç kategoriye ayrılabilir:

Bunlardan birincisi, bilgisayar ve benzeri elektronik cihazlardır. Bilhassa, benzeri elektronik cihazlar olarak kullanılan kavram, her geçen gün teknoloji ile birlikte hızla çeşitlenmektedir. Akıllı telefonlar, tabletler, avuç içi bilgisayarlar olmak üzere benzeri taşınabilir cihazlar, bilişim suçlarında kullanılan unsurlar haline gelmektedir. İkincisi ise bu cihazlar arasında, veri iletişiminin sağlanması için gereken iletişim ortamıdır. Bu iletişim ortamı da, teknolojik gelişmelerle birlikte değişime uğramaktadır. İnternetin yaygınlaşması, kablosuz ağ ve 3G gibi taşınabilir mobil iletişim hizmetlerinin kullanımının artması sonucunda, bilişim suçlarında da bir artış meydana gelmiştir. Son olarak, bilişim ortamının tamamlanması için, bilişim cihazlarının çalışması için gerekli enerjinin sağlanması, bilişim sahasının bir diğer unsurudur.

[90] Kurt, 2005a, **a.g.e.** , s. 30

"*Bilişim suçlarının özelliklerinin en başında işlenebilmesindeki kolaylık ancak tespit edilmesi ve cezalandırılmasındaki zorluktan bahsetmek gerekir."*[91] Bilişim suçlarının kovuşturulmasında, kovuşturma organlarının karşılaştığı diğer bir husus da suçu işleyen faillerin arkalarında iz bırakmaması olarak ifade edilebilir. [92]

Bilişim suçlarının ortaya çıkarılmasında, suça ait delillerin toplanması, diğer suçlara göre daha zordur. Bilişim suçlarında delillerin toplanmasında, sanal ve fiziki sahanın aynı anda incelenmesi gerektiğinden, bilişim suçlarının çözümü daha da zor hale gelmektedir. Literatürde bilişim suçlarını, klasik suçlardan ayıran en önemli özelliğinin suçun işlenmesinden sonra, herhangi bir delil bırakılmaması sebebiyle, suçun çözümü ve faillerinin bulunmasının oldukça zor olduğu hakkında fikir birliği bulunmaktadır. Değirmenci'ye göre, "*bilişim suçlarını klasik suç tiplerinden ayıran en önemli etkenin suçun işlenmesinden sonra arkada herhangi bir iz bırakılmaması sebebiyle ortaya çıkan zorluktur."*[93]

Bilişim suçları yapısal olarak, zaman ve yer unsurlarını ortadan kaldırmaktadır. Dünya'nın herhangi bir yerinden internet protokolüne uygun şekilde bağlanan biri, kısa süre içinde dünyanın başka bir yerinde bulunan diğer bir bilgisayara erişebilir ve bilişim suçunu işleyebilir. Bu durum, bilhassa ceza yargılama hukuku bakımından yeni sorunlar çıkarmaktadır ve yerel ve milletlerarası sahada yeni düzenlemeler gerektirmektedir. Bununla birlikte bilişim suçlarında, zaman etmeninin yeni bir boyutu bulunmaktadır ve çok kısa süre içinde bilişim suçları işlenebilmektedir. Bilhassa internetin sınırsız ve mesafe tanımaz özelliğinden dolayı, faillerin saptanması çoğu zaman mümkün olmamaktadır ve tespit edilse bile, devletlerarası suçlarda farklı usul uygulamaları sebebiyle, suçun kovuşturulması çoğu zaman olanaksız olmaktadır.

Klasik suçları, bilişim suçlarından ayıran diğer bir önemli özellik, klasik suçlarda, faillerin davranışlarını fiziki davranışla uygular ve etkileri bilişim suçlarına göre sınırlı olurken, bilişim suçlarında ise faillerin fiziki davranışlarının çok sınırlı olmalarına karşın, etkilerinin daha ağır olmasıdır. Bu sebepledir ki, bilişim suçlarının faillerinin suçüstü yakalanmalarına ait hükümlerin uygulanmasında hukuki bir engel olmamasına karşın, pratikte tatbiki oldukça güçtür.

---

[91] Kurt, 2005a, **a.g.e.** , s. 56
[92] Gözüşirin, **a.g.e.** , s. 31
[93] Değirmenci, Olgun, ***Bilişim Suçları***, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2002, s. 75.

"*Bilişim suçları zaman ve mekân kavramından bağımsız gerçekleşir ve anlık olurlar."*[94] Bununla birlikte, küreselleşme ile birlikte ekonomi ve milletlerarası yapıda bozulmalara yol açmakla birlikte, bilişim suçları da klasik suçlara göre daha fazla artış göstermektedir.

Bilişim suçlarının mağduru bazen bir birey, bazen bir kurum, bazen de toplumun hepsi olabilmektedir. Bilişim suçlarını klasik suçlardan ayıran bir diğer özellik, bilişim suçlarının klasik suçlardan farklı bir şekilde olması nedeniyle, bilişim suçlarının klasik polisiye ile önlenmesi mümkün olmamaktadır. Bu nedenle, bu suçlarla mücadele edecek olan güvenlik güçlerinin de, belli bir teknik bilgiye sahip olması gerekmektedir. Bilişim suçlarının önlenmesi ve suçluların yakalanmasında kurumlar arası işbirliği gereklidir. Bazı durularda, uluslararası işbirliği dahi gerekli olmaktadır.

Bilişim sistemleri ile işlenilen suçlarda, ilgili kanıtlar değişik şekil ve biçimlerde, suçun işlenmesi sonrasında dijital kanıt olarak bulunabilmektedir. Dijital kanıt toplama ve kanıtlandırma süreci de klasik suçlarda ele geçirilen kanıtlardan farklıdır.

Bilişim suçunun işlenmesi sonrası, yüksek oranlarda maddi kazancın kolay ve risksiz bir şekilde elde edilebildiği durumlar ortaya çıkmaktadır.

Bilişim suçlarının ortaya çıkmasıyla, klasik suçları bulunduran hukuki dallardan ayrı bir şekilde, yeni gereksinimleri giderecek bilişim hukuki adında ayrı bir hukuk dalı ortaya çıkmıştır. Ancak, bilişim hukuku her zaman ceza hukukuna ilişkin bir konu olmayıp özel hukuka dair durumlarda da öne çıkmaktadır.

1.8. SINIFLANDIRILMASI

Literatürde bilişim suçlarının sınıflandırılması hakkında farklı yaklaşımları bulunduğu görülmektedir. Bunun nedeni, sınıflandırma yapılırken, suçun işleniş şekli, hukuki metinler ve uluslararası düzenlemeler gibi farklı unsurların dikkate alınmasıdır.

Bu suçlarda yapılan sınıflandırmaların büyük bir kısmı, söz konusu suçların klasik suçlardaki biçimine dayanmaktadır. Öncelikle, bilgisayar suçun/suçlunun

[94] Kurt, Levent, (2005b), ***Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması***, Seçkin Yayıncılık, Ankara, s.56.

hedefi olabileceği gibi (bilgisayar donanımı veya yazılımlarının çalınması gibi) bilgisayarın kendisi de suçun konusu olabilir. Yani, burada bilgisayar, suçun fiziki yapısı, kaynağı veya nedenidir; çeşitli şekillerde zarar verme söz konusu olabilir. Ek olarak, bilgisayar klasik suçları daha karmaşık şekilde işlemek için suçta araç olarak kullanılabilir.[95]

Avrupa Konseyi Siber Suç Sözleşmesi'ne göre bilişim suçları; bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar, bilgisayarlarla ilişkili suçlar, içerikle ilişkili suçlar ve fikri mülkiyet haklarının ihlali ile ilgili suçlar şeklinde sınıflandırılmıştır. [96]

Avrupa Topluluğunda ise bilgisayar suçları şöyle tasnif edilmektedir:[97]

- Bir kaynağın veya herhangi bir değerin gayri kanuni olarak transferini sağlamak için kasten bilgisayar verilerine ve/veya programlarına girmek, bozmak, silmek ve/veya yok etmek;
- Bir sahtekârlık yapabilmek için kasten bilgisayar verilerine ve/veya programlarına girmek, bozmak, silmek ve/veya yok etmek;
- Bilgisayar ve/veya telekomünikasyon sistemlerinin çalışmasını engellemek amacıyla kasten bilgisayar verilerine ve/veya programlarına yahut bir bilgisayar sistemiyle bir bağlantı bir bağlantı sağlayan mekanizmaya girmek, bozmak, silmek ve/veya yok etmek,
- Piyasaya sürmek ve ticari olarak yararlanmak amacıyla bir bilgisayar programının yasal malikinin sahip olduğu hakları zarara uğratmak,
- Bir bilgisayar ve/veya telekomünikasyon sistemi sorumlusunun izni olmaksızın veya mevcut emniyet tedbirlerini aşarak bu sistemlere kasten girmek veya müdahalede bulunmaktır.

Suç çeşitleri ayrımında 11.06.1999 tarihinde Birleşmiş Milletler (BM) ve Avrupa Birliği (AB) tarafından hazırlanan "Bilişim Suçları" raporuna göre; suç çeşitleri altıya ayrılmaktadır.

[95] Karagülmez, **a.g.e.** , s. 52.
[96] Akarslan, 2012, **a.g.e.** , s. 16
[97] Kurt, 2005b, **a.g.e.** , s. 78

Bunlar; [98]

- Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme
- Bilgisayar Sabotajı
- Bilgisayar Yoluyla Dolandırıcılık
- Bilgisayar Yoluyla Sahtecilik
- Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı
- Diğer Suçlar (yasadışı yayınlar, pornografik yayınlar, hakaret ve sövme) şeklinde sıralanmaktadır.

Bilişim suçlarının sınıflandırılmasında bir diğer dikkate alınan kaynak, Interpol tarafından hazırlanan Interpol Bilgisayar Suçu El Kitabı esas alınmak üzere, BM'in hazırladığı BM Bilgisayar Suçunu Önleme El Kitabı ve Avustralya polis teşkilatının hazırladığı Temel Bilgisayar Suçunun Araştırılmasının Minimum Şartları kitapçığında, yukarıdaki ayrıma yasadışı yayınlar maddesi eklenerek bilişim suçlarının yediye ayrıldığı görülmektedir.[99]

Bilişim suçları Türk Ceza Kanunu'nda iki biçimde sınıflandırmaya tabi tutulmuştur:

* "*Doğrudan Bilişim Suçları (Gerçek Bilişim Suçları)*
** Dolayısıyla1 Bilişim Suçları (Bilişim Bağlantılı Suçlar)*

Türk Ceza Kanunu'nda da bu sistem kabul edilmiştir. Şöyle ki: Bilişim sisteminden amaç, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren manyetik sistemlerdir. Bilişim alanı ise, bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alanlardır. Ceza Yasası'nın 2. Kitap, 3. Kasım, 10. Bölümünde "Bilişim Alanında Suçları" başlığında 243. maddede "Bilişim Sistemine Girme"; 244. maddede "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", 245. Maddede "Banka veya Kredi Kartlarının Kötüye Kullanılması", düzenlenmiştir.

Dolayısıyla bilişim suçlan ise, klasik suçların bilişim sistemlerinden yararlanılarak işlenmesi olup, bu suçların nitelikli şekli olarak o suçla ilgili bölümlerde yer almaktadır. TCK'nin 112, 113, 125, 132, 133, 134, 135, 136, 138, 142/2-e, 158/1-f, 213-218, 226, 228 v. s. maddelerinde yazılı suçların bilişim sistemleri kullanılarak işlenmesi mümkündür."[100]

Bu bilgi ışığında bilişim sistemine karşı işlenen suçların kendi içinde;

---

[98] Dilek, **a.g.e.** , s. 14
[99] Aynı, s. 15.
[100] Yargıtay Ceza Genel Kurulu E. 2009/11-193, K. 2009/268, 17.11.2009, (Erişim) http://www.turkhukuksitesi.com/serh.php?did=6165 , 13 Aralık 2016.

- Bilişim sistemine karşı işlenen suçlar
- Sistemdeki program ve verilere karşı işlenen suçlar,
- Bilgisayar kullanıcılarına karşı işlenen suçlar şeklide üç gruba ayırma yoluna gidilebilmektedir.

Bilişim sisteminin kullanılmasıyla işlenen suçlar da;

- Ekonomik suçlar
- Sahtecilik suçları
- Ahlaki suçlar
- Şahsi haklara tecavüz suçları şeklinde dörde ayrılması yoluna gidilebilmektedir.[101]

İnternetin kullanımının yaygınlaşması ile özellikle bankacılık alanında çok çeşitli finans enstrümanları geliştirilmiştir. Bu enstrümanlar ile bireysel ya da kurumsal yatırımcıların kolayca işlem yapması ya da finansal araçları kullanması amaçlanmaktadır. Bu araçlar ile yapılan ve parasal işlemler ihtiva eden faaliyetler internet ortamında suç faillerinin bu ortamları da hedef almasına, bilişim suçlarının bu alanda giderek artmasına sebep olmaktadır. Tüm bunlara paralel olarak önleyici, tespit edici ve düzeltici tedbirlerin alınmasında da teknolojik ve hukuki altyapı oluşturulmaktadır. Bu çerçevede geleneksel anlamda işlenebilen suçların elektronik ortamlarda işlenmesine dönük düzenlemelerde genel olarak suçun nitelikli halinin yeniden tanımlanması yoluna gidilmektedir.[102]

1.8.1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme

Interpol Bilgisayar Suçları El Kitabına göre "*Yetkisiz erişim, bir bilgisayar sistemi veya ağına, yetkisiz bir şekilde erişimdir. Suçun hedefi, bir bilgisayar sistemi veya ağıdır.*"[103]

---

[101] Avşar ve Öngören, **a.g.e.** , s. 124.

[102] Turan, Metin ve Külcü, Özgür, "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi", ***Türk Kütüphaneciliği Dergisi***, 28(1), 2014, s. 20.

[103] Özkan, Tezcan, ***Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi***, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Ağustos 2006, s. 71.

Bilişim sistemlerine hukuka aykırı olarak erişme suçu mukayeseli hukukta birçok ülke ceza kanununda yaptırıma bağlanmıştır. Bu suç siber suçlar içinde en sık görülenidir.[104]

Erişim, sistemin bir kısmına ya da bütününe ve programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli değildir. Bu bir kişi tarafından bir bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, dolaylı olarak uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de olabilir.[105]

Yetkisiz erişim, illegal olarak bilişim sistemlerine erişilerek işlevlerinin kullanılması ve bu sistemlerde bulunan verilere yetkisiz kişiler tarafından ulaşılmasıdır. Saldırgan sistemin bir kısmına ya da bütününe, programlara veya içerdiği verilere ulaşma çabasındadır. İletişim metodu önemli değildir. Saldırgan bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de erişebilir.[106]

Erişim sistemin bir kısmına, bütününe, bilgisayar ağı veya içerdiği verilere, programlara; yine programlar, casus yazılımlar, virüsler, Trojan horses (Truva atları), worms (solucanlar) vb. ile ulaşma anlamındadır. Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler, erişimler, izinsiz kişi ya da kurum bilgisayarlarına, sistemlerine girmek suç olarak kabul edilmiştir.[107]

Erişim dışında, iletişim için kurulu iki bilgisayar sisteminin iletişiminin dinlenmesi de, aynı olarak değerlendirilmektedir. İletişimin dinlenmesi, sadece bilgisayarla iki kişinin görüşmesinin dinlenmesi değil, birbirine bilgi gönderen bilgisayarların ağ içinde gönderilen bilgilerin dinlenmesi de dinlenme olarak değerlendirilmektedir.

Yetkisiz dinleme, "*Bir bilgisayar veya ağ sistemine, sisteminden veya sistemi içinde yapılan iletişimin yetkisi olmaksızın teknik anlamda dinlenmesidir."* [108] Teknik anlamda dinleme, iletişimin içeriğinin izlenmesi, verilerin kapsamının ya

[104] Değirmenci, **a.g.e.** , s. 76.
[105] Dilek**, a.g.e.** , s. 24
[106] Tunçbilek, **a.g.e.** , s. 27
[107] Dilek, **a.g.e.** , s. 15
[108] Aynı, s. 25

direk olarak (bilgisayar sistemini kullanma ya da erişme yoluyla) ya da dolaylı olarak elektronik dinleme cihazlarının kullanımı yoluyla) elde edilmesi ile ilgilidir.[109]

Günümüzde daha modern bir yapıya ulasan iletişim kavramı artık bilgisayarlar üzerinden yapılmakta ve hatta kişilere ait önemli bilgiler bu ortamda iletilebilmektedir. Kişilerin, bankaların, hastanelerin, hatta güvenlik ve istihbarat birimlerinin tutmuş olduğu bilgiler bilgisayarlarda saklanmaktadır. Bu bilgilere ulaşmakta yine bilgisayar teknolojileri kullanılarak yapılmaktadır. İşte bu noktada gizlilik gerektiren bilgilere yetkilisi haricinde yapılan erişimler bu suç tipine girmektedir.[110]

Interpol Bilgisayar Suçları El Kitabında hesap ihlali, "*Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının dijital hesabını kötüye kullanma.*"' olarak açıklanmaktadır.[111] Bu tip suçlar, normalde klasik suç kapsamında bulunan hırsızlık, dolandırıcılık suçları gibidir. Hesap ihlali, yetkisiz erişim yaparak, başkasının hesabını rızası olmadan, sistemden yararlanmak şeklinde kullanma şeklindedir. Kişisel bilgilerin bulunduğu bu sistemlere ve bilgisayarlara yetkisiz erişmek, hukuk sisteminde bir suç olarak kabul edilmektedir.

Günümüzde, yasal izin olmadan telefon dinlemeleri ya da özel mülklerine girmek yasadışı olduğu gibi, kişiler ya da kurumlar arası iletişimin bilgisayarla dinlenmesi ya da bilgilerin izinsiz alınması da, kişinin özel mülkü ya da kişilerin kişiliklerine taciz olarak kabul edilmekte ve suç oluşturmaktadır.

Bir bilgisayar ya da sisteme yetkisiz erişim sağlayan kişi / gruplar, yalnızca eriştiği bilgileri incelemek ya da kopyalamakla kalmamakta, kendi çıkarları doğrultusunda bilgileri değiştirebilir, silebilir ya da kanuna aykırı şekilde kullanılması için diğer kişilere satabilmektedir.

1.8.2. Bilgisayar Sabotajı

Yetkisiz erişimin eyleme geçmiş hali olarak nitelendirilen Bilgisayar Sabotajı, sisteme yetkisiz erişimle birlikte, aynı zamanda eriştiği sistemin içerdiği bilgileri silme veya değiştirme olarak ifade edilmektedir. Bir bilgisayara veyahut sisteme

[109] Dilek, **a.g.e.** , s. 25
[110] Aynı, s. 15
[111] Aynı, s. 25

yetkisiz erişim sağlayanlar; sadece eriştiği bilgileri incelemekle ve kopyalamakla kalmamakta, bu bilgileri değiştirebilmekte, silebilmekte ya da bu bilgileri kanun dışı kullanmak isteyenlere satabilmektedirler.[112] Bilgisayar sabotajı, yetkisiz erişimin ikinci aşamasıdır. Bunun sebebi, yetkisiz erişimde bulunan bir kişinin yalnızca pasif bir harekette bulunup, özel hayatın gizliliğini ihlal ederken, bilgisayar sabotajının, yetkisiz erişimden sonra elde edilen bilgilerin silinmesi ve değiştirilmesini içermesidir.

Bilgisayar sabotajı, mantıksal ve fiziksel olarak iki şekilde yapılmaktadır. Interpol Bilgisayar Suçları El Kitabında mantıksal bilgisayar sabotajı, "*Bir bilgisayar ya da iletişim sisteminin fonksiyonlarını engelleme amacıyla bilgisayar verileri veya programlarının girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir."*[113] Bir bilgisayar ya da iletişim sisteminin fonksiyonlarının çalışmasını engellemek amacıyla verilerin yada programların Zaman Bombası (Logic-Time Bomb), Truva Atları (Trojan Horses), Virüsler, Solucanlar (Worms) gibi yazılımlar kullanarak değiştirilmesi, silinmesi, ele geçirilmesi ya da çalışmaz hale getirilmesidir.[114]

Interpol Bilgisayar Suçları El Kitabında fiziksel bilgisayar sabotajı, "*Bir bilgisayar ya da iletişim sistemine fonksiyonlarını engelleme amacıyla fiziksel yollarla zarar vermedir."*[115] Fiziki bilgisayar sabotajı, sistemin fiziki şiddet uygulanarak zarar görmesi ve bilgilerin silinmesidir. Bundaki amaç, maddi zarara neden olmak değil, sistemin çalışmasını engellemektir.

1.8.3. Bilgisayar Yoluyla Dolandırıcılık

Bilgisayar yoluyla dolandırıcılık, klasik dolandırıcılık suçunun bilgisayar ve bilişim sistemleri üzerinden yapılmasıdır. Bilişim sisteminde bulunan dataların ve programların değiştirilmesi, sahte datalar girilmesi, mevcut datalara zarar verilmesi gibi hileli hareketler sonunda haksız çıkar kazanmaya yönelik davranışlar, bilişim sistemlerinin kullanıldığı dolandırıcılık aktiviteleridir.

---

[112] Tunçbilek, a. g. e . , s. 28
[113] Dilek, **a.g.e.** , s. 26
[114] Aynı.
[115] Aynı.

Bilişim sistemleri kullanılarak kişiler; kendileri veya başkaları lehine hukuka aykırı yararlar sağlayabilirler. Bu; bilişim sistemlerinde yer alan programların veya verilerin değiştirilmesi, sahte veya değiştirilmiş veriler girilmesi, mevcut verilerde oynamalar yapılması, hileli bir takım hareketlerle bilişim sistemlerinin işleyişinin değiştirilmesi suretiyle mümkün olabilir. [116]

Interpol Bilgisayar Suçları El Kitabında bilgisayar yoluyla dolandırıcılık, "*Bilgisayar ve iletişim teknolojileri kullanarak verilerin alınması, girilmesi, değiştirilmesi, silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek veya mağdura zarar vermektir."* şeklinde ifade edilmektedir.[117]

Bilgisayar dolandırıcılığındaki amaç suçluya veya bir başkasına mali kazanç sağlamak ya da mağdura ciddi kayıplar verdirmektir. Bilgisayar dolandırıcılığı suçlarının, suç işleme teknikleri açısından klasik dolandırıcılık tekniklerinden farklılıkları vardır.[118]

Bilgisayar bağlantılı dolandırıcılık suçu, genelde dolandırıcılığın klasik ceza yasaları içinde bulunan tanımlarında olduğu gibi değerlendirilmektedir ve kovuşturması bu kapsamda yapılmaktadır. Bilgisayar bağlantılı dolandırıcılık suçunda suçlunun hedefi, kendisi ya da başkasına maddi kazanç sağlamak veya mağdura maddi kayıplar verdirmektir. Bilgisayar dolandırıcılığı suçları, suçlunun modern bilgisayar teknoloji ve ağ sistemlerinin faydalarını kullanmaları ile klasik dolandırıcılık suçlarından farklılık göstermektedir.

Bilgisayar yoluyla dolandırıcılık, banka / kredi kartlarının kopyalanması, hesaba izinsiz erişim, sahte e-posta gönderimi gibi yollarla kişileri dolandırarak kendilerinden para ya da mali bilgilerin alınması şeklinde işlenmektedir.

1.8.4. Bilgisayar Yoluyla Sahtecilik

Bilgisayar yoluyla sahtecilik, klasik ortamda yapılan sahtecilik suçunun, bilgisayarla yapılmasıdır. Bilişim sistemi kullanılarak yapılan sahtecilik ikiye ayrılmaktadır. Birincisi, klasik sahtecilik suçunun bir bilişim cihazı kullanılarak yapılmasıdır. Bir diğer ifade ile yapılan sahtecilik, sanal olarak değil, günlük hayatta

[116] Zakir ve Öngören, **a.g.e.** , s. 127
[117] Dilek, **a.g.e.** , s. 26
[118] Tunçbilek, **a.g.e.** , s. 28

genellikle matbu olarak hazırlanmasıdır. İkincisi, tamamen sanal ortamda yapılan sahtekârlıktır. Bu, hem sanal ortamda bulunan dataların değiştirilmesi hem de sahte unsurların hazırlanması olarak gerçekleşebilmektedir.

Bu durum hem sanal ortamda mevcut olan verilerin değiştirilmesi hem de sahtelerinin hazırlanması şeklinde gerçekleşebilir. Bilişim sistemlerinde, delil niteliği taşıyan bir takım bilgisayar çıktısı belge, veri ve programlarda yapılan sahtecilik eylemleri ceza kanunlarında bilişim sistemleri aracılığıyla işlenen sahtekarlık suçu olarak değerlendirilmektedir. Siber sahtekarlık, bilişim alanında para veya bir değeri elde etmek için bilgilerin değiştirilmesi veya bilerek yanlış bilgi kullanılmasıdır. Alman Ceza Kanunu'nun düzenlemesine göre, bilişim sistemine girilmek suretiyle hukukça hükmü haiz bir belge sahte olarak veya üzerinde değişiklik yapılmak suretiyle temin edilir ve temin edilen bu belge kullanılırsa bilişim sistemleri ile sahtekârlık suçu oluşur. [119]

Interpol Bilgisayar Suçları El Kitabında, bilgisayar yoluyla sahtecilik;

"*Kendisine veya başkasına yasa dışı ekonomik menfaat temin etmek veya mağdura zarar vermek maksadıyla; bilgisayar sistemlerinin kullanılarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır."*

şeklinde tanımlanmaktadır.[120]

1.8.5. Bilgisayar Yazılımının İzinsiz Kullanımı

5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nda, eser olarak kabul edilen bilgisayar yazılımlarının lisans haklarına aykırı olarak kullanılmasıdır. Kanunla korunmuş bir yazılımın izinsiz kullanımı, yazılımların; yasadışı yöntemlerle kopyalanmasını, çoğaltılmasını, satılmasını, dağıtılmasını ve kullanılmasını ifade eder. Bilgisayar yazılımları satın alınırken üzerinde gelen lisans sözleşmesine göre bir yazılımın bir adet kopyası ancak satın alan şahıs tarafından yapılacağı ve bu yazılımın başka bir kişi tarafından kopyalanmayacağı ve kiralanmayacağı belirtilmektedir. [121]

[119] Ergün, İsmail, ***Siber Suçların Cezalandırılması ve Türkiye'de Durum***, 2008, s. 38
[120] Dilek, a**. g. e.** , s. 28
[121] Aynı.

Interpol Bilgisayar Suçları El Kitabında, bilgisayar yazılımının izinsiz kullanımı "*Kanunla korunmuş yazılımların izinsiz olarak çoğaltılmasını, yasadışı yöntemlerle elde edilen bilgisayar yazılımlarının satısını, kopyalanmasını, dağıtımını ve kullanımını ifade eder."* şeklinde ifade edilmektedir. [122]

Kanunla korunmuş bir yazılımın izinsiz kullanımı altı şekilde gerçekleşmektedir. Bunlar;

- Lisansız Sözleşme İhlali
- Lisans Sözleşmesine Aykırı Kullanma
- Lisans Haklarına Aykırı Çoğaltma
- Lisans Haklarına Aykırı Kiralama
- Taklitçilik
- İzinsiz İthalat şeklinde sıralanabilmektedir.

1.8.6. Yasadışı Yayınlar

Yasadışı yayınlar, illegal materyaller bilişim sistemleri ile yayınlanması ve dağıtılmasıdır. "*Yasadışı olarak kabul edilen unsurların bilgisayar sistemleri, ağları, Internet aracılığıyla yayınlanması ve dağıtılması olarak ifade edilir. Kanunun yasaklamış olduğu bu materyaller; Web siteleri (sayfaları), BBS'ler (Bulletin Board Services-Duyuru Tahtası Hizmetleri), elektronik postalar, haber grupları, forumlar, iletişim sağlayan her türlü araç, optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilir.*" [123]

Interpol Bilgisayar Suçları El Kitabında, yasadışı yayınlar "*Yasadışı yayınların saklanmasında ve dağıtılmasında bilgisayar sistem ve ağlarının kullanılmasıdır.*" olarak ifade edilmektedir. [124]

Yasadışı yayınları üç gruba ayrılmaktadır:

- Ülkenin bölünmez bütünlüğü karşıtı hazırlanmış, terörist faaliyetler lehine hazırlanmış terör içerikli internet sayfalarıdır. Özellikle terör örgütlerinin hazırladığı

[122] Dilek, **a. g. e.** , s. 28
[123] Aynı, s. 19
[124] Aynı, s. 29

bu sayfalarda, kendi illegal ideoloji ve fikirlerini internet ortamında kolay bir şekilde yayınlayabilmektedir. Bu tür sitelerdeki amaç, anayasa ve çeşitli yasalarla yasak konulmuş ve hakkında cezai işlem uygulanması hükmedilen içerikleri, anonim olan internet üzerinde paylaşarak, kendilerine destekleyici taraflar toplamak ve hatta üye kazandırmayı, kendi illegal düşüncelerini internet ortamında rahatça yaymaktır.

- İkinci grupta, halkın sahip olduğu manevi değer ve genel ahlaka aykırı çeşitli pornografik internet sayfalarıdır. Yurtdışında genelde yasaklar, çocuk pornografisi üzerine yoğunlaşmışken, Türkiye'de çocuk ve büyük pornografisi olarak bir ayrım yapılmamış, bütün pornografik siteler yasaklanmıştır.

- Üçüncü olarak, bir kişi aleyhine yapılan hakaret ve sövme suçudur. Bu suç, internet üzerinden başkalarının izni olmadan onların adına e-postalar göndererek, kişi ya da kurumların itibarını zedelemeyi amaçlamaktadır. Bir diğer yol da, yine kişi ya da kurumların isimleri ve lakapları internet üzerinden satın alarak, kişi aleyhine yayınlarda bulunmaktır. Bu tür olaylar sıklıkla yaşanmaktadır. Kişi aleyhine hakaret ve Türkiye'de sövme suçu üzerine ne yazık ki etkin bir önlem alınmamıştır. Bu tür suçla karşılaşılması durumunda mağdurların bu durumu kendi başlarına halletmeye çalıştıkları, yargı mercilerine başvurunun az olduğu görülmektedir. Ancak, bu suçun internette işlenme potansiyeli yüksek bir suçtur.

1.8.7. Terörist Faaliyetler

Terörist faaliyetler, bilişim sistemleri üzerinde, elektronik araç, bilgisayar programı ya da diğer elektronik iletişim sistemlerinin kullanılmasıyla, milli değer ve çıkarların tahribini amaçlayan, bireysel ve politik şekilde motive olmuş, amaçlı etkinliklerdir.

Sanal / siber terör, bilgi sistemleri kapsamında elektronik araçların, bilgisayar programlarının veya diğer elektronik komünikasyon araçlarının kullanılmasıyla milli denge ve çıkarların tahrip edilmesini amaçlayan, kişisel veya politik olarak motive olmuş amaçlı eylem ve etkinlikler, enformasyona, bilgisayar programlarına ve doğrudan savaşın içinde olmayan hedeflerin verilerine karşı önceden planlanmış, politik nedenlerden kaynaklanan bir saldırı, belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı

bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılması, siber / sanal terör olarak tanımlanmaktadır. [125]

Stanford Üniversitesi, Uluslararası Güvenlik ve İşbirliği Merkezi tarafından siber suçlarla ilgili olarak yapılan çalışmada da siber terörizm kavramına açıklık getirilmeye çalışıldığı için, Stanford Taslağı olarak bilinen belgede siber terörizm şöyle tanımlanmaktadır:[126]

"Hukuken yetkili kılınmış görevlilerinin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü ya da yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara veya mallara karşı önemli zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması veya yapılacağı tehdididir."

Terör örgütleri internet ortamında propaganda ve eğitim, haberleşme, bilgi toplama ve sanal saldırı faaliyetleri gerçekleştirmektedir. Kısaca, terör eylemlerinin internet üzerinden yürütülmesi işlemidir. Siber terörizmi diğer internet yoluyla islenen suçlardan ayıran başlıca fark, suçun mağdurunun devlet olması ya da devlet dışındaki bir yapı olduğunda bile bu mağdurun siyasi bir sebeple mağdur durumunda kalmasıdır. Siber terörizmi tanımlarken temelde terör olgusunun nitelikleri değil ancak terör olgusunun nasıl hayata geçirildiği önem taşımaktadır.[127]

Türkiye'de, internet üzerinden yapılan terörist eylemler, kullanıcıların tespitinin zor olması için internet kafeler üzerinden kendilerine ait olmayan bilgisayarlardan yapılmaktadır. Aynı olarak, hakaret ve şantaj içerikli e-postalar ve sahte ihbarlar bu kafelerden yapılmakta, oturum ve kullanıcı tespitinin yapılmadığı ve kamera gibi güvenlik sistemleri olmayan denetimsiz yerler yapılan bu suçlarda, failin tespiti zorlaşmaktadır.

Günümüzde bilgisayarların kullanım alanı son derece yaygındır. Uçuş denetim sistemlerinden, şehir içi trafik sistemine, borsadan, askeri ve emniyet güvenlik sistemlerine, eğitim kurumlarından, ulusal yargı ağı projesi (UYAP), MERNİS, TAKSİS, PRO2000, e- Devlet Kapısı Projesi gibi hayatın her alanını kapsayan çok büyük alanlara varıncaya kadar her yerde bilgisayarlar kullanılmaktadır. Bu tür bilgisayar ağları, insanlara günlük hayatlarını kolaylaştırmak için internete de bağlanmıştır. Bu iletişim kolaylığı kuşkusuz ki, başta terörist eylemciler olmak üzere

[125] Avşar ve Öngören, **a.g.e.** , s. 129
[126] Özcan, Mehmet, ***Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk***, Bilgi Üniversitesi Yayınları, İstanbul, 2002, s.309
[127] Özkan**, a.g.e.** , s. 82 ve 87.

pek çok kötü niyetli girişimcilerin de ilgisini çekmekte; onlara da "kolaylıklar" sağlamaktadır. Uçakların, uçuş yollarını (rotalarını) belirleyen, iniş ve kalkışlarını düzenleyen sisteme ulaşabilen bir terörist, sistemdeki bilgileri değiştirerek tüm uçuş planlarını alt üst edebilir ve kazalara neden olabilir. Şehir içi trafik bilgisayarına ulaşan bir terörist trafiği alt üst edebilir. Eğer bir terörist borsanın bilgisayarına ulaşırsa neler yapabileceği açıktır.[128] Gerek terörist eylemi gerçekleştirmek için, gerekse terörist eylem planını yapabilmek için internet kullanılmakta, internetin terör suçlarına aracılık etmesi söz konusu olmaktadır.

1.8.8. Çocuk Pornografisi

İnternet başta olmak üzere bilişim teknolojilerinde, genel ahlaka aykırı içerikli görsel ve videoların üretim ve dağıtımı günümüzde daha kolay ve ucuzdur. Bu nedenle, internet, pornografik unsurların hazırlanması ve dağıtılmasına katkı sağlamaktadır. Bu olumsuz gelişme, toplumun genel ahlak kurallarına aykırı açık bir tehdittir.

Çocuk istismarı, fiziksel ya da psikolojik olarak bir çocuğa bir yetişkin tarafından kötü davranılmasıdır. İstismar fiziksel, cinsel ve sözel yolla ortaya çıkabilmektedir. Çocuk istismarı içeriği çok geniş bir kavram olmakla birlikte tüm dünya ülkelerinin mücadelede hemfikir olduğu bir konudur.[129]

İnterpol Çocuklara Karşı İşlenen Suçlar Uzman Grubu tarafından yapılan tanımlamaya göre ise; *"Çocuk pornografisi; çocuğun kötüye kullanımı veya cinsel istismarı sonucu oluşmaktadır. Çocuğun cinsel davranışları ve uzuvlarına odaklanmış yazılı ve sesli materyallerin kullanımı da dâhil, çocuğun cinsel istismara yöneltilmesi veya betimlemesi anlamındadır."* şeklinde tanımlanmaktadır.[130]

İnternetin yoğun olarak kullanılmaya başlamasıyla birlikte çocuk istismarı konusunda ön plana çıkan en önemli sorunlar; akran istismarı, cinsel istismar ve

---

[128] Avşar ve Öngören, **a.g.e.** , s. 130

[129] Güler, Niyazi – Bayzan, Şahin ve Güneş, Abdülhamit, ***İnternette Çocuklara Yönelik Riskler ve Ailelerin Bilinçlendirme Faaliyetlerindeki Rolü***, (Erişim) http://s3.amazonaws.com/academia.edu.documents/45841666/icits2016_makale_tam_metin_24NISAN.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1481654665&Signature=7SpotRR40CmlcqnL15EIy%2BMkcOA%3D&response-content-disposition=inline%3B%20filename%3DInternette_Cocuklara_Yonelik_Riskler_ve.pdf, 12 Aralık 2016.

[130] Dokurer, Semih, ***Bilişim Suçları Laboratuvarlarında Çocuk Pornografisi İncelemeleri***, s. 3, (Erişim) http://www.dokurer.net/files/documents/cocukporncelemeleri.pdf , 12 Aralık 2016.

çocuk pornografisidir. Akran istismarı, birini isteyerek, bilinçli bir şekilde incitmek, tehdit etmek ya da korkutmak amaçlı bir kişinin ya da gurubun bir bireye yönelik sürekli uyguladığı, zarar verici ve incitici saldırgan davranış olarak adlandırılır. İnternet ortamında da çocuğun hoşlanmayacağı bir İnternet profili oluşturarak İnternet üzerinden istismar etmesi veya İnternet ortamında pek çok arkadaşın bulunduğu bir platformda bir arada bulunmak suretiyle paylaştığı bir etkinlikte onun yer almasını engelleyerek veyahut hoşa gitmeyen, sözler, fotoğraflar yayınlayarak akran istismarı ortaya çıkabilmektedir. Avrupa'da yapılan bir araştırmanın sonuçlarına göre, İnternette akran istismarına uğrayan çocukların % 80'i yapılan istismarı herhangi biriyle paylaşmakta, % 20'si ise paylaşmamaktadır. Paylaşmama oranının Türkiye'de daha yüksek olduğu tahmin edilmekle birlikte, böyle bir çalışma yapılmadığı için bilinmemektedir.[131]

Avrupa Çevrimiçi Çocuklar Projesi (EU Kids Online, 2010) kapsamında Avrupa'nın 25 ülkesinde 2010 yılında, İnternet kullanan 9-16 yaş çocuklar arasından seçilen 25,142 çocuk ve ebeveynlerinden her birisi ile yüz yüze görüşmeler yapılmıştır. İncelenen çevrimiçi riskler şunlardır: pornografi, zorbalık, cinsel içerikli mesaj almak, daha önce tanımadığı kişilerle iletişime geçmek, çevrimiçi görüştüğü kişilerle çevrimdışı görüşmek, kullanıcı tarafından oluşturulmuş potansiyel zararlı içerik ve kişisel bilgi istismarıdır. Projeye göre, her 12 çocuktan 1'i çevrimiçi görüştüğü kişi ile çevrimdışı iletişimde bulunmuştur.[132]

Çocuk pornografisi, genel olarak yasal yaş sınırının altındaki çocukların cinsel istismarını bulunduran görsel ve videolardan oluşan, ulusal ve uluslararası olarak yasaklanmış pornografik türdür. Bu tür filmlerin çekilmesi, indirilmesi, dağıtılması, paylaşması suç teşkil etmektedir.

TCK'nin 103. maddesinde[133]; *çocuğu cinsel yönden istismar eden kişi, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır. Cinsel istismar deyiminden;*

- *On beş yaşını tamamlamamış veya tamamlamış olmakla birlikte fiilin hukukî anlam ve sonuçlarını algılama yeteneği gelişmemiş olan çocuklara karşı gerçekleştirilen her türlü cinsel davranış,*

[131] Alikaşifoğlu, Müjgân, ***İnternet Kullanımı ve Çocuk ve Ergen Sağlığı*** Türk Pediatri Kurumu TBMM Sunusu, 2012, (Erişim) https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/Turk_Pediatri_Kurumu_.internet%20Kullanimi%20ve%20cocuk-Ergen-sagligi.pdf , 12 Aralık 2016.

[132] Güler, Bayzan ve Güneş, **a.g.e.** , s.8.

[133] 5237 Sayılı Ceza Kanunu Madde 103, ***Çocukların Cinsel İstismarı***, (Erişim) http://www.turkhukuksitesi.com/mevzuat.php?mid=3934, 12 Aralık 2016.

- *Diğer çocuklara karşı sadece cebir, tehdit, hile veya iradeyi etkileyen başka bir nedene dayalı olarak gerçekleştirilen cinsel davranışlar, şeklinde belirtilerek 15 yaşından küçük çocuklar cinsel istismara karşı koruma altına alınmıştır.*

15 yaşını doldurmuş olan çocuklara karşı *"Reşit olmayanla cinsel ilişki"* başlıklı 104. maddede *"Cebir, tehdit ve hile olmaksızın, on beş yaşını bitirmiş olan çocukla cinsel ilişkide bulunan kişi, şikâyet üzerine, altı aydan iki yıla kadar hapis cezası ile cezalandırılır*."[134] İfadesiyle takibi şikâyete bağlı suç olarak nitelendirilmiştir.

Ayrıca 226. Maddede[135];

- *Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,*
- *Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,*
- *Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,*
- *Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,*
- *Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,*
- *Bu ürünlerin reklamını yapan, kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılmaktadır.*

İfadesiyle çocuk pornografisi görüntülerini ne şekilde olursa olsun kullananların cezalandırılacağı belirtilmektedir.

1.8.9. Kartlı Ödeme Sistemlerinde Sahtecilik ve Dolandırıcılık Teknikleri

Türkiye'de en çok işlenen bilişim suçu, kredi kartı ve banka kartları sahteciliği ve dolandırıcılığıdır. Kredi kartı ve banka kartı dolandırıcılığı, çeşitli interaktif yollarla yapılabileceği gibi bilgisayar yoluyla klasik dolandırıcılık yöntemleri kullanılarak da yapılmaktadır.

[134] 5237 Sayılı Ceza Kanunu Madde 104, ***Reşit Olmayanla Cinsel İlişki***, (Erişim) http://www.ceza-bb.adalet.gov.tr/mevzuat/5237.htm , 12 Aralık 2016.

[135] 5237 Sayılı Ceza Kanunu Madde 226, ***Müstehcenlik***, (Erişim) http://www.turkhukuksitesi.com/mevzuat.php?mid=5174 , 12 Aralık 2016.

Bu suça bakıldığında, kişiler adına çıkarılmış sahte kimlik ve belgelerle başkalarının hesaplarından para çekilmesi, banka ve kredi kuruluşlarından sahte evrak kullanılarak kredi çekilmesi gibi yollarla işlendiği görülmektedir.

Dolandırıcılar, sahte alışveriş, bahis siteleri ya da cep telefonlarını arama ya da mesaj göndermek aracılığıyla kredi kartı bilgilerini alarak banka hesaplarına ya da kredi kartlarına kolayca ulaşabilir ve kart sahiplerini mağdur edebilirler. Bu dolandırıcılık türü, bazı klasik dolandırıcılık unsurlarını da içerdiğinden, diğer bilişim suçlarına göre farklılık göstermektedir.

1.8.10. Sahte Kişilik Oluşturma ve Kişilik Taklidi

Hileyle kendisi ya da başkasına yarar sağlamak ya da zarar vermek için hayali bir kişilik oluşturmak ya da başka birinin bilgilerini kullanarak o kişinin kişiliğini taklit etmektir.

Bilgisayar sistemlerine yetkisiz erişim sağlamak ya da kullanma hakkı kazanmak amacıyla gerçek kişilerin taklidi ya da hayali kişiler oluşturmak etkili metotlardan biri olarak bilinir. Bu metotta, gerçek kişilere ait bilgileri kullanarak o kişinin arkasına saklanılmakta ve o kişinin muhtemel bir suç durumunda sanık durumuna düşmesine neden olunmaktadır. Ayrıca kredi kartı numara oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgilerin hayali kişiler oluşturulmasında kullanılmasıyla menfaat sağlanmakta ve zarar verilmektedir.[136]

1.9. İNTERNET SUÇLARININ KAMUSALLIĞI

Kanun koyucunun, bilişim alanında suçları topluma karşı suçlar arasında düzenlemesinin sebebi muhtemelen "sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, …" sahte banka kartıyla yarar sağlamanın sahtekârlık suçunu oluşturduğunun düşünülmesi olabilir. Böyle bir yorum yanlıştır. Çünkü Kanunun topluma karşı işlenen suçların dördüncü bölümünü oluşturan kamu güvenine karşı suçlar bölümünde kamunun, doğru olduğuna inanılan paralar, kıymetli kâğıtlar, damgalar, belgeler üzerindeki sahtekârlıklar cezalandırılmaktadır. Kamu bu

[136] Dilek, **a. g. e.** , s. 31

belgelerin doğruluğuna inandığı için sahtekârlığın yapılmasıyla suç meydana gelir. Ancak özel evrakta sahtekârlığın meydana gelmesi için sahte özel evrakın kullanılması da gerekmektedir. Kamu güvenine karşı suçlarda korunan değer kamunun para, belge ve evrakın doğru ve sahihliğine olan güvendir. Dolayısıyla mağdur da toplumdur.[137]

Kamusal alanı genişleterek toplumsal katılımı ve söylem imkânlarını zenginleştiren İnternet'in sadece tanı ortaya koymak veya tartışmaktan ibaret olmayan, kimi yerde baskı oluşturmak ve çözüm üretmek gibi boyutlar da içeren demokrasiye ciddi bir katkıda bulunduğu açıktır. Kamusal alanla siyasal alan arasında "birebir" bir ilişkinin bulunmadığını kamusal alanın siyasal alana tercüme edilişinde değişik dinamiklerin yer aldığını da unutmamak gerekir. İnternet'in uluslararası niteliğine karşın sorunların çözümünde başvurulan mekanizmaların hâlâ ulusal düzeyde işlediklerini göz önüne alarak, İnterneti derin bir coşku ve sarhoşluk kaynağı olarak değil, gelecek adına yeni bir umut olarak karşılamak gerekir. Ayrıca İnternet'in demokratik sürece yaptığı katkının sağlığı için de söz konusu olanağın toplumun en azından çoğunluğu tarafından kullanılabilir bir noktada olması gerekir. Zira bu noktada bilginin yoksulları ile varsılları arasında mevcut olan uçurum kısa vadede kapanacak gibi gözükmüyor. Tersine, İnternet orta vadede bu uçurumu derinleştireceğe benziyor. İnternet'in gerçek anlamda bilgi ve enformasyonun demokratikleşmesinde ciddi bir adım teşkil edebilmesi için, İnternet'in sağladığı imkânların kullanımı için gerekli asgari donanımın yeterince ucuzlayarak herkesçe edinilebilir olmasını beklemek gerekiyor.[138]

1.10. İŞLENME ŞEKİLLERİ

Bilişim suçlarını, klasik suçlardan ayıran en önemli özellik, bilişim suçlarının işlenme şekillerinin farklılığıdır. Bilişim suçlarında, diğer suçlara göre daha çok ve yeni işlenme şekilleri uygulanmaktadır. Klasik suçlarda, suçun maddi unsurundan olan eylemler, faillerin fiziksel hareketlerinden oluşurken, bilişim suçlarında failin bilgisayarın faresi ya da klavyesine dokunması dışında başka bir fiziksel hareketi bulunmamaktadır. Bununla birlikte, failin getireceği zararlar daha fazla olmaktadır.

[137] Soyaslan, Doğan, Ceza Hukuku Özel Hükümler, Yetkin Yayınları, Ankara, 2014, s.689.
[138] http://bilisimci2007.blogcu.com/kamusal-alan-ve-kamusal-alan-olarak-internet/2652009

Bilişim suçları ayrıca, kısa bir süre içinde ve az ipucu bırakacak şekilde çok büyük zararlara sebep olabilmektedir. İşlenen suçların ve faillerin tespiti de klasik suçlara göre daha zor olmaktadır. Bilişim teknolojisindeki gelişmeler, bilişim suçlarının işlenme şekillerini de gün geçtikçe arttırmaktadır.

1.10.1. Virüsler

Bilgisayar dünyasındaki olumsuz gelişmelerde ilk akla gelen durum bilgisayar virüsleridir. Bilgisayar virüsleri özel olarak yazılmış küçük birer programdır. Yani, herhangi bir iş, oyun, müzik programı gibi bilgisayar programcıları tarafından yazılmış birer programdır. Farklı olan yönleri diğer programlara kendilerini bulaştırabilmeleridir ve bu şekilde çoğalıp yayılırlar. [139]

Virüsleri aşağıda tanıtılacak olan solucan, truva atlarından ayıran en önemli özellik kendi kendilerine çoğalabilmeleridir. [140]

Virüsler kendi başlarına çalışabilen, kopyalayabilen zararlı programlardır. Virüsler, bilişim sistemlerini kullanılamayacak hale getirir ve kolaylıkla tespit edilememektedir. Virüslerin en önemli özellikleri, kolay şekilde kopyalanabilir olmasıdır. Bu kopyalama işlemi, virüs bulaşması olarak adlandırılmaktadır. Virüsler, disket, cd, e-posta gibi yollarla bilgisayarlara bulaşırlar. Günümüzde virüsler en çok e-posta yoluyla gönderilmektedir.

1.10.2. Truva Atları

Truva atları ismini herkes tarafından bilinen tarihteki truva atından almaktadır ve aynı plan ve yöntem üzerinde çalışırlar. Bir truva atı (trojan horse), legal bir program içindeki illegal talimatlar ya da bir işi yapıyormuş gibi görünüp kullanıcısından habersiz işlemler yapan zararlı bir programdır. [141]

Genel olarak bir truva atı iki bölümden oluşur, istemci ve sunucu bölümü. Sunucu tarafında hedef seçilen kişinin bilgisayarında, istemci tarafı ise diğer bilgisayarda yani uzaktan illegal olarak erişen ve yöneten kişinin bilgisayarında

---

[139] Bahtiyar, Ziya, ***Virüsler ve Güvenlik***, Pusula Yayınları, İstanbul, 2003, s.2
[140] Yazıcıoğlu, **a.g.e.** , s. 164
[141] Yılmaz, Davut, ***Hacking Bilişim Korsanlığı ve Korunma Yöntemleri***, Hayat Yayınları, 2005, s.380.

çalışır. Truva atları sıklıkla bilişim sistemlerine yönelik yapılan saldırılarda kullanılsa da bazen legal olarak bilişim sistemlerinden sorumlu teknik personel tarafından da kullanılabilmektedir. [142]

Truva atı, sistem sahibinin haberi ve isteği olmadan, gizli ve genelde kötü amaçlı faaliyette bulunan bir programdır. Truva atı, virüs olarak sınıflandırılmaz ve kendi kendini çoğaltmaz, yalnızca sabit diskteki bilgilere zarar verir. Truva atı kendisini zararsız bir program gibi gösterir ve ilk çalıştığında zararsız bir program gibi durmaktadır. Çalıştığında bilgisayardaki verileri silebilir ya da bozabilir. Kısaca, truva atı yazılımı, kurulduğu bilgisayarın yazılım açıklarından faydalanarak bütün sisteme egemen olmakta ve failin tüm komutlarını uygulamaktadır. Truva atları, genelde kullanıcılar tarafından indirilen müzik, dosya, programlar ya da uygulamalarla bulaşmaktadır. Truva atları, diğer zararlı yazılımlar gibi kendi kendilerine işlem yapamamaktadır. Truva atlarının zarar verme kapasitesi kullanıcının davranışlarına bağlıdır. Truva atlarının kendilerini dağıtsalar da, kullanıcının etkilenmesi için truva atı sahibi programı çalıştırması gerekmektedir.[143]

Bu tür yazılımlara verilebilecek en güzel örnek 1990 yılında CIA dâhil pek çok istihbarat örgütü tarafından kullanılan *Promis* örnek verilebilir. [144] Truva atı usulüne örnek olarak, ABD ve İsrail'in, ana belleğinde "promis" adlı truva atı yazılımını içeren bilişim sistemlerini Ürdün'e satması verilebilir. Böylelikle Ürdün'ün Filistin hakkında ellerinde bulundurdukları dosyalar, truva atı yazılımının işletilmesi yoluyla ABD ve İsrail'in eline geçmiştir. [145]

1.10.3. Ağ Solucanları

Ağ solucanları, kullanıcının etkisi olmadan kendi kendine çalışabilen ve aynen kendisi gibi bir kopyasını, veri iletim ağına bağlantısı olan diğer bilişim sistemine kopyalayabilen yazılımlardır. [146]

Ağ solucanları, kullanıcının bilgisi dışında ve komut olmadan çalışabilen ve bir kopyasını iletişim araçlarını kullanarak diğer sisteme yayarak çoğalan yazılımlardır.

---

[142] Yılmaz, Davut, **a.g.e.** , s. 380-381.
[143] Akıncı, Alıç ve Er, **a.g.e.** , s. 183.
[144] Gözüşirin, **a.g.e.** , s. 35
[145] Odabaşı, Arda, "*Bilgi Toplumu mu, Gözetim Toplumu mu?"*, ***Bilim ve Ütopya***, İstanbul, 1999, s.29-30.
[146] Dülger, 2004, **a.g.e.** , s. 73

Sistem içine yüklenen ağ solucanı, virüs gibi sisteme zarar verebilir, aynı zamanda Truva atı bırakarak da sisteme zarar verebilir. Solucanların ana çalışma ilkesi, kendilerini kopyalayarak çoğalmadır. Bu sebeple kısa süre içinde çok sayıda sisteme yayılır, ağ ve bilgisayarları kullanılamaz hale getirir ve çökertirler.[147]

Ağ solucanları genellikle bilişim virüsleri ile karıştırılmaktadır. Ancak ağ solucanları, sisteme zarar vermeden de sistem içine girerek sistemde hareket edebilmektedirler. Ağ solucanları, genellikle iyi oluşturulmamış güvenlik duvarını aşarak bilişim sistemine girmekte ve eylemlerine başlamaktadırlar. Ağ solucanları bilişim sisteminin güvenlik duvarını astıktan sonra sistemin içinde serbestçe dolaşarak ya sistemde bulunan yazılımlara zarar vermekte ya da üzerinde taşımış olduğu bir Truva atı yazılımını sisteme bırakmaktadırlar. Sistem içindeki bu eylemleri oluşturan ağ solucanları genellikle hareketlerine ilişkin izleri de silmekte ve bulunmalarını imkânsız hale getirmektedirler. [148]

Solucanlar, yayılmalarının hızlı ve kolay olması sebebiyle suç dünyasında kullanılmaktadır. Yüzlerce bilgisayar ve kullanıcısı olan büyük şirket ve finans kuruluşlarına yapılan yasa dışı siber saldırılarda solucan kullanımı tercih edilmektedir. Hedef alanının geniş olduğu bu saldırılarda, takipte zor olmaktadır.

1.10.4. Mantık Bombaları

Mantık bombaları, bilişim sistemi ya da ağlarda, önceden belirlenmiş durumların oluşması durumunda, sistemde zarar verici sonuçlar oluşturan programlardır. Mantık bombaları aslında bir çeşit Truva Atı yazılımı çeşidi sayılabilirler. Bu programlar daha önceden tanımlanmış belli durumların oluşması halinde çalışmaya başlarlar, aksi takdirde çalışmazlar. [149]

Mantık bombası, Truva atı yazılımının bir türüdür. Bilişim sistemini şaşırtmak, bozmak veya felç etmek için programlanmaktadır ve bunu gerçekleştirebilmek için, bilgisayara ya mantık dışı ya da yapılan işlemin aksine sürekli bilgi göndermektedir.[150] Bu konuda verilebilecek en güzel örnek Türkiye'de 1999 yılında görülen ve oldukça zarar veren Çernobil Virüsüdür. Programın yazılımı gereği,

[147] Yılmaz, Davut, **a.g.e.** , s. 288.
[148] Değirmenci, **a.g.e.** , s.87
[149] Kurt, 2005a, s. 73
[150] Yazıcıoğlu, **a.g.e.** , s.157

Çernobil virüsü girdiği bilgisayarın belleğinde beklemekte ve her ayın 26'sında zarar verici eylemlerine başlamaktadır. [151]

1.10.5. Bukalemunlar

Truva atına benzeyen bukalemun tekniği, diğer normal ve güvenilir programlar gibi davranır ve gerçek hile ve aldatmalar içermektedir. Uygun olarak programlandıklarında, kanunla belirlenmiş yazılımların her hareketini taklit edebilir. Adını girdiği sistemde gizlenmedeki başarısından alan bukalemunlar, kullanıcı şifreleri için giriş kısımlarını taklit edecek şekilde programlanarak, özellikle çok kullanıcılı sistemlerde, kullanıcı adı ve şifreleri bir dosyaya kaydeder ve sistemin geçici bir bakım için kapanacağı ikazını verir. Daha sonra fail, bu dosyaya girerek kişilere ait bilgileri alır.[152]

1.10.6. Salam Tekniği

Salam tekniği genellikle bankacılık sektöründe gerçekleşen bir bilişim suçu yöntemidir. Bu yöntemle fail, kişilerin banka hesaplarındaki meblağların küsuratlarını ya da virgüllü tutarlarda virgülden sonraki bir ya da iki rakamlı tutarları kendi hesaplarına aktarmaktadır. Bu şekilde banka çalışanları ya da hesap sahipleri hesaplarda meydana gelen küçük kayıpları fark edememektedir. Bu teknikte genellikle Truva atının çeşitleri ya da benzer özelliğe sahip yazılımlar kullanılmaktadır.[153]

1.10.7. Tavşanlar

Tavşanlar, virüs ya da solucanlara göre daha az yaygındır, ancak tavşanlar da kendi kendilerine çoğalma niteliği taşırlar. Tavşanlar, mantık bombası gibi davranıp sistemde kendini kopyalar ve sisteme gereksiz komutlar verir ve sistemi yavaşlatır. Hızlı bir çoğalma özelliği taşıyan tavşanlar, içinde bulunduğu sistemin içindeki işlemciye, devamlı anlamsız komut verir ve işlemcinin sistem içindeki işleyişini engeller ve sistemin yavaş çalışmasına, sonunda sistemin çökmesine sebep

[151] Dülger, 2004, **a.g.e.** , s. 75
[152] Yılmaz, Davut, **a.g.e.** , s. 310.
[153] Dülger, **a.g.e.** , s. 75.

olmaktadır. Tavşanların uygulamaya başlamaları için dışarıdan bir etkiye maruz kalmasına ihtiyaç yoktur. Tavşanlar, virüslerden farklı olarak, veri kütüklerinin sonuna eklenir, asalak özellikleri yoktur ve kendi kendilerine yetebilirler.[154]

1.10.8. Gizli Kapılar

Gizli kapılar ya da hile kapıları; işletim sisteminde veya çok işlevli ve kullanıcılı sistemler hazırlayan programcıların, ileride ortaya çıkabilecek durumlara göre sistem üzerinde gerekli değişiklikleri yapabilmeyi ya da sistem üzerine yeni şifreler girebilmek amacıyla sistemlere bıraktıkları boşluklardır. [155] Gizli kapılar, bir sistemde kimlik doğrulama sistemini devre dışı bırakarak, başka bir yöntem ile yasadışı olarak sisteme girme ve datalara erişim yöntemidir.

Bu kapılar yasal olmasına rağmen, hata ya da sonra kullanılmak için kapatılamaz ya da açık bırakılırlar. Bu durumda, kötü niyetli kişiler, gizli kapılardan yararlanarak illegal aktivitelerde bulunabilir.

1.10.9. Süper Darbe

Süper darbe ismi "*super zap"* kelimesinden gelmekte ve özellikle IBM merkezlerinde sistem programı olarak kullanılan oldukça yararlı bir "*master"* programını ifade etmektedir. [156]

Bu programlar genelde, bilgisayarların hırsızlığa karşı mevcut güvenlik programlarının sürekli olarak denetlenmesi ya da işletme veya programların kendilerinden kaynaklanan sebeplerden dolayı çalışamaz hale gelen bilgisayar sistemlerinin yeniden etkin hale getirilmesi için kullanılırlar. [157]

1.10.10. Veri Aldatmacası

Veri aldatmacası ile kastedilen husus, verinin bilgisayara ya da belleğe kaydı sırasında verinin değiştirilmesi, bilgisayara yanlış veri girilmesi veya bazı verilerin

[154] Yenidünya ve Değirmenci, **a.g.e.** , s. 87.
[155] Yazıcıoğlu, **a.g.e.** , s. 156
[156] Yazıcıoğlu, **a.g.e.** , s. 156
[157] Kurt, 2005a, s. 66

kasten bırakılmasıdır. Bilişim suçları içerisinde işlendikten sonra meydana çıkarılmasının çok zor olması nedeniyle en çok tercih edilen suç yöntemidir. [158]

1.10.11. Bilişim Korsanlığı (Hacking)

Bilişim korsanlığı, sisteme izinsiz girilerek, sistem işleyişini denetleme ve sistemdeki datalardan bilgi sahibi olma ve sistem işleyişini durdurma ve / ya da yönlendirme işlemidir. Bu izinsiz giriş, genellikle işletim yazılım yapanların, gerektiği durumda sistemin korunması için bıraktıkları arka kapıları bularak buradan girme yoluyla gerçekleşir.

Kelime itibarıyla *"hack*": "kendisine ulaşım imkânı olmayan özelliklere kullanıcının, uyarlanmış olan bir alet ya da program yardımıyla girme imkânının verilmesi" olarak tanımlanabilir. [159] Bilişim korsanı olan kullanıcıları, sahip olduğu korsanlık bilgilerini kullanarak kısa sürede maddi kazanç elde etmeye çalışmakta ve para kazanmak için ilk olarak kendi isimlerini duyurma olduğuna inanmaktadır.

Bilişim suçları, özellikle internetin gelişimi ve yayılmasından sonra, veri iletim ağları ile bilişim sistemlerine girme konusunda artış olduğu söylenebilmektedir.

Bilgisayarın bulunmasıyla, bilişim sistemlerinin işleyiş yapısını merak eden ve sisteme müdahale eden kişiler kendilerine "*hacker"* demiştir. Ancak zaman içerisinde bu kavramının yanında bir de *"cracker"* kavramı ortaya çıkmıştır. *Crackerlar* kötü niyetli olarak kendisine veya başkasına çıkar sağlamak maksadıyla sistemlerin güvenlik duvarlarını aşarak, sistem dâhilindeki verileri bozan değiştiren kimselere verilen addır. *Hackerler* ise, bilişim sisteminin içine girerek her türlü bilgiye ulaşmalarına rağmen sisteme herhangi bir zarar vermezler ancak bugün itibarıyla her iki kavramın da iç içe geçtiği söylenebilir. [160]

1.10.12. İstem Dışı Alınan Elektronik Postalar (Spamming)

Günümüzde özellikle büyük bilişim sistemlerinin önemli bir sorunu haline gelen istem dışı alınan elektronik postalar (spam), bir bülten veya haber gurubu

[158] Aynı, s. 62
[159] Gözüşirin, **a.g.e.** , s. 39
[160] Gözüşirin, **a.g.e.** , s. 39

üzerinden ticari amaç taşımayan, bu forum konuları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklâm olarak tanımlanmaktadır. [161]

Spam sözcüğü, ABD kaynaklı olup ilk defa Firma Hormel Foods Corporation'un ürettiği gıdalarla ilgili kullandığı bir kısaltmadır ve "spiced pork and ham" sözcüklerinin baş harflerinden oluşmaktadır. [162]

Spam, genelde ticari bir ürünün promosyonunun yapılması veya pazarlanmasında geniş kitlelere ulaşmak için kullanılmaktadır. Fakat spam mailleri yalnızca ticari içerikli maillerden ibaret değildir. *"Spam mailleri aynı zamanda politik bir görüşü yansıtan, kamuoyu oluşturma amaçlı kullanılan ya da piramit benzeri pazarlama yapıları oluşturan çeşitleri bulunmaktadır"* [163]

Ülkemiz açısından istem dışı alınan elektronik postalara özgü yasal bir düzenleme bulunmamasına karşılık, bunu engelleyebilecek hükümlerin var olduğu görülmektedir. Bu sebeple de spam ile ilgili problemlerin Tüketicinin Korunması, Haksız Rekabet ve Medeni Kanun hükümlerine göre çözümlenmesi düşünülebilir. Gönderilen e-postaların içeriğine göre Türk Ceza Kanunu'nun uygulama alanı bulması da mümkündür. E-postanın içeriğinde tehdit, hakaret yasal olmayan propagandalar varsa bu takdirde bunlar ayrıca ceza davalarının konusunu oluştururlar. Bunun yanında istem dışı alınan elektronik postalar, sistemi engelleyecek boyuta ulaştığı takdirde bu, 5237 sayılı TCK'nin 244. maddesinde düzenlenen *"bilişim sisteminin engellenmesi"* kapsamında değerlendirilebilecektir.[164]

1.10.13. Başlık Bilgilerini Tahrip Etme (Spoofing)

Spoofing, e-posta başlıklarının değiştirilmesi ile iletinin orijinal göndericisi yerine başka bir yerden ya da kurumdan geliyormuş gibi gösterilme işlemidir. *Spam* yapanlar iletilerinin dikkate alınıp okunması ve cevap verilmesi için *spoof* yaparak ciddi ve saygın kuruluşların isimlerini kullanabilirler. [165]

---

[161] Yazıcıoğlu, **a.g.e.** , s. 157
[162] Dülger, 2004, **a.g.e.** , s. 77
[163] Değirmenci, **a.g.e.** , s. 98
[164] Memiş, Tekin, "*Hukuki Açıdan Kitlelere E-posta Gönderilmesi"*, ***AÜEHFD***, S. 1-4, 2001, s.432
[165] Gözüşirin, **a.g.e.** , s. 40

Bu durum, saldırıya uğrayan kuruluşların ticari ünlerini zedelemekte, zaman ve müşterilerini kaybetmelerine sebep olmaktadır. Bunun düzeltilmesi için kurumlar harcama yapmakta, bu da kuruma mali yük getirmektedir. Bazen kurumların itibar kayıpları, mali harcama ile de düzeltilmeyecek hale gelmektedir.

1.10.14. Olta Atmak (Phishing)

Phishing, mağdurun şifre, banka hesap numarası, kredi kartı bilgisi gibi kişisel ve güvenlik gerektiren ve ikinci şahısların bilmesi durumunda mağdurların zor durumda kalmasına sebep olan bilgileri, mağduru aldatma yoluyla elde etmedir. Phishing, mağduru kandırmak için güvenilir gibi gözüken e - posta ya da web siteleri hazırlanıp bu bilgileri paylaşmalarını isteme durumudur.

Phishing yönteminde dolandırıcı, hazırladığı e - postaları, elinde bulunan posta listelerini spam şeklinde gönderir. Bu postalarda bir banka / finans kuruluşunun sisteminde güncelleme yapıldığı ve sistemde eksik bilgilerin bulunduğu ve tamamlanması istenir. Bu postaların altında dolandırıcının önceden hazırlamış olduğu sitenin adresi, belli gizleme yöntemler ile mağdur aldatılacak şekilde konulur. Bu postaya inanan mağdur, kendi bilgilerini dolandırıcıya bu sitelerde yer alan alanlara yazarak verir. Bu şekilde dolandırıcı, mağdurdan aldığı bilgileri maddi çıkar kazanmak için kullanmaktadır.[166]

1.10.15. Tuş kaydediciler (Keylogger)

Keylogger, internette resim ya da programların içinde saklanarak, kullanıcının bilgisayarına, bilgisi dışında yüklenen programlardır. Bu program, kullanıcının bilgisayarında çalışmaya başladığından itibaren, klavyeyle yazılan tüm bilgi ve fare ile tıklanan her bölgenin resimlerini kaydederek rapor haline getirir ve bilgisayarda bulunan zararlı programı düzenleyen kişi ya da kişilere internetten gönderilir. Böylece, bahsi geçen kötü yazılımı kullanıcının bilgisayarına gönderen kişi ya da kişiler, kullanıcının bilgisayarından yapılan bütün işlemlerin şifrelerini ele geçirmektedir.

[166] Dülger, 2004, **a.g.e.** , s. 113.

1.10.16. Cep Telefonu Casus Yazılımları

Günümüzde cep telefonları, küçük bir bilgisayar haline gelmesi ve birçok işlevi üzerinde bulunduran işletim sistemi ve uygulamalardan oluşmaktadır. Bu nedenle kötü amaçlı kullanılan bazı yazılımlar, cep telefonlarına yerleşerek, iletişimin gizliliğini ihlal etmektedir. Cep telefonlarına satın alınarak ya da indirilerek kullanılarak bazı kötü amaçlı yazılımlar ile ortam dinleme, telefon dinleme, mesaj bildirimi, arama bildirim, SIM bilgisi, yer bilgisi alma işlemleri kötü niyetli kişilerin eline geçebilmektedir.

İKİNCİ BÖLÜM

İNTERNET SUÇLARININ KİŞİSEL HAK VE ÖZGÜRLÜKLERE VERDİĞİ ZARARLAR

İnternet suçlarının kişisel hak ve özgürlükler üzerindeki etkisini ortaya koyabilmek adına, öncelikle kişilik ve kişilik hakkı kavramları üzerinde durularak, kişisel hak ve özgürlüklerin çerçevesi çizilecektir. Bunu takiben 5237 sayılı Türk Ceza Kanunu'nda tanımlanan internet suçlarının üzerinde tek tek durularak kişisel hak ve özgürlükler üzerinde işlenen suçların etkisi ele alınacaktır. Kişisel verilerin ve kişiliğin korunması konusunda internet servis sağlayıcılarının sorumluluğu üzerinde durularak, suçların etkileri ortaya konulmuş olacaktır.

2.1. KİŞİLİK VE KİŞİLİK HAKKI KAVRAMLARI

Kişilik ve kişilik hakkı kavramları birbiriyle ilintili ve iç içe geçmiş bir yapı sergilediği gibi, kişilik denildiğinde de öncelikle kişi kavramından hareket etmek gerekliliği doğmaktadır. Öncelikle kişi kavramı ve kişi türleri ele alınıp, devamında kişilik kavramı üzerinde durarak, kişilik hakkının ne olduğu ve neleri kapsadığı üzerinde durulacaktır.

2.1.1. Kişi Kavramı

Kişilik kavramının tanımının yapılması için ilk olarak kişi kavramının açıklanması gereklidir. Latince "Persona" karşılığına gelen kişi kelimesi, eski zamanlarda tiyatrocuların sahneye çıkarken taktıkları maskeyi tanımlamak için kullanılmış olup, daha sonra oyuncu ve rolü tanımlamak için kullanılmıştır. Günümüzde ise kişi, yalnızca birey olarak insanı değil, kişi ve mal grubu olarak kurulmuş olan tüzel kişileri de ifade etmektedir.[167]

[167] Soysal, Tamer, "Elektronik Posta Yoluyla Kişilik Haklarına Elektronik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk", ***Ankara Barosu Dergisi***, Yıl: 65, Sayı: 1, Kış 2007, s. 147.

Hukuki olarak kişi, çeşitli hak ve yükümlülüklere sahip olabilen bir varlık anlamına gelmektedir. Kişi denildiğinde akla ilk gelen insandır, fakat günümüz hukuk doktrininde kişi, yalnızca insandan ibaret değildir.[168]

Toplum gereksinimlerine yanıt vermek için kanun koyucu, gerek kişilerin yanında, belli bir amacı gerçekleştirmek için bazı varlıklara da çeşitli hak ve yükümlülükler sahibi olma olanağı tanımıştır. Bunlara da tüzel kişiler denmektedir. Bu nedenle, hukuki işlemde kişi denildiğinde hak ve yükümlülüklere sahip gerçek kişi ve tüzel kişiler ifade edilmektedir. Medeni Kanunumuz da, kişileri iki gruba ayırmaktadır.

2.1.1.1. Gerçek Kişiler

Gerçek kişiler, insanlar için kullanılan bir ifadedir. Günümüz modern hukuk sisteminin hepsinde gerçek kişi insan için kullanılmakta ve modern hukuk, kişilik olarak insanı kabul etmektedir. Ancak, tarihi süreç içinde, eski hukuk sistemi içindeki bu durum 19. yy. da dahi devam etmiştir, insanların eşya olarak sayılmaları ve bu nedenle kira ve alım satım sözleşmesine konu olmalarından dolayı, her insan, kişi olarak kabul edilmemekteydi. Köleliğin kaldırılması ile tüm insanların kişi olarak kabul edilmesi olanaklı olmuş ve günümüzde insanlar arasında ayrım bulunmamakta, bütün insanlar eşit bir kişi olarak sayılmaktadır.

Hukuk dilinde de kişi, hak ehliyetine sahip varlıkları ifade eder. Hak ehliyetine sahip olmak demek, haklara sahip olabilmek ve borç altına girebilmek demektir. Kimlerin hak sahibi olabileceğini ve borç altına girebileceğini de yani hangi varlıkların kişi olarak kabul edileceğini kanun koyucu belirlemiştir.[169]

2.1.1.2. Tüzel Kişiler

Tüzel kişi, kendisini oluşturan bireylerden bağımsız olan kişilikleri bulunan kurum ve kuruluşları ifade etmektedir.[170] Bazı amaçların gerçekleşmesi için, gerçek kişilerin kimi zaman gücünü kimi zaman ömrünü aşabilecek özellikte olmaktadır. Bu

[168] Dural, Mustafa – Öğüz, Tufan, ***Türk Özel Hukuku Cilt 2 Kişiler Hukuku***, Filiz Kitabevi, İstanbul, 2012, s.5.
[169] Remzi, Mehmet, Aydın, Sezer ve Ispartalı, Murat, ***Medeni Hukuk,*** İkinci Sayfa Yayınları, İstanbul, 2010, s.76.
[170] Akıntürk, Turgut - Karaman, Derya Ateş, ***Medeni Hukuk***, Beta Yayınları, İstanbul, 2011, s.178.

nedenle hukuk sistemi, bu gibi çeşitli amaçların gerçekleşmesi için kimi kişi ya da mal gruplarına, kendilerini oluşturan gerçek kişiliklerinden ayrı ve bağımsız bir kişilik tanımıştır. Bağımsız bir varlığı bulunan tüzel kişiler, kendisini oluşturan bireylerden farklı bir iradeye sahip olduğu ve bu iradeyi hukuki organlar ile açıkladığı kabul edilir.

Tüzel kişiler, yaş, cinsiyet gibi sadece gerçek kişilere (insanlara) ait olan özellikler dışında, hak elde etme ve yükümlülük elde etme ehliyetine, gerçek kişilerde olduğu gibi eşit seviyede sahiptir. Yalnız şunu da belirtmek gerekir ki, tüzel kişiler hukukunda sınırlı sayı ilkesi (numerus clausus) geçerlidir. Yani tüzel kişi türleri kanunla belirlenmiş ve sınırlanmıştır. Kişiler, kendi iradeleri ile kanun koyucu tarafından belirlenmiş tüzel kişi türlerinden başka yeni bir tüzel kişi modeli icat edemezler. [171]

2.1.2. Kişilik Kavramı

Kişilik kavram olarak, toplumların kültür, örf ve adetlerine göre değişkenlik gösteren bir kavramdır. Bu nedenle kişilik kavramının tanımlanmasında, kesin sınırlar çerçevesinde ifade edilememektedir. Literatür ve doktrinde yapılan farklı tanımlamalar incelendiğinde, bu tanımlamaların kişilik kavramının belli unsurları üzerinde durularak ifade edildiği ve bu ifadelerin bir tarafının eksik kaldığı görülmektedir.

Kişilik kavramı insanın fiziki varlığından çok, toplum hayatındaki yerini ifade eder. Kişilik kavramı statik ve durağan bir kavramı ifade etmekten çok dinamik ve hayatın ve mekânın değişimine paralel olarak değişen ve dönüşen bir kavramı ifade etmektedir.[172]

Doktrinde kişilik kavramının biri dar diğeri geniş olarak iki anlamı bulunmaktadır. Dar anlamda kişilik, hak ve yükümlülüklere sahip olmayı, diğer ifade ile hak ehliyetini ifade etmektedir. Geniş anlamda kişilik, hak ehliyeti ile sınırlı olmadan, onunla birlikte eylem ehliyeti, kişisel durum ve kişisel hakları ifade etmektedir. Bu bağlamda, kişilik *"ehliyet"*, "kişisel durum" ve *"kişisel hak"*

[171] Deryal, Yahya, ***Medeni Hukuk Bilgisi***, Seçkin Kitabevi, Ankara, 2010, s. 88.
[172] Özel, Sibel, ***Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması***, Seçkin Kitabevi, Ankara 2004, s.36.

kavramlarından oluşmaktadır. Kısaca kişilik, sadece hak ehliyetini değil, aynı zamanda fiil ehliyeti, kişisel durum ve kişilik hakkını ifade etmektedir.[173]

2.1.3. Kişilik Hakkı Kavramı

Türk Medeni Kanununda, kişilik hakkı tanımlanmamış, bu hakkın tanımı doktrin ve yargıya bırakılmıştır. *"Kişilik hakkının içeriği İsviçre ve Türk Medeni Kanununda belirtilmiştir. İsviçre ve Türk hukuku kişilik hakkını çerçeve bir hükümle düzenleyerek zamana, yere ve topluma göre değişen kişisel değerleri daha geniş hatlarla koruma altına alınmıştır."*[174] Bu amaçla yapılan tanımlamalarda genel olarak kimi kişilik değerleri vurgulanmakta, kişilik hakkının bu değerler üzerinde bir hak olduğu ifade edilmektedir.

Kişilik hakkının doktrin ve yargıda çeşitli tanımları bulunmaktadır. Örnek olarak, Yargıtay 4. Hukuk Dairesinin 6. 6. 1972 tarih, 14724 E. 5389 K. sayılı kararında kişilik hakkı, *"Kişinin hayatı, sağlığı, beden ve ruh tamlığı, şeref ve haysiyeti, saygınlığı gibi varlıkların bütünü kişiliğini oluşturur. Yasa koyucu, kişisel varlıkları birer birer sayarak hâkimi bağlamak istememiştir."* şeklinde tanımlanmıştır.[175]

Yine de kişilik hakkını tanımlarken, kesin sınırlarla çizmek, bir çerçeve içine almak olanaklı değildir. Çünkü kişilik hakkı, zaman ve yere göre devamlı değişen, tek bir kültür ve görüşe bağlı olmayan bir kavramdır. Bu nedenle, kişilik kavramının içerik ve ifade ettiği değer ile toplumdaki diğer değerler içindeki yeri tarihi süreç içinde devamlı değişmiştir. Bunun en güzel örneği yine Yargıtay'ın 2000'li yıllarda verdiği bir kararda görülmektedir. *"...kişilik hakkı; kişinin özgür ve başkasına bağlı olmadan varlığını sürdürmesi, kendine özgü yaşam biçimini sağlamasını amaçlar. Bu haklar insanın doğumu ile kazanılan ve kişiliğe bağlı olan haklardır."*[176]

Gerçekten, kişisel değerlerin mutlak ve değişmez bir listesini belirleyerek kişilik hakkının tanımının yapılması zamanın değişen koşulları nedeniyle ortaya çıkan yeni kişisel değerleri korumasız bırakacaktır. Ancak kişisel değerlerin

---

[173] Öztan, Bilge, ***Medeni Hukukun Temel Kavramları***, Turhan Kitabevi, Ankara 2000, s.209.

[174] Kara Kılıçarslan, Seda, ***Kişilik Hakkına Saldırıda Üstün Nitelikte Özel ve Kamusal Yarar***, Yayımlanmamış Yüksek Lisans Tezi, T. C. Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 4

[175] Karahasan, Mustafa Reşit, ***Tazminat Davaları***, İstanbul, 1976, s.886

[176] Yargıtay 4. H.D. , 15.02.2001, 2000/10596 E. , 2001/1501 K. , ***Yargıtay Kararları Dergisi***, C.27, S.8, s.1170.

tanımının yapılmamasının hukuki belirsizliğe yol açacağı da savunulan bir görüştür.[177]

İsviçre ve Türk düzenlemesi karşısında Alman hukuku kişisel değerleri genel bir hükümle düzenlememiş, doğal hukukun etkisindeki Fransız sisteminden ve Roma hukukunun kazuistik sisteminden etkilenerek karma bir yapı benimsemiştir. İsviçre ve Türk hukukundaki genel kişilik hakkına en yakın düzenlemeye Alman hukukunda BGB (Alman Medeni Kanunu) m. 823 / f. 1 ve 2'de rastlamaktayız. Bu düzenlemeye göre, [178]

"*Kasten veya ihmalle bir başkasının hayatını, sağlığını, özgürlüğünü, mülkiyetini veya diğer bir hakkını hukuka aykırı olarak ihlal eden kişi, o şahsa karşı, bundan doğan zararı tazmine etmekle yükümlüdür. Aynı yükümlülük, bir başkasını koruma amacı güden yasayı ihlal eden kişi için de mevcuttur. Yasanın içeriğine göre bu yasayı kusur olmadan da ihlal etmek mümkünse, tazminat yükümlülüğü ancak kusur halinde doğar*."

Alman hukukunun yaklaşımı karşısında, İsviçre ve Türk hukukunda kişilik hakkı yalnızca genel bir düzenlemeyle yetinmemiştir. Genel düzenlemenin yanı sıra, çeşitli kanunlarla münferit düzenlemelere yer verilmiştir. Başka bir ifadeyle, Türk hukukunda TMK m. 23, 24, 25'te genel bir düzenleme benimsenmişken, TMK m. 26, 27, TBK. M. 47, FSEK. M. 14 vd., 70, 85, 87 ve TTK m. 56 gibi özel düzenlemelerle kişilik hakkını korumuştur. Ancak sözü edilen özel düzenlemeler, genel kişilik hakkı yaklaşımından uzaklaşıldığı anlamına gelmemekte, yalnızca genel kişilik hakkının çeşitli görünümlerini göstermektedir. Gerçekten kişilik hakkının yere ve zamana göre değişen bir kavram olması nedeniyle, tek tek sayarak kişilik hakkını korumak akılcı bir çözüm olmayacak, gerekli koruma sağlanamayacaktır. Dolayısı ile önceden düzenleme yaparak zamanın ihtiyaçlarına cevap verememek yerine, kişilik hakkının içeriğinin saptanmasını hâkime bırakmanın daha yararlı olacağı açıktır. [179]

Yaşam, sağlık, onur ve haysiyet, özel hayat, isim, fotoğraf gibi kişilik değerleri üzerinde bulunan hak, kişilik hakkını ifade etmektedir. Hukukumuzda, tek bir kişilik hakkının farklı ifadeleri bulunmaktadır. Kişilik değerleri üzerinde ayrı ayrı kişilik hakkı yer almamaktadır. TMK m. 24 ve 25. ile 6098 sayılı Türk Borçlar

[177] İşgüzar, Hasan, "3444 Sayılı Kanunla Değiştirilen Borçlar Kanunun 49. Maddesine Göre Kişilik Hakkının İhlali Nedeniyle Manevi Tazminat Davasının Şartları", ***Ankara Barosu Dergisi***, S. 6, Aralık, 1990, s. 857.
[178] Kara, Kılıçarslan, **a.g.e.** , s. 4
[179] Aynı, s. 6

Kanununun 58. Maddesinde bulunan kişilik hakkı kavramı kullanılarak, tek ve genel bir kişilik hakkından bahsedilmiştir. Kişilik değerleri üzerinde geçerli olan haklardan söz edilebilir; fakat bunlar esasen temel bir kişilik hakkının yansımaları olarak değerlendirilir.[180]

2.1.4. Kişilik Hakkının Konusu

Kişilik hakkını oluşturan değerler, kişiye bireysellik kazandıran ve özel duygularda dâhil olmak üzere bireyler arası ilişkilerde korunmaya değer her şeyi ifade eder. [181]

Kanunda kişilik hakkı kapsamında olan kişisel değerlerin ne olduğu tek tek belirtilmemiş, bu görev yargı ve doktrine bırakılmıştır.

"Kişiler arasındaki ilişkiler zamanla gelişmekte, karmaşık bir hal almakta, bu değişim de daha önce görülmemiş kişilik hakkı ihlallerinin ortaya çıkmasına sebep olmaktadır. Ayrıca, kişilik hakkı kapsamına giren değerlerin neler olduğunun teker teker sayılması burada belirtilmeyen değerlerin önemsiz olduğu konusunda bir fikrin oluşmasına sebep olabilir."[182]

Bu nedenle, kişilik hakkı kapsamına girmiş olan değerlerin ne olduğunun, önceden bilinmesi olanaksızdır. Bu bağlamda, doktrinde, kişilik değerlerinin sıralanması ve sınıflandırılması zordur ve bu nedenle özel bir hakkın konusu kapsamında olmayan bütün kişilik değerleri kişilik hakkını oluşturmaktadır.

2.1.4.1. Maddi Kişisel Değerler

Kişilik hakkını oluşturan maddi değerler, kişinin hayatı, sağlığı ve bedensel bütünlüğüdür. Anayasanın 17. Maddesine göre, *"herkesin yaşama hakkına, maddi ve manevi varlığını koruma ve geliştirme hakkına sahip olduğuna"* hükmedilmiştir. Ayrıca, Türk Medeni Kanununun (TMK'nun) 23, 24, 25. Maddelerinde ve Türk Borçlar Kanununun (TBK'nın) 56. Maddesinde hayat, sağlık, bedensel bütünlüğe karşı yapılan saldırılara karşı yaptırımlarda bulunulmuştur.

---

[180]Tümerdem, Murat, ***İnternette Kişilik Hakkı İhlâlinden Kaynaklanan Manevi Tazminat***, Yayımlanmamış Yüksek Lisans Tezi, T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2013, s.2.

[181] Kılıçoğlu, Mustafa, ***Sorumluluk Hukuku***, C.1, Sözleşme Dışı Sorumluluk, Ankara 2002, s. 60.

[182] Helvacı, Serap, ***Gerçek Kişiler***, İstanbul, 2013, s. 73

Kişiye işkence ve eziyet yapmak, insan haysiyetiyle bağdaşmayan bir muamelede bulunmak, sürekli psikolojik baskı ve tehdit altında tutmak sonuçta kişilik hakkının ihlali anlamına gelmektedir. [183]

İnternet aracılığıyla kişilik hakkı ihlâlinde maddi kişisel değerlerden olan hayat ve bedensel bütünlüğe doğrudan hukuka aykırı müdahalede bulunmak mümkün değildir. İnternet aracılığıyla ancak fiziki ve/veya ruh sağlığına müdahalede bulunmak mümkün olabilir.[184]

2.1.4.2. Manevi Kişisel Değerler

Manevi kişisel değerler şeref ve haysiyet, kişinin ismi, resmi, sesi ve de hürriyetleridir. Ayrıca fikri çabalar neticesinde oluşan eserler hakkında da diğer kimselerden saygı gösterilmesini istemek de manevi değerlere ilişkin bir haktır. [185]

Manevi bütünlüğe ilişkin kişisel değerler kişinin toplumla olan ilişkisinden kaynaklanmaktadır. Kişinin manevi varlığı ve değerleri onun manevi kişiliğini oluşturur. Kişilik hakkının konusunu oluşturan manevi kişisel değerler ise; kişinin şeref ve haysiyeti, ismi, resim ve sesi ile hayat alanıdır. Kişiler özgürlüklerinin, şeref ve haysiyetlerinin, isimlerinin, resimlerinin, özel hayatlarının, saygınlıklarının her türlü saldırıdan korunmasını talep etme hakkına sahiptir. [186]

Özgürlük, kişilerin hukuki sınırlar içerisinde kalmak şartıyla istediği faaliyette bulunması, istediği gibi davranması şeklinde ifade edilmektedir.[187] Özgürlükler, kişiye onun insan olmasından dolayı tanınan ve vazgeçilemez değerlerdir. Özgürlükler, başta Anayasa olmak üzere kanunlarca koruma altına alınmıştır. Anayasanın *"Temel Hak ve Özgürlükler"* başlıklı ikinci kısmında kişinin sahip olduğu çeşitli özgürlükler belirtilmiş ve kanunen koruma altına alınmıştır. Bu bağlamda haberleşme, din ve vicdan, düşünce ve kanaat, hak arama hürriyeti temel haklar kapsamına alınmıştır. Anayasanın 12. Maddesinde bulunan *"Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir"* ifadesi ve TMK'nun 23. Maddesinin 2. Fıkrasında bulunan *"Kimse özgürlüklerinden*

[183] Tümerdem, **a. g. e.** , s. 6
[184] Aynı, s. 6
[185] Sırabaşı, Volkan, ***İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz***, Adalet Yayınevi, Ankara, 2007, s. 29
[186] Tümerdem, **a.g.e.** , s. 7
[187] Arpacı, Abdülkadir, ***Kişiler Hukuku Gerçek Kişiler***, Beta Yayınları, İstanbul, 2010, s. 109.

vazgeçemez veya onları hukuka ya da ahlâka aykırı olarak sınırlayamaz" ifadesine göre, özgürlükler, kişinin sınırlandırılamaz bir hakkıdır ve kişinin kendisinin istemesi durumunda bile vazgeçilemez temel kişilik değeri olduğu görülmektedir.[188]

Kişilik haklarından bir diğer kişisel değer, kişinin şeref ve haysiyetidir. Şeref ve haysiyet, kişiye bulunduğu toplum tarafından atfedilen manevi değerlerin tümüdür. Kişi, toplumun atfettiği bu değerlerin bazılarını doğarken, bazılarını da sonradan kazanır. Bu bağlamda şeref ve haysiyet ahlaki şeref ve haysiyet ve toplumsal şeref ve haysiyet olmak üzere iki unsurdan oluşmaktadır. Ahlaki şeref ve haysiyet, kişinin insan olarak doğmasından dolayı kazandığı şereftir. Kişiler, insan olmalarından dolayı, sahip olduğu insani değerleri, toplum içindeki statüleri ne olursa olsun kaybetmek istemezler. Mesela, suçu ne olursa olsun, bir suçluya insan şeref ve haysiyeti ile uyuşmayacak şekilde hitap edilemez ya da muamele de bulunulamaz. Bu şekilde davranılması, kişinin insan olarak doğması ile kazandığı manevi değerlerin ihlali anlamına gelmektedir.

Toplumsal şeref ve haysiyet, sonradan kendi davranışlarıyla edindiği değerlerdir. Toplumsal şeref ve haysiyet, kişinin davranış ve yetenekleri ile orantılıdır ve herkesin bu değerlere sahip olduğu yolunda karine bulunmaktadır.

TMK hem ahlaki şeref ve haysiyeti hem de toplumsal şeref ve haysiyeti koruyucu maddeler içermektedir. Şeref ve haysiyet kişiye toplum tarafından atfedilen nesnel değer yargıları olduğundan, şeref ve haysiyetin atanmasında kişinin öznel değer yargıları, hukuki bir kıstas olarak alınamaz. Bu bağlamda, kişinin kendi kişiliğine fazla değer verip, toplum açısından olumsuz olarak kabul edilmeyen bir ithamı, aşağılayıcı olarak görmesi ya da toplum tarafından aşağılayıcı olarak atfedilen ithamı, aşağılayıcı olarak kabul etmemesi hukuk sisteminde önem taşımamaktadır.

Şeref ve haysiyet, TMK m. 24'te bulunan kişilik değerleri kapsamında olduğu için, bu değerlerin ihlali sebebiyle manevi ya da maddi zarar oluşabilir. Örnek olarak, bir internet sayfasında, bir işadamının şeref ve haysiyetinin ihlal edilmesi sebebiyle müşteri kaybetmesi durumu maddi zarar unsuru olabilir. Şeref ve haysiyet sadece gerçek kişilerin sahip olduğu bir hak değil, tüzel kişiler için de kullanılan bir haktır. Tüzel kişiler, şeref ve haysiyetlerinin ihlal edilmesi ile duygu yönünden zarara

[188] Arpacı, **a.g.e.** , s. 109.

uğramaz ancak, prestijleri zedelenebilir ya da hukuka aykırı olarak maddi zarara uğrayabilirler.[189]

Kişinin sahip olduğu manevi kişilik değerlerinden biri de isimdir. İsim, bir kişiyi toplumdaki diğer kişilerden ayıran, kişinin belli bir aileye ait olduğunu belirten, toplum içinde bulunmanın getirdiği ilişkilerde kişiyi belirleyen ve tanıtan bir sembol şeklinde ifade edilebilir. Kişinin, toplum ile olan ilişkilerinde, kendisini diğer kişilerden ayıran bir tanıtım aracı olan isim, kişiliğe ait özelliklerden biridir. Fakat kişiliğe ait özelliklerden hiçbiri kişinin bulunduğu toplum ile olan ilişkilerinde isim kadar devamlılık gösteren bir özelliğe sahip değillerdir. Bu nedenle, TMK'nın 26. ve 27. Maddelerinde, isim üzerindeki hak özel olarak düzenlenmiş, isim üzerindeki hak kişilik hakkı olarak kabul edilmiştir.

İsim üzerindeki hakkın korunmasıyla birlikte kişinin tek ve yerine konulamaz özelliğe sahip olması sebebiyle kişiyi diğer kişilerden ayırmaya yarayan tüm işaretler de korunur. Kişinin gerçek anlamdaki isminin yanı sıra toplum içinde kişiyi ayırmaya yarayan unvan, müstear ad gibi değerler de kişilik hakkının korunmasından yararlanır. [190] Bunun yanında, internet ortamında e - posta adresleri de kişilik hakkı kapsamında korunması olanaklıdır.

Kişinin manevi kişilik değerlerinden bir diğeri resim ve sestir. Resim, kişinin sahip olduğu özellikleri ifade eden bir semboldür. Bu nedenle, kişinin resmi de kişilik hakkı kapsamına alınan manevi kişisel değerlerden biridir. Kişinin resminin yasa dışı çekilmesi, basılması, çoğaltılarak yayımlanıp dağıtılması, kişisel hak kapsamında men edilmiştir.

Resim, kişinin dış yaşama yansıyan ve onu öteki kişilerden ayıran görünümüdür ve kişi, bu görünümüne saygı duyulmasını isteme hakkına sahiptir. [191] Bu yetki kapsamında, kişinin, kendi resmini kendi iradesi dışında kullanma yetkisini kısıtlama ve yasaklama imkânına sahiptir. Kişi, kendi rızasıyla resmi üzerindeki yasal haklarından vazgeçebilir. Bu bağlamda günümüzde internet aracılığıyla, kişilerin resimlerinin kullanımı, kişinin rızası dışında kullanılması söz konusu olmakta ve kişilerin resimleri, farklı mecralarda farklı amaçlarda kullanılabilmektedir. Bu nedenle kişinin izinsiz olarak resminin yapılması, çekilmesi,

[189] Akipek, Jale – Akıntürk, Turgut, ***Türk Medeni Hukuku, Birinci Cilt: Başlangıç Hükümleri, Kişiler Hukuku***, Beta Yayınları, İstanbul, 2007, s. 386.
[190] Tümerdem, **a. g. e.** , s. 11
[191] Aynı, s. 12

sergilenmesi, yayımlanması, reklam aracı olarak ilanlarda, broşürlerde, reklam panolarında ve diğer yerlerde kullanılması kişilik hakkına yönelik hukuka aykırı saldırı oluşturur.[192]

Kişinin bir diğer manevi kişilik hakkı da sestir. Ses de, resim gibi kişinin niteliklerini taşıyan işaretlerden biridir. Kişinin sesi, başkası tarafından izinsiz kaydedilemez, yayınlanamaz, açıklanamaz, kullanılamaz.

Bu bağlamda, resim ve ses hakkındaki kişisel hakların korunması için TMK 24, 25. Maddelerinde, TBK 58. Maddesinde, 5846 sayılı FSEK 84. , 86. Maddelerinde yasal olarak düzenlenmiştir.

Manevi kişisel kapsamına alınan bir diğer kişisel değer, hayat alanıdır. Topluma ait bir kişi olan insan, hayatını devam ettirirken çevresi ile iletişim halinde yaşamaktadır. "Hayat alanı, kişinin en yakın olanı aile bireylerinden, toplumdaki diğer kişilere, hatta diğer toplumdaki kişiler ve devletlere kadar olan ilişkileri kapsayan ve özellikleri değişiklik gösteren ilişkilerin yaşandığı ortak alandır." Günümüzde, teknolojik gelişmelerle birlikte, kişilerin özel hayatıyla ilgili bilgilerin başkaları tarafından öğrenilmesi tehlikesi daha da artmıştır. Bunun sonucu olarak da kişiler zayıf ve korumasız duruma düşmekte ve her an hayat alanlarına yönelik saldırılarla karşı karşıya kalabilmektedir. [193]

Kişi, kendine ait özel hayat alanı ile diğer kişilerin karışmasına olanak vermeden, istediği gibi yaşamını devam ettirme olanağına sahiptir. Bu sebeple, kişi, sahip olduğu hayat alanına saygı bekleme hakkına sahiptir.

Kişilere özel hayat alanı, hem uluslararası hukuk kurallarında ve iç hukukumuzda çeşitli hükümlerle tanınmış ve korunmuştur. Anayasamızın *"Özel Hayatın Gizliliği ve Korunması"* başlığı altındaki maddelerde kişinin sahip olduğu özel hayat alanı ile ilgili tanımlar ve koruyucu kanun maddeleri yer almış, bu bağlamda özel hayatın ve aile hayatının korunması, konut dokunulmazlığı, haberleşme hürriyeti gibi haklar, temel haklar kapsamında koruma altına alınmıştır.

İnsan Hakları Evrensel Beyannamesi'nin 12. Maddesine göre *"Hiç kimse özel hayatı, ailesi, meskeni veya yazışması hususlarında keyfi karışmalara, şeref ve*

[192] Akipek ve Akıntürk, **a.g.e.** , s. 391.
[193] Tümerdem, **a. g. e.** , s. 13

şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır." (İnsan Hakları Evrensel Beyannamesi)

Ancak, hayat alanı ile ilgili tek bir tanım yapılması oldukça zordur. Bu nedenle doktrin, genel olarak kişinin hayat alanı kamuya açık alan, özel alan, gizli alan olmak üzere üçe ayrılmaktadır.

Kamuya açık alan; ister toplum içinde meydana geldikleri için ister ilgili kişi belirli bir aleniyet verdiği için herkesçe bilinen ve dolayısıyla, kişinin başkalarının bilmesinden rahatsız olmadığı konu ve olaylardan oluşan yaşam çevresidir. [194]

Kamuya açık alana, bir kimsenin alenileştirilmesinde sakınca görmediği olaylar girer yani kişinin, herkesçe bilinmesinde herhangi bir sakınca görmediği olaylar hep bu alana dâhildir. [195]

Kamuya açık alan, kişisel değer kapsamında kişilik hakkının korunmasından faydalanamaz. Bu alanda yaşanan olaylar toplumdaki diğer kişiler tarafından kolaylıkla öğrenilebildiğinden, bu alanın diğer kişilerden gizli tutulması olanağı yoktur. [196]

Kamuya açık alan kapsamında bir olayın açıklanmasında, kamunun bir faydasının olup olmadığına bakılmamaktadır. Bu bağlamda, kamuya açık alan kapsamında gerçekleşen olayların diğer kişilere anlatılması, kişilik hakkı ihlali gerçekleştirmez.

Fakat kişilerin kamuya açık alanına her türlü katılım ve karışım da yasal değildir. Kişilerin kamuya açık alanlarıyla alakalı yanlış bilgiler yaymak ya da kişiyi küçük düşürmek için ve kötü amaçlı olarak bu alan ile ilgili bilgileri diğer kişilere anlatması, kişilik hakkı ihlaline yol açar.

Hayat alanı kapsamında bulunan bir diğer alan, özel alandır.

"*Doktrinde genel olarak özel alan; kişinin gizli alanına dâhil olmayan sadece belirli kişiler tarafından (ailesi, arkadaşları, akrabaları gibi) bilinmesini istediği, onlarla paylaşımda bulunduğu ve kamudan sakladığı olaylardan oluşan hayat alanı olarak tanımlanmaktadır."* [197]

---

[194] Tümerdem, **a. g. e.** , s. 14

[195] Öztan, Bilge, ***Şahsın Hukuku Hakiki Şahıslar***, Filiz Kitabevi, Ankara, 1997, s. 135

[196] Zevkliler, Aydın - Acabey, M. Beşir, Gökyayla, M. Emre, ***Medeni Hukuk***, Türkmen Kitabevi, Ankara, 2000, s. 467.

[197] Peker Demir, Esra, ***İnternet Aracılığıyla Kişilik Haklarına Saldırı***, Yayımlanmamış Yüksek Lisans Tezi, Kültür Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014, s. 17

Bu alandaki olaylar kamuya açık alanda olduğu gibi kişi ve sayı bakımından belirsiz kişilere açık değildir. Bu olayları bilen kişilerin sayısı her yaşam faaliyetine göre değişebilir.[198] Özel alan içinde yaşanan olaylar, kişinin belirleyeceği belli kişilere açıkken, diğer kişilere kapalıdır. Özel alana girme hakkını veren ilişki, beraber yaşama, çalışma, dolaşma gibi çeşitli sebeplerden dolayı olabilir. Burada önemli olan, bir olayın, sayısı belli olmayan kişilerle değil, belirli sayıdaki kişilerle birlikte gerçekleşmesidir.

Kişinin özel alanı, kişilik hakkına dair korumadan yararlanmaktadır. Bu alanda gerçekleşmiş olayların, diğer kişilere anlatılması, kişilik hakkını ihlal etmektedir. *"Ancak, bu durumda da somut olaya göre değerlendirme yapılması gerekir. Kişinin özel alanındaki olayları paylaştığı kişilerin edindikleri bilgileri başkalarına açıklamaları hukuka aykırı sayılmaz. Zira kişi bu olayları paylaştığı kişilerin bunları başkalarına iletebileceğini düşünür."*[199]

Hayat alanı kapsamındaki diğer bir alan, gizli alandır. *"Kişi gizli alanında sadece kendisi için saklı tuttuğu ve başkalarının bilmesini istemediği hayat alanını yaşar."*[200] Gizli alan, kişinin yaşam alanını üçüncü kişilerden sakladığı ya da güvendiği kişilerle paylaştığı alandır. Kişi, yaşadığı bazı olayları, kendisi dışında ya da güvendiği başka kişiler dışında başkasının bilmemesini ister. Kişinin bu hakka sahip olması, kişinin en doğal hakkıdır.

Gizli alan, özel hayatın bir parçasıdır ve kişilik hakkı kapsamında yer almaktadır. Bir olayın, kişinin gizli alanına girmesi ve hukuki olarak korunması için, nesnel ve öznel olmak üzere iki şartın birlikte gerçekleşmesi gerekmektedir. Nesnel şart, o olayın herkes (kişinin kendisi ve bilmesini istediği kişiler) tarafından bilinen ve izlenen bir şey olmamasıdır. Bu bağlamda, kişinin düşünce, inanç, telefon konuşmaları, e - postaları nesnel olarak gizli alandadır. Öznel şart ise, kişide bahsedilen olayı gizli tutma iradesinin bulunmasıdır.

Kişinin gizli alanı ile özel alanı mutlak bir koruma altındadır ve bu alanlara ilgili olmayan kişilerin müdahalesi, şeref ve haysiyetin ihlal edilip edilmediğine

---

[198] Kılıçoğlu, Ahmet, ***Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk***, Ankara, 1993, s. 84

[199] Tümerdem, **a. g. e.** , s. 16

[200] Peker Demir, **a. g. e.** , s. 19

bakılmaksızın kişilik hakkına saldırı sayılır ve bu alan içine girmiş olan kimselerde kendilerine verilmiş olan sırları saklamakla yükümlüdürler. [201]

Kişinin özel ve gizli alanına müdahalede bulunulması kural olarak hukuka aykırıdır. Bu hayat alanlarına yapılan müdahalelerde üç istisnai halde hukuka aykırılık ortadan kalkar. Özel ve gizli alana yapılan müdahalenin hukuka aykırı sayılmadığı ilk durum, açıklamanın kişinin rızasıyla yapılmasıdır; ikinci durum, daha üstün bir kamusal veya özel yararın bulunmasıdır; üçüncü durum da kanunun verdiği yetkinin kullanılmasıdır.[202]

Günümüzde bilgi ve iletişim teknolojilerinde meydana gelen hızlı gelişmeler sayesinde kişilerin özel yaşam alanlarına ya da daha özel olan gizli yaşam alanlarına saldırılar son derece kolaylaşmış ve tarihsel süreç içerisinde bir kişinin evine gizlice girme, eşyalarını karıştırıp mektuplarını açma, konuşmalara kulak misafiri olma gibi geleneksel sızma yollarının yanında, modern araçlarla yapılan gizli gözetlemeler ve dinlemeler giderek çoğalmıştır. Bilgi ve iletişim teknolojilerindeki gelişmeler sayesinde kişilerin konuşmalarını ya da davranışlarını çok uzak mesafelerden dahi dinleyerek veya görüntüleyerek kayıt altına alma, bunları saklama, değiştirme ve çok geniş bir coğrafyaya ve kitleye yaymak oldukça kolaylaşmış ve hatta bilgisayarlar aracılığı ile veri gözetlemeleri bile mümkün hale gelmiştir.[203]

2.1.4.3. Kişinin Mesleki ve Ekonomik Hakları

Kişinin korunması için sadece kişinin maddi ve manevi kişisel değerlerinin korunması yetersizdir. *"Kişilik hakkının konusunu oluşturan bir diğer değer de, diğerlerinden farklı olarak parasal sonuçlar doğurmaya elverişli olan mesleki ve ticari değerlerdir."* [204]

Kişiliğin tam olarak korunabilmesi için kişinin statik kişiliğinin yanı sıra dinamik kişiliğinin de korunması gerekir. Dinamik kişilik; kişinin meslek, sanat ve

[201] Arpacı, **a. g. e.** , s.141.
[202] Tümerdem, **a.g.e.** , s. 19
[203] Yüksel, Mehmet, "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", ***Ankara Üniversitesi SBF Dergisi***, 58-1, 2003.
[204] Peker, Demir, **a.g.e.** , s.21

ticari faaliyetlerinin kişiliğine dâhil edilmesinden oluşur. Bir başka deyişle, dinamik kişilik, kişinin yeteneklerini kullanarak toplum içinde elde ettiği yeridir. [205]

Kişinin mesleki ve ekonomik hakları da diğer kişilik hakları gibi anayasayla güvence altına alınmıştır. Anayasamızın 17. Maddesi, kişinin maddi varlığını geliştirme hakkını, 48. Maddesi de dilediği sahada çalışma hürriyeti, temel hak kapsamına alınmıştır. Kişinin mesleği, sanatı, ticari hayatına yapılacak saldırılar kişinin faaliyetine veya doğrudan kişiliğine yönelik olabilir.[206] Saldırının kişiliğe yönelmesi durumunda, kişiliği koruyan genel hükümler, kişilik hakkını koruyacak şekilde düzenlenmiştir.

Kişinin mesleki ve ekonomik haklarını, maddi ve manevi haklarından ayıran unsur, mesleki ve ekonomik hakların parasal sonuç oluşturma olanağına sahip olmasıdır. Kişinin mesleki ve ekonomik hakları, kişinin ekonomik özgürlüğü, mesleki şeref ve haysiyeti, mesleki ve ticari sır alanı olmak üzere üçe ayrılmaktadır.

Kişinin Ekonomik Özgürlüğü

Ekonomik yaşam, para ya da para yerine kullanılan çeşitli değerlerin sağlanmasına dair insan aktivitelerine dayanmaktadır. Kişinin hayatını idame ettirmesi, iktisadi etkinliklerini karşılaması için iktisadi varlığını koruması gerekmektedir.

Bu bağlamda, kişilerin bu amaçla çaba ve uğraşta bulunmaları, en temel haklarıdır. Bu sebeple bu hak, kişisel değer kapsamında alınmaktadır.

Kişinin ekonomik varlık ve özgürlüğü, Anayasanın 17. ve 48. Maddelerinde temel bir hak olarak güvence altına alınmıştır. TCK'nin 117. Maddesinde iş ve çalışma özgürlüğüne yönelik ihlal konusu da düzenlenmiştir.

Kişinin sahip olduğu bu haklara yapılan saldırı, kişinin kişilik haklarına da saldırı niteliği taşımaktadır. Bir meslek, sanat ya da ticari etkinliklerde bulunan kişinin aynı meslek sahibi kişilerin rekabetiyle karşılaşması durumunda, rekabet kanuni olarak uygun olduğu sürece, kişi karşı rekabete katlanmalıdır. Bu rekabetin haksız rekabete dönüşmesi durumunda, kişi kanunen korunmalıdır. TTK ve TBK'da bu konu ile ilgili hükümler, kişinin korunması sağlanacaktır. Buna karşın, haksız

[205] Tümerdem, **a.g.e.** , s. 19
[206] Doğan, Pınar Bahar, "Çatışan İki Değer: Haber Verme Hakkı ve Kişilik Hakkı", **Ankara Barosu Dergisi**, Sayı 4, 2014, s. 481.

rekabete dair hükümler, hukuki koruma açısından yetersiz kalması durumunda, kişiliği koruyan genel hükümlere başvurulabilmektedir.

Kişinin Mesleki Şeref ve Haysiyeti

Genel şeref ve haysiyetin özel bir türü olan mesleki şeref ve haysiyet, kişinin belli bir meslek ve sanat ile uğraşı içinde olmasından dolayı, bu meslek ve sanatı icra ederken toplum tarafından ona verilen değerler toplamını ifade eder ve kişinin mesleki şeref ve haysiyetinin çiğnenmesi, onun ekonomik yaşam içindeki varlığına da olumsuz etkiler yapar.[207]

Mesleki şeref ve itibar, kişilik hakları kapsamındadır. Toplum içindeki diğer kişilerin, başkalarının mesleki şeref ve itibarına saygılı olmaları gerekmektedir. Kişinin mesleki şeref ve itibarına saldırı gerçekleşmesi, onun ekonomik hayatını da olumsuz etkilemektedir. Manevi kişisel değerler kapsamında yer alan genel şeref ve haysiyetin yanında, mesleki şeref ve haysiyeti farklı kapsamda değerlendirilmelidir.

Kişinin Mesleki ve Ticari Sır Alanı

Mesleki ve ticari sır; kişinin mesleki ve ticari faaliyeti sebebiyle aynı zamanda sahip olduğu özel bilgileri ifade eder. Diğer bir deyişle, kişinin işleriyle ilgili kayıt ve belgeleri, hesapları, defterleri, çalışma ve işletme usulü ve buna ilişkin teknik bilgileri, müşterileriyle olan ilişkileri bir arada onun mesleki ve ticari sır alanını oluşturur. [208] Kişinin mesleki ve ticari sırlarına dair bilgilerin tetkiki, kopyalanması, kişinin isteği dışında öğrenilmesi kişilik hakkının ihlalini oluşturur. Fakat bankaların, kredi kartı isteyen müşterisinin mesleki ve ticari bilgilerini alması gibi, belli durumlarda, çeşitli bilgilerin toplanması, araştırılması kişilik hakkının ihlaline yol açmamaktadır.

2.2. 5237 SAYILI TCK'YA GÖRE İNTERNET SUÇLARININ KİŞİSEL HAK VE ÖZGÜRLÜKLERE VERDİĞİ ZARARLAR

TCK'nin 244. maddesinin bir ve ikinci fıkralarında klasik mala zarar verme suçunun özel bir şekli düzenlenmiş, 3. fıkrada nitelikli haline, 4. fıkrada ise haksız çıkar sağlanmasına yer verilmiştir. Bilişim sistemlerinin veya verilerin zarar görmesi

[207] Peker Demir, **a.g.e.** , s. 22
[208] Tümerdem, **a.g.e.** , s. 22

halinde, kişinin malvarlığında bir azalma meydana geleceği gibi toplumun 'bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişi etkilendiği bilişim sistemlerinin zarar görmeden işler durumda bulunmasında toplumsal yarar olduğu için yasanın "topluma karşı işlenen suçlar" kısmına alınmıştır. Maddede yazılı suçun oluşması için, bir bilişim sisteminin işleyişine yönelik engelleyici ve zarar verici fiiller bulunmalıdır. Diğer bir anlatımla bilişim sistemine yapılan müdahalelerle sistemin; veri işleme fonksiyonunu yerine getirmesi engellenmeli, fonksiyonunu tamamen veya kısmen kaybetmeli veya verilere zarar verilmelidir.

Maddenin 4. fıkrasında kabul edilen bilişim sistemi aracılığıyla haksız yarar sağlama suçu, bileşik suç olup, 1 ve 2. fıkrada yazılı suçların işlenerek bir çıkar sağlanması halinde gerçekleşecektir. Yani failin, bilişim sisteminin işleyişini engellemesi, bozması, verileri yok etmesi, değiştirmesi, bozması, erişilmez kılınması, sisteme veri yerleştirip veya mevcut verileri başka yere göndermesi sonucu kendisine ya da bir başkasına haksız çıkar sağlaması hallerinde bu suç oluşacaktır.

Ayrıca maddede "başka bir suçu oluşturmaması halinde" denilerek "tali norm" niteliğinde bir düzenleme yapılmıştır. Yani bilişim sistemleri aracılığıyla bir çıkar sağlandığında öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık, zimmet gibi asli (birinci derecede)olan önce uygulanması gereken bir başka suçun oluşup oluşmadığı tartışılmalı, eylem başka bir suçu oluşturmamışsa, o zaman TCK'nin 244/4. maddesi irdelenmelidir.[209]

2.2.1. Kişisel Verilerin Kaydedilmesi Suçu

Kişisel verilerin korunması kapsamında TCK'da alınan ilk suç, kişisel verilerin hukuka aykırı olarak kaydedilmesidir. 5237 sayılı TCK'nin 135. maddesinin 1. fıkrasında, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi suç haline getirilmiştir. 2. fıkrasında ise, kişilerin siyasal, felsefi ve dinsel görüşlerinin, ırksal

[209]Yargıtay Ceza Genel Kurulu E. 2009/11-193, K. 2009/268, 17.11.2009, (Erişim) http://www.turkhukuksitesi.com/serh.php?did=6165 , 13 Aralık 2016.

kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak yerleştirilmesi eylemleri suç tipi olarak düzenlenmiştir. [210]

Maddenin gerekçesinde; *"Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir".* Bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu *"Kişisel Nitelikteki Verilerin Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin ilgili hükümlerine geçerlilik tanınmıştır"* denilmektedir. [211]

Kişisel verilerin kaydedilmesi suçunda korunmakta olan hukuki değer, genellikle özel hayatın dokunulmazlığı kavramıdır. Bu durum, TCK'nin 135. Maddesinde, *"özel hayata ve hayatın gizli alanına karşı suçlar"* başlıklı bölümde düzenlenmiştir. Maddede, kişisel verilerin hukuka aykırı kaydı durumu aranmakta, fakat verilerin sır olarak vasıflandırılması ve sır sahibinin başka kişilerin ulaşımına izin vermemesi durumu aranmamaktadır. Bu sebeple, bu suçun hukuki değerini, sırrın korunması meydana getirmektedir.

TCK Madde 135 dışında 6698 Sayılı Kişisel Verilerin Korunması Kanunu da kişisel verilerin kaydedilmesiyle ilgili olduğu, ilgili kanunun 3. Maddesinde yer alan Tanımlar bölümündeki "Kişisel verilerin işlenmesi" kavramının tanımlanmasından anlaşılmaktadır.

6698 sayılı kanunun 3. Maddesinde kişisel verilerin işlenmesi; *"Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi ifade eder"*[212] denilmektedir.

6698 sayılı *"Kişisel Verilerin Korunması Kanunu"* çerçevesi dâhilinde kalan durumların *"Kişisel Verileri Koruma Kurulu" tarafından herhangi bir şikâyet durumunda incelenerek, nihai sonuca ulaşılacak ve "kişisel verilere ilişkin suçlar*

[210] Değirmenci, **a.g.e.** , s.156–157
[211] 5237 Sayılı Türk Ceza Kanunu Gerekçesi, Madde 135.
[212] ***6698 Kişisel Verilerin Korunması Kanunu***, Madde 3: Tanımlar, (Erişim) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf , 12 Aralık 2016, s. 12301.

bakımından 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun 135 ila 140'ıncı madde hükümleri"[213]nin uygulanması yoluna gidilecektir.

Aynı kanunun 6. Maddesinde de nelerin kişisel veri kabul edildiğine ayrıntılarıyla değinilmektedir. Buna göre;

"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."[214]

Kanunun 6. Maddesinin 3. bendinde belirtilen hususlarda kişisel verilerin kaydedilmesi konusunda, kişinin iznine ihtiyaç duyulmayacağı da ayrıca belirtilmektedir.

2.2.1.1. Suçun Maddi Unsuru

Kişisel verilerin kaydedilmesi suçunun maddi unsurları; hareket, fail, suçun konusu, mağdur, netice şeklinde sıralanabilir. Şimdi sırasıyla bu unsurlar üzerinde durarak, kişisel verilerin kaydedilmesi suçunun maddi unsurlarını yakından tanımak faydalı olacaktır.

2.2.1.1.1. Hareket

Suçun maddi unsurları bakımından incelendiğinde, suçun hareket noktasının, yani kişisel verilerinin hukuka aykırı olarak ele alınmasının, bir sistem ya da veri taşıma aracına hukuk dışı girilebileceği gibi, kişisel bilgilerin el yazısı ya da bilgisayar ile yazılması şeklinde de olabilmektedir.

135. maddede düzenlenen suçun maddi unsuru, kişisel verilerin kaydedilmesidir. Kanunda kaydetmenin ne anlama geldiğine ilişkin bir tanıma yer verilmemiştir. TDK sözlüğüne göre; *"kaydetme"* genel olarak yazmak, bazı önemli noktaları tespit etmek; herhangi bir şeyi bir yere mal etmek, bir şeyin tarih, numara veya adını bir deftere geçirmek; hatırlamak için yazmak, not etmek; sesi veya resmi

[213] ***6698 Kişisel Verilerin Korunması Kanunu,*** Madde 17, s. 12307.
[214] Aynı, Madde 6, s. 12302.

manyetik bant üzerine geçirmek; bilişim açısından ise, elektronik veya sayısal araçlarda bilgiyi korumaya almak anlamlarını taşımaktadır.[215]

135. maddede, suçun işlenme şekli ve alanı sınırlandırılmamıştır. Kişisel verilerin hukuka aykırı olarak her türlü kayıt edilmesi fiili bu suçu oluşturmaktadır. Burada önemli olan, kayıta konu verinin olması, bu verinin gerçek kişiye ait olması, kişisel olması ve hukuka aykırı şekilde kayıt edilmesi gerekmektedir. [216]

6698 sayılı kanuna göre de, kişisel verilerin kaydedilmesinde 6. Madde 3. bendinde belirtilen durumlar dışında, kişinin izni olmaksızın kişiye ait verilerin kaydedilmesi yasaklanmıştır.

2.2.1.1.2. Fail

Kişinin verilerinin kaydedilmesi suçunun failleri bakımından, yasalarda madde metninde herhangi bir özellik belirtilmemiştir. Bu sebeple, bu suçun faili herkes olabilir. Fakat 137. Maddenin 1. Fıkrasının a bendine göre, bu suç kamu görevlisi tarafından işlenirse, ceza yarı oranda artırılır. Gene aynı maddenin b bendine göre, belli bir meslek ve sanatın sağladığı kolaylıktan faydalanması ile işlenmesi durumunda da verilecek ceza yarı oranda artırılacaktır.

2.2.1.1.3. Suçun Konusu

135. Maddenin gerekçesinde, *"Suçun konusu, kişisel verilerdir. Gerçek kişiyle ilgili her türlü bilgi, kişisel veri olarak kabul edilmelidir"* denilmiştir. [217]

Bununla birlikte, aynı maddenin 2. Fıkrasında düzenlenen durumlara ait kişisel veriler de suçun konusunu oluşturmaktadır. Aynı şekilde, maddenin gerekçesinde, verilerin sanal sahafa ya da somut kâğıt üzerinde kayıt edilmesinin fark teşkil etmediği belirtilmiştir. Bu bağlamda, isim, soy isim, kimlik numarası, telefon numarası, resim, ses gibi kişisel veri kapsamında bulunan bilgilerin izinsiz kullanılması kişisel verinin ihlal edilmesini oluşturmaktadır.[218] Kişisel verinin ne

[215] Ketizmen, **a.g.e.** , s. 289
[216] Yaycı, **a.g.e.** , s. 124
[217] Özgenç, İzzet, ***Türk Ceza Kanunu Gazi Şerhi***, Genel Hükümler, Ankara, 2005, s.868.
[218] Türk Ceza Kanunu Madde Gerekçeleri, ***Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar,*** İkinci Kitap, Dokuzuncu Bölüm, Madde 135, (Erişim) www.ceza-bb.adalet.gov.tr/mevzuat/madde**gerekce**.doc , 12 Aralık 2016, s.63.

olduğuyla ilgili tanımlama 6698 Sayılı *"Kişisel Verilerin Korunması Kanunu"* içinde 6. Maddenin birinci fıkrasında açık olarak;

"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."[219]

şeklinde tanımlanmaktadır.

2.2.1.1.4. Mağdur

Kişisel verilerin kaydedilmesi hakkında suçun düzenlendiği TCK'nin 135. Maddesinde, suçun mağduru hakkında herhangi bir nitelik belirtilmemiştir. Bu sebeple, bu suçun mağduru her türlü gerçek kişi olabilir. Fakat tüzel kişiler bu suçun mağduru olamaz. 6698 Sayılı Kanunda mağdur konumunda olacak kişinin açık olarak gerçek kişi olacağı 2. Madde de ifade edilmektedir.

2.2.1.1.5. Netice

Verilerin kaydedilmesi suçunun oluşumu için kişisel verilerin yayınlanması ya da başkasının kullanımına açılması gerekmemekte yalnızca verilerin kaydedilmesi, suçun oluşumu için yeterli olmaktadır. Yani kayıt etme fiilinin aleniyete dökülüp dökülmemesinin bu suçun oluşumuna bir etkisi yoktur. Ayrıca suçun gerçekleşmesi için söz konusu eylemler neticesinde bir zararın meydana gelmesi aranmamakta, kayıt etme işleminin gerçekleşmesi ile suç meydana gelmektedir. Kişisel verilerin bilişim sistemine, veri tasıma aracına veya bir kâğıda işlenmesi ile kaydetme işlemi de gerçekleşmiş olacaktır.[220] 6698 Sayılı Kanunda kişinin açık rızası olmadan ve kanunda belirtilen özel durumların dışında kişisel verilerin her türlü kayıt altına alınması suç teşkil etmekte ve bu suçun ilgili kanun çerçevesinde oluşup oluşmadığını inceleme yetkisi, Kişisel Verileri Koruma Kurumu'na ait bulunmaktadır. Suçun ortaya çıkması durumunda TCK'nin 135 ila 140. Maddelerindeki hükümlerin uygulanacağı, kabahatin ortaya çıkması durumunda da genel olarak para cezasına çarptırma yoluna gidileceği Madde 17 ve Madde 18'den anlaşılmaktadır.[221]

---

[219] ***6698 Kişisel Verilerin Korunması Kanunu,*** Madde 6, s. 12302.
[220] Yaycı, **a.g.e.** , s. 126
[221] ***6698 Kişisel Verilerin Korunması Kanunu,*** Madde 17-18, s. 12307.

2.2.1.2. Suçun Manevi Unsuru

Kişisel verilerin kaydedilmesi suçunun manevi unsurları; kast ve taksir şeklinde iki başlık altında toplanmaktadır.

2.2.1.2.1. Kast

Kişisel verilerin kaydedilmesinde, suçun faili suçu bilerek ve isteyerek işlemelidir. Bu bağlamda, fail, kanunda belirtilmiş olan suçu gerçekleştirirken, hukuka aykırı olarak davrandığını bilmelidir. TCK'nin 135/2. Maddesine göre, "kişilerin siyasi, felsefi veya dinsel görüşlerine ve ırksal kökenlerine" dair verilerin kaydedilmesi bakımından, failin yaptığı fiilin hukuka aykırı olması durumunu bilmesi aranmıştır. Bu bağlamda, kanun koyucunun, kişilerin siyasi, felsefi ya da dini görüşlerine ve ırksal kökenine dair bilgilerin kaydedilmesi hakkında daha hassas davrandığı görülmektedir.

2.2.1.2.2. Taksir

Kanunumuzda, bu suçun failinin bilmek ve istemek suretiyle işlemesinin aranmasından dolayı, bu suçun taksir ile işlenmesi olanaksızdır.

2.2.1.3. Hukuka Aykırılık Unsuru

Kişisel verilerin kaydedilmesinde, mağdurun rıza sahibi olması, kaydedilme eylemini hukuka uygun duruma getirecektir. Mağdurun rızası kapsamında oluşan hukuka uygun olma sebebinde, rızanın suçun işlendiğinde bulunuyor olması gerekmektedir. Bunun dışında, rızanın açık ya da zımni olarak verilmesi şartına bakılmaz.

Kanunun verdiği yetkiye dayanılarak kişisel verilerin kaydedilmesi diğer bir hukuka uygunluk sebebidir. 5237 sayılı TCK'nin 135. Maddesinin gerekçesinde *"bu suçun oluşabilmesi için kişisel verilerin hukuka aykırı bir şekilde kayda alınması gerekir. Kişinin rızası ile kendisi ile ilgili verilerin kayda alınmasının suç oluşturmayacağı muhakkaktır. Belirli nitelikteki kişisel verilerin kayda alınması kanun hükmünün gereği olarak yapılmaktadır. Bu bakımdan, çeşitli kamu kurumlarında verilen kamu hizmetinin gereği olarak kişilerle ilgili bazı bilgiler ilgili*

kanun hükümlerine istinaden kayda alınmaktadır. Bu durumda söz konusu suç oluşmayacaktır" denilmektedir. [222]

5217 sayılı CMK (Ceza Muhakemesi Kanunu)'nun 134. Maddesinin 3. Fıkrasının, *"bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır"* hükmüne göre, bu veriler içine kimi zaman, kişisel veriler de dâhil olabilecektir.

2.2.1.4. Suçun Özel Görünüş Şekilleri

Kişisel verilerin kaydedilmesi suçunun özel görünüş şekilleri; teşebbüs, iştirak ve içtima başlıklarından oluşmaktadır.

2.2.1.4.1. Teşebbüs

TCK'nin 135. Maddesinde bulunan kişisel verilerin kaydı suçunun, teşebbüs durumunda kalması olanaklıdır. Suçun failinin suçu icra etmesine başladıktan sonra, bu davranışların yarıda kalmasında da teşebbüs durumunda da gerçekleşebilmektedir. Çünkü kişisel verilerin kaydı suçu bakımından bir zarar gelmesi durumu aranmamakta, fiilin gerçekleşmesi ile suç tamamlanmaktadır.

2.2.1.4.2. İştirak

TCK'nin 37, 38, 39 ve 40. Maddelerinde suça katılımla ilgili genel hükümler düzenlenmiştir ve bu bağlamda ortaya çıkan durumlar, kişisel verilerin kaydedilmesi suçunda uygulanacaktır. Bunun sebebi, suça iştirak bakımından, kişisel verilerin kaydedilmesi suçunda böyle bir özellik bulunmamasıdır. Fakat suça katılanların kamu görevlisi olması veya bu konuyla ilgili bir meslek ya da sanat sahibi olması durumunda, bu kişilere ceza TCK'nin 137. Maddesine göre arttırılarak verilmektedir.

2.2.1.4.3. İçtima

TCK'nin 135. Maddesinde belirtilen suçun işlenmesi için, TCK'nin 243. Maddesinde belirtilen hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçunun da işlenmesi durumunda, sadece TCK'nin 135. Maddesinde belirtilen

[222] Özgenç, **a.g.e.** , s.867

ceza, faile verilecektir. Bunun sebebi, fikri içtimaı düzenleyen TCK'nin 44. Maddesine göre fail, en ağır cezayı gerektiren suç kapsamında cezalandırılır.

2.2.1.5. Suça Etki Eden Sebepler

TCK'nin 135. Maddesinde belirtilen suça etki eden sebepler, TCK'nin 137. Maddesinde öngörülmüştür. Belirtilen durumlardan birinin gerçekleşmesi durumunda, suçun failine verilen cezanın yarı oranda artırılacağı belirtilmiştir. 137. Maddenin a bendinde, suçun kamu görevlisi tarafından görevini kötüye kullanması ile işlenmesi durumunda faile verilecek cezanın artırılacağı belirtilmiştir. 137. Maddenin b bendinde, belli bir meslek ve zanaatın sağlamış olduğu kolaylıktan faydalanarak bu suçun işlenmesi durumunda, failin cezasının artırılacağı belirtilmiştir.

2.2.1.6. Yaptırım

Yasada, kişisel verilerin kaydedilmesi suçunu gerçekleştirenler hakkında, suçun cezasını bir yıldan üç yıla kadar hapis cezası olarak belirtilmiştir. TCK'nin 140. Maddesine göre, bu suç işlenerek, tüzel kişilere hukuka aykırı fayda sağlanması durumunda, TCK'nin 60. Maddesine göre, bu maddede gösterilen kendilerine dair güvenlik önlemlerinin uygulanacağı belirtilmiştir.

2.2.2. Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu

Günümüzde internet ve sosyal medyanın kullanımının artması ile hemen hemen tüm kullanıcıların, kendi kişisel bilgileri, kendi istekleri ile internette bazı sitelerde bulunmaktadır. Bu verilerin yasa dışı olarak üçüncü kişilere verilmesi ya da ele geçirilmesinin önlenmesi için kişisel verilerin hukuka aykırı bir şekilde başkasına verilmesi ya da ele geçirilmesi ayrı bir suç olarak TCK'nin 136. Maddesinde düzenlenmiştir.

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunda korunan hukuki değer, kişilerin özel hayatının dokunulmazlığıdır. TCK'nin 136. Maddesinde

düzenlenen kişisel verilerin kaydedilmesinde korunan hukuki değer ile ilgili açıklamalar, bu suç için de geçerlidir.

2.2.2.1.Suçun Maddi Unsuru

Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi unsurları; hareket, fail, suçun konusu, mağdur ve netice alt başlıklarından oluşmaktadır.

2.2.2.1.1. Hareket

Kişisel verileri hukuka aykırı olarak üçüncü kişilere verilmesi ya da üçüncü kişiler tarafından ele geçirilme suçunda, verilerin kaydedilme türü ne olursa olsun, aşağıda belirtilen durumların gerçekleşmesi ile suç oluşmuş olacaktır. Bu suç tipinde eylemlerin biri ya da birkaçı gerçekleşmesi ile bu suç işlenmiş olarak sayılacak ve faile tek bir suçun cezası verilecektir.

2.2.2.1.1.1. Kişisel Verileri Başkasına Verme Eylemi

Yazılı verilerin **e**lden veya posta ile başka kişilere verilmesi ya da sanal sahada bulunan verilerin bir disk ya da cd ile veya internet üzerinden başka kişilere verilmesi kişisel verileri başkasına verme suçunu teşkil eden durumlardır.

2.2.2.1.1.2. Kişisel Verileri Yayma Eylemi

Temel olarak kişisel verileri verme ile yayma eylemleri birbirine benzer niteliktedir. Ayrıca, verme fiili, yayma seviyesinde olmayan bir fiildir ve kişisel verileri yayma fiili, verme durumundan daha ileri seviyededir. Başka bir ifade ile yayma durumu, birden fazla kişiye, kişisel verilerin aktarılmasıdır. Kişisel verilerin yazılı olarak ya da sanal sahada erişilebilir kılarak kişisel verileri yayma eylemi gerçekleşmektedir.

2.2.2.1.1.3 Kişisel Verileri Ele Geçirme Eylemi

Kişisel verileri ele geçirme, kişisel verilerin bulunduğu belge ya da bilişim sistemine girilerek, verilerin ortamdan alınması şekliyle yapılmaktadır.

2.2.2.1.2. Fail

TCK'nin ilgili maddesinde fail açısından bir nitelik belirtilmemiştir. Bu bakımdan suçun faili herkes olabilmektedir. Fakat 137/1. Maddenin a bendine göre, bu suçların, kamu görevlisi tarafından, görevini kötüye kullanma şeklinde işlenmesi durumunda, verilecek ceza yarı oranda arttırılmaktadır.

Aynı maddenin b bendine göre, belli bir meslek ya da zanaatın sağlamış olduğu kolaylıktan faydalanarak işlenmesi durumunda da, verilecek ceza yarı oranda artırılmaktadır.

2.2.2.1.3. Suçun Konusu

Bu suçun konusunu, kişisel veriler oluşturmakta olup, TCK'nin 135. Maddesinde düzenlenmiş olan kişisel verileri kaydetme suçunun konusu hakkında yapılan izahat, bu suç tipi ile aynıdır.

2.2.2.1.4. Mağdur

TCK'nin ilgili maddesinde mağdur ile ilgili bir özellik belirtilmemiştir. Bu bağlamda, herkes bu suçun mağduru olabilir.

2.2.2.1.5. Netice

Bu suçun oluşması bakımından, işlenen suçun neticesinde bir zarar aranmamaktadır. Önceki bölümlerde belirtilen durumların gerçekleşmesi, suçun oluşması için yeterlidir. Kişisel verileri başkasına verme ve ele geçirme eylemlerinde, aleni olarak bir ortam gerekli değildir. Ancak yayma eyleminde, yaymaya konu olan verinin, aleni bir şekilde olması söz konusudur.

2.2.2.2. Suçun Manevi Unsuru

Kast ve taksir, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunda, suçun maddi unsurlarını oluşturmaktadır.

2.2.2.2.1. Kast

Suçun failinin bilerek ve isteyerek davranması, bu suçun gerçekleşmesi için kâfidir. Suçun faili, yasada belirtilen fiili gerçekleştirirken, davranışın hukuka aykırı olduğunu bilmeli ve gerçekleştirdiği fiil ve sonuçlarını isteyerek yapmalıdır.

2.2.2.2.2. Taksir

Yasada, bu suçun kasıtlı olarak işlenmesi arandığı için, taksir ile işlenmesi olanaklı olmamaktadır.

2.2.2.3. Hukuka Aykırılık Unsuru

Kişisel verilerin ele geçirilmesi veya verilmesi suçunda, mağdurun rızası ya da kanunla yetki verilmesi, suçu hukuka uygun duruma getirecektir. Bir kişinin, veri sahibi veya ilgisinin iznine dayanarak, verileri vermesi, yayması ya da ele geçirmesi veya görevli bir kişinin, kanuna dayanarak aynı fiilleri gerçekleştirmesi halinde suç oluşmayacaktır.

2.2.2.4. Suçun Özel Görünüş Şekilleri

Teşebbüs, iştirak ve içtima, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunda, suçun özel görünüş şekillerini oluşturmaktadır.

2.2.2.4.1. Teşebbüs

TCK'nin 136. Maddesine göre, suçun, teşebbüs durumunda kalması mümkündür. Suçun failinin suçun icrasına başlamasından sonra, bu hareketlerin yarıda kalması durumunda, teşebbüs durumu gerçekleşmektedir. Çünkü bu suç için

bir zarar oluşması aranmamakta, belirtilen fiilin gerçekleşmesi durumunda da suç tamamlanmış olmaktadır.

2.2.2.4.2. İştirak

TCK'nin 37., 38., 39. ve 40. maddelerinde suça iştirake dair genel hükümler düzenlenmiş, bu bağlamda ortaya çıkan durumlar bu suç için de uygulanabilmektedir. Çünkü suça iştirak bakımından bu suçta bir nitelik söz konusu değildir.

Fakat suça iştirak edenlerin, kamu görevlisi unvanına sahip olması ya da konu ile ilgili meslek ya da zanaat sahibi olması durumunda, bu kişilere TCK'nin 137. Maddesine göre, ceza artırılarak verilecektir.

2.2.2.4.3. İçtima

Failin, kişisel verileri hukuka aykırı üçüncü kişilere vermesi ya da ele geçirmesi suçunu, aynı suçu işleme kararı bağlamında, birden çok işlemesi ve işlenen suçların mağdurunun aynı kişi olmasında, TCK'nin 43. Maddesinde düzenlenmiş zincirleme suç oluşturacaktır. Bu durumda, faile, bu suçların hepsinden teker teker değil, ceza bir defa verilmektedir, ancak cezanın oranı artmaktadır. Aksi durumda, her bir suç bağımsız bir suç olma niteliği taşır ve olayda cezaların içtimaı hükümleri uygulanmaktadır.

TCK'nin 136. Maddesinde belirtilmiş olan suçun işlenmesi için, TCK'nin 243. Maddesinde belirtilen yasa dışı olarak bilişim sistemine girme ya da sistemde kalma suçunun da işlenmesi durumunda, suç failine sadece TCK'nin 136. Maddesinde belirtilen ceza uygulanacaktır. Bunun sebebi, fikri içtimaının düzenlendiği TCK'nin 44. Maddesine göre, fail, en ağır cezayı gerektiren suçtan dolayı ceza alır. Örnek olarak, failin düşmanlık beslediği bir kişinin özel hayatını yaymak için, bu kişi hakkında olan verileri ilk olarak kaydeder. Bu durumda, fail 135. ve 136. Maddede geçen kişisel verilerin kaydedilmesi ve verilerin hukuka aykırı olarak verilmesi ya da ele geçirme suçunu işlemiş olur. Bu durumda, TCK'nin 44. Maddesi uyarınca, fail, iki suç içinde en ağır cezayı gerektiren 136. Maddedeki suça göre ceza alır.

2.2.2.5. Suça Etki Eden Sebepler

TCK'nin 136. Maddesinde bulunan suça etki nedenler, 137. Maddede belirtilmiştir. Bu durumlardan birinin oluşması durumunda, faile verilecek olan ceza yarı oranda artırılır.

TCK'nin 137. Maddesinin a bendinde suçun kamu görevlisi tarafından ve görevinin verdiği yetkinin kötü kullanımı ile gerçekleşmesi durumunda, failin cezası artırılarak verileceği belirtilmiştir.

Aynı maddenin b bendine göre, belli bir meslek ve zanaatın sağladığı kolaylıktan faydalanarak suçun işlenmesi durumunda faile ceza yine artırılarak verilir.

2.2.2.6. Yaptırım

Yasada, kişisel verilen hukuk dışı olarak verme ya da ele geçirme suçunu işleyenler hakkında, suçun cezası bir yıldan dört yıla kadar hapis cezası verileceği belirtilmiştir.

TCK'nin 140. Maddesine göre, bu suç sonucu olarak tüzel kişilerin hukuk dışı yarar sağlaması durumunda TCK'nin 60. maddesine göre kendilerine özgü güvenlik tedbirleri uygulanır.

2.2.3. Verilerin Yok Edilmemesi Suçu

TCK'nin 138. Maddesine göre, kanuni sürenin dolmasına rağmen, kişisel verileri sistem içinde yok etmekle vazifeli kişilerin bu görevlerini yapmamaları, suç tipi olarak düzenlenmiştir. Fakat ilk olarak failin, bu görevle yükümlü olup olmadığı anlaşılmalıdır. Bununla birlikte suç açısından, yasaların belirlediği sürenin geçmiş olması da gerekmektedir.

Bu suçla, kamu idaresine karşı duyulan güven koruma altına alınmaktadır. Bunun sebebi, yasada verileri silmek ile görevlendirilen kişi bunu, kamu görevi olarak yapmaktadır.

Bu suçla korunmaya çalışılan bir diğer unsur, genelde kişilerin özel hayatının dokunulmazlığıdır. Çünkü yasa koyucu, bu suçu diğer suçlar ile birlikte TCK'nin ‘’özel hayata ve hayatın gizli alanına karşı suçlar ‘’ bölümünde yer almaktadır.

2.2.3.1. Suçun Maddi Unsurları

Bu bölümde suçun maddi unsurlarından hareket, suçun konusu, mağdur, netice unsurları incelenecektir.

2.2.3.1.1. Hareket

Bu suç, ihmali bir hareketle gerçekleştirilmektedir. İhmal, davranış normlarıyla kişiye belli bir icrai davranışta bulunma yükümlülüğünün tahmil edildiği hallerde, kişinin yükümlülüğü yerine getirmemesidir. İhmali suçlarda söz konusu olan fiil ise, belli bir davranışın gerçekleştirilmemesi, belli bir davranışta bulunulmamasıdır. [223]

Aynı biçimde TCK'nin 138. Maddesine göre, verilerin yok edilmemesi suçu da failin, verilerin yok edilmesi görevini ifa etmemesiyle işlenebilmektedir. Örnek olarak, CMK'nın 137. Maddesinin 3. Fıkrasında, 135. Madde kapsamında verilen kararın, uygulanması esnasında, şüpheli hakkında kovuşturmaya yer olmadığı kararının verilmesi ya da aynı maddenin 1. Fıkrasına göre, hâkim onayının olmaması durumunda, uygulamaya Cumhuriyet savcısı tarafından son verilir. Bu durumda, yapılan tespit ve dinlemeye dair kayıtlar, savcı kontrolü altında en geç on gün içinde yok edilir. Bu bağlamda tespit ve kayıtların yok edilmemesi durumunda 138. Maddede belirtilen suç gerçekleşir.

2.2.3.1.2. Fail

Bu suçun faili, verileri yok etmekle görevli kişidir. Fail, kamu görevlisi olmak zorunda değildir. Bu suçta, inceleme konusu suç tipinin özel türde, kendine özgü bir görevi ihmal suçu olmasından dolayı failin kamu görevlisi olma durumu bulunmamaktadır.

[223] Özgenç, **a. g. e.** , s. 231

2.2.3.1.3. Suçun Konusu

Verileri yok etmeme suçunun konusunu kişisel veriler oluşturur. TCK'nin 135. Maddesinde bulunan suç tipinin konusu ile inceleme konusu suç tipinin konusu birdir. Bu sebeple 135. Maddede konu bakımından yapılan açıklamalar, bu suç için de geçerlidir.

2.2.3.1.4. Mağdur

Yasada, mağdur bakımından bir nitelik bulunmaktadır. Bu nedenle herkes bu suçun mağduru olma potansiyeline sahiptir. Fakat genelde bu suçun mağduru toplum olmaktadır. Bunun yanı sıra, kendisine ait verileri yok edilmeyen kişi, suçtan zarar gören kişi olmaktadır ve kovuşturma safhasında davaya katılma isteğinde bulunabilir.

2.2.3.1.5. Netice

Bu suçta, yasanın belirlemiş olduğu sürenin sonunda veriler yok edilmemişse, suç gerçekleşmiş olmaktadır. Bununla birlikte, verileri yok etmekle vazifeli kişinin, bu işi gerçekleştirmeyeceğini aleni olarak söylemesi durumunda da, sürenin geçmesine gerek kalmadan suç gerçekleşir.

2.2.3.2. Suçun Manevi Unsuru

Kast ve taksir, verilerin yok edilmesi suçunda, suçun manevi unsurlarını oluşturmaktadır.

2.2.3.2.1. Kast

Bu suçun faili, yasada belirtilmiş fiili gerçekleştirirken, yasaya aykırı davrandığını bilmelidir. Fail, suçun yasal tanımındaki unsurları bilerek ve isteyerek gerçekleştirmelidir.

2.2.3.2.2. Taksir

Yasada bu suçun, kasten işlenme durumu arandığı için, taksir ile işlenmesi olası değildir.

2.2.3.3. Hukuka Aykırılık Unsuru

Bu suç tipinde, hem mağdurun rızası hem de yasadan kaynaklanan bir hukuki uygunluk sebebi bulunmaz. Çünkü bu suçun mağduru kamu düzenidir. Fakat mücbir sebep bakımından, bu suç için bir hukuki uygunluk sebebi oluşmaktadır.

2.2.3.4. Suçun Özel Görünüş Şekilleri

Teşebbüs, iştirak ve içtima, verilerin yok edilmesi suçunda, suçun özel görünüş şekillerini oluşturmaktadır.

2.2.3.4.1. Teşebbüs

Bu suç türü, ihmal ile işlenebileceğinden, bu suçta teşebbüs hali olası değildir.

2.2.3.4.2. İştirak

TCK'nin 37, 38, 39 ve 40. Maddelerinde, suça iştirake dair genel hükümler bulunmakta olup, bu bağlamda beliren durumlar, bu suç için de uygulanabilmektedir. Çünkü suça iştirak açısından, bu suçta bir özellik bulunması olası değildir.

2.2.3.4.3. İçtima

Suçun failinin, verileri yok etmeme suçunu, aynı suçu işleme kararı içinde, birden çok işlemesi ve işlenen suçların mağdurunun tek bir kişi olması durumunda, TCK'nin 43. Maddesinde belirtilen zincirleme suç oluşmaktadır. Bu durumda, faile bu suçların her biri için teker teker değil, ceza oranı artırılarak tek bir ceza verilmektedir.

2.2.3.5. Yaptırım

Yasada bu suçun failleri için belirtilen ceza, bir yıl ile iki yıla kadar hapistir. TCK'nin 140. Maddesine göre bu suçun işlenmesiyle tüzel kişilerin hukuk dışı yarar sağlanması durumunda, TCK'nin 60. Maddesine göre, kendilerine ait güvenlik önlemleri uygulanacaktır.

2.2.4 Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu İle Verilerin Yok Edilmesi veya Değiştirilmesi Suçu

TCK'nin 244. Maddesinin 1. ve 2. Fıkralarında bilişim sistemine veya verilere zarar verme eylemleri ayrı suç tipleri olarak düzenlenmişlerdir. Birinci fıkrada "*bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması"* , ikinci fıkrada ise "*bilişim sistemindeki verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi"* eylemleri suç haline getirilmiştir. [224]

Söz konusu suç tipleri her ne kadar yasanın aynı maddesinde düzenlenmişlerse de bu durum benzer ancak farklı suç tipleri olduğu gerçeğini değiştirmemektedir, aynı maddede farklı suç tiplerinin düzenlenmesi yöntemine TCK'nin diğer maddelerinde de rastlanılmaktadır. [225]

Bu suçla, Avrupa Siber Suç Sözleşmesinin 4. Maddesinde düzenlenen '' verileri etkileme '' ve 5. Maddesinde düzenlenen '' sisteme etki etme '' maddelerine paralellik sağlanmaya çalışılmıştır. [226]

Bu suçlardan 244 / 1, 765 sayılı ETCK (Eski Türk Ceza Kanunu)'nın 525 b/1 maddesinde düzenlenen '' sisteme veya veri işleme zarar vermek suçunun '' yerine geçmek üzere, 244 / 2 ise kısmen 525 a/2'nin yerine geçmek üzere yer almaktadır. Ancak öğretide haklı olarak belirtildiği üzere 244 / 1' deki düzenlemenin 525 b / 1'deki düzenlemenin bire bir karşılığı olduğunu söylemek mümkün değildir. [227]

Günümüzün modern yaşam düzeninin ana konularını oluşturan ekonomik, sağlık, eğitim, bilimsel araştırmalar, idare, savunma gibi pek çok yaşamsal alanda

---

[224] Dülger, Murat Volkan, ***Bilişim Suçları ve İnternet İletişim Hukuku***, Seçkin Yayınları, 2012, s. 379.
[225] Dülger, 2012, **a.g.e.** , s. 380
[226] Erdoğan, Yavuz, ***Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)***, Legal Yayıncılık, İstanbul, 2012, s. 180
[227] Erdoğan, **a.g.e.** , s. 179

bilişim sistemleri vazgeçilmez araçlar olmuşlar, bu alanların pek çok yerinde geri dönülemez şekilde insanların yerini almışlardır. Bu nedenle bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin kendisinin ya da içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin geçici süreyle de olsa çalışamaması çok büyük zararlara yol açabilmektedir. Özellikle çok iyi üretilmiş bilişim virüsleri, kurtçuklar, Truva atları gibi zarar verici yazılımlar bilişim ağlarında geometrik hızla yayılarak bunları hazırlayan ve verilere zarar vermek amacıyla sanal alana sokan faillerin dahi öngördüğünden daha fazla zarara yol açabilmektedir. Yasa koyucu da bu büyük tehlikeyi öngörerek sisteme ve / veya verilere zarar verme eylemlerini bu maddeyle suç haline getirmiştir. [228]

Bu düzenleme ile bilişim sisteminin her nasıl olursa olsun çalışmasının engellenmesi, sistemin bozulması ve verilere zarar verilmesi ya da erişilmez hale getirilmesi cezalandırılmak istenmektedir. Maddenin gerekçesinde de, bu maddeyle bilişim sistemlerine yöneltilen ızrar (mala zarar verme) eylemlerinin ayrı bir suç haline getirildiği belirtilmektedir. Ayrıca yine maddenin gerekçesinde, yapılan düzenleme ile *"aracın fizik varlığı ve işlenmesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır"* denilerek bilişim sisteminin somut ve soyut bütün unsurlarının bu suçun konusu oluşturacağı ifade edilmektedir. Maddenin gerekçesinde de *"özel bir ızrar eylemi"* denilmek suretiyle bilişim sisteminin çalışmasını engellemeye yönelik eylemler kastedilmektedir. [229]

2.2.4.1. Suçlarla Korunan Hukuksal Değerler

Yasa koyucu bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçuyla bilişim sistemlerinin yalnızca veri ve yazılımlardan oluşan soyut unsurlarını koruma altına almamış aynı zamanda bilişim sistemlerinin somut unsuru olan donanım kısmını da koruma altına almıştır. Bu 1nedenle bu suçlarla korunan hukuksal değerler karma bir nitelik göstermektedir. [230]

Her iki suç tipi birlikte değerlendirildiğinde bu suçlarla korunan hukuksal değerin genel olarak, bilişim sistemi ve / veya bilişim sisteminin içerdiği veriler

[228] Dülger, 2012, **a.g.e.** ,s. 380
[229] Karagülmez, **a.g.e.** , s. 209
[230] Dülger, 2012, **a.g.e.** , s. 381

üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma bilgi vb. değerlere herhangi bir engel, arıza ya fa gecikme olmadan ulaşması ve kullanmasındaki çıkarı olduğu görülmektedir. Bir başka deyişle hem bilişim sisteminin hem de bu sistem içerisinde yer alan verilerin veya diğer unsurların sağlam bir şekilde çalışabilirliği korunmaktadır. [231]

Ancak bazı durumlarda failin hareketinin her iki fıkradaki suç tipine de girmesi halinde – örneğin değiştirilen verinin sistemi de bozması ya da engellemesi durumunda olduğu gibi – failin kastının belirlenebilmesi için bu suçlarla korunan hukuksal değerlerin de ayrı ayrı ortaya konulması gerekmektedir. [232]

Öğretide ise 1. Fıkrada yer alan suçla korunan hukuksal değerin ne olduğu konusunda çok sayıda farklı görüş olmakla beraber bunlar birbirine yakın görüşlerdir. Buna göre sistemin doğru şekilde faaliyetine devam etmesi ve haberleşme özgürlüğü, malvarlığı hakkı ve bilişim sistemlerinin zarar görmeden işler halde bulundurulmasındaki toplumsal yarar, mülkiyet hakkı ve teknolojik gelişim özgürlüğü, bilişim sisteminin güvenliği ile mülkiyet hakkı, veri güvenliği, bilişim sistem ve sistemin güvenliği, sistemin işleyişi ve özellikle donanımsal yanı, mülkiyet hakkı ve buna bağlı olarak toplumun menfaati, sistemin toplum nazarındaki güvenilirliği ve toplumun menfaatleri ile bilişim sisteminin güvenliği bu suçla korunan hukuksal değerler olarak gösterilmektedir. [233]

244. maddenin 2. Fıkrasında ise *"veri"* suçun konusunu oluşturmakta ve verilerin varlığının ortadan kaldırılmasına ve verilere erişimin engellenmesine yönelik hareketler suç haline getirilmektedir. Ayrıca bir bilişim sisteminde yer alan her veri, sistemin işleyişini bozmayacağı ve engelleyemeyeceği için 1. Fıkradaki suça nazaran daha az ceza ile cezalandırılmaktadır. Dolayısıyla bu suç tipiyle de verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliği korunmaktadır. Buna göre 2. Fıkrada korunan veriler bilişim sisteminin işleyişine ilişkin veriler olmayıp sistemin içerisinde bulunan, ancak sistemin işleyişine etkisi olmayan verilerdir. Zira bilişim sisteminin işleyişini etkileyecek verilere müdahale halinde 1. Fıkranın

[231] Karagülmez, **a.g.e.** , s. 211.
[232] Dülger, 2012, **a.g.e.**, s. 382.
[233] Aynı, s. 382.

uygulanması gerekecektir. Bir başka deyişle, 2. Fıkra ile sistemin içinde yer alan ancak sistemin yapı taşı olmayan veriler korunmaktadır. [234]

TCK'nin 244. Maddesinin 2. Fıkrasındaki suç tipiyle korunan hukuksal değer konusunda belirtmek istenilen bir diğer husus iste TCK'nin 135 ve 136. Maddelerindeki benzer eylemleri içeren suç tipleriyle arasındaki farkın özellikle korunan hukuksal değerlerden kaynaklandığıdır. 244 / 2'de yukarıdan belirtildiği üzere verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliği korunmakta iken, 135 ve 136. Maddelerde kişisel verilerin bizzat kendisi korunmaktadır. Buradan hareketle 244 /2'de ayrım yapılmaksızın her türlü veri suçun konusunu oluşturabilmektedir, 135 ve 136'da ise yalnızca kişisel veriler suçun konusunu oluşturmaktadır. Öte yandan 135 ve 136'da her türlü yer ve araçta kayıtlı kişisel veriler suçun konusunu oluşturuyor iken, 244 / 2'de yalnızca bilişim sistemlerinde yer alan veriler suçun konusu oluşturmaktadır. [235]

244. maddenin 1. ve 2. Fıkrasında düzenlenen suçlarla paralel olan AKSSS (Avrupa Konseyi Siber Suçlar Sözleşmesi)'nin 4. ve 5. Maddelerine ilişkin açıklayıcı raporda, 4. Maddede korunan hukuksal değerin bilişim sisteminde yer alan verilere veya yazılımlara zarar verilmesini, veri ve yazılımların bozulmasını, zarar görmesini engellemek, böylelikle bunların doğru ve işlevsel olarak çalışmalarını sağlamak olduğu ifade edilmektedir. AKSSS'nin 5. Maddesinde korunan hukuksal değerin ise temel olarak bilişim sistemlerine karşı gerçekleştirilen saldırıların önlenmesi, bilişim sistemlerinin sağlıklı şekilde kullanımının sağlanması ve buna yönelecek haksız davranışlara engel olunması olduğu belirtilmektedir. Böylelikle bilişim sistemi kullanıcılarının bu sistemleri işlevsel bir şekilde kullanmaya yönelik hakları korunmaktadır. [236]

Failin kastının yalnızca kişinin malvarlığına zarar vermek olduğu ve bu nedenle örneğin kişinin bilgisayarını parçaladığı durumda TCK'nin 244. Maddesinin 1. Fıkrası uygulanmayacak, bu eyleme uygun suç tipi olan "mala zarar verme suçunun" düzenlendiği TCK'nin 151. Maddesi uygulanacaktır. Ancak failin kastının kişinin malvarlığına zarar vermek değil bilişim sisteminin donanım kısmına zarar

[234] Erdoğan, **a.g.e.** , s. 215.
[235] Erdoğan, **a.g.e.** , s. 208
[236] Dülger, 2012, **a.g.e.**, s. 383

vermek ve dolayısıyla bilişim sisteminin çalışmasını engellemek olduğu durumlarda ise fail inceleme konusu suç tipi nedeniyle cezalandırılacaktır. [237]

2.2.4.2. Tipiklik

Bu bölümde tipikliğin maddi ve manevi unsurları incelenecektir.

2.2.4.2.1. Tipikliğin maddi unsurları

Tipikliğin maddi unsurları kapsamında fail, mağdur, suçların konusu, eylem ve suçun nitelikli hali incelenecektir.

2.2.4.2.1.1. Fail

Herkes bu suçların faili olabilir, yasa maddesinde bu açıdan bir özellik belirtilmemiştir. Bu suçlar ile hem bir bütün halinde bilişim sistemine hem de verilere zarar verilmesi eylemlerini suç olarak düzenlemektedir. Bu nedenle kişinin, başkasının haklarına zarar vermeksizin herhangi bir bilişim sisteminde bulunan kendisine ait verilere zarar vermesi suç oluşturmayacağından failin tespit edilmesi önem taşımaktadır. Ancak failin kendisine ait olmayan bir bilişim sisteminde bulunan kendisine ait olan verileri yok etmek ya da erişilmez kılmak için sistemin işleyişini bozması ya da engel olması halinde ise her ne kadar 244. Maddenin 2. Fıkrasındaki suç gerçekleşmeyecek olsa da 1. Fıkradaki suç gerçekleşmiş olacaktır.[238]

Bu suçların failinin tespiti için, eğer eylem bilişim sistemine yönelik olarak gerçekleştirilmişse sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelik gerçekleştirilmişse bu verilerin, hem bilişim sistemine hem de verilere karşı gerçekleştirilmişse her ikisinin ayrı ayrı mülkiyeti, kullanım ve tasarruf haklarının kime ait olduğu ve zararı kimin meydana getirdiği açıkça ortaya konulmalıdır. [239]

Zarara uğrayan bilişim sistemi ya da veri taşıma aracının malikiyle verilerin maliki her zaman aynı kişi olmayabilir. Bilişim sisteminin veya veri taşıma aracının malikinin, bunların tamamının veya bir kısmının kullanım hakkını devretmesi

[237] Dülger, 2012, **a.g.e.**, s. 384
[238] Dülger, 2012, **a.g.e.** , s. 384
[239] Dülger, 2012, **a.g.e.** , s. 384

mümkündür. Bu durumda sistemin ya da aracın maliki, içindeki verilerin maliki değildir, bu olasılıkla başkasının verisine zarar verebilmek için kişinin kendi sistemine ya da veri taşıma aracına zarar vermesi durumunda fail, bizatihi bilişim sisteminin ya da veri taşıma aracının maliki olacaktır. [240]

2.2.4.2.1.2. Mağdur

Bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunda herkes suçun mağduru olabilir, suç tipleri bu açıdan bir özellik göstermemektedir. Yukarıda suçlarla korunan hukuksal değerler ve fail konularında yapılan açıklamalar ışığında ifade edilmelidir ki bu suçların mağduru olmak için mutlaka bilişim sisteminin ya da zarara uğrayan verilerin maliki veya zilyedi olunması gerekmemektedir. [241]

Bu suçları oluşturan hareketlerin gerçekleştirilmesi sonucunda; bilişim sistemine ve / veya verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşılmasında ve kullanılmasında çıkarı bulunan ve bilişim sistemi ve / veya veriler üzerinde tasarruf yetkisi bulunan kişi bu suçun mağduru olacaktır.

Ayrıca belirtilmelidir ki bilişim sistemine, verilere veya veri işleme zarar veren kişinin bilişim sisteminin maliki veya kullanım hakkı sahibi olmasına göre suçun mağduru da değişecektir. [242]

2.2.4.2.1.3. Suçların Konusu

Bilişim sisteminin işleyişinin engellenmesi ve bozulması suçunun konusunu bilişim sistemi oluştururken, verilerin yok edilmesi veya değiştirilmesi suçunun konusunu ise bilişim sistemlerinde yer alan veriler oluşturmaktadır. Her ne kadar yasa metninde ayrıca yazılımlar belirtilmemişse de, yazılımların verilerden meydana gelen bir bütün olduğu kabul edildiğinden 244/2'deki suçun konusunu yasa metninde ayrıca belirtilmese de bir bütün halinde yazılımlar da oluşturmaktadır. [243]

[240] Dülger, 2012, **a.g.e.** , s. 384.
[241] Aynı.
[242] Aynı, s. 385
[243] Aynı.

2.2.4.2.1.4. Eylem

Bu suçların eylem unsurları 244. Maddenin 1. Fıkrasında "bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması", 2. Fıkrada ise "bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi" şeklinde tanımlanmıştır. Buna göre her iki suç tipi de seçimlik hareketli olarak düzenlenmiştir. Ayrıca her iki suç tipinde yer alan hareketler de ayrı ayrı yalnızca suçun gerçekleşmesi için Gerekli olan neticeler gösterilmek suretiyle serbest hareketli olarak düzenlenmişlerdir. [244]

Bu suçların eylem unsurları 244. Maddenin 1. Fıkrasında "bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması", 2. Fıkrada ise "bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi" şeklinde tanımlanmıştır. Buna göre her iki suç tipi de seçimlik hareketli olarak düzenlenmiştir. Ayrıca her iki suç tipinde yer alan hareketler de ayrı ayrı yalnızca suçun gerçekleşmesi için gerekli olan neticeler gösterilmek suretiyle serbest hareketli olarak düzenlenmişlerdir.

2.2.4.2.1.4.1. Hareket

Bu suçun gerçekleştirilmesi değişik şekillerde olabilmektedir. Bunları;

- Bilişim sisteminin işleyişini engellemek
- Bilişim sisteminin işleyişini bozmak
- Verileri bozmak
- Verileri yok etmek
- Verileri değiştirmek
- Verileri erişilmez kılmak
- Bilişim sistemine veri yerleştirmek
- Bilişim sisteminde var olan verileri başka bir yere göndermek şeklinde sıralamak mümkündür.

[244] Dülger, 2012, **a.g.e.** , s. 387

2.2.4.2.1.4.1.1 Bilişim sisteminin işleyişini engellemek (244/1)

Bilişim sisteminin işleyişini etkileyerek, sistemin normalde işlemesi gerektiği şekilde işlememesi sonucu, normal işlemesi durumunda sağlanacak yararın sağlanamamasıdır. Burada söz konusu edilen sistemin işleyişini engellemek eyleminin kapsamı oldukça geniştir ve sistemin işleyişini engelleyen her türlü eylem kastedilmektedir.[245]

Bilişim sisteminin işlemesini engelleme, sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılmasıdır. Burada sistemin işleyişi bozulmamakta, fakat işlemesi bir şekilde engellenmektedir. Madde metninde yer alan düzenleme ile nasıl olduğunu aramaksızın sistemin işleyişini bozmak dışında sistemin işlemesini engelleyen her türlü fiili bu cümleden saymıştır. Yani engelleme fiili bakımından serbest hareketli bir suç söze konudur. Bilişim sisteminin işleyişinin engellenmesi halinde sistemin bozulması söz konusu olmayıp normalde yerine getirdiği fonksiyonlarını ifa etmesi engellenmektedir. Sistemde normal şartlarda yerine getirebilen işlevler gereği gibi yerine getirilememektedir. Ancak sistem bozulmuş değildir. Fail bir kısım eylemlerle işleyişi engellemektedir.[246]

Bu suç esasen icrai hareketle işlenebilecektir. Ancak teknik destek sorumlusunun kasıtlı olarak bir virüs saldırısını önlemek için gerekli yazılımları sisteme yüklememesi ya da sistemi dışarıdan saldırıya karşı savunmasız bırakması halinde olduğu gibi istisnai durumlarda suçun ihmal suretiyle işlenmesi de mümkün olabilecektir. [247]

Bu anlamda ister isteyerek, ister bir ihmal sonucu oluşmasına olanak sağlanan mevcut sistemin işleyişinin engellenmesi durumu suç oluşturmakta ve TCK'nin 244'ncü maddesinin birinci fıkrasında bir yıldan 5 yıla kadar hapis cezasıyla cezalandırılacağı belirtilmektedir.[248]

---

[245] Dülger, 2012, **a.g.e.** , s. 387
[246] Kurt, (2005a), **a.g.e.** , s. 161.
[247] Dülger, 2012, **a.g.e.** , s. 388
[248] ***5237 Sayılı Türk Ceza Kanunu***, Madde 244, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

2.2.4.2.1.4.1.2. Bilişim Sisteminin İşleyişini Bozmak (244/1)

Bilişim sisteminin işleyişini bozmak, TCK'nin 244'ncü maddesinin birinci bendinde belirtilmektedir. Sistemin işleyişini engelleme yoluyla, fayda sağlayacak kişilerin mevcut faydayı sağlayamaması ya da zarar görmeleri durumunu ortaya çıkaracağından, bilişim sisteminin işleyişini bozmak TCK açısından suç sayılmakta ve bir yıldan beş yıla kadar hapis cezasını gerektirmektedir.

Verilerin, bilginin sayısal koda dönüştürülmüş hali olduğu yukarıda belirtilmişti, bazen bu kodlardan birinin dahi olmaması verinin kullanılmasını engellemekte veya verilerden oluşan bütünü (örneğin bir resim ya da yazı dosyasını) bozmaya yetmektedir. Bu nedenle bunların kısmen ya da tamamen bozulması açısından bir fark bulunmamaktadır. Aynı durum verileri içeren bilişim sistemi ya da veri taşıma aracı açısından bir fark bulunmamaktadır. Aynı durum verileri içeren bilişim sistemi ya da veri taşıma aracı açısından da geçerlidir, ancak kısmen bozma eyleminin bunlar açısından gerçekleşebilmesi için bozulan kısım nedeniyle bilişim sistemi içinde bulunan verilerin bir daha kullanılamaz hale gelmesi gerekmektedir. Örneğin bilişim sisteminin işlemcisine ya da güç dağıtıcısına etkide bulunulmadan sabit diskinin kırılması durumunda bu her ne kadar bilişim sisteminin bir kısmının bozulması anlamına gelmekteyse de sistemin içerdiği verilere bir daha ulaşılamayacağı ve dolayısıyla bilişim sisteminden beklenilen işi yapamayacak duruma geleceğinden suç gerçekleşmiş olacaktır.

Bunun dışında bozmak eyleminin nasıl gerçekleştirileceği suçun oluşumu açısından önemli değildir. Fail ister verilerin düzenini bozsun, ister verilerin bulunduğu bilişim sistemine virüs göndererek verileri tahrip etsin, isterse tahrip edilmek istenilen verilerin bulunduğu bilişim sistemini baltayla parçalasın sonuç fark etmeyecek ve suç gerçekleşmiş olacaktır.

Bilişim sisteminin işleyişinin bozulması eyleminin gerçekleştirilmesi için özellikle virüsler ve kurtçuklar uygun araçlardır. Nitekim yukarıda bilişim suçlarının işlenme şekilleri konusunda virüs yazılımları açıklanırken belirtildiği üzere, virüs gönderilerek birçok kişinin bilişim sistemleri ya da içerdiği verileri ya tamamen ya da kısmen işlemez hale getirilmiştir. [249]

[249] Dülger, 2012, **a.g.e.** , s. 389

2.2.4.2.1.4.1.3. Verileri bozmak (244/ 2)

Veriler üzerinde gerçekleştirilebilecek bir icra hareketidir. Bu icra hareketi ile verilerin bilinemeyecek hale gelmesi, bellek üzerinde bulunduğu noktaya ulaşılmasını sağlayan bağların koparılması ve ulaşımın engellenmesi kastedilmektedir.[250]

Bilişim sisteminin işleyişinin bozulması eylemi verilerin bozulması eylemiyle de gerçekleştirilebilecektir; ancak görüldüğü üzere verilerin bozulması eylemi 244. Maddenin 2. Fıkrasında ayrıca düzenlenmiştir. Bunun nedeni her ikisinin faildeki farklı maksatlarla gerçekleştirilen hareketler olmasıdır, ancak bu maksat, suç tipleri açısından bir unsur oluşturmamakta, yalnızca hangi fıkranın uygulanacağının belirlenmesi açısından bir yorum aracı olmaktadır. Bilişim sisteminin işleyişinin engellenmesi için verilerin bozulması halinde failin amacı sistemde bulunan verilere zarar vermek değil bir şekilde bilişim sisteminin işleyişini bozmaktır; oysaki maddenin 2. Fıkrasında yer alan verileri bozmak hareketinde fail bilişim sisteminin işleyişine zarar vermek istememekte bilişim sisteminin içerdiği bir kısım verileri örneğin bir uygulama yazılımını ya da depolanmış bazı bilgileri kullanılamaz hale getirmek istemektedir.[251]

Kısacası bu düzenleme ile bilişim sisteminin her nasıl olursa olsun çalışmasının engellenmesi ya da sistemin bozulması cezalandırılmak istenmektedir.[252]

2.2.4.2.1.4.1.4. Verileri yok etmek (244/2)

Yoketmek sözcüğünün anlamı TDK'nın sözlüğünde *"varlığına son vermek, ortadan kaldırmak, ifna etmek, izale etmek"* olarak açıklanmaktadır. Ancak bilişim sistemlerinde yer alan veriler açısından yukarıda açıklanan gerçek anlamında olduğu gibi verileri tamamen ortadan kaldırmak ya da varlığına son vermek her durumda mümkün değildir. Bu nedenle yasa koyucunun bu ifadeyle somut anlamda yok etmek eylemini değil, bilişim alanında geçerli olan soyut anlamda mantıksal yok etmek eylemini kastettiği belirtilmelidir. [253]

[250] Ergün, **a.g.e.** , s. 95.
[251] Dülger, 2012, **a.g.e.** , s. 390
[252] Soyaslan, Doğan, Ceza Hukuku Özel Hükümler, Yetkin Yayınları, Ankara, 2014, s.698.
[253] Aynı.

Gerçekten de bir bilişim sisteminde herhangi bir veriyi yok etmek için sil komutu verildiğinde o veriler defterden yazının silindiği gibi tamamen yok olmamakta yalnızca dosyalama sistemine göre o verilere ulaşımı sağlayan anahtar veriler değiştirilmekte ve bilişim sisteminin dosyalama sistemi sayesinde bir daha normal yollarla söz konusu veriye ulaşılması engellenmektedir. Ancak bazen kolayca bazen de uzun, zaman alıcı ve masraflı çalışmalar sonucunda verilerin tekrar elde edilmesi mümkün olmaktadır. Bu nedenle bilişim alanında silmek kavramı kullanıldığında aslında verilere ulaşımın engellenmesi ifade edilmektedir; yasa koyucu da verilere ve veri işleme zarar verme suçunun maddi unsurlarından olan verileri yok etmek eyleminde aslında mantıksal silme eylemini öngörmektedir. Örneğin genel olarak verilerin yok edilme yöntemi olarak bilinen *"bilgisayara format atma"* işleminde, aslında veriler silinmemekte ancak bilgisayarın sabit diskinde verilerin nerede bulunduğunu gösteren fihristteki kayıtlar silinmekte, böylelikle fihristte bu verilerin bulunduğu sektörler, yeni verilerin yazılabilmesi için boş gösterilmektedir. Dolayısıyla bu sektörlerin üzerine yeni veriler yazılmadıkça, veri kurtarma programlarıyla bu verilerin geri getirilmesi mümkün olmaktadır. Verilerin gerçek anlamda silinmesi ise *"wape"* denilen işlemle sabit diske elektromanyetik şok verilmesi ve sabit diskin katmanları üzerinde bulunan ve okuyucu kafanın izlediği çizgilerin (eksi plaklardaki iğnenin üzerinden geçtiği çizgiler gibi) yok edilmesiyle gerçekleştirilmektedir. Buna göre söz konusu hareketin gerçekleşmiş olması için verilerin mantıksal olarak silinmesi yeterli olup mutlaka *"wape"* işlemine tabi tutulmuş olması gerekmemektedir. [254]

Bu hareket bakımından belirtilmesi gereken bir diğer konu da, verilerin birçok işletim yazılımında olduğu gibi yok etmek maksadıyla *"geri dönüşüm kutusuna"* yollanması fakat ortadan kaldırılmaması veya bilişim sisteminde yüklü olan işletim sisteminin *"geçici öğeler klasöründe"* kopyası mevcut olan unsurların silinmesi durumunda yok etme fiilinin gerçekleşmiş sayılıp sayılmayacağıdır.

2.2.4.2.1.4.1.5. Verileri Değiştirmek (244/2)

Verilerin değiştirilmesi, mevcut sistemde var olan bir verinin yerine başka bir veri koyarak yeni bir görünüm kazanmasını sağlamaktır. Var olan verinin değiştirilen

[254] Dülger, 2012, **a.g.e.** , s. 390.

kısmının büyük ya da küçük olması, bir bölümünün ya da tamamının değiştirilmesi çok da önemli değildir. Önemli olan değiştirme eylemi ve bu eylem sonucu sistemdeki verinin aldığı yeni görünümdür.

Fail verileri menfaat temin etmek için değiştirmiş ve kendisinin ya da başkasının yararına bir menfaat sağlamış ise eylem başka bir suçu oluşturmuyorsa, faile TCK' nun 244/4 maddesince ceza verilir.[255]

2.2.4.2.1.4.1.6. Verileri Erişilmez Kılmak (244/2)

Maddi anlamda yok etmemekle birlikte verilere ulaşılması için gereken işlem bağının ortadan kaldırılmasıdır.

Verilerin erişilmez olmasından kasıt edilen verileri kullanan ya da bu verilerle malik olan kişinin dilediği zaman verilere ulaşmasının engellenmesidir. Burada önemli olan verilerin mutlaka malikine ait olması değil, verilere ulaşabilmenin engellemiş olmasıdır.[256]

Erişilmez kılınan veriler bir bilişim sisteminde olabileceği gibi bir veri taşıma aracında da bulunabilecektir. Ayrıca verilerin üzerinde bulunduğu bilişim sisteminin ya da veri taşıma aracının mülkiyetinin kimde olduğunun suçun oluşumu açısından bir önemi yoktur; verilere ulaşılmasının engellenmesi suçun oluşumu için yeterlidir.

Bu hareket, verilerin silinmesi, başka bir yere taşınması ya da verilere ulaşılmak istenildiği anda sistemin elektriğinin kesilmesi gibi çeşitli şekillerde gerçekleştirilebilecektir. Verilerin silinmesi amacıyla da olsa verilerin bulunduğu bilişim sisteminin bozulması ya da çalışmasının engellenmesi halinde ise 1. Fıkradaki hükmün uygulanması gerekecektir. Ancak, 1. Fıkrada bilişim sisteminin işleyişi korunduğu için, tek başına bir sistem olmayıp, ancak bir sistemin parçası olabilecek veri taşıma araçlarındaki verilerin erişilmez kılınması için bozulması ya da çalışmasının engellenmesi halinde ise 2. Fıkradaki hükmün uygulanması gerekmektedir.

Verilerin bilişim sisteminde belirli bir düzen içinde bulundukları ve bu düzen sırasına göre bir araya gelerek belli yazılımları oluşturdukları ya da işlev kazandıkları

[255] Parlar, Ali – Hatipoğlu, Muzaffer, ***Türk Ceza Kanunu Yorumu,*** Cilt: 4, Seçkin Yayınevi, Ankara, 2008, s. 3476.
[256] Dülger, 2012, **a.g.e.** , s. 391.

belirtilmiştir. İşte bu sıranın bozulması ya da bir yazılım içine farklı bir verinin sokulması da verileri erişilmez hale getirebilecektir. Verilerin erişilmez kılınması hareketinin geçici süreyle ya da sürekli olması arasında yasada bir ayrım yapılmadığı için her iki durumda da suç gerçekleşmiş olacaktır.

2.2.4.2.1.4.1.7. Bilişim Sistemine Veri Yerleştirmek (244/2)

Sistemi kullanmakla yetkili olan kimsenin izni alınmaksızın dışarıdan birinin sisteme girerek veri yerleştirmesidir. Bu İşlem kaydetme, ekleme veya yükleme şeklinde gerçekleştirilebilir.[257] Bileşim sistemine veri yerleştirmek hareketiyle, fail tarafından bilişim sistemine ya da veri taşıma aracına dışarıdan ve sistemin maliki ya da ilgilisinden izin alınmaksızın çeşitli verilerin sisteme kaydedilmesi, yüklenilmesi ya da eklenilmesi kast edilmektedir.

Bu yerleştirme hareketi, bilgisayarın başına oturup *"harici bellek"* ya da *"USB"* gibi veri taşıma aracını sürücü donanıma yerleştirip içindeki verileri bilgisayara yüklemek şeklinde yapılabileceği gibi; internet üzerinden veri yüklemek şeklinde de gerçekleştirilebilecektir.

Bu hareketin meydana gelmesi bakımından, veri yüklenen bilişim sistemine failin hukuka aykırı ya da hukuka uygun şekilde girmiş olmasının bir önemi yoktur. Örneğin bedeli karşılığı hizmet veren bir internet sitesine bedel ödenerek ve gerekli şifreler alınarak girilmesi kişiye bu siteye veri yükleme hakkını vermemektedir. Ancak birçok kez bir web sitesine hukuka uygun şekilde girme hakkı, bu sisteme veri yükleme hakkını da içerebilmektedir; bu nedenle hukuka uygun bir giriş hakkının bulunduğu veri yükleme işlemlerinde söz konusu hakkın somut durum açısından "*veri yükleme hakkını*" da içerip içermediği araştırılmalı ve buna göre karar verilmelidir.

2.2.4.2.1.4.1.8. Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek (244/2)

Verilerin transferi, başka yere aktarılması, kaydedilmesi ya da kopyalanması anlamına gelmektedir. Verilerin gönderilmesi eylemi veri ileti ağları üzerinde

[257] Taşkın, Şaban Cankat, ***Bilişim Suçları***, Beta Yayınevi, Bursa, 2008, s. 48.

Örneğin internette veya bilgisayara bağlanan veri taşıma aracı üzerine kaydedilerek gerçekleştirilebilir.[258] Bununla, bilişim sisteminde bulunan verilerin bilişim sistemi dışında bulunan bir başka bilişim sistemine ya da veri taşıma aracına aktarılması, kaydedilmesi ya da kopyalanması hareketleri belirtilmektedir.

Bilişim sistemlerinde verilerin kaydı yapılırken, kayıt yapılan esas veriler bir başka yere kayıt esnasında yok edilebildiği gibi (kes-yapıştır), asıl veriler olduğu yerde korunarak verilerin yeni bir kopyası da oluşturulabilmektedir (kopyala-yapıştır). Bu hareketle kastedilen, verilerin yeni bir kopyasının bir başka sisteme aktarılmasıdır; çünkü verilerin yok edilmesi yine bu suç tipinde fakat ayrı bir hareket olarak tanımlanmaktadır.

Başka yere göndermek ile kastedilen verilerin kayıt edilmesi, kopyalanması ya da aktarılmasıdır, yoksa somut varlığı olmayan verilerin somut bir hareketi içeren göndermek eylemiyle açıklanması mümkün değildir. Ancak bilişim alanında özellikle elektronik posta yoluyla veri aktarılmasında, somut posta hizmetleri için geçerli olan "*göndermek*" sözcüğü yaygın bir şekilde kullanılmaktadır. Bu nedenle olsa gerektir ki yasa koyucu da bu kavramdan esinlenmiş ve suç tipinde bu eyleme yer vermiştir.

Bilişim sisteminde var olan verilerin başka yere gönderilmesi eylemi veri iletim ağları üzerinden örneğin internet ya da *"wifi"* ile bir başka bilişim sistemine verilerin aktarılması yoluyla gerçekleştirilebileceği gibi, verilerin bulunduğu bilgisayara bir veri taşıma aracının bağlanması ve verilerin bu aracın üzerine kaydedilmesi yoluyla da yapılabilecektir.

Dolayısıyla söz konusu hareket seçimlik suçu oluşturan hareketlerden birisi de olsa da bizatihi hareketin kendisi serbest bir şekilde işlenebilecektir. Ancak yukarıda da ifade ettiğimiz üzere kişisel verilerin bir yerden bir başka yere aktarılması halinde TCK'nin 135. maddesinde düzenlenen kişisel verilerin kaydedilmesi veya 136. maddesinde düzenlenen kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu; YCGK (Yargıtay Ceza Genel Kurulu)'nın 2009 tarihli kararında belirttiği parayı temsil eden verilerin bir yerden başka bir yere aktarılması halinde ise 142. maddede düzenlenen bilişim sistemleri suretiyle nitelikli hırsızlık suçu oluşacaktır.

[258] Parlar ve Hatipoğlu, **a.g.e.** , s. 3478.

2.2.4.2.1.4.1.9. Değerlendirme

Gerek 5237 Sayılı Ceza Kanunu, gerekse 6698 Sayılı Kişisel Verilerin Korunması Kanunuyla bilişim alanında işlenebilecek suçlar tanımlanmaya çalışılmış ve çerçevesi çizilmiştir. Ancak yapılan incelemede görüldüğü üzere, verilerle ilgili birden fazla eylemin bir maddede toplanma durumu ortaya çıkmakta, bu da çoğu zaman zihinlerde karışıklık yaratabilmektedir. Ayrıca tanımlanan eylemlerin bilişim suçu olarak her ne kadar yaygın bir nitelik kazanma eğilimi gözlense de, özellikle 6698 Sayılı Kişisel Verilerin Korunması Kanununun zamanlama anlamında da çok yeni olması nedeniyle algısal anlamda sıkıntıların ortaya çıkacağı düşünülmektedir. Çünkü tanımlanmaya çalışılan eylemlerin birbirleriyle olan ilişkisi o denli iç içedir ki, kimi zaman suç olarak tanımlanan eylemlerin birbirinden ayrılması mümkün olmamaktadır. Ancak yukarıda belirttiğimiz üzere korunan hukuksal değer, suçun konusunu ve failin amacı ortaya konulduğunda bu ayrımın yapılması mümkündür. Dolayısıyla, suç tipinde cezalandırılmayan hareketlerin bulunmasındansa geniş tutularak her harekete yer verilmesi daha doğru bir tercih olmuştur.

İnceleme konusu suç tiplerinin her ikisi de seçimlik hareketli suçlardı. Suçların eylem unsurunda belirtilen 1. fıkra açısından bilişim sisteminin işleyişini engellemek veya bilişim sistemin işleyişini bozmak; 2. fıkra açısından ise verileri bozmak, bilişim sistemine veri yerleştirmek, bilişim sisteminde var olan verileri başka bir yere göndermek, verileri erişilmez kılmak, verileri değiştirmek veya verileri yok etmek hareketlerinden biri ya da bir kaçının aynı anda gerçekleştirilmesi durumunda, tek bir suç işlenmiş kabul edilecek ve faile gerçekleştirdiği harekete göre ya 1. fıkradaki ya da 2. fıkradaki suçun cezası verilecektir.

Ayrıca bu suçlar genellikle icrai bir hareketle işlenebilecektir. Ancak bazı durumlarda failin ihmal suretiyle de bu suçları gerçekleştirmesi mümkündür. Gerçekten de bir kuruluşun bilişim alanında teknik destekten sorumlu olan yetkilisinin veri işlemeye engel olmak kastıyla, örneğin bir virüs saldırısının önlenmesi için gerekli olan yazılımları bilişim sistemine yüklenmemesi durumunda fail ihmali hareketle suçu gerçekleştirmiş olacak ve suç icrai bir hareket yapılmaksızın meydana gelmiş olacaktır. Bu durumda yalnızca verilere zarar verilmesi halinde 2. fıkra, tüm sisteme zarar verilmesi halinde ise 1. fıkra uygulanacaktır.

Bunun dışında söz konusu eylemlerin meydana getiriliş tarzının suçun oluşumu açısından bir önemi yoktur, bu hareketler direkt sisteme fiziki etki yoluyla olabileceği gibi sisteme veri iletim ağı yoluyla bir virüs yazılımının gönderilmesi yoluyla da gerçekleştirilebilecektir. Bir başka deyişle her iki suç tipinde yer alan hareketlerin tümü serbest hareketli olarak düzenlenmişlerdir.

2.2.4.2.1.4.2. Suç Tipinde Yer Alan Hareketlerin Avrupa Konseyi Siber Suçlar Sözleşmesi (AKSSS) ile Paralelliği

AKSSS'nin "*Sistemin Bütünlüğünün İhlali*" başlıklı 5. Maddesinde;

"*Her taraf iç hukukuna uygun olarak, bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle bir bilişim sisteminin işletilmesine kasten ve haksız olarak engel olunmasını suç haline getirmek için gerekli görülen yasal tedbirleri ve diğer tedbirleri kabul eder*"[259] düzenlemesi yer almaktadır. Bu madde Avrupa Konseyinin (89) 9 no'lu "*bilgisayar sabotajı*" ile ilgili Tavsiye Kararına dayanmaktadır.

Nitekim 244. maddenin 1. fıkrasındaki düzenlemeyle AKSSS'nin 5. Maddesi arasında tam bir paralellik bulunduğu görülmektedir.

AKSSS'nin "*Veriye Müdahale*" başlıklı 4. maddesinde "*1. Her bir taraf devlet, bir kimsenin bilgisayar verisine hakkı olmadığı halde, bilerek ve isteyerek zarar verme, silme, bozma, değiştirme ya da ortadan kaldırma eylemleri işlemesini suç olarak düzenlemek üzere gerekli yasal düzenlemeyi yapmalı ve gerekli diğer önlemleri almalıdır. 2. Taraf devlet 1. Paragrafta belirtilen durumun oluşmasını ciddi zarar oluşma olasılığına bağlı tutma hakkına sahiptir*"[260] düzenlemesi yer almaktadır.

5237 Sayılı TCK'nun ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu ile AKSSS'nin karşılaştırılması halinde karşımıza bir uyum tablosunun çıktığını söylemek yanlış olmayacaktır.

Yukarıda anılan AKSSS ile TCK arasındaki paralel düzenlemelere karşın Sözleşmenin "*Yasadışı Müdahale*" başlıklı 3. maddesiyle 244. madde arasında olması gereken paralellik sağlanmamıştır. Sözleşmenin 3. Maddesinde;

"*Taraflardan her biri, aşağıda sözü edilen bilgisayar verilerinin üzerinde bulunduğu bir bilgisayar sisteminden elektromanyetik dalgalar yayılması da dâhil*

---

[259] Akarslan, Hüseyin, ***Avrupa Konseyi Siber Suçlar Sözleşmesi (Türkçe),*** 26.10.2010, (Erişim) http://www.bhd.org.tr/dokumanlar/Avrupa%20Konseyi%20Siber%20Suclar%20Sozlesmesi%20TR.docx , 12.12.2016.

[260] Akarslan, 2010, **a.g.e.**

olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar sistemi üzerinden veri iletimine haksız surette dâhil olma fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, sahtekârlık amacını güden bir fiil şeklinde veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler."[261] düzenlemesi yer almaktadır.

AKSSS bu maddeyle veri iletişiminin gizliliğini güvence altına almayı amaçlamaktadır. AKSSS ile paralelliği sağlama bağlamında 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun ikinci bölümünde *"Kişisel Verilerin İşlenmesi"* başlığı altında yer alan Madde 4, Madde 5 Madde 6, Madde 7, Madde 8, Madde 9 yeterli olduğu düşünülmektedir.

2.2.4.2.1.4.3. 244. Maddenin 1. ve 2. Fıkralarındaki Hareketlerin Farkı ve Uygulaması

244. maddenin 1. ve 2. Fıkralarında yer alan suç tipleri TBMM Genel Kurulu'na sunulan tasarıda tek fıkra halinde ve tek bir suç tipiyken, Genel Kurul'da kabul edilen önerge ile iki fıkra haline getirilmiştir. Suç tipi, Adalet Komisyonu'nda kabul edilen metinde "*Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir*" şeklinde düzenlenmekteydi. 244. maddenin her iki fıkrasında yer alan hareketlerin tümüne aynı suç kalıbında yer alan seçimlik hareketler olarak yer verilmişti ve hepsi için aynı ceza öngörülmüştü.

TBMM Genel Kurulu'nda kabul edilen ve yasalaşan 244. maddenin 1. fıkrası için ise "*bir yıldan beş yıla kadar hapis cezası*", 2. fıkrası için ise "*altı aydan üç yıla kadar hapis cezası*" öngörülmüştür. Bu değişiklik için TBMM Genel Kurulu'na verilen önergenin gerekçesinde "*suç tanımlarında belirliliği sağlamak ve ceza miktarlarını işlenen fiillerin ağırlığına uygun olarak belirlemek amacıyla madde metninde değişiklik yapılması uygun görülmüştür*"[262] denilmektedir.

---

[261] Sokullu-Akıncı, Füsun, ***Avrupa Konseyi Sıber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi***, (Erişim) www.journals.istanbul.edu.tr/iuhfm/article/download/1023004153/1023003747 , 12.12.2016, s.16.

[262] Noyan, Erdal, ***Ceza Hukuku 1***, Ankara, Şubat 2005, s.576.

Birinci fıkrada, bir bütün olarak bilişim sisteminin işleyişi korunmak istenirken, ikinci fıkrada ise, sistemin içinde yar alan veriler korunmak istenmektedir.

Benzerliği nedeniyle TCK'nun 135. (Kişisel verilerin kaydedilmesi) ile 136. (Verileri hukuka aykırı olarak verme veya ele geçirme) maddeleriyle, TCK'nun 244/2. maddesindeki suç tiplerini birbirine karıştırmamak gerekir. Yukarda da belirtildiği üzere TCK'nun 244/2. maddesinde verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliği korunmakta iken, 135 ve 136. maddelerde kişisel verilerin bizzat kendisi korunmaktadır. Ayrıca 135 ve 136. maddelerde her türlü yer ve araçta kayıtlı kişisel veriler suçun konusu iken, 244/2. maddede yalnızca bilişim sistemlerinde yer alan veriler suçun hukuki konusudur.[263]

244'ncü madde birinci fıkrada yer alan hareketler her ne kadar suç tanımı açısından seçimlik hareketli olsalar da, kendi içlerinde serbest hareketlidirler. Bir başka deyişle, sistemin işleyişini bozma veya engelleme hareketlerinin nasıl yapıldığının tipiklik açısından bir önemi yoktur, suçun gerçekleşmesi için gerekli olan neticede sisteminin işleyişinin engellenmesi veya bozulmasıdır.

2.2.4.2.1.4.4. Netice

Bu başlık altında incelediğimiz, tipiklik açısından suçun gerçekleşmiş sayılması için, bir neticenin aranıp aranmadığıdır. Yukarıda da ifade ettiğimiz üzere, her iki suç tipinde de hareketlerin nasıl yapılacağı gösterilmeyip, serbest hareketli suçlar düzenlenmiştir. Suç tipinde yer verilen hareketlerin bir diğer özelliği ise, aslında bunların failin serbest şekilde gerçekleştirdiği hareketlerin sonunda ortaya çıkan neticeler olmalarıdır. TCK'nin 244. maddesinde hareketler "*engelleyen, bozan, yerleştiren, gönderen, erişilmez kılan, değiştiren ve yok eden*" şeklinde gösterilmiş, yani hareketin meydana getirilmesi ve bir sonucun ortaya çıkması aranmış, ancak engelleme, bozma, yerleştirme, gönderme, erişilmez kılma, değiştirme ve yok etmenin nasıl yapılacağı belirtilmemiştir. Dolayısıyla, 244. maddenin 1. ve 2. fıkralarında yer alan her iki suç tipinde de netice aranmaktadır.[264]

[263] Yılmaz, Sacit, "5237 Sayılı TCK'nin 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", ***TBB Dergisi***, 92, 2011, s.66.
[264] Yılmaz, Sacit, **a.g.e.**, s. 77.

2.2.4.2.1.5. Suçun Nitelikli Hali (244/3)

TCK'nin 244. maddesinin 3. fıkrasında, her iki suç tipinde tanımlanan eylemlerin "*bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi*"[265] suçların nitelikli hali olarak öngörülmüştür. Buna göre, nitelikli halin gerçekleşmesi durumunda faile verilecek ceza yarı oranında arttırılacaktır.

TCK'nin 244. maddesinin 3. fıkrasında suçun ağırlaştırıcı nedeni düzenlenmiştir. Buna göre, bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza arttırılacaktır. Tüm kamu kurum veya kuruluşlarına ait bilişim sistemleri üç numaralı fıkra kapsamında değerlendirilebilecektir. Özel kurumlardan ise banka veya kredi kurumu niteliği olan tüm özel kurum veya şirketler TCK 244/3 kapsamında değerlendirilecektir. TCK 158/1.j'de kredi kurumunun ne olduğu söyle tanımlanmaktadır: *"Kredi kurumu deyiminden, banka olmamasına karşın, kanunen borç para vermeye yetkili kılınan kurumlar anlaşılır."* Şu halde, özel finans kurumları da kredi kurumu olarak kabul edilmelidir.[266]

TCK'nin 244. maddesinin üçüncü fıkrası ile maddenin 765 sayılı TCK'daki karşılığı olan 525 b.1'deki önemli bir eksiklik giderilmiş ve zarar verilen sistemin bankaya, kredi kurumuna ya da bir kurum ve kuruluşa ait bilişim sistemi olması ağırlaştırıcı neden sayılmıştır. Nitekim bir kişisel bilgisayarın işleyişinin engellenmesinden doğacak zarar ile bir bankanın bilgisayarının işlemesinin engellenmesinden doğacak zarar arasında ciddi fark vardır. Bu nedenle bankanın sistemine verilen zarar nedeniyle failin daha ağır bir cezaya çarptırılması da hakkaniyetle bağdaşmaktadır.[267]

Gerçekten de Türkiye'de kamusal hizmetlerin ve alt yapı hizmetlerinin yerine getirilmesini kamu kurum ve kuruluşları sağlamaktadır, benzer şekilde banka ve finans kurumları da tüm ekonomik sistemin işleyişini ilişkili oldukları kamu

---

[265] ***5237 Sayılı Türk Ceza Kanunu***, Madde 244, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

[266] Cankat, **a.g.e.** , s. 65.

[267] Dülger, 2004, **a.g.e.** , s. 243.

kurumları ve kamu bankalarıyla birlikte gerçekleştirmektedirler. Söz konusu kurum ve kuruluşlar ile banka ve finans kurumları tamamen bilişim sistemleri üzerinden her türlü işlemlerini yapmakta ve hizmetlerini kesintisiz ve sorunsuz bir şekilde yerine getirmektedirler. Bu kuruluşların bilişim sistemlerinde meydana gelecek bir sorun, kesinti veya bozukluk ya da bunların bilişim sistemlerinde yer alan verilerin bozulması, erişilmez kılınması veya değiştirilmesi yalnızca bu kurumlar ya da bankaların kendisi açısından değil, hizmet verdikleri kesimler ve dolayısıyla toplumun büyük bir kısmı açısından da büyük sorunların meydana gelmesine yol açacaktır. Bu nedenle suçun nitelikli haline bu şekilde yer verilmiş ve bize göre son derece yerinde bir düzenleme yapılmıştır.

TCK'nin 244. maddesinde düzenlenen suçlar şikâyete bağlı olmayıp, C. Başsavcılığı tarafından doğrudan soruşturma yapılır. Yargılama yetkisi ise asliye ceza mahkemelerine aittir.[268] 6698 Sayılı Kişisel Verilerin Korunması Kanunuyla 5237 Sayılı TCK, bilişim sisteminde gerçekleştirilebilecek suçların önüne geçmeyi amaçlasa da, bu noktada birbirinden ayrılmaktadır. Çünkü 6698 Sayılı Kanun, Kişisel Verilerin Korunması Kurumu'nun faaliyetlerini bir şikayete bağlamış bulunmaktadır.

2.2.4.2.2. Tipikliğin Manevi (Sübjektif) Unsuru

244. maddenin 1. ve 2. fıkrasında yer alan her iki suçun da manevi unsurunu kast oluşturmaktadır. Ayrıca bu suçlarda failin belli bir saikle hareket etmesi aranmamaktadır. Ancak 2. fıkrada tanımlanan verilere ilişkin hareketlerin gerçekleştirilmesiyle sistemin işleyişinin engellenmesi veya bozulması da mümkündür. İşte böyle bir durumda failin eyleminin hangi fıkraya göre cezalandırılacağının belirlenmesinde suçun unsuru olarak belirtilmemişse de faildeki amacın yorum aracı olarak belirlenmesi gerekecektir. Suç tiplerinde açıkça belirtilmediği için her iki suçun da taksirle işlenmesi mümkün değildir.[269]

---

[268] Yılmaz, Sacit, **a.g.e.** , s. 85.

[269] Bikirli, Alper Yükselen, ***5237 Sayılı Türk Ceza Kanununda Düzenlenen Bilişim Suçları***, Ankara, (Erişim), https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjwspOoo_PQAhVBaRQKHWA7DBUQFggrMAI&url=http%3A%2F%2Fwww.taa.gov.tr%2Findir%2Falper-yukselen-bikirli-yargitay-8-ceza-dairesi-uyesi-c2F5ZmF8NzhjNTMtOWRjZDAtMWZlNDItNGRhZDYuZG9jeHwyMTc%2F&usg=AFQjCNEE1ErXJyI_OAW_Mrll1PRm7qXkgw , 12 Aralık 2016, s.15.

2.2.4.3. Hukuka Aykırılık Unsuru

TCK'nin 135. ve 136. maddelerdeki suçların tanımında failin eylemlerini *"hukuka aykırı olarak"* gerçekleştirmesi gerektiği ayrıca ifade edilmektedir. Nitekim TCK'nin 135. ve 136/1. maddesindeki suçlarda "hukuka aykırı olarak" ifadesi bu anlamda kullanılmaktadır.[270]

Suçla korunan hukuksal değer konusunda daha önce açıklandığı üzere, bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile sistemin kesintisiz ve sağlıklı çalışması korunmaktadır. Verilerin yok edilmesi ya da değiştirilmesi suçu ile veriler üzerinde tasarruf yetkisi bulunan kişinin, verilere herhangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarının korunması söz konusu olmaktadır. Bu nedenle söz konusu bu hakların sahibinin ya da yetkilisinin rızası, hukuka uygunluk sebebi oluşturacaktır.[271]

Bunun dışında bu suç açısından özellikle CMK'nın 134. maddesi kapsamında kolluk güçleri tarafından yapılan delil elde etmeye yönelik işlemler yasanın verdiği yetkiye dayanan bir hukuka uygunluk nedeni oluşturmaktadır.[272]

TCK'nin 26/2. maddesinde*, "Kişinin üzerinde mutlak surette tasarruf edebileceği bir hakkına ilişkin olmak üzere, açıkladığı rızası çerçevesinde işlenen fiilden dolayı kimseye ceza verilmez"* ifadesi yer almaktadır. Burada mağdurun rızası, hareketi hukuka uygun hale getirmektedir. Teorik olarak, rızanın fiili hukuka uygun hale getirmesi bakımından belli şartları taşıması gerekir. Bunlar, kişinin üzerinde mutlak surette tasarrufta bulunulabilecek bir hakkın varlığının olması; rıza gösterenin rızasının kapsamını ve önemini algılayacak durumda olması ve rıza beyanının, mutlaka suçtan önce veya suçun icra hareketlerinin yapılması sırasında olmasıdır.[273]

Bilişim sisteminin kullanım hakkı devredildiğinde bilişim sisteminin içinde bulunan verilerin, devir olunan tarafından zarara uğratılması durumudur. Bilgisayarı kullanmak için alan kişi, bilgisayarın malikine ait içindeki işletim yazılımına ya da

[270] Dülger, Murat Volkan – Modoğlu, Gözde, ***Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku Uygulama Rehberi***, Avrupa Birliği ve Avrupa Konseyi Ortak Yayını, Ankara, 2014, s. 80-81.

[271] Korkmaz, İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", ***TBB Dergisi***, Sayı 124, 2016, s. 96.

[272] Özen, Muharrem ve Özocak, Gürkan, "Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134***)***", ***Ankara Barosu Dergisi***, Sayı: 1, 2015, s. 67.

[273] Yılmaz, Sacit, **a.g.e.**, s. 79.

uygulama yazılımına zarar vermek kastıyla müdahalede bulunduğunda 244. maddenin 2. fıkrasında tanımlanan suç gerçekleşmiş olur. Burada artık kullanım hakkının devredildiği kişiye baştan verilen rızanın sınırları aşılmış ve bu kişinin yaptığı eylem hukuka aykırı bir hal almıştır.[274]

Bilişim sisteminin kullanım hakkını devretmeden de yukarıda anlatılan duruma benzer bir durum, bilişim sistemi için teknik destek alınması sırasında ortaya çıkabilmektedir. Bilişim sisteminin olağan kontrolü ya da bir başka işlem için çağırılan teknik destek görevlilerine bilişim sisteminin teslim edilmesi ve içindeki verilere müdahale etme yetkisinin verilmesi, bu kişilere sistemin içindeki bütün verileri yok etme ya da zarar verme yetkisini vermemektedir. Söz konusu kişilerin zarar vermek kastıyla hareket ederek, sistemde bulunan verilere zarar vermesi durumunda da bilişim sisteminde yer alan verilerin yok edilmesi ya da değiştirilmesi suçu (244/2) ortaya çıkmaktadır. Burada da baştan verilen ve hukuka uygunluk durumu yaratan rızanın sınırları aşılarak, teknik destek görevlilerinin gerçekleştirdiği eylemler, hukuka aykırı nitelik taşıyacaktır.[275]

2.2.4.4. Suçun Özel Görünüş Biçimleri

Suçun özel görünüş biçimleri teşebbüs, iştirak ve içtima başlıkları altında ele alınacaktır.

2.2.4.4.1. Teşebbüs

Bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi ya da değiştirilmesi suçunun teşebbüs halinde kalması mümkündür. Bu; icra hareketlerine başlandıktan sonra bu hareketlerin yarıda kalması şeklinde olabileceği gibi suçun icrasına ilişkin bütün eylemler tamamlandıktan sonra suçun oluşumu için aranan netice meydana gelmeden failin elinde olmayan nedenlerle suçun gerçekleşmemesi şeklinde de olabilecektir [317].

Bir bilişim sistemine ve/veya içerdiği verilere zarar verilmesi amacıyla sisteme bir bilişim virüsünün yüklenmesi ve bu yazılım harekete geçmeden bunun sistemin sahibi tarafından fark edilerek etkisiz duruma getirilmesi durumunda suça teşebbüs

[274] Korkmaz, **a.g.e.**, s. 106.
[275] Aynı, s. 99.

gerçekleşmiş olacaktır. Benzer bir şekilde, bir mantık bombası yazılımının harekete geçme zamanından önce fark edilerek etkisiz kılınması durumunda da suça teşebbüs gerçekleşmiş olacaktır.

İnceleme konusu suç tipleri, seçimlik hareketli suçlar olduğu için, failin suç tipinde yer alan tüm hareketleri yapması ancak bazı hareketler sonucunda neticenin meydana gelmesi, bazılarının sonucunda ise meydana gelmemesi durumunda, diğer hareketler teşebbüs derecesinde kalmış olsalar da suç tamamlanmış sayılacak ve faile tamamlanmış suçun cezası verilecektir.

2.2.4.4.2. İştirak

Suça iştirak açısından bir özellik söz konusu olmayıp TCK'nin 37., 38., 39. ve 40. Maddelerindeki suça iştirake ilişkin genel hükümler çerçevesinde ortaya çıkan durumlar değerlendirilecektir.

2.2.4.4.3. İçtima

Bu suçların zincirleme şekilde işlenmesi mümkündür. Örneğin sistemin çalışmasının engellenmesi ya da hukuka aykırı olarak veri yerleştirilmesi için kısa zaman aralıklarıyla ve aynı suç işleme kastıyla bilişim sistemine birçok kez etkide bulunulması halinde zincirleme suç gerçekleşecektir.

TCK'nin 43. Maddesinin 2. fıkrasında *"Aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da, birinci fıkra hükmü uygulanır."* denilmek suretiyle aynı neviden fikri içtimaın bu halinde, aynı eylemle aynı suçun farklı kişilere karşı aynı anda işlenmesi söz konusu olmaktadır. Örneğin bir virüsün fail tarafından internet sitesinde yayınlanması ya da aynı elektronik postayla çok sayıda alıcıya gönderilmesi neticesinde çok sayıda kişinin bu virüsü bilişim sistemine indirmesi ve sistemlerinin zarar görmesi halinde aynı neviden fikri içtima söz konusu olmaktadır.[276]

Aynı şekilde bu suçun mütemadi olarak işlenmesi de olanaklıdır. 244. Maddede belirtilen hareketlerden özellikle 1. fıkradaki sistemin engellenmesi ve 2. fıkradaki verilere ulaşımın engellenmesi devam eden bir şekilde işlenebilecektir. Bu

[276] Dülger, Murat Volkan, ***Suçların Birleşmesine İlişkin Tanımlar, Sorunlar ve Çözüm Önerileri,*** 25 Mart 2015, (Erişim) http://www.hukukgunlugu.org/suclarin-birlesmesi/ , 12 Aralık 2016.

durumda suçlar, devam eden eylemin bittiği zaman gerçekleşmiş kabul edilebilecek ve zamanaşımı da bu andan itibaren işlemeye başlayacaktır. Örneğin elektriğin kesilmesi ya da veri taşıma araçlarının saklanması eylemlerinde olduğu gibi suçu oluşturan eylemlerin devamlılık kazandığı hallerde bu durum gerçekleşebilecektir.

TCK'nin 244. Maddesinin 1. fıkrasıyla, TCK'nin 151. Maddesinde düzenlenen mala zarar verme suçu arasındaki ilişkinin de burada açıklanması gerekmektedir. TCK'nin 151. Maddesinde düzenlenen mala zarar verme suçunda, suçun konusunu *"başkasının taşınır ya da taşınmaz malı"* oluşturmaktadır. İnceleme konusu suç tipinde suçun konusunu bilişim sistemi oluşturmaktadır; ancak burada kastedilen bilişim sistemi bir mal olarak duran ve vitrin bekleyen bir eşya değil; işlerliği olan, bilişim sistemi olarak kullanılan ve bir bilişim sisteminden beklenen işlevleri yerine getiren bir araçtır. Bu nedenle 151. Maddeyle 244. Maddenin 1. fıkrası birbirinden tamamen farklı iki suç tipini düzenlemekte ve suç politikasıyla belirlenen iki farklı hukuksal değeri koruma altına almaktadır. Dolayısıyla iki madde arasında özel hüküm – genel hüküm ilişkisi bulunmadığı gibi salt mala zarar verme kastıyla yapılan bir eyleme 151. Maddenin uygulanması gerekirken 244. Maddenin gerekçesinde çelişkili şekilde *"ızrar"* yazıyor diye bu maddenin uygulanması da söz konusu olmamalıdır; çünkü maddelerin gerekçelerinde suç tipini oluşturan eylemlerin ya da suçun konusunu oluşturan nesnelerin belirlenmesi mümkün değildir.[277]

Yukarıda da belirttiğimiz üzere TCK'nin 243. Maddesinde düzenlenen *"hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu"* inceleme konusu suç tipi açısından geçit suçu oluşturmamaktadır. Zira 244. Maddenin 1. ve 2. fıkralarındaki suçların mutlaka 243. Maddedeki eylem gerçekleştirilmek suretiyle işlenmesi gerekmez. Dolayısıyla failin 244. Maddenin 1. ve 2. fıkralarındaki suçları işlemek için, 243. Maddedeki suçu da işlemesi halinde faile, her iki suçtan da ayrı ayrı ceza verilmesi gerekmektedir.[278]

2.2.4.5. Yaptırım, Soruşturma ve Kovuşturma

TCK'nin 244.maddenin 1. ve 2. fıkralarında yer alan her iki suç için de yalnızca hürriyeti bağlayıcı ceza öngörülmüştür. Yasada bu suçların cezası olarak 1.

[277] Dülger, 2015, **a.g.e.**
[278] Aynı.

fıkra açısından bir yıldan beş yıla kadar hapis cezası, 2. fıkra açısından ise altı aydan üç yıla kadar hapis cezası öngörülmüştür. Suçun düzenlendiği 244. Maddenin 3. Fıkrasında yer alan suçun nitelikli halinin gerçekleşmesi halinde ise faile verilecek olan ve alt ile üst sınırı yukarıda belirtilmiş olan cezalar yarı oranında artırılacaktır.

Bilişim sisteminin işleyişini engelleme veya bozma eylemi, sistemde yer alan verilere yönelik eylemlere göre daha ağır nitelikte görülerek, 1. fıkradaki eylem için 2. fıkradaki eyleme göre daha ağır ceza öngörülmüştür. Bu yaklaşım, bilişim sisteminin işleyişinin, sistem içinde yer alan verilere göre daha önemli sayılmasından kaynaklanmaktadır. Ancak, çoğu zaman bilişim sistemi içerisindeki bir veri, bilişim sistemin işleyişinden çok daha değerli ve önemli olabilmektedir. Böyle bir olasılıkta verinin değeri, 244. Maddenin 2. fıkrasında yapılacak bir düzenleme ile suça konu verinin değerinin mağdur açısından çok önemli olması halinde cezanın artırılması mümkün hale getirilmelidir.[279]

TCK'nin 246. maddesi gereğince bu suçun işlenmesinden tüzel kişilerin hukuka aykırı yarar sağlaması halinde, bunlara TCK'nin 60. maddesinde gösterilen kendilerine özgü güvenlik tedbirleri uygulanacaktır.

Mahkemelerin görev ve yetkilerinin düzenlendiği 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10., 11. ve 12. Maddeleri uyarınca bu suçların yargılanmasında görevli mahkeme, asliye ceza mahkemesidir.[280]

2.2.5. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu (m. 244/4)

TCK'nin 244. maddesinin 4. fıkrasında *"bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu"* düzenlenmiştir. Özellikle bilişim sistemi aracılığıyla hileli ya da aldatıcı hareketler yapılarak haksız çıkar sağlanmasında, hileli ya da aldatıcı hareketlerin kişiye karşı yapılmaması, fiillerin bilgisayar sistemi içerisinde yapılması ve bilişim sisteminde somut olmayan veriler üzerinden suçun işlenebilmesi nedeniyle, mukayeseli hukukta klasik dolandırıcılık ve hırsızlık suçlarından farklı

[279] Yılmaz, Sacit, **a.g.e.** , s. 85.

[280] ***5235 Sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun***, (Erişim) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5235.pdf , s. 8954-8955.

olarak bilişim sistemleri aracılığıyla yarar sağlama hali yeni bir suç tipi olarak kabul edilmiştir.[281]

Bu suç tipi 244. maddenin 4. fıkrasında, 1. ve 2. fıkralarda yer alan suç tiplerine atıf yapılmak suretiyle düzenlenmiştir. Her iki fıkra birlikte okunduğunda 244. maddenin 4.fıkrasında yer alan suç tipi şu şekilde olmaktadır:[282]

"Bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemin içerdiği verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi, erişilmez kılınması, değiştirilmesi ve yok edilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanmasının başka bir suç oluşturmaması halinde iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur".

Bu suç tipi 765 sayılı ETCK'da 525 b/2 maddesinde çok geniş bir şekilde düzenlenmiş ve durum öğretide eleştirilmiş, uygulamada ise çeşitli zorluklara yol açmıştır. 5237 sayılı TCK'da bilişim suçları düzenlenirken öğretiden gelen bu eleştiriler dikkate alınmış ve ETCK'daki suç tipi olması gerektiği gibi dört parçaya bölünmüştür. Buna göre ETCK'nin 525 b/2 maddesinin içerdiği *bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlamak, banka ve kredi kartlarını kötüye kullanmak, bilişim sistemi aracılığıyla dolandırıcılık ve bilişim sistemleri aracılığıyla hırsızlık* eylemleri farklı suç tipleri olarak düzenlenmiştir. İşte işleme konusu olan suç tipiyle de yalnızca "*bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama*" eylemi düzenlenmiş ve bunların nasıl gerçekleştirileceği suç tipinde açıkça belirtilmiştir.

Ayrıca, suç tipinin düzenlendiği 4.fıkrada "*başka bir suç oluşturmaması halinde*" ifadesi kullanılarak, aynı eylemlerin gerçekleştirilmesi suretiyle hukuka aykırı yarar elde edilmesinin başka bir suçu oluşturması halinde 244.maddenin 4.fıkrasının uygulanmayacağı belirtilmiştir. Bu düzenleme ile ne anlaşılması gerektiği yasanın gerekçesinde belirtilmiştir; buna göre;[283]

"Bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir".

---

[281] Yılmaz, Sacit, **a.g.e.**, s. 85.

[282] ***5237 Sayılı Türk Ceza Kanunu***, Madde 244, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

[283] Türk Ceza Kanunu, Türk Ceza Kanunun Madde Gerekçeleri, (Erişim) www.**ceza**-bb.adalet.gov.tr/mevzuat/**madde**gerekce.doc , 13.12.2016, s. 264.

Ancak görüldüğü üzere, suç normundaki düzenleme ile gerekçe arasında farklılık bulunmamaktadır.

2.2.5.1. Suçla Korunan Hukuksal Değer

Bu suçun yasa maddesindeki tanımına göre, failin bilişim sistemi aracılığıyla gerçekleştirdiği eylemler neticesinde suçun oluşması için failin hukuka aykırı bir yarar elde etmesi gerekmektedir; ancak bunun nasıl bir yarar olduğu açıklanmamıştır. Yararın türü bakımından bir ayrım yapılmadığına göre fail tarafından elde edilen maddi ya da manevi yarar suçla korunan hukuksal değeri oluşturmaktadır.[284]

Failin elde ettiği yarar, suçun mağduru açısından bir zarar oluşturmaktadır ve bu suçla mağdurun zarara uğratılan hakkı korunmaktadır. Ancak belirtelim ki, uygulamada fail açısından yarar mağdurun açısından ise zarar oluşturan bu değerin, aşağıda yer verdiğimiz Yargıtay kararlarında da görüleceği üzere, genellikle malvarlığına ilişkin, özellikle de para cinsinden bir değer olduğu görülmektedir. Ancak bununla sınırlı değildir.

ETCK'nin 525 b/2 maddesinde düzenlenen "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçu" ile korunan hukuksal değer konusunda öğretide çeşitli tartışmalar ve görüşler bulunmakta idi; çünkü bu suç tipi ile birden fazla suç tipinin *"bilişim sistemleri aracılığıyla işlenmesi"* durumu düzenlenmekteydi. TCK'nin 244. maddesinin 4. fıkrasında düzenlenen *"bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçu*" açısından ise benzer tartışmaların olması mümkün görülmemektedir; çünkü bu suç tipi diğer suç tiplerinden ayrılmış ve maddi unsurunu oluşturan eylemler tek tek gösterilmiştir. Bu nedenle artık ETCK'nin 525 b/2 maddesi açısından belirtilen suçla korunan hukuksal değerin *"kişinin malvarlığı olduğu*" görüşü TCK'nin 244. maddesinin 4. fıkrasında düzenlenen suç tipi açısından geçerli olmamaktadır.

244. maddenin ifadesinden ve gerekçesinden çıkarılan sonuç *"dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunun*" bu madde kapsamı içinde olmadığıdır; söz konusu suç tiplerinden özellikle dolandırıcılık ve hırsızlık suçlarında malvarlığı korunmaktadır. İnceleme konusu suç tipini oluşturan eylemlerin gerçekleştirilmesi nedeniyle mağdurun malvarlığında bir zararın meydana gelmesi

[284] Yılmaz, Sacit, **a.g.e.**, s. 87.

durumunda ise genellikle ya dolandırıcılık suçu ya da hırsızlık suçu gerçekleşmiş olacaktır. Dolayısıyla bu suç tipinin yeni düzenlemesi karşısında suçla korunan hukuksal değerin mağdurun manevi bir hakkının olması da olası görülmektedir.

2.2.5.2. Fail

Bu suçun faili herkes olabilir, yasada bu açıdan bir özellik gösterilmemiştir. Bunun dışında fail konusunda 244.maddenin 1. ve 2. fıkralarında düzenlenen suç tipleri açısından yapmış olduğumuz açıklamalar bu suç tipi açısından da geçerlidir.

2.2.5.3. Mağdur

Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçunda mağdur açısından herhangi bir özellik aranmamıştır. ETCK'nin 525 b/2 maddesinde düzenlenen benzer suç tipi için mağdur konusunda öğretide çeşitli görüşler ortaya çıkmıştır. Buna göre bazı yazarlar bu suçun mağdurunun bilişim sisteminin maliki ya da zilyedi olabileceğini belirtirlerken,[285] bazı yazarlar da bu suçun mağdurunun bilişim sisteminin maliki ve zilyedinin yanı sıra bunların müşterisi de olabileceğini kısaca failin gerçekleştirdiği eylem sonucu zarar gören herkesin bu suçun mağduru olacağını ifade etmektedirler[286].

Aynı tartışmaların gerçekleşmesi TCK'da düzenlenen bu suç tipi açısından da olasıdır. Ancak bu suçun mağdurunu bilişim sisteminin maliki ve zilyediyle sınırlamak mümkün değildir; çünkü özellikle verilere zarar verilerek hukuka aykırı yarar sağlanması durumunda, zarara uğratılan verilerin maliki ile verilerin üzerinde kayıtlı olduğu bilişim sisteminin ya da veri taşıma aracının maliki aynı kişiler olmayabilecektir. Hatta mağdur olmak için zarara uğratılan verilerin maliki dahi olunması gerekmemektedir, bir şekilde verinin ilgilisi olmak suçun mağduru olmak için yeterlidir.

Örneğin bir internet servis sağlayıcısından aldığı erişim, teknik destek ve veri taşıma hizmetiyle (host) üyelerine günlük ekonomi haberlerini ve tahminleri ileten bir internet sitesinde bulunan verilerin, rakip site tarafından değiştirilmesi yoluyla yanlış haber ve değerlendirmelerin girilmesi sonucu, güvenilirliğinin zedelenmesi

[285] Yazıcıoğlu, **a.g.e.** , s. 256; Yenidünya ve Değirmenci, **a.g.e.** , s. 188.
[286] Akıncı, Alıç ve Er, **a.g.e.** , s. 147.

durumu ortaya çıkacaktır. Böylece rakip site tarafından haksız yarar sağlanması durumunda, ekonomi haberleri veren site ne bilişim sisteminin ne de verilerin malikidir ancak mağdur durumundadır. Aynı şekilde; internette yayınlanan bir sanal ekonomi gazetesinde sistemdeki veriler değiştirilerek bir ticari şirket hakkındaki olumlu haberlerin olumsuz haberlere dönüştürülmesi sonucu şirketin hisse senetlerinin menkul değerler borsasında aniden değer kaybetmesi ya da bu haber yüzünden şirketin bir krediyi alamaması durumunda da, şirket mağdur olacaktır.

Bu suçun bir başka işlenme şekli de yeni TTK'daki düzenlemelerden kaynaklanabilecektir. 6102 sayılı yeni TTK'nın 1524. maddesinde ticaret şirketleri için internet sitesi açmak ve ister yeni açılsın, ister hali hazırda mevcut olsun bu sitede 1524.maddede belirtilen şirketçe kanunen yapılması gereken ilanlar, şirketin mali durumu ve ortaklık yapısına ilişkin bilgiler ile şeffaflık ilkesi ve bilgi toplumu açısından açıklanması zorunlu bilgiler gibi duyuru ve bilgilerin bu sitelerde yer alması gerekmektedir.

TTK'nın "Suçlar ve Cezalar" başlıklı 562. maddesinin 12. fıkrasında ise 1524. maddede belirtilen yükümlülüklere uyulmaması şirket yöneticileri açısından suç haline getirilmiştir. İşte failin ticaret şirketinin web sitesine erişimi olanaksız hale getirmesi, verileri değiştirerek gerçek dışı veriler yüklemesi ya da TTK'ya göre bulunması gereken verileri yok etmesi, şirket yöneticileri için hem cezai yaptırım uygulanmasına hem de itibar kaybına neden olacaktır. Bu sonuçların özellikle haksız rekabet yapan rakip şirketler ya da bu kişi ya da şirketlere karşı kişisel düşmanlık besleyen kişiler açısından maddi ya da manevi yarar sağlayıcı olduğu tartışmasızdır. Dolayısıyla suçun mağduru suçun işleniş şekline göre değişiklik gösterecektir.

2.2.5.4. Suçun Konusu

Bu suçunun konusunu failin sağladığı *"hukuka aykırı yarar*" oluşturmaktadır. Bu yarar ekonomik değeri olan mali bir yarar olabileceği gibi ekonomik bir getirisi ve değeri olmayan tamamen duyguları tatmine yönelik manevi bir yarar da olabilecektir. Ancak yukarıda da belirttiğimiz üzere, suç tipinde kuramsal olarak bu yönde bir sınırlama olmamakla birlikte uygulamada genellikle suçun konusunu malvarlığı değerlerinin oluşturduğu görülmektedir.

2.2.5.5. Eylem

Bu suç tipi 244. maddenin 4. fıkrasından aynı maddenin 1. ve 2.fıkralarına yapılan atıfla düzenlendiği için; 244.maddenin 1. ve 2.fıkralarında düzenlenen bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunun maddi unsurunu oluşturan eylemler, bu suçun da eylem unsurunu oluşturmaktadır. Buna göre bu suçun oluşabilmesi için failin bilişim sisteminin işleyişini engellemek, bilişim sistemin işleyişini bozmak, verileri bozmak, bilişim sistemine veri yerleştirmek, bilişim sisteminde var olan verileri başka bir yere göndermek, verileri erişilmez kılmak, verileri değiştirmek ve verileri yok etmek hareketlerinden birini ya da bir kaçını gerçekleştirmesi gerekmektedir. Dolayısıyla, bu suç da seçimlik hareketli bir suç olarak düzenlenmiştir.[287]

Söz konusu hareket biçimleri 244. maddenin 1. ve 2. fıkralarında düzenlenen suç tipleri açısından yukarıda ayrıntılı olarak açıklanmıştır; inceleme konusu suç tipini oluşturan eylemlerle ilgili açıklamalar açısından 244. maddenin 1. ve 2. fıkralarında yer alan suç tiplerinin eylem unsuru konusuna bakılabilir.

Bu suç tipini oluşturan hareketlerden birisi olan verilerin değiştirilmesi suretiyle hukuka aykırı yarar sağlamak hareketine örnek olarak, manyetik telefon kartlarının üzerindeki verilerin değiştirilmesi suretiyle ücret ödenmeksizin telefon görüşmesi yapılması gösterilebilir. Nitekim Yargıtay Ceza Genel Kurulu buna ilişkin vermiş olduğu kararında, bu eylemin bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunu oluşturduğuna karar vermiştir:[288]

"Sanığın telefon kulübelerinden topladığı kredisi bitmiş telefon kartlarına barkod ve manyetik bant yapıştırmak suretiyle kontör yükleyip bunları diğer sanık S….. T….. ile birlikte katılan Kurum'a ait kulübelerde bulunan telefon cihazlarına sokup kullandıkları, bu yöntemle kısa süre içinde toplam 35210 kontörlük görüşme yapıldığı dosyadaki kanıtlardan anlaşılmaktadır…

Ankesörlü telefonlar, manyetik kart, kredi kartı ve smart kart ile çalışan hizmet telefonlarıdır. Bu telefonlar katılan Kurum tarafından ücretsiz olarak meydanlar, hastaneler, terminaller, garlar, limanlar, metro istasyonları, askeri tesisler, toplu konut alanları gibi halka açık yerlere tesis edilmekte, ARMS olarak adlandırılan merkezi bilgisayar sistemi ile yönetilmektedir. ARMS sisteminin, suçun işlendiği bölgede hizmet veren ve kendisine bağlı olan 200 adet D-3 manyetik kartlı ankesör makinesinin çalışma bilgilerini, (kullanılan kontör miktarı, manyetik karta ait barkod numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi

[287] Dülger, 2004, **a.g.e.** , s. 246.
[288] Bikirli, **a.g.e. ,** s. 18.

v.s) bünyesinde topladığı anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkod numaraları dahi bu sayede tespit edilebilmiştir. Suç tarihinde kullanılan sistemin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura ihtiyaç vardır. Bunlardan birincisi, manyetik telefon kartı, diğeri ise kontör olarak adlandırılan kredidir. Bunlara sahip olunmadan, bir bilgi işlem biriminin parçası olan ve ARMS denilen sisteme bağlı bulunan ankesörlü makinelerden, Kurum'ca acil durumlarda kredisiz görüşme yapılabilmesine olanak sağlanmış bulunan sınırlı sayıdaki numara dışında görüşme yapılabilmesine olanak yoktur. Bu *sistemde, manyetik kart üzerindeki barkodu okuyan makine, manyetik kart üzerinde kullanılmış kredi bilgileri bulunmadığı taktirde, okuduğu taktirde, okuduğu kartın kredi sınıflandırma özelliklerine göre 100, 60 veya 30 kontör kredi yüklemesi yapmak suretiyle kulanıma hazır hale getirmekte, kullanım süresince yaptığı hesaplamaların sonucuna göre kalan kredi miktarını saptayıp manyetik karta işlemektedir. Başka ifadeyle sistem, makineye takılan karttaki verilerin alınıp değerlendirilmesi suretiyle işlemektedir.*

Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasasının 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren 5237 sayılı Türk Ceza Yasasının 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır. Uygulamada hangi Yasanın daha lehe sonuç verdiği hususu da Yerel Mahkemece değerlendirilip saptanmalıdır. Bu itibarla, Yargıtay Cumhuriyet Başsavcılığı itirazının reddine karar verilmelidir."[289]

Ancak bu karara muhalefet şerhinde, bilişim sistemlerini daha dar yorumlayarak telefonlarının bilişim sistemine dâhil olmadığını zira genel işlem yapabilme kapasitelerinin bulunmadığını, dolayısıyla bu olayda karşılıksız yararlanma suçunun oluştuğu belirtilmektedir. Bu davayla ilgili olarak yapılan değerlendirme ise şu şekildedir:[290]

"...bilişim sistemleri aracılığıyla haksız yarar sağlama eylemlerinin kapsamının daraltılması suretiyle ayrı bir suç olarak düzenlenmesinin sonucu olarak uygulamada daha kesin çizgilerle bir takım sağlıklı sonuçlara varılmakta; suç teşkil eden fiillerin tasnifi kolaylaşırken, daha adil cezalara hükmolunmaktadır. İncelenen karar uyarınca somut olayda dolandırıcılık suçu bakımından unsur olarak aranan hileli davranışların gerçek kişiye yönelmesi ve özellikle bu hileli davranışlar neticesinde mağdurun veya bir başkasının malvarlığı aleyhine ve sanığın veya başkasının yararına haksız bir menfaat sağlanması şartı gerçekleşmediğinden

[289] T.C. YARGITAY 11. CEZA DAİRESİ E. 2006/1800 K. 2008/7126 T. 1.7.2008, (Erişim) http://www.cetinavukatlik.com/2015/11/15/bilisim-sistemleri-araciligiyla-haksiz-yarar-saglama/ 13.12.2016.

[290] T.C. YARGITAY 11. CEZA DAİRESİ E. 2006/1800 K. 2008/7126 T. 1.7.2008, (Erişim) http://www.cetinavukatlik.com/2015/11/15/bilisim-sistemleri-araciligiyla-haksiz-yarar-saglama/ 13.12.2016.

sanığın eylemleri; bilişim sistemini engelleme, bozma verileri yok etme veya değiştirme suretiyle haksız yarar sağlama olarak belirlenmiş, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezası yerine iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası aralığı benimsenmiştir. TCK madde 244/4 ile tanımlanan suçun, yardımcı norm olarak düzenlenmiş olması ve fakat dolandırıcılık suçunun özel bir şekli olarak düşünülmemesi karşısında bu suçun unsurları ile klasik dolandırıcılık suçuna göre sınırlarının belirlenmesi önemlidir. Somut olayda sanığın, katılan Türk Telekom A.Ş. tarafından üretilen ve ankesörlü telefonlardan konuşma yapmaya yarayan telefon kartlarının manyetik şeritleri üzerinde bir takım değişiklikler meydana getirerek sistemin verileri farklı algılamasını sağladığı ve sistemi yanıltmak suretiyle kaçak görüşmeler yaptığı, böylelikle hukuka aykırı yarar elde ettiği; ancak gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin saptanamaması nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı anlaşılmaktadır. Zira 5237 sayılı TCK'nin 243. madde metninde kullanılan "bilişim sistemi" ibaresi ile madde gerekçesinde bilişim sistemi, "Verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistem" olarak tanımlamıştır. Burada kullanılan veri kavramınınsa, bilişim suçlarının üzerinde işlendiği suç konusu olduğu kabul edilmiştir. Bunun yanında tamamen bilişim sistemi içinde gerçekleştirildiğinden dolandırıcılık suçunun unsurlarını taşımayan eylemin, değiştirilen verilerin taşınabilir bir mal olarak kabul edilmesinin olanaklı olmaması nedeniyle hırsızlık suçunun unsurlarını da taşımadığı açıktır. Zira hırsızlık suçunun tanımlandığı madde metninde "Zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya başkasına bir yarar sağlamak maksadıyla bulunduğu yerden alan kimse" hakkında cezaya hükmolunacağı açıklanmaktadır. Bu suçun nitelikli hali olarak "Bilişim sistemlerinin kullanılması suretiyle" gerçekleştirilmesinin söz konusu olabilmesi için de yine suç konusu bakımından taşınabilir bir mal olması şartı arandığı sonucuna varılmaktadır. Bu bakımdan başka bir suç oluşturmadığı tespit olunan somut olaya ilişkin eylemlerin, bilişim sistemleri aracılığıyla haksız yarar sağlama suçunu oluşturduğu kabulü, yasanın lafzına ve ruhuna uygun bulunmaktadır."

2.2.6. Tehdit ve Şantaj

Bilişim aracılığıyla tehdit, günümüzde çokça kullanılan bilişim suçu yöntemlerindendir. Özellikle internetin kullanıcılarına anonim kimlik vermesi, kötü niyetli kişileri, diğer mağdur sıfatı kazanacak kişileri e – posta, anlık mesajlaşma, sosyal paylaşım sitelerinde mesaj, yorum vb. yollarla çeşitli sebepleri öne sürerek maddi ve manevi tehdit yoluna başvurmaktadır.

Farklı ülkelerde konuyla ilgili yapılan çalışmalar incelendiğinde siber zorbalığın okullarda yaygın bir sorun olduğu anlaşılıyor. 2007'de Kanada'da yapılan bir araştırmada, çalışmaya katılan bireylerin yüzde 27,3'ünün e-posta aracılığıyla, yüzde 36,4'ünün ise sohbet odalarında sanal zorbalığa maruz kaldığı görülüyor. Aynı yıl ABD'de yapılan bir diğer çalışmaya göre katılımcılardan yüzde 11'inin son 2 ay içerisinde sanal zorbalığa maruz kaldığı ifade ediliyor. Türkiye'deki durumun diğer

dünya ülkelerinden çok da farklı olduğu söylenemez. 2007 yılında yapılan bir araştırmaya göre Türkiye'deki 'sanal zorba' oranının yüzde 28, 'sanal kurban' oranının ise yüzde 30 olduğu belirtiliyor. Öyle ki, örnekler arasında kişisel tacizler, sanal ilişki teklifleri, bir başkasının bilgisini kullanarak e-mail yoluyla şantaj, tehdit, şifre kırma, sistemi ele geçirme yer alıyor. Sanal tehlikelerin yol açtığı intihar olayları Türkiye'de de görülmektedir. [291]

TCK'nin 106. Maddesine göre,

(1) Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit eden kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. Malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehditte ise, mağdurun şikâyeti üzerine, altı aya kadar hapis veya adlî para cezasına hükmolunur.

(2) Tehdidin;

a) Silahla,

b) Kişinin kendisini tanınmayacak bir hale koyması suretiyle, imzasız mektupla veya özel işaretlerle,

c) Birden fazla kişi tarafından birlikte,

d) Var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak,

İşlenmesi halinde, fail hakkında iki yıldan beş yıla kadar hapis cezasına hükmolunur.

(3) Tehdit amacıyla kasten öldürme, kasten yaralama veya malvarlığına zarar verme suçunun işlenmesi halinde, ayrıca bu suçlardan dolayı ceza verilir. (TCK, m. 106)

TCK'nin 73. Maddesine göre, şikâyete bağlı suçlarda zaman aşımı 6 ay olarak düzenlenmiştir.

Bir kimseyi, bir şeyi yapmaya veya yapmamaya zorlamanın özel bir şeklini teşkil eden şantaj suçu, TCK'nin özel hükümler başlıklı ikinci kitabında, hürriyete karşı suçların düzenlendiği yedinci bölümde yer alan suç tiplerinden biridir.[292] Suç, TCK'nin 107. maddesinde şu şekilde düzenlenmiştir:

"Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlayan kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır. (Ek fıkra

[291] İnternette Zorbalık - Katlanmak zorunda değilsiniz, Şikâyet edin, (Erişim) http://www.guvenliweb.org.tr/guvenlik/node/154, 10.Ocak.2016

[292] Üzülmez, İlhan, ***Yeni Türk Ceza Kanunu'nun Hürriyete Karşı İşlenen Suçlar Sistemi Çerçevesinde Tehdit, Şantaj ve Cebir Kullanma Suçları***, Ankara, Turhan, 2007, s. 131.

29.06.2005 tarihli ve 5377 sayılı Kanun m. 14) Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde de birinci fıkraya göre cezaya hükmolunur."[293]

Maddeyle, şantaj fiilleri suç hâline getirilmiş olmaktadır. Şantajda da kişiyi bir şeyi yapmaya veya yapmamaya zorlama söz konusudur. Ancak, bu durumda kişiye bir kötülük yapılacağından, kişinin sahip bulunduğu bir değere saldırıda bulunulacağından bahisle bir zorlama söz konusu değildir. Aksine, kişi, hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle başkasını zorlamaktadır. Örneğin, kişinin suç işlemiş olan bir kimseyi ihbar edeceğinden bahisle, kendisine bir menfaat temin etmeye zorlaması hâlinde, şantaj suçu oluşur. İşlenmiş olan bir suç vakıası karşısında ihbarda bulunmak, kişiler açısından hem bir haktır hem de bir yükümlülüktür. Aynı şekilde, bir gazetecinin, bir siyasî şahsiyeti, kendisine muayyen miktar para verdiği takdirde, hakkında ileri sürülen yolsuzluk iddialarını haber konusu yapmayacağından bahisle, menfaat teminine zorlaması hâlinde şantaj suçu oluşur.[294]

Şantaj yapılmakla, kişi kanuna aykırı bir davranışta bulunmaya zorlanmış olabilir. Örneğin belediyede meclis üyesinin, yaptırmış bulunduğu kaçak inşaatı yıktırması hâlinde belediye meclisinde muhalefetle işbirliği yapacağından bahisle belediye başkanının bu inşaatı yıktırmamaya zorlaması; keza, taahhüt işleriyle uğraşan bir kişinin, belediye başkanını bir yol inşaatına ilişkin ihalenin kendilerine verilmemesi halinde, hakkında rüşvet suçundan dolayı ihbarda bulunacağından bahisle bu ihaleyi mevzuata aykırı olarak kendisine verdirmeye zorlaması, şantaj suçunu oluşturur.

Şantaj yapılmakla, kişi yükümlü olmadığı bir davranışta bulunmaya zorlanabilir. Örneğin, bir iş adamının, kamu oyunda gündemde olan yolsuzluk olaylarıyla ilgili olarak hazırlanan gazete haberinde adından söz etmeme karşılığında menfaat teminine veya bir kuruluşa bağışta bulunmaya zorlanması hâlinde, şantaj suçu oluşur. Şantaj suçunun oluşabilmesi için, mağdurun zorlanması yeterlidir. Bu

[293] 5237 Sayılı Türk Ceza Kanunu, Madde 107, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237 , 12 Aralık 2016.

[294] Taner, Fahri Gökçen, Ceza Hukukunda Şantaj Suçu, ***TBB Dergisi***, 92, 2011, s. 121-122.

zorlama karşısında, mağdurun isteneni yapması suçun oluşması için gerekli değildir.[295]

Şantaj suçunun ortaya koyduğu özellik, kişinin hak veya yükümlülüklerini kötüye kullanarak haksız bir çıkar sağlamaya çalışması ya da başkasını bir şeyi yapmaya veya yapmamaya mecbur etmesidir. İster tehdit suçu isterse şantaj suçu olsun, birebir bilişim suçları içinde yer almasa da, dolaylı olarak bilişim suçları arasında yer almaktadır.

Tehdit suçu internetin bir iletişim aracı olarak kullanılması yoluyla da gerçekleştirilebilir. İnternet üzerinden gönderilen bir elektronik posta içeriğinde bir kişiyi vücut dokunulmazlığına saldırı gerçekleştirileceğinden bahisle tehdit eden fail, bu eyleminden dolayı cezalandırılacaktır. Tehdit eylemi, elektronik posta, hızlı mesaj, sohbet, web sitesi gibi internette sunulan hizmetlerden herhangi birisiyle gerçekleştirilebilir.[296]

Şantaj suçu internetin bir iletişim aracı olarak kullanılması yoluyla da gerçekleştirilebilir. İnternet üzerinden gönderilen bir hızlı mesaj içeriğinde bir kişiye şantaj yapan fail, bu eyleminden dolayı cezalandırılacaktır. Şantaj eylemi, elektronik posta, hızlı mesaj (ICQ, MSN Messenger), sohbet (chat) gibi internette sunulan hizmetlerden herhangi birisiyle gerçekleştirildiğinde bilişim alanında bir suç haline gelmektedir.[297]

2.2.7. Haberleşmenin Engellenmesi

Haberleşmenin engellenmesi konusu 5237 Sayılı TCK'nin 124. Maddesinde ele alınmaktadır. Bu maddeye göre;[298]

"Madde 124
(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.
(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

---

[295] 5237 Sayılı Türk Ceza Kanunu Madde Gerekçeleri Madde 107, s.51, (Erişim) www.ceza-bb.adalet.gov.tr/mevzuat/madde**gerekce**.doc , 12 Aralık 2016.
[296] Çekiç, Burak, ***İnternet Aracılığıyla İşlenen Suçlar***, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 102.
[297] Çekiç, **a.g.e.** , s. 103.
[298] ***5237 Sayılı Türk Ceza Kanunu***, Madde 124, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur."

5237 sayılı TCK'nin İkinci Kitabı'nın *"Kişilere karşı suçlar"* başlıklı İkinci Kısmı'nın *"Hürriyete karşı suçlar"* başlıklı Yedinci Bölümü'nün 124. Maddesinde düzenlenen *"haberleşmenin engellenmesi suçu"*, her türlü iletişim aracıyla yapılan haberleşmeyi kapsamakta ve dolayısıyla bilişim sistemleri aracılığıyla yapılan iletişimi de içermektedir.

Günümüzde gerçekleştirilen haberleşmenin büyük bir çoğunluğunu elektronik posta ve sohbet oluşturmaktadır. Bu yöntem diğerlerine göre hem daha ucuz hem de çok daha hızlı olması nedeniyle artık daha çok tercih edilir hale gelmiştir. Bunların yanı sıra, veri iletim ağları üzerinden yapılan telefon görüşmeleri ve telekonferanslar da elektronik haberleşmenin diğer çeşitleri olarak görülmektedir.

TCK'nin inceleme konusu maddesinde yalnızca haberleşme denildiği, bu haberleşme araçları tek tek sayılmadığı için haberleşme hangi araçla gerçekleştirilirse gerçekleştirilsin bunun engellenmesi inceleme konusu suçu oluşturacaktır, nitekim bu durum maddenin gerekçesinde de açıkça ifade edilmiştir. Bu nedenle bilişim sistemleri aracılığıyla gerçekleştirilen haberleşmenin engellenmesi eylemleri de TCK'nin 124. maddesinde düzenlenen suç tipinin koruma kapsamında değerlendirilecektir. Bilişim sistemleri üzerinden yapılan haberleşmenin engellenmesi amacıyla bilişim sistemine veya sistemde yer alan verilere zarar verilmesi halinde ise failin tek eylemiyle yasanın birden fazla suç normu ihlal edilmiş olacağı için, düşünsel birleşme kuralı uygulanarak cezası daha fazla olan suçun cezası faile verilecektir. Bu durumda failin kişiler arasındaki haberleşmeyi engellemek amacıyla bu eylemi gerçekleştirmesi halinde TCK'nin 244/1-2. maddesinde düzenlenen bilişim sistemine ve verilere zarar vermek suçu uygulanacaktır. Failin 124. maddenin 2. fıkrasında düzenlenen kamu kurumları arasındaki haberleşmeyi engellemek amacıyla eylemini gerçekleştirmesi halinde ise, bu suçun cezası 244/1-2'ye göre daha fazla olduğu için faile 124/2. madde uygulanacaktır. [299][300]

[299] Dülger ve Modoğlu, **a.g.e.** , s. 75-76.

[300] Yokuş Sevük, Handan, "Haberleşme Hakkının Kullanımının Türk Ceza Kanunu Hükümleri ile Korunması (Tck M.124, Tck M.298/1)", (Erişim) www.dicle.edu.tr/Contents/a3dba4dd-975a-47d3-98c3-76e3fd469268.pdf, (06.02.2017).

2.7.8. Hakaret

5237 sayılı TCK, hakareti kişisel hak ve özgürlüklere bir saldırı olarak görmüş, bu nedenle de hakareti bir suç olarak 125. Maddesinde;[301]

"Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnatta bulunmak veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran..... Mağdurun gıyabında hakaretin cezalandırılabilmesi için, fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir"

şeklinde düzenlenmiştir.

Hakaret suçunda maddi unsuru incelerken ikili bir ayrım yapmak gerekir. Birincisi, somut bir fiil veya olgu isnadında bulunma, ikincisi sövmedir. Somut bir fiil veya olgudan anlaşılması gereken, maddi bir olaydır. Yani, dış dünyadan algılanabilen, dış dünyada bazı değişikler yaratabilen fiili bir durumdur. Bu nedenle sövme, somut fiil veya olgu isnadında, yer ve zaman gösterilmesi gerekir. Örneğin, sen dün şu yerden şu saatte şunları alarak hırsızlık yaptın denmesi halinde, somut fiil veya olgu isnadı söz konusu olur ve somut bir fiil veya olgu isnadı suretiyle hakaret suçu işlenmiş sayılır. Somut bir fiil veya olgu isnadının mutlaka suç olması veya gerçek olması gerekmez. İsnatta bulunulan durumun suç olması, hakaret suçunun varlığına engel olmamalıdır. Bir kişiye isnat edilen somut bir fiil veya olgunun geçmişte işlenmiş veya halen yapılmakta olan bir duruma ilişkin olması gerekir. Yoksa gelecekte olabilecek bir duruma ilişkin yapılan tahminler, bu kapsamda değerlendirilemez. Ancak şartları oluşursa iftira suçu olabilir. Aynı şekilde, isnat edilen somut bir fiil veya olgu konusunda, mağdurun yeteneğinin olup olmaması da önemli değildir. Mesela, hadım olan veya iktidarsız olan bir kişiye, 15 yaşını bitirmiş bir kızla rızaya dayalı bir cinsel birleşme isnadında bulunulsa bile suç gerçekleşir. Çünkü hakaret suçunda korunmak istenen hukuki yarar, mağdurun toplum içindeki, onur, şeref ve saygınlığı olunca, bu tür bir isnat, hukuki yarara zarar verebilecek niteliktedir.[302]

Hakaret suçu, doğrudan kastla işlenebileceği gibi, olası kastla da işlenebilir. Bu nedenle, bilinçli taksirle işlenmesi mümkün değildir. Ancak, kanun koyucunun olası kastla bilinçli taksiri düzenlerken, kullandığı dildeki özensizlik, bilinçli taksirle de bu

---

[301] ***5237 Sayılı Türk Ceza Kanunu***, Madde 125, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

[302] Özen, Mustafa, "Hakaret Suçu ve İnternetle İşlenmesi", ***TBB Dergisi***, Sayı 75, 2008, s.96.

suçun işlenebilme yolunu açacak niteliktedir. Çünkü iki durum arasındaki tek fark, öngörülen neticenin kabul edilip edilmemesinde yatmaktadır.[303]

İnternet üzerinden işlenen hakaret suçlarında en önemli sorun, suçun failinin belirlenmesidir. Gerçekten bu yeni teknolojik imkânın sayısız faydaları karşısında sayısız zararları da vardır. Öyle ki, zarar veren kişilerin bulunmasının zorluğu zararın boyutlarını biraz daha arttırmaktadır. İnternette kişiler kendi adlarına web sayfaları açabilmekte, e –mail adresleri alabilmektedirler. Bu web sayfası veya e-mail adresi alınırken sahte kimlik kullanılabilmektedir. Bir başka ifadeyle, takma ad veya her hangi bir gerçek dışı isimle kişiler kendi adlarına web sayfası veya e-mal adresi alabilmektedirler. Böyle bir imkânın olması, internet aracılığıyla işlenen suçlarda gerçek suçluyu bulmayı zorlaştırmakta hatta imkânsızlaştırmaktadır. Aynı şekilde, işlenen bir suçun cezai takibatının yapılabilmesi için, suçun işlendiği zamanın belirlenmesi önemlidir. Çünkü her suça ilişkin bir dava zamanaşımı söz konusudur. Suçun failinin belirlenmesindeki güçlük aynı şekilde suçun işlendiği zamanın belirlenmesinde de geçerlidir.[304]

2.2.9. Haberleşmenin Gizliliğinin İhlali

TCK'nin 132. maddesinin 1. fıkrasında, kişiler arasındaki haberleşmenin gizliliğinin ihlal edilmesi eylemleri suç haline getirilmiştir. Fıkranın diğer bir cümlesinde haberleşme içeriğinin kayıt edilmesi eylemi ayrı bir suç tipi olarak düzenlenmiştir. Maddenin 2. fıkrasında ise kişiler arasındaki haberleşme içeriğini hukuka aykırı şekilde açıklanması eylemi suç haline getirilmiştir. Kişinin kendisi tarafından yapılan haberleşmenin bu haberleşmeyi yapan diğer tarafın izni olmaksızın açıklanması da maddenin 3. fıkrasında suç hali olarak düzenlenmiştir. Haberleşme içeriğinin basın ve yayın yoluyla açıklanması da 4. fıkrada ağırlatıcı neden olarak öngörülmüştür.[305]

Gelişen teknoloji sayesinde bilişim sistemleri yardımıyla haberleşme türleri çeşitlenmiştir. Özellikle de internet aracılığıyla elektronik posta, elektronik sohbet (chat), internet üzerinden telefon görüşmesi ya da tele konferans, forum, haber

---

[303] Özen, **a.g.e.** , s. 99.
[304] Özen, **a.g.e.** , s. 106.
[305] ***5237 Sayılı Türk Ceza Kanunu***, Madde 132, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

grupları, hızlı mesaj servisleri gibi çeşitli yöntemlerle haberleşme sağlanmaktadır. Yapılan haberleşmeyi koruma altına almak ve bu tür haberleşmeyi ihlal edenleri cezalandırmak için TCK'da ilgili madde düzenlenmiştir.[306]

TCK'nin 132. Maddesi TCK'nin 195. maddesinde düzenlenen posta ve telefon haberleşmesinin gizliliği suçundan farklı olarak bu maddede yalnızca "haberleşme" kavramı kullanılmış; ancak bunun nasıl gerçekleştirildiği belirtilmemiştir. O hâlde her türlü haberleşme bu maddenin koruması kapsamındadır. İşte bilişim sistemi aracılığıyla gerçekleştirilen pek çok yeni haberleşme yöntemi de TCK'nin söz konusu maddesinin düzenlemesiyle koruma altına alınmakta ve bu tür haberleşmeyi ihlal edenler de cezalandırılmak istenmektedir. Bu durum maddenin gerekçesinde de açıkça belirtilmiştir.[307]

2.2.10. Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması

TCK'nin 133. Maddesiyle kişiler arasındaki konuların dinlenmesi ve kayda alınması durumu kanun maddesi altında üç bentte açıklanmaktadır.

"(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(3) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dört bin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."[308]

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunda, suç olarak ifade edilen konu kişilerin yaptıkları konuşmaların dinlenerek kayıt altına alınması eylemidir. Teknolojik gelişmeye paralel olarak cep telefonlarının özelliklerinin gelişerek hem ses kayıt cihazı, hem de kamera işlevini içinde barındırması, aynı zamanda ortamdaki sesleri ve görüntüyü kaydetme amaçlı cihazların boyutlarının minimize olması, söz konusu eylemlerin kolaylıkla ve sıklıkla ortaya çıkmasına neden olmaktadır.

---

[306] Çekiç, **a.g.e.** , s. 203.
[307] Dülger ve Modoğlu, **a.g.e.** , s. 76.
[308] ***5237 Sayılı Türk Ceza Kanunu***, Madde 133, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

Maddenin 1. fıkrasında kişiler arasında aleni olmayan konuşmaların taraflardan herhangi birinin rızası olmaksızın bir aletle dinlenmesi veya bunların ses alma cihazıyla kaydedilmesi suç olarak tanımlanmıştır.

Maddenin 2. fıkrasında ise, kişinin kendisinin de katıldığı aleni olmayan bir söyleşiyi ses alma cihazıyla kaydetmesi de suç olarak betimlenmiştir.

Maddenin 3. fıkrasında ise 1. ve 2. fıkralarda düzenlenen suçların işlenmesi suretiyle elde edilen bilgilerden, failin bilgilerin bu özelliğini bilerek yarar sağlaması veya bunları başkasına vermesi veya diğer kişilerin bilgi edinmesi sağlaması halleri suç olarak düzenlenmiştir. Ayrıca bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de aynı cezanın verileceği belirtilmiştir.[309]

İlk iki fıkradaki suçları işleyen fail, daha sonra son fıkrada yer ala suçu da işlerse, bu suçların ikisi için de farklı farklı cezalandırılması söz konusudur. Çünkü konuşmayı dinleyen ve kayıt altına alan kişinin mutlak surette bunları açıklayarak, üçüncü şahıslara vererek, bir fayda elde etmesi gerekli değildir. Son fıkrada yer alan suçu işlemek için fail ya da failler, ilk iki fıkrada yer alan suçlardan en az birini işlemelidir. Bu nedenle de, son fıkradaki suçun cezalandırılıp, ilk iki fıkradaki suçların cezasız bırakılması, olanaksızdır.[310]

2.2.11. Özel Hayatın Gizliliğini İhlali

TCK'nin 134. Maddesi özel hayatın gizliliğinin ihlali durumunu bir suç olarak ifade etmektedir ve ilgili madde şu şekildedir:[311]

"(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat arttırılır.

(2)Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

Özel hayatın gizliliğini ihlal suçu sıklıkla görülmekte ve basın organları yoluyla özel hayatın gizliliğini ihlal eden eylemlere büyük ölçüde rastlanmaktadır.

---

[309] **Türk Ceza Kanunu Madde Gerekçeleri**, İkinci Kısım, Dokuzuncu Bölüm: Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar, 133. Madde Gerekçesi, s. 219.

[310] Aynı.

[311] ***5237 Sayılı Türk Ceza Kanunu***, Madde 134, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

Söz konusu suç, 5237 Sayılı TCK'yla ceza hukukuna 134. Maddeyle kazandırılan yeni bir suç tipi olarak karşımıza çıkmakta, bu maddeyle amaçlanan da Anayasa da Madde 20'de yer alan kişilerin özel hayatının ve aile hayatının gizliliğini korumaya yönelik olarak ortaya konmaktadır. Bu suç, TCK'da Kişilere Karşı Suçlar başlığındaki İkinci Kısım'da Dokuzuncu Bölümde Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar başlığı altında yer almaktadır. Bölümün adından da anlaşılacağı üzere, bu bölümde yer alan 132, 133, 135, 136 ve 138. Maddelerle özel hayatın gizliliğiyle ilgili bilgiler ve veriler korunmaya çalışılmaktadır. 134. Madde de bu doğrultuda "özel hayatın gizliliğini ihlal eden kimse" şeklindeki genel ifadeyle suçu tanımlama yoluna gidilmiştir. Buradan hareketle 134. Maddede belirtilen suçun, diğer maddelerde yer alan suçlara nazaran daha genel olması, özel hayatı korumaya yönelik diğer maddelerin uygulanamadığı durumlarda bu maddenin tatbik edilmesi gerektiğini düşündürmektedir.

134. Madde incelendiğinde 1. fıkranın 1. tümcesi, özel hayatın gizliliğini ihlal eden bütün eylemleri suçun işlenmesi için yeterli görmüş ve burada suç serbest hareketli olarak yer almıştır. 1. fıkranın 2. Tümcesi ise; özel hayatın gizliliğini ihlal eden eylemin görüntünün veya sesin kaydedilmesi yoluyla gerçekleştirilmesi durumu suçun nitelikli hali olarak ele alınmış ve bu durumda verilecek cezanın bir kat arttırılacağı ifade edilmiştir. Aynı maddenin 2. fıkrası, özel hayatın gizliliğine yönelik olarak kişilere ait görüntülerin ve seslerin yayılmasını farklı suç olarak düzenleyerek, basın ve yayın organları aracılığıyla bu görüntü ve sesleri yaymayı suçun nitelikli hali olarak görmüştür.[312]

2.2. KİŞİSEL BİLGİLERİN (VERİLERİN) GİZLİLİĞİ VE KORUNMASI

Türkiye'de kişisel verilerin korunmasıyla ilgili özel bir kanun hazırlamak üzere ilk komisyon 1989 yılında kurulmuş ancak çalışmalarını tamamlayamamıştır.[313] Daha sonra 2000 yılında kurulan ikinci komisyon üç yıllık çalışma sonucunda Kişisel Verilerin Korunması Kanun Tasarısı'nı hazırlamıştır. Adalet Bakanlığı tarafından 7

[312] **Türk Ceza Kanunu Madde Gerekçeleri**, İkinci Kısım, Dokuzuncu Bölüm: Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar, 134. Madde Gerekçesi, s. 219.

[313] Aydın, Sedat Erdem, ***AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2014, s. 98.

Eylül 2003 tarihinde açıklanan Tasarı, Avrupa Birliği ilerleme raporları ve e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planları gibi çeşitli belgelerde yer almasına karşın kanunlaşamamıştır.[314]

Kişisel Verilerin Korunması Kanunu Tasarısı Adalet Bakanlığı'nca yenilenerek Başbakanlık tarafından 26.12.2014 tarihinde tekrar TBMM'ye gönderilmesine rağmen TBMM seçimleri nedeniyle bu defa da yasalaşamayarak hükümsüz kalmıştır. Tasarı, 18.01.2016 tarihinde tekrar Türkiye Büyük Millet Meclisi Başkanlığı'na gönderilmiştir. TBMM Başkanlığı tarafından 19.01.2016 tarihinde esas komisyon olarak Adalet Komisyonuna, tali komisyonlar olarak Anayasa Komisyonu, Avrupa Birliği Uyum Komisyonu, İnsan Haklarını İnceleme Komisyonu ve Plan ve Bütçe Komisyonuna gönderilen tasarı hakkında Adalet Komisyonu 12.02.2016 tarihinde raporunu vermiştir. 6698 Sayılı Kişisel Verilerin Korunması Kanunu 24 Mart 2016 tarihinde nihayet TBMM'nde kabul edilerek kanunlaşmıştır.[315]

Kişisel Verilerin Korunması Kanunu'nun 2. Maddesi "Kapsam" başlığını taşımaktadır ve ilgili kanunun kapsamı bu madde de belirtilmektedir.

"*Kapsam*

Madde 2 - ...kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."[316]

Günümüzde bilgisayar, internet ve cep telefonları gibi modern iletişim araçlarının yardımıyla bireylere ait kişisel verilere kolayca ulaşılabilmekte ve bu veriler kişiler, şirketler ve ülkeler arasında çok hızlı şekilde paylaşılabilmektedir. Bu durum, kişisel verilerin sahibi olan bireylerin hukuki güvenliğini tehdit edecek ve özel yaşamlarının gizliliğini bozabilecek bir seviyeye gelmiştir. Bütün bu karmaşa içinde, veri işlem faaliyetleri kapsamında geri planda kalan bireyin kişiliğini koruyarak geliştirmeye devam edebilmesi için, kişisel verilerin korunması hususunda düzenlemeler yapılması gerekmiştir.

Uluslararası ve ulusal kaynaklarda, temel hak ve özgürlükler arasında, bireylerin özel hayatlarının gizliliğinin bir parçası olarak görülen kişisel verilerin

---

[314] Başalp, Nilgün, ***Kişisel Verilerin Korunması ve Saklanması***, Yetkin Yayınları, 2004, s. 107.
[315] Korkmaz, **a.g.e.**, s. 85.
[316] **6698 Sayılı Kişisel Verilerin Korunması Kanunu**, Madde 2, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.6698&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=6698 , 12 Aralık 2016.

korunması, bireylerin kişiliklerini koruyarak, kendilerini serbestçe geliştirmeleri ve verileri üzerinde kontrol sağlayarak onların geleceğini belirleyebilmeleri için son derece önemlidir. Bireyin kişisel verilerinin korunması, onun aynı zamanda özel yaşamın gizliliği, haberleşme özgürlüğü, düşünceyi açıklama özgürlüğü gibi diğer temel hak ve özgürlüklerinin garanti altına alınmasıyla da ilgilidir. İnsan onuru temeline dayanan kişisel verilerin korunması hakkı; kişisel verilerin işlenmesi nedeniyle bireyin maruz kaldığı riskler karşısında korunmasını sağlayan anayasal bir haktır. Kişisel verilerin korunması hukuku, kişisel verilerin işlenmesi sırasında bireylerin özel hayatlarının gizliliğini korumakla birlikte, kişisel verilerin güvenle paylaşılabilmesini amaçlamaktadır. Böylece birey kişisel verileri üzerinde serbestçe karar verebilecek ve böylece bireyin temel hak ve özgürlükleri korunacaktır.[317]

2.3. KİŞİLİK HAKKINA YAPILAN SALDIRIYA KARŞI KİŞİLİĞİN KORUNMASI

İnternet sitelerinde yazı ve resim yoluyla kişinin gerek şeref ve haysiyeti gerekse özel hayatı ve sırları ihlal edilebilmektedir. Elektronik gazetecilik, basılı olanlardan daha hızlı ve kolay şekilde okuyucuya ulaşabilmektedir. Başka amaçlarla oluşturulan web sitelerinde de kişilik haklarını ihlal edecek, özellikle reklam amacıyla resmin yayınlanması gibi yayınların yapıldığı görülmektedir. Yine elektronik posta yoluyla da kişilik hakları kolaylıkla ihlal edilebilmektedir.

Kitle iletişim araçlarını denetleyen bir kamu otoritesi Radyo Televizyon Üst Kurulu (RTÜK) olduğu gibi, özdenetim yapan sivil otoriteler de (Basın Konseyi) bulunmaktadır. Ancak, internet ortamında denetim yapan kamusal bir otorite yoktur. Zaten kamusal bir denetim mekanizması internetin doğasına aykırı bulunmaktadır. Sivil otorite ise belirli bir yere kadar özdenetim yapabilmektedir. Bu sebeple, internet ortamında sık sık rastlanan değişik hak ihlalleri ortaya çıkmaktadır. Örneğin, bir marka hakkında asılsız e-posta zincirleri, saygın bir kişi adına açılan ahlaka aykırı siteler, sohbet ve forum ortamlarındaki asılsız isnatlar, hakaretler, özel hayatı deşifre eden görüntü ve mesajlar hep internetin sağladığı kolaylıklarla yapılabilmektedir.

[317] Korkmaz, **a.g.e.** , s. 149.

Yine facebook ve twetter da internet üzerinden kişilik haklarının ihlalinin gerçekleştiği alanlar olarak karşımıza çıkmaktadır.[318]

Kişilik hakkının internet yoluyla ihlalinde web sitelerinde yapılan yayınlar önemli bir yer tutmaktadır. Bu yayınlar bir kimsenin kişilik hakkına saldırı oluşturan unsurlar taşıyabilir. Örneğin, bir kimsenin sırlarının açıklanması, özel hayatına ilişkin olayların aktarılması, şeref ve haysiyetini ihlal edici hakaretlerin yer alması, küçük düşürücü, aşağılayıcı veya alay edici ifadelerin bulunması veya resminin izni olmaksızın ya da reklam amacıyla yayınlanması halinde böyledir. Ayrıca link vermek suretiyle de bu tür saldırlar gerçekleştirilebilir. Örneğin, bir link veya frame vasıtasıyla bir kimse hakkında şeref ve haysiyeti veya özel hayat ve gizliliği ihlal edici bilgiler sunan bir web sitesine dikkat çekilmesinde böyle bir durum söz konusudur. Bütün bu hallerde bir kimsenin kişilik hakkına yönelik bir saldırı bulunmaktadır.[319]

Hukuka aykırı zararların giderilmesi sağlayan davalar özellikle tazminat davalarıdır. Tazminat davası, kişilik hakkına yapılmış saldırı sonucu ortaya çıkan zararın tazmini yönünde karar verilmesi istemiyle açılan bir alacak davasıdır. Alacak davası olduğu için de istisnalar dışında sadece zarar verene karşı açılabilir. MK. m. 25 f. 3 hükmü maddi tazminatla birlikte manevi tazminat davasını da düzenlemiştir. Bu sebeple kişilik haklarına yönelik hukuka aykırı bir saldırı sonucunda bu saldırıya uğrayan kimse, saldırı dolayısıyla manevi bir zarara uğramış ise manevi tazminat davası açma hakkına sahiptir.

Manevi tazminat davasında amaç haksız saldırıyı gerçekleştiren kişinin hukuk tarafından bir müeyyide ile karşılaşması ve de mağduru tatmin etmektir. Bu nedenle manevi tazminat, verilişindeki amacın gerçekleşmesini sağlayacak tutarda ve adalete uygun olarak belirlenmelidir. Manevi tazminat davası aynı zamanda BK. m. 49'da da düzenlenmiştir. İnternet ortamında yapılan saldırılar dolayısıyla da MK. m. 25'e dayanarak maddi ve manevi tazminat davası talep

[318] Durak, Yasemin, "İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukuki Korunma", ***Selçuk Üniversitesi Hukuk Fakültesi Dergisi***, Cilt 22, Sayı 1, 2014, (Erişim) http://www.mutlakbutlan.com/2016/12/internet-yoluyla-kisilik-haklarina-saldiri-ve-hukuki-korunma.html , 12 Aralık 2016.

[319] Fırat, Muhammed Sabır, "Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu", ***Hacettepe HFD***, 5(2), 2015, s. 109.

edilebilir. Kişinin bunu ispatlaması için ise gönderilen e-posta mesajını silmemesi ve bilgisayarında saklaması ayrıca bunu yazılı olarak da alması gerekecektir.[320]

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, en son 6 Şubat 2014 tarih ve 6518 sayılı Kanunla değiştirilen 9'uncu maddesinde yeni düzenleme getirmiştir. Buna göre;[321]

"(1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir.

Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Birliğe gönderilir.*

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka

---

[320] Durak, **a.g.e.**

[321] ***5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun***, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5651&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=5651 , 12 Aralık 2016.

internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Birliğe müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."

***Kanunda Birlik:** Erişim Sağlayıcıları Birliğini ifade etmektedir.*

Kişilik haklarına internet ortamında yapılan bir yayınla saldırıda bulunulan kişi, isterse 5651 sayılı Kanunun 9'uncu maddesindeki usulle sulh ceza hâkimine başvurur ve "bir yayının bir kişinin kişilik haklarını apaçık bir şekilde ihlâl ettiğinin daha ilk bakışta anlaşılması" durumu var ise hızlı bir koruma elde eder. İsterse TMK, m.24 ve 25'e göre hukuk hâkimine başvurur. İsterse bunların ikisine birden de başvurabilir. Çünkü her iki başvurunun kabul şartları farklıdır. Keza önce 5651 sayılı Kanunun 9'uncu maddesindeki usulle sulh ceza hâkimine başvurur; bir yayının bir kişinin kişilik haklarını apaçık bir şekilde ihlâl ettiğinin daha ilk bakışta anlaşılması" durumu bulunmadığı için talebi reddedilirse, bu sefer TMK m.24 ve 25'e göre hukuk hâkimine başvurabilir.[322]

2.4. İNTERNET SERVİS SAĞLAYICILARININ HUKUKİ SORUMLULUĞU

Erişim sağlayıcılar, 5651 sayılı Yasanın 2. maddesinin 1. fıkrasının (e) bendinde kişilere internet ortamına erişim olanağı sağlayan gerçek veya tüzel kişiler olarak tanımlanmıştır. Türkiye'de erişim sağlayıcı olarak faaliyette bulunabilmek için Faaliyet Yönetmeliği'nde belirtilen esaslara göre faaliyet belgesinin alınması gerekmektedir. Söz konusu erişim sağlayıcıların kimler olduğu ve faaliyet belgelerine ilişkin ayrıntılı bilgilere Bilgi Teknolojileri Kurulu (BTK)'nun web sayfasından ulaşılabilmektedir.[323]

5651 sayılı Yasanın 6. maddesinde erişim sağlayıcıların yani İSS'lerin hukukî sorumluluğu ve yükümlülükleri düzenleme konusu yapılmıştır. Buna göre erişim sağlayıcı öncelikle herhangi bir kullanıcısının yayınladığı hukuka aykırı içeriği, 5651 sayılı Yasa'ya göre haberdar edilmesi hâlinde erişimi engellemekle yükümlüdür. Yeni düzenleme ile madde metninden *"teknik olarak engelleme imkânı bulunduğu ölçüde"* ibaresi çıkarılmıştır. Dolayısıyla, erişim sağlayıcıların engellemeyi

[322] Fırat, **a.g.e.** , s. 113.
[323] Dülger, **a.g.e.** , s. 124-125.

gerçekleştirebilmeleri için gerekli her türlü teknik donanım ve yazılıma sahip olmaları gerekmektedir. [324]

Yeni düzenleme ile, ilgili maddenin ilk fıkrasına *"Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla yükümlüdür."* şeklinde bir hüküm eklenmiştir. Madde metninde alternatif yolların neler olduğuna ilişkin herhangi bir açıklama yapılmamıştır. Dolayısıyla erişim sağlayıcıların yükümlülükleri konusunda belirsizlik söz konusudur. Erişim sağlayıcıların tüm yolları araştırma yükümlülükleri bulunmakta mıdır? Eğer böyle bir yükümlülükleri var ise hangi araçlar ile bunu gerçekleştireceklerdir ve bu maliyeti nasıl karşılayacaklardır? Belirtilmiş olunan soruların cevaplandırılmaları önemlidir çünkü yasanın ilgili maddesinin 3. fıkrası ile yükümlülükleri yerine getirmeyen erişim sağlayıcısına Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanlığı tarafından on bin TL'den elli bin TL'ye kadar idari para cezası öngörülmüştür.

5651 sayılı Yasanın 6. maddesinin 1. fıkrasında ikinci olarak erişim sağlayıcının sağladığı hizmetlere ilişkin, ilgili yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlü olacakları düzenlenmektedir. Erişim sağlayıcılara iki yıla kadar bütün trafik bilgilerinin saklanmasına yönelik bir yükümlülük getirmek bazı açılardan sakıncalı bazı açılardan ise olumlu bir düzenlemedir. Böyle bir yükümlülük trafik bilgilerinin tutulması için erişim sağlayıcıların ek yatırım yapmasını gerektirecektir. Söz konusu bilgilerin tutulması için ek aygıtlar ve bu aygıtların bulundurulacağı ek tesisler, erişim sağlayıcılar için önemli miktarda maliyet anlamına gelmektedir ki, bu düzenlemenin olumsuz yönüdür. Düzenlemeye diğer yönden bakıldığında ise, bu bilgilerin uzunca bir süre saklanması internet üzerinden işlenen suçlarla mücadele edilmesi açısından çok önemli ve gerekli bilgilerin kaybolmasını önleyecek ve faillerin ortaya çıkarılmasını sağlayacaktır. Bu ise düzenlemenin olumlu yönünü oluşturmaktadır.

İnceleme konusu yasanın 6. maddesinin 1. fıkrasının "c" bedinde ise, erişim sağlayıcının faaliyetine son vermesi durumunda, faaliyetine son vermeden en az üç ay önce durumu Telekomünikasyon Kurumu'na, içerik sağlayıcılarına ve müşterilerine bildirmekle yükümlü olduğu düzenlenmiştir. Fıkranın devamında

[324] Durak, **a.g.e.**

faaliyetine son verecek erişim sağlayıcının internet iletişimine ilişkin saklamakla yükümlü olduğu trafik bilgilerini bu konuda çıkarılacak yönetmelikte belirtilecek esas ve usullere göre Telekomünikasyon Kurumu'na teslim etmekle yükümlü oldukları belirtilmektedir.[325]

Yeni düzenleme ile 6.maddenin 1. fıkrasının d bendi, *"Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür."* şeklinde düzenlenmiştir. Yine içerik sağlayıcı ve yer sağlayıcının yükümlülüklerinin değerlendirildiği kısımda açıklanmış hususlar aynı şekilde bu bent için de geçerlidir.

5651 sayılı Yasanın 6. maddesinin 2. fıkrasında yukarıda da belirtildiği üzere, erişim sağlayıcıların kendi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadığını ve hukukî sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü olmadıkları düzenlenmektedir. Bu düzenleme Alman Teleservisler Yasası'nın benzeri olup erişim sağlayıcıların sorumluluğu açısından olumlu bir düzenlemedir.[326]

5651 sayılı Yasa erişim sağlayıcıların sorumluluğunu yer sağlayıcılarla aynı esaslara göre düzenlemiştir. Yasanın 8. maddesinin 10. fıkrasına göre, *"Koruma tedbiri olarak verilen erişimin engellenmesi kararının gereğini yerine getirmeyen yer veya erişim sağlayıcılarının sorumluları, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, beş yüz günden üç bin güne kadar adlî para cezası ile cezalandırılır."* 8. maddenin 11. fıkrasında ise, idari tedbir olarak verilen erişim engelleme kararlarının yerine getirilmemesi halinde ise Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı tarafından erişim sağlayıcısına, on bin TL'den yüz bin TL'ye kadar idari para cezası verileceği düzenlenmektedir. İdarî para cezasının verildiği andan itibaren yirmi dört saat içinde kararın yerine getirilmemesi hâlinde ise, BTK'nin yetkilendirmenin iptaline karar verilebileceği düzenlenmektedir.

5651 sayılı Yasanın 6. maddesinin son fıkrasında ise 1. fıkranın (b) ve (c) bentlerinde düzenlenen yükümlülükleri yerine getirmeyen erişim sağlayıcısına Ulaştırma Bakanlığı tarafından on bin TL'den elli bin TL'ye kadar idari para cezası verileceği düzenlenmektedir. Yasanın 8. Maddesinin 12. fıkrasında yasada tanımlanan kabahatler dolayısıyla başkanlık veya kurum tarafından verilen idari para

[325] Dülger, **a.g.e.** , s. 125.
[326] Durak, **a.g.e.**

cezası kararlarına karşı 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre yasa yollarına başvurulacağı belirtildiği için, 6. Maddenin 3. fıkrasına göre idari para cezası verilmesi halinde bu kararın iptali için altmış gün içinde idari yargıda iptal davası açılması mümkündür.[327]

[327] Dülger, **a.g.e.** , 126.

ÜÇÜNCÜ BÖLÜM

TÜRK HUKUKUNDA İNTERNET SUÇLARI

Türkiye'de internet suçları başlığı altında, öncelikle internet suçlarının ortaya çıkması durumu üzerinde durulacak, ilk suçun ortaya çıkışından itibaren nasıl bir seyir izlediği konuyla ilgili yapılan araştırmalardan yola çıkarak ortaya konacaktır. Ardından mevzuattaki yeri başlığı altında, internet suçlarının tahkikat aşamasından cezalandırmaya kadar olan süreçte ulusal yasal düzenlemeler doğrultusunda nasıl bir uygulamanın var olduğu yer yer örneklerden hareketle açıklanacaktır.

3.1. SUÇUN ORTAYA ÇIKMASI

Günümüzde ilerleyen teknolojinin yaşamın her alanına girdiği şüphe götürmez bir gerçektir. Bugünün insanı teknolojiyi ve özellikle de interneti yaşamın vazgeçilmezleri arasında görmekte, alış verişten resmi kurumlardaki işlerine kadar pek çok işini yerinden bile kıpırdamadan internet üzerinde yapabilmektedir. Bütün bu kolaylıklarına rağmen, gelişen teknolojiye bağlı olarak internetin yaşamın içine soktuğu riskler de bulunmaktadır. İşte bu yüzden de ceza hukuku ile bilişim olarak adlandırdığımız internet birçok noktada kesişmektedir. Denilebilir ki, sağladığı pek çok faydaya rağmen bilişim aletleri ve internet, potansiyel bir suç aracı işlevi görmektedir.[328]

Bilişim sistemlerinde;[329]

- Bilgi saklama ortamlarının, bilgi saklama kapasitelerinin ve saklanılan bilgiye erişim hızının çok yüksek olması,

- Bilgiyi muhafaza etme maliyetlerinin çok düşük olması,

---

[328] Kızıltan, Burak, ***5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006, s.29.

[329] Alaca, Bahattin, ***Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile),*** Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2008, s. 39.

- Veriler üzerinde hiçbir iz, silinti ve kazıntı bırakmadan değişiklik yapılabilme imkânının varlığı,

- Söz konusu bilgilerin yeniden derlenme olanakların bulunması ve

- Bilgilerin elektronik ortamda iletilebilmesi gibi özellikler, aynı zamanda bilgi yoğunlaştırmasının suç yaratıcı faktörleridir.

Bilişim teknolojileri vatandaşlar ve devlet için yukarıda sayılan kolaylıkları sağlamakla birlikte suça meyilli kişilere ve suç örgütlerine de birçok fırsatlar sunmaktadır. İnternet suç işlemek için daha fazla imkânlar sunabilmektedir. Siber suçlarda fail ile mağdur arasındaki fiziksel sınırlar ortadan kalkmış ve önemsiz hale gelmiştir.[330]

Öngörülemeyen bir hızla yayılan internet aracılığıyla bir insanın aradığı bilgiye erişme olasılığı ve hızı milyonlarca kat artmakta, pek çok bilgi bireylerin ulaşabileceği noktada bulunmaktadır. Faydalı işler için kullanıldığında güzel bir gelişme sayılan bu durum, bireysel internet kullanıcılarının hızla artması sayesinde, istemli ya da istem dışı olarak pek çok kişisel veriyle ticari bilginin ulaşılabilir kılınmasını sağlamakta, suç için uygun bir zemin hazırlamaktadır. İnternet sayesinde pek çok yeni ticari sektörün doğması ile gelir elde etme yolunun bir hayli açıldığı görülmektedir. Böylece bitmez tükenmez isteklerini karşılamak için durmadan gelir elde etmek isteyen insanların farklı arayışlar içine girmesi durumu ortaya çıkmaktadır. [331]

İnternet sayesinde sayfalarca kâğıtlara sığacak bilgi, kısa sürede kilometrelerce ötelere aktarılabilmekte, bilgiler hiçbir iz bırakmadan değiştirilebilmektedir. Büyük miktarda bilginin toplanması ve bilgi-işlem sırasında yapılan hatalar, bu bilgilere ulaşmak ve bu hatalardan istifade etmek isteyenler için bulunulmaz bir fırsat olmaktadır. Çünkü bilişim sistemlerinde veriler manyetik ortamlarda saklanmaktadır. Bu verilerde yapılacak değişiklikler geride hiçbir iz bırakmadan gerçekleştirilebilmektedir. Ayrıca megabaytlarla ifade edilen bilgiler çok küçük disketlerde kopyalanarak, bilişim sistemlerinin dışına çıkartabilmektedir. Bu iki özellik, bilişim sistemlerinde suç nitelikli eylemlerin icrasını kolaylaştırmaktadır.

---

[330] Yetim, Servet, "Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi", ***Türkiye Adalet Akademisi Dergisi***, S: 17, 2014, s. 181.

[331] Şamlı, Rüya, "Türk ve Dünya Hukukunda Bilişim Suçları", ***Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri***, 10 - 12 Şubat 2010 Muğla Üniversitesi, s.97.

Bilişim sistemlerinin iş hayatında kullanımı ile beraber, bu sistemlere olan aşırı güvenden dolayı, manuel birçok kontrol tedbiri uygulamadan kaldırılmıştır. Kontrol tedbirlerinin kaldırılmasına rağmen, bilişim sistemlerinde hata yapılmasını önleyici veya kötü niyetli girişimleri engelleyici yeterli tedbirler alınmamaktadır. Bilişim sistemlerinde kontrol tedbirlerinin yeterli düzeyde bulunmaması, suç nitelikli girişimlerin artmasına neden olmaktadır.[332]

Rekabetin sınır tanımadığı günümüzde ticari sırlara erişmenin ve potansiyel müşterilere kolaylıkla ulaşmanın riski, söz konusu bilgilere kötü niyetli insanların ulaşması olasılığını göstermektedir. Hatta çoğu zaman olasılıktan ziyade, gerçekleşme aşamasına gelen en bu riskler, internet kullanıcılarının zor durumda kalmalarına ve kayıplarla karşılaşmalarına neden olmaktadır. Ücret karşılığında yayınları ve telif hakkına ait ürünleri ücretsiz kullanmak isteyen ya da her türlü medyayı internetten ücretsiz bir şekilde indiren insan grubu, internet suçlarının başka bir boyutunu oluşturmaktadır. Böyle bir durumda insanlar, daha yayına girmemiş bulunan filmleri, müzikleri, hatta yazılımları, illegal olarak kullanarak suç işlemektedirler.[333]

1990'ların başından itibaren internetin bireysel kullanıma açılması ve bireylerin kendi bilgisayarlarına sahip olmaları nedeniyle bilişim suçlarında bir artış görülmektedir. Bugün için bakıldığında internet bilişim suçlarının işlenmesinde bu yol en etkin araç kabul edilmektedir. Çünkü internet sadece iyilere değil, aynı zamanda kötülere de eşit fırsatlar sunmaktadır. Nitekim günümüzde terör örgütleri, propagandalarını zaman zaman internet üzerinden yapmakta ve eleman toplama faaliyetlerini yine internet üzerinden gerçekleştirmektedirler. Aynı şekilde organize suç örgütleri haksız kazanç sağlamak amacıyla internet üzerinden kredi kartı dolandırıcılığı suçunu işlemektedirler.[334]

Türkiye'de işlenen bilişim suçlarının yani internet suçlarının ortaya çıktığı günden yakın tarihe kadar nasıl bir gelişim gösterdiği yapılan araştırmalar ve kolluk kayıtlarından yola çıkılarak aşağıda ortaya konmaya çalışılmaktadır. İnternet

[332] Alaca, **a.g.e.,** 40.
[333] Şamlı, **a.g.e.**, s. 98.
[334] Kızıltan**, a.g.e.**, s.29.

suçlarıyla ilgili yapılan bir araştırmaya göre[335], suçların ortaya çıkışı ve yıllar içinde geçirdiği değişim, Tablo 1'de görülmektedir.

Tablo 1. Yıllara ve suçlara göre toplam dava dosya sayıları (1990-2010)

YIL	Banka / Kart	Bilişim Sistemi	Müstehcenlik	Kişisel Veri	Telif Hakkı	Çocuk İstismarı	5651
1990	1	0	0	0	0	0	0
1991	1	0	0	0	0	0	0
1992	0	0	0	0	0	0	0
1993	0	0	0	0	0	0	0
1994	2	0	0	0	0	0	0
1995	2	0	0	0	0	0	0
1996	1	0	0	0	0	0	0
1997	5	1	0	0	1	0	0
1998	7	0	0	0	2	0	0
1999	8	0	2	0	8	0	0
2000	12	2	1	0	12	0	0
2001	22	1	0	0	45	0	0
2002	35	1	2	0	49	0	0
2003	77	5	3	4	77	0	0
2004	201	8	27	0	191	2	0
2005	604	57	99	8	552	22	0
2006	1970	302	739	22	697	171	0
2007	3881	1133	1336	79	901	525	2
2008	6391	2381	1131	143	1287	443	13
2009	9254	3412	1139	286	1481	445	13
2010	11789	3572	1150	536	2189	531	16

Kaynak: İlbaş, Çığır ve Köksal, Mehmet Ali, ***Türkiye'de Bilişim Suçları 1990-2011***, 2015, s. 13, (Erişim) http://docplayer.biz.tr/15849702-Adli-bilisim-uzm-cigir-ilbas-av-mehmet-ali-koksal.html, 12.01.2017.

Tablo 1'e göre, Türkiye'de bilişim alanında ilk suç, 1990 yılında nitelikli dolandırıcılık suçunun işlenmiş olduğu görülmektedir. 1991 yılında da aynı suçun

[335] İlbaş, Çığır ve Köksal, Mehmet Ali, ***Türkiye'de Bilişim Suçları 1990-2011***, 2015, s. 22, (Erişim) http://docplayer.biz.tr/15849702-Adli-bilisim-uzm-cigir-ilbas-av-mehmet-ali-koksal.html, 12.01.2017.

aynı miktarda ortaya çıktığı yapılan araştırmayla ortaya konmaktadır. 1992 ve 1993 yıllarında bilişim alanında suç işlendiğinin tespit edilmediği, 1994 ve 1997 yılları dâhil olmak üzere, bilişim alanındaki suçların sadece nitelikli dolandırıcılıktan ibaret olduğu, 1997 yılıyla birlikte bu alanda düzenli bir artış olduğu görülmektedir. 1994-1995 yıllarında ise, iki adet nitelikli dolandırıcılık suçu işlenmişken, 1996 yılında sadece bir adet nitelikli dolandırıcılık suçunun işlendiğine rastlanmaktadır. İnternetin çok yaygın kullanılmadığı bu yıllarda suç çeşitliliğinin dar ve suçun işlenme miktarının da az olduğu böylece dikkatten kaçmamaktadır.

Yukarıdaki tabloya bakıldığında, telif hakkıyla ilgili suçların 1997 yılında ilk kez ortaya çıktığı, yıllar içinde artış göstererek, 2000'li yıllardan itibaren belirgin bir ivme kazandığı ve nihayet 2010 yılında 2189 rakamına ulaştığı görülmektedir.

Bilişim sistemiyle ilgili ilk suçun 2000 yılında 2 adet suçla sınırlı iken, 2004 yılında nispi bir artış gösterdiği gözden kaçmamaktadır. Ancak 2005 yılında 2004 yılına göre yedi kat artış gibi bir patlamayla 57 adet bilişim suçuna ulaştığı, 2006'da da bu rakam 302'ye çıktığı ve 2007 itibariyle de 1000 rakamını aştığı tespit edilmiştir. 2010 yılı verilerine göre ise bilişim suçunun, 3572 rakamını bulduğu anlaşılmıştır.

Müstehcenlik suçu ise, ilk kez 1999 yılında işlenen 2 adet suçla kayda girmiş, 2004 yılına kadar da bir ülke için düşünüldüğünde oldukça az sayıda bu suçun işlendiği belirlenmiştir. 2004 yılında ise, 2003 yılına göre dokuz kat artış göstererek 27 adet işlenen müstehcenlik suçu, ilerleyen yıllarda da katlanarak artmaya devam etmiş, aynen bilişim suçunda olduğu gibi 2007 yılıyla birlikte binlerle ifade edilir hale gelmiştir.

Kişisel veri suçunun da, ilk kez 2003 yılında işlendiği Tablo 1'de görülmektedir. 2004 yılında kişisel veri suçu işlenmezken, 2005 yılıyla birlikte bu suçun işlenmesinde kayda değer bir artışın olduğu görülmüştür. 2010 yılında ise söz konusu artış hızlanarak 536 rakamına tırmanmıştır.

Türkiye'de çocuk istismarı suçuna ilk kez, 2004 yılında 2 adet suçla rastlandığı dikkat çekmektedir. 2005'de toplam 22 çocuk istismarı suçu işlenirken, 2006'da bu rakam 171'e, 2007'de 525'e yükselmiştir. 2008 ve 2009 yıllarında küçük bir gerileme eğilimi gözlemlense de, 2010 itibariyle bu suçun 531'e baliğ olduğu müşahede edilmiştir.

5651 Sayılı İnternet Ortamında Yapılan Yayınlar yoluyla işlenen suçlarla ise Türkiye ilk olarak 2007 yılında tanışmıştır. Anılan yılda 2 adet olan bu suç miktarı, 2008 ve 2009 yıllarında 13'er adet, 2010 yılında ise toplam 16 adet olarak belirlenmiştir.

Aynı araştırma verilerine göre[336], 1990 ile 2010 yılları arasında internet ve bilişim suçu addedilen eylemlerle ilgili olarak ceza ve hukuk davası suçlara ilişkin durum, Tablo 2'de görülmektedir.

Tablo 2. Yıllara göre toplam ceza ve hukuk dava dosya sayıları (1990-2010)

Yıl	Ceza Davası	Hukuk Davası	Toplam Dava	Suç Türü
1990	1	0	1	Nitelikli Dolandırıcılık
1991	1	0	1	Nitelikli Dolandırıcılık
1992	0	0	0	
1993	0	0	0	
1994	2	0	2	Nitelikli Dolandırıcılık
1995	2	0	2	Nitelikli Dolandırıcılık
1996	1	0	1	Nitelikli Dolandırıcılık
1997	6	1	7	Nitelikli Dolandırıcılık
1998	7	2	9	Nitelikli Dolandırıcılık/ Manevi Hak İhlali
1999	10	8	18	Nitelikli Dolandırıcılık
2000	15	12	27	Nitelikli Dolandırıcılık
2001	23	45	68	Kanuna aykırı çoğaltılan nüshayı bulundurma ve satma
2002	38	49	87	Nitelikli Dolandırıcılık
2003	89	77	166	Nitelikli Dolandırıcılık
2004	238	191	429	Nitelikli Dolandırıcılık
2005	790	552	1342	Nitelikli Dolandırıcılık
2006	3204	697	3907	Nitelikli Dolandırıcılık/ Müstehcenlik/ Çocuk İstismarı
2007	6954	903	7857	Nitelikli Dolandırıcılık/Müstehcenlik / Çocuk İstismarı
2008	10489	1300	11789	Nitelikli Dolandırıcılık/Bilişim sistemi yoluyla haksız çıkar sağlama
2009	14536	1494	16030	Nitelikli Dolandırıcılık/Bilişim sistemi yoluyla haksız çıkar sağlama
2010	17578	2205	19783	Nitelikli Dolandırıcılık/Bilişim sistemi yoluyla haksız çıkar sağlama

Kaynak: İlbaş, Çığır ve Köksal, Mehmet Ali, ***Türkiye'de Bilişim Suçları 1990-2011***, 2015, s. 21, (Erişim) http://docplayer.biz.tr/15849702-Adli-bilisim-uzm-cigir-ilbas-av-mehmet-ali-koksal.html, 12.01.2017.

[336] İlbaş, ve Köksal, **a.g.e.**, s. 21.

Tablo 2'ye göre; 1997 yılında ani bir şekilde artış gösteren (7 Adet) bilişim suçlarında ortaya çıkan suç türü, yine nitelikli dolandırıcılıktır. 1998 yılında bilişim suçları sayısal olarak artmakta (9 Adet), ancak yapısal olarak bir farklılık görülmemekte, yeni bir suç türü olarak manevi hak ihlali olarak betimlenen durum ilk kez görülmektedir. Bilişim suçları anlamında 1999 yılı çok dikkat çekici bir yıl olarak yorumlanabilir. Çünkü 1999 yılında işlenen bilişim suçları bir önceki yıla göre iki kat artış göstererek 18 rakamına ulaşmaktadır. Sayısal artışa rağmen, suç türünde bir değişiklik görülmemekte, işlenen suçun yine nitelikli dolandırıcılık olduğu görülmektedir.

Bilişim suçlarının gelişimine ilişkin olarak yapılacak olan temellendirmede "internet ile sunulan hizmetin ulusal sınırları aşarak herhangi bir kitle haberleşme aracına kıyasla daha fazla etki yapması" bilişim suçlarının kapsamını bir hayli genişletmiştir.[337] Tablo 1'de 2000'li yıllarla birlikte bilişim suçlarında gözle görülür bir artış yaşanmaya başlandığı, 2006 yılından itibaren de suçların türlerinde değişiklikler olduğu dikkat çekmektedir. Farklı olarak 2001 yılında tespit edilen ve hukuki yollara başvurulan bilişim suçu, nitelikli dolandırıcılık değil, kanuna aykırı çoğaltılan nüshayı bulundurma ve satma suçunun toplam 68 davayla sonuçlandığı ve bu suç türünün ilk kez karşımıza çıktığı, araştırma sonuçlarından anlaşılmaktadır. 2002 yılından itibaren yine nitelikli dolandırıcılık suçu öne çıkmakta ve hızla büyümektedir. Araştırma sonuçlarını sayısal olarak ifade etmek gerekirse, 2002 yılında sadece 87 nitelikli dolandırıcılık suçu işlenmişken, 2005 yılında bu rakam binlerle ifade edilmeye başlanarak, 1342 rakamına ulaşmış olduğu ortaya konmaktadır.

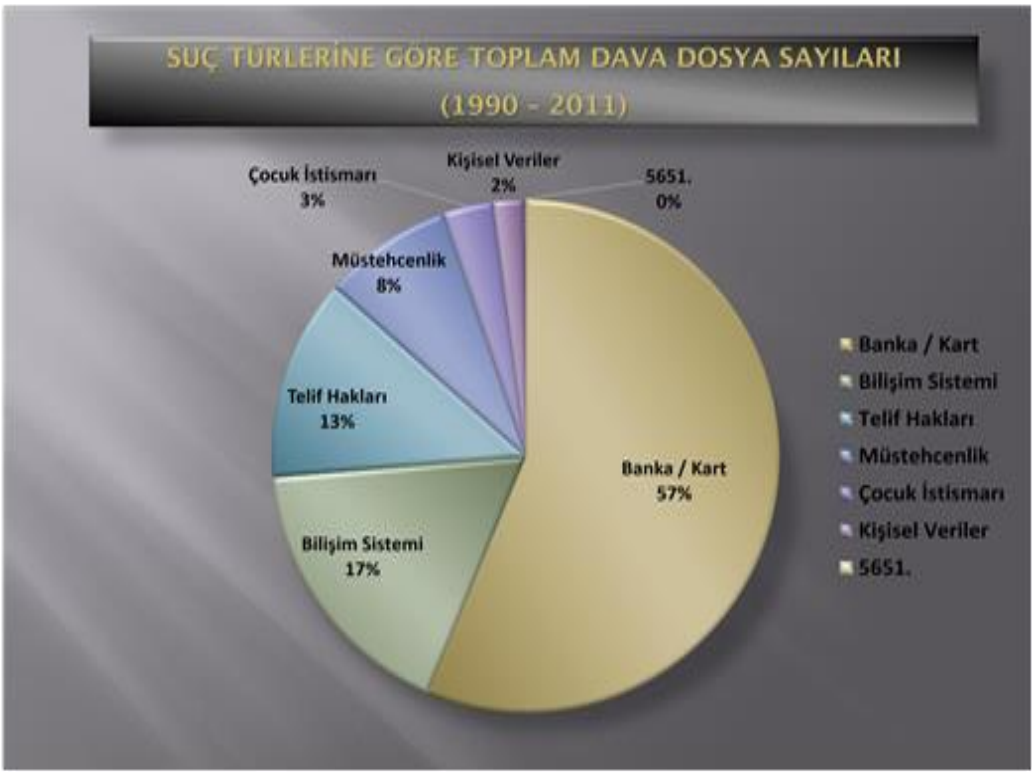
1990-2003 tarihleri arasında dava sayılarındaki düşüklüğün sebebi; 5237 sayılı TCK'nin 2004 tarihinde kabul edilmesi ve önceki yıllarda kolluk kuvvetlerinin siber suçlarla mücadele etmemesi, bu yıllar arasında bilgisayar kullanımı yaygınlığı ve bilişim okuryazarlığı oranlarının düşüklüğü ve suça maruz kalan şahısların yasal haklardan yoksun oluşu şeklinde yorumlanmaktadır.[338]

2006 yılı da bilişim suçlarının tavan yaptığı ve çeşitlilik sergileği bir yıl olarak karşımıza çıkmaktadır. Nitelikli dolandırıcılık suçu yanında, müstehcen yayınlar ve

[337] Tepe, İlker, "Modern Ceza Hukuku Teorisinde İnternet ve İnternet Suçluluğunun Konumu", Veli Özer Özbek (Ed.), ***Ceza Hukuku Dergisi***, Ankara, Yıl:4 Sayı:9, 2009, 269.
[338] İlbaş ve Köksal, a.g.e., s. 26.

çocuk istismarı suçları bu yıl karşımıza çıkmakta, 2007 yılında da aynı suçların işlendiğine tanık olunmaktadır. 2006 yılında işlenen suç sayısı 3901 iken, 2007 yılında 7857 rakamına ulaşarak bir önceki yılın neredeyse iki katına baliğ olmuştur.

2008-2009 ve 2010 yıllarında değişik bir suç tipi olan bilişim sistemi yoluyla haksız kazanç sağlama suçu, nitelikli dolandırıcılık suçuyla birlikte belirlenmiştir. 2008'de 11.789 olan suç miktarı, 2010 yılında 19.783 rakamlarıyla ifade edilir hale gelmek suretiyle bilişim suçlarının ne kadar hızla arttığını açıkça göstermektedir.



Şekil 6. Suç türlerine göre toplam dava dosya sayıları (1990-2011)[339]

Elde edilen sonuçlar, Türkiye'deki bilişim suçlarının, lisans haklarının ihlali, dolandırıcılık, sahtecilik, yasadışı yayınlar ve bilgisayar sabotajı şeklinde geliştiğini göstermektedir. Sanal âlemdeki dolandırıcılık suçlarının büyük bir kısmı kredi kartları üzerinden yapılmaktadır. Değişik yöntemlerle ele geçirilen kredi kartı numaralarıyla bilgisayar üzerinden alışveriş yapılması en yaygın yöntem seçilmiştir. Otomatik para çekme makineleri olarak bilinen ATM (Auto Telle Machine) dolandırıcılığı ise kredi kartlarından sonra ikinci sırada yer almaktadır. Kredi kartlarının ATM cihazında sıkıştırılması, değişik hilelerle şifrelerin öğrenilmesi veya

[339] İlbaş ve Köksal, a.g.e., s. 21.

kartların hırsızlık yoluyla elde edilmesi suretiyle dolandırıcılık yapılmaktadır. Evrak, para, Milli Piyango bileti, kimlik kartları, sigorta poliçeleri, pasaportlar ve yazarkasa fişlerinin sahtelerinin kullanılarak işlenen sahtecilik suçları da bu kapsamda mütalaa edilmektedir.[340]

Tablo 3. 2002-2012 yılları arası polis istatistiklerine göre işlenen internet suçları

Suçun Nevi Ve Yıllara Göre Olay Sayıları	Kredi Kartı Sahteciliği ve Dolandırıcılığı	Banka Dolandırıcılığı	Bilişim Suçları ve Dolandırıcılığı	İnternet Aracılığıyla Dolandırıcılık	Diğer	Toplam
Olay Sayısı 2003	80	15	X	X	X	95
Olay Sayısı 2004	146	22	16	X	X	184
Olay Sayısı 2005	195	9	91	X	X	295
Olay Sayısı 2006	122	98	4	X	X	224
Olay Sayısı 2007	594	642	416	X	91	1.743
Olay Sayısı 2008	830	1.177	560	X	157	2.742
Olay Sayısı 2009	1.511	550	353	412	45	2.871
Olay Sayısı 2010	1.131	151	972	71	28	2.353
Olay Sayısı 2011	1.772	141	1.738	111	31	3.793
Olay Sayısı 2012	1.724	264	3.669	278	783	6.718

Kaynak: Taşçı, Ufuk ve Can, Ali, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014", ***Fırat Üniversitesi Sosyal Bilimler Dergisi***, Cilt: 25, Sayı: 2, Sayfa: 229-248, Elazığ, 2015, s. 235.

Görülüyor ki, lisans hakları ihlali içinde en yüksek oranı % 82 ile filmlerin çoğaltılması oluşturmaktadır. Bilgisayar oyunları ve müzik CD'lerinin çoğaltılması da sanal âlemin diğer lisans hakkı ihlalleridir. Araştırma verileri, yasadışı yayın suçları arasında ilk sıranın % 40 ile çocuk pornografisine ait olduğunu göstermektedir. Genel anlamdaki pornografik yayınların oranı ise % 25 olarak ifade edilmektedir. Bunlar, daha çok internet kafe gibi ortamlarda pornografik içeriklerin gösterimi ve CD'lerinin satışı biçiminde ortaya çıkmaktadır. Terör içerikli web sayfalarının hazırlanması suretiyle işlenen suçların oranı ise, % 30 olarak tespit

[340] Turhan, a.g.e., s.171.

edilmiştir. Şikâyete bağlı suçlardan kişilik haklarına saldırı ve hakaret ise % 5 oranında kalmıştır.

Türkiye'de genel olarak, bilişim suçları denince akla iki tür eylem gelmektedir: Kredi kartları ve pornografik CD'ler ve telif haklarının konusunu teşkil eden korsan CD'ler. Bilişim suçlarına ilişkin olarak yapılan üçlü sınıflandırma göz önüne alınırsa bilgisayar aracılığıyla işlenen suçların Türkiye'de daha yaygın olduğu görülmektedir. Ancak bilgisayar sistemleri aracılığıyla işlenen suçların birçoğu takibe bağlı suçlardan olduğu için mağdurların şikâyeti olmadan resen harekete geçilememektedir. Örneğin elektronik posta yoluyla yapılan bir tehditte, tehdit edilen kişi veya kurum tarafından bildirmeden polisin bu olaydan haberdar olması ve işlem yapması mümkün olmamaktadır. Riptech'in yayınladığı rapora göre, siber saldırılar en fazla ABD'de işlenirken, Türkiye 6. sırada yer almaktadır. Türkiye'de işlenen bilişim suçlarına ait oransal veriler ise lisans hakları ihlallerinin % 4 müzik, % 14 oyun ve % 82 film şeklinde tespit edilmiştir.

İnternet suçlarının artmasında ve daha önce adli suç işlememiş kişilerin internet aracılığıyla suç işler hale gelmesinde, suç işlemenin kolaylaşmasının yanı sıra kullanıcıların internet üzerinden gerçekleştirilen eylemlerin herhangi bir yasal yükümlülüğünün ve yasal düzenlemenin bulunmadığına dair yanlış bir kanaatin bulunması rol oynamaktadır. Suçluların profillerinin incelenmesi sonucunda, bu suçları işleyenler arasında, yaptıklarının suç olup olmadığını bilmeyen veya düşünmeyen, sadece bilinmezin, büyüsüne kendini kaptırıp eylemlerin çok derin hasarlar bıraktığının farkında olmayan, büyük bölümü çocuk yaştaki insanlar bulunmaktadır. İnterneti, çoğunlukla teknolojinin yaramaz çocukları olarak adlandırılan geleneksel olarak bireyleri suç işlemeye götüren nedenlerle hareket eden, sistemlerin açıklarını bularak bu sistemlere atak yapan ve sisteme izinsiz girerek çeşitli hasarlar yaratan programcılar ve bilgisayar ile uğraşan hackerlar kullanmaktadırlar.[341]

İnternet suçlarıyla karşılaşılması durumunda, mağdurun yapması gerekenler ve sürecin akışı ise şu şekilde gerçekleşmektedir. Bilişim suçlarında mağdur konumunda olan kişinin, işlenen suç her ne olursa olsun, savcılığa suç duyurusunda

[341] Ergüç, Seher, ***Türk Bankacılık Sisteminde İnternet Bankacılığı ile Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku,*** Yayımlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2008, s. 62.

bulunması çok önem arz etmektedir. Ancak, bu şekilde faillere karşı bir karşı atak yapmak ve caydırıcı olmak mümkün hale gelebilir. Savcılık suç duyurusuna istinaden soruşturma başlattıktan sonra olay emniyete intikal eder ve ilgili birim olayın detayı hakkında araştırma yaparak gerekli verileri toplar. Kolluk, bilişim suçunun gerçekleştirildiği IP (servis sağlayıcı) numarasını tespit ederek, IP (servis sağlayıcı) numarasının hangi telefon ve adrese kayıtlı olduğunun bilgisini Türk Telekom'dan resmi olarak talep eder. İnternet suçunu işleyen fail ya da faillerin, kolluk güçleri tarafından toplanan bilgiler ışığında belirlenerek, yargı makamlarına bildirilmesiyle süreç tamamlanır.[342]

Suç ortaya çıkmadan suçun gerçekleşmesini önlemek internet suçları için de son derece önemli bir konudur. Gerçek ve köklü bir suçla mücadele yöntemi olan suç önleme sürecinin aşamaları aşağıdaki gibidir;

- Suç ve suçlularla ilgili tüm bilgilerin toplanması,

- Suç oluşumunu kolaylaştıran şartların tespiti ve analizi,

- Suça zemin hazırlayan şartların önünü alabilecek olası önleyici vasıta ve tedbirlerle ilgili çalışmaların yapılması,

- Ekonomik ve uygulanabilir en isabetli tedbirlerin seçimi ve uygulamaya konulması,

- Uygulama sonuçlarının takibi ve değerlendirilmesi.[343]

Öte yandan, bilişim suçlarının ve özellikle de internetin sınır tanımayan yapısı, coğrafi sınırları aşarak devletlerin bilişim suçları konusundaki denetimini zorlaştırmaktadır. Bu anlamda bilişim suçları olarak da bilinen internet suçlarının soruşturma ve kovuşturulması için uluslararası işbirliğini içeren düzenlemelerin daha fazla önem kazandığı ortadadır.[344]

Bilişim suçları konusunda yapılan en etkin hukuki düzenlemenin, Avrupa Konseyi tarafından 23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suçlar Sözleşmesi olduğu söylenebilir. Hazırlanan sözleşmenin hedefi ortak bir ceza politikasının oluşturulmasıyla toplumun siber suça karşı korunması, özellikle gerekli

[342] Ergüç, a.g.e., s. 61.
[343] Aydın, Ahmet Hamdi, "Suç Önlemenin Önemi ve Etkisi", ***KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi***, Sayı 16, Özel Sayı I, 2014, s. 83.
[344] Kızıltan, a.g.e., s.29.

mevzuatın düzenlenmesi ve uluslararası işbirliğinin geliştirilmesidir.[345] Türkiye, Avrupa Konseyi Siber Suçlar Sözleşmesine 10 Kasım 2010 tarihinde imza koyarak taraf olduğu hâlde, bu Sözleşmeyi iç hukukun parçası hâline getirecek işlemleri tamamlamaya ve iç hukuka aktarmaya yönelik adımları henüz atmamıştır.

İnternetin her geçen gün yaygınlaşması ve kullanım alanlarının artması doğal olarak internet suçları ve suçlularının artmasını beraberinde getirmiştir. Bu şekilde interneti ve bilişimi ilgilendiren suçların artış göstermesi konunun hukuki boyutunu da önemli bir sorun olarak gündeme taşımıştır. Ayrıca söz konusu gelişmelerin ortaya çıkardığı suç tiplerini ve hukuki düzenlemeleri de önümüze koymuştur. [346]

3.2. MEVZUATTAKİ YERİ

Türkiye'nin iç mevzuatında ilk defa, 1991 yılında 765 sayılı Türk Ceza Kanununda, daha sonra da 3756 sayılı TCK'nin 525/a, b, c ve d maddeleriyle eklenen Bilişim Alanında Suçlar yer almıştır. 2004 yılında çıkarılan 5237 sayılı yeni TCK'da siber suçlar, siber suçların güncel gelişimi göz önüne alınarak oldukça ayrıntılı şekilde açıklanmıştır. 5237 sayılı yeni TCK'da bilişim alanında suçlar;

- Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243),
- Bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m.244/1-2),
- Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m.244/4),
- Banka veya kredi kartlarının kötüye kullanılması suçu (m.138) şeklinde düzenlenmiştir.

Ayrıca özel hayata ve hayatın gizli alanına karşı suçlar bölümündeki bilişim suçları;

- Kişisel verilerin kaydedilmesi (m.135),
- Kişisel verileri hukuka aykırı olarak verme veya ele geçirme (m.136),

[345] Helvacıoğlu, Aslı Deniz, "Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi", Yeşim Atamer (Ed.), ***İnternet ve Hukuk***, Bilgi Üniversitesi Yayınları No: 51, İstanbul, 2004, s.279.
[346] Dülger, a.g.e., s. 59.

- Verilerin yok edilmemesi suçları (m.138) biçiminde sıralanmaktadır.

TCK'da bilişim sistemleriyle işlenebilecek diğer suçlar;

- Organ ticareti (Madde 91: 6. Fıkra),
- Cinsel taciz (Madde 105),
- Tehdit (Madde 106),
- Şantaj (Madde 107),
- Haberleşmenin engellenmesi (Madde 124),
- Hakaret (Madde 125),
- Haberleşmenin gizliliğinin ihlal edilmesi (Madde 132),
- Özel hayatın gizliliğini ihlal (Madde 134: 2.),
- Bilişim sisteminin kullanılması yoluyla işlenen hırsızlık (Madde 142: 2. fıkra (e) bendi),
- Bilişim sistemlerinin kullanılması yoluyla işlenen dolandırıcılık (Madde 58: 1. fıkra 1. bendi),
- Uyuşturucu veya uyarıcı madde kullanılmasını alenen özendirme veya bu nitelikte yayın yapma (Madde 190: 3. fıkra),
- Halk arasında korku ve panik yaratmak amacıyla tehdit (Madde 213: 1. fıkrası ve Madde 218),
- Suçu ve suçluyu övme (Madde 215: 1. fıkra ve Madde 218),
- Halkı kin ve düşmanlığa tahrik veya aşağılama (Madde 216 ve Madde 218),
- Yasalara uymamaya tahrik (Madde 217 ve Madde 218),
- Örgütün veya amacının propagandasını yapma eylemi (Madde 220: 8. fıkra),
- Müstehcenlik (Madde 226),
- Göreve ilişkin sırrın açıklanması (Madde 258),
- İftira suçu (Madde 267),
- Gizliliği ihlal suçu (Madde 285),
- Cumhurbaşkanına hakaret (Madde 299),

- Devletin egemenlik sembollerini aşağılama (Madde 300)
- Türklüğü, cumhuriyeti, devletin kurum ve organlarını aşağılama (Madde 301)
- Halkı askerlikten soğutma (Madde 318) olarak sıralanmaktadır.[347]

Böylelikle TCK'da suç olarak kabul edilen ve aynı zamanda asayiş ve terör alanlarına giren birçok suç internet ya da bilişim suçu kapsamına girebilmektedir.

TCK'dan ayrı olarak bilişim suçlarının düzenlendiği diğer bir kanun olan 5846 sayılı Fikir ve Sanat Eserleri Kanununda, bilişim suçlarına konu olabilecek eylemler düzenlenmektedir. Bu kanunda, özellikle bilgisayar programlarına ilişkin telif hakkı suçları ve hukuka aykırı hareketler özel olarak düzenlenmiş ve internet aracılığıyla telif haklarına aykırı fiiller de bu kapsamda değerlendirilmiştir. Kanuna göre, bilgisayar programları, web sayfaları dâhil olmak üzere her türlü fikir ve sanat eserlerini izinsiz olarak kullanan, çoğaltan, işleyen, bilgisayar programlarını koruyan aygıtları geçersiz kılan teknik araçları bulunduran ya da dağıtan ve bu tip eser ve programları izinsiz olarak yayınlayan kişiler bilişim suçu işlemiş kabul edilmektedir.[348]

Bilişim suçlarının internet ortamında artan oranda işlenmesi, internetle alakalı bazı özel kurumların oluşması ve belli bir düzenin geliştirilmesi amacıyla, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun kabul edilmiştir. Bu kanun; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları ile internet ortamında işlenen belirli suçlarla içerik, yer ve erişim sağlayıcıları üzerinden mücadeleye ilişkin esas ve usulleri düzenlemek amacıyla çıkarılmıştır (Md: 1).

Kanunla internet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan; 5237 sayılı TCK'da yer alan suçlar şunlardır;

- İntihara yönlendirme (Madde 84),
- Çocukların cinsel istismarı (Madde 103, birinci fıkra),

[347] Güngör, Necmi Murat, ***Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, İstanbul, 2007, s. 79-147.

[348] Avşar ve Öngören, a.g.e., s. 148.

- Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (Madde 190),

- Sağlık için tehlikeli madde temini (madde 194),

- Müstehcenlik (Madde 226),

- Fuhuş (Madde 227),

- Kumar oynanması için yer ve imkân sağlama (Madde 228) Ayrıca, 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar hakkında ilgili mercilerin kararıyla erişimin engellenmesine karar verilebileceği hüküm altına alınmıştır (Md: 8).

Klasik veya siber suçların takibi, şüphelilerin yakalanması, suç delillerin elde edilmesi, muhafazası gibi adli kolluk faaliyetlerinin Cumhuriyet Savcılarının gözetiminde icra edilirken kolluğun uyacağı usul ve esaslar 5271 sayılı Ceza Muhakemesi Kanununda açıklanmaktadır. Bu kanunda, kolluğun adli kolluk görevlerini yerine getirirken uyacağı usul ve esasları ayrıntılı şekilde yer almaktadır.[349]

Bilişim suçlarında toplanan deliller diğer klasik suçlardan farklı olarak bilişim sistemleri aracılığıyla işlenmeleri nedeniyle dijital deliller olarak adlandırılmaktadır.[350] Bu nedenle 5271 sayılı kanunda ayrı bir maddede, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma başlıklı bölümde, siber suçların işlendiği bilişim teknolojileri araçlarında hukuka uygun olarak kolluk tarafından yapılacak delillendirme faaliyetlerinin usul ve esasları yer almaktadır. Bu maddeye göre;[351]

1. Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet Savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

2. Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması

[349] Taşçı, Ufuk ve Can, Ali, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014", ***Fırat Üniversitesi Sosyal Bilimler Dergisi***, Cilt: 25, Sayı: 2, Sayfa: 229-248, Elazığ, 2015, s. 234.
[350] Yetim, a.g.e., s. 184.
[351] Taşçı ve Can, a.g.e., 234.

halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

3. Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

4. İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

5. Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır (Md: 134).

Ancak bu kanunun uygulanmasında bazı eksiklerin var olduğu ifade edilmektedir. Bunlar şu şekilde sıralanmaktadır:[352]

- Bilgisayarın şifrelenmiş olduğunun veya gizlenmiş bilgiler barındırdığının nasıl anlaşılacağı,

- El koyma yetkisinin iki durumla sınırlanmasının olay yeri inceleme birimlerinin çalışmasını zorlaştırıcağı,

- İçinde suç unsuru (çocuk pornografisi vb.) bulunan dijital medyanın kopyalandıktan sonra iade edilip edilmeyeceği veya hangi formatta verileceği,

- Yedeklerin kimin tarafından, nasıl ve ne kadar süre muhafaza edileceği,

- Sisteme el koymaksızın da kopyasının alınabileceği, bu durumda alınan verilerin kâğıda yazdırılması sırasında binlerce sayfa tutması halinde neler yapılacağı hususun kolluk birimlerinde sıkıntılara neden olabileceğidir.

Türkiye, iç mevzuatının dışında, siber suçlarla mücadelede kabul ettiği önemli bir uluslararası sözleşme olan ve Avrupa Konseyi (AK) tarafından hazırlanan Siber Suçlar Sözleşmesini 10.11.2010 tarihinde imzalamıştır.

6533 sayılı (Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun) kanun olarak meclis tarafından uygun bulunarak 2 Mayıs 2014 tarihinden itibaren bir kısım çekincelerle birlikte yürürlüğe

[352] Hekim, Hakan ve Başıbüyük, Oğuzhan, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", ***Uluslararası Güvenlik ve Terörizm Dergisi***, C: 4, S: 2, 2013, s. 152.

konmuştur.[353] Bu sözleşme internet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin ilk uluslararası sözleşmedir. Anılan sözleşme özellikle telif haklarının ihlali, bilgisayarla bağlantılı sahtecilik, çocuk pornografisi ve güvenlik ağlarının ihlali konularına odaklanmaktadır. Sanal ortamda işlenen suçların ortak tanımlarının yapılmasını, bu alanda ülkelerin maddi ceza hukuku unsurlarını uyumlu hale getirmesini, suçların soruşturulması ve kovuşturulması için gerekli olan yerel ceza usul hukuku yetkilerini sağlamayı ve etkin bir uluslararası işbirliği rejimi oluşturmayı amaçlayan küresel düzeyde etkilere sahip olabilecek bir hukuki belge olarak görülmektedir.[354] Başka bir ifadeyle, Türkiye'nin iç politikasında, bilişim suçlarıyla mücadele politikasını etkileyen önemli dış faktör olarak gözükmektedir. Türkiye bu sözleşmeyi 2010 yılında imzalayıp 2014 yılında onaylasa da, 2004 tarihli 5237 ve 2007 tarihli 5651 sayılı kanunların ve 5846 sayılı kanunda yapılan değişikliklerin, bu sözleşmenin içeriği, amacı ve tanımlarından kısmen de olsa etkilenmiş şekilde kabul edildiğini söylemek yanlış olmayacaktır.

Bilişim suçları ve internet iletişimiyle ilgili Türkiye'de ulusal kanun düzenlemelerini şu şekilde özetlemek mümkündür:[355]

- TCK'nin yukarıda belirtilen ilgili maddeleri,
- CMK'nın ilgili maddeleri,
- Polis Vazife ve Salahiyetleri Kanunu,
- Jandarma Teşkilat, Görev ve Yetkileri Kanunu,
- İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 Sayılı),
- Elektronik Haberleşme Kanunu (5809 Sayılı),
- Elektronik İmza Kanunu (5070 Sayılı),
- Fikir ve Sanat Eserleri Kanunu'nun (5846 Sayılı) ilgili maddeleri,
- 633 Sayılı Diyanet İşleri Başkanlığı Kuruluş ve Görevleri Hakkında Kanunun 6. Maddesinin 5. Fıkrası,

[353] Yetim, a.g.e., s. 187.
[354] tbmm.gov.tr, (2015), "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676).
[355] Dülger, Murat Volkan, ***Bilişim Suçları ve İnternet İletişim Mevzuatı***, Ankara, 2015, s. 9-11.

- 1262 Sayılı Sağlık Bakanlığı'nın İspençiyari ve Tıbbi Müstahzarlar Kanununun 18. Maddesi,
- 6362 Sayılı Sermaye Piyasası Kanununun 115. Maddesi,
- 4733 Sayılı Tütün ve Alkol Piyasası Düzenleme Kurumu Teşkilat ve Görevleri Hakkında Kanunun 8. Maddesinin Beşinci Fıkrasının K Bendi,
- 7528 Sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlemesi Hakkında Kanunun 5. Maddesi,
- 5187 Sayılı Basın Kanunu
- 6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun,
- 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu

Türkiye'de ulusal bazda yapılan bu yasal düzenlemeler yanında yönetmelik bazında da düzenlemeler yapılmakta, bilişim suçları ve internet iletişimiyle ilgili mevzuatı oluşturma çalışmaları ortaya çıkan gereklilikler doğrultusunda devam etmektedir.

3.2.1. İnternet Suçlarında Tahkikat Aşaması

Bilişim suçlarının tahkikat aşaması maddeler halinde şu şekilde sıralanabilir;

- "Suçun Oluşması
- Müşteki/Mağdurun Savcılığa müracaat etmesi
- Savcılık Tarafından İlgili Birime (Emniyet / Jandarma) Havale
- Müşteki / Tanıkların İfadelerinin Alınması
- Suç Hakkında Teknik İnceleme Yapılarak Tespitlerin Yapılması
- Tespit Edilen Bilgilerin İlgili Kuruluşlara Savcılık Havaleli Sevk Edilmesi
- İlgili Kurumlardan Gelen Bilgilere İstinaden Şüpheli Adres Tespitlerinin Yapılması
- Adres Araması ve Bilgisayarların İncelemesi
- Suç Delillerinin Tespiti Halinde Şüphelinin Yakalanması

- Şüphelinin İlgili Savcılıklara Alınacak Talimata İstinaden Sevk Edilmesi"[356]

Ceza muhakemesi, bir kişinin fiilinin suç olduğu şüphesi üzerine yapılan ve bu şüpheyi gidermeye yönelik sürdürülen ortak faaliyeti düzenlemektedir. Bu faaliyette bir suçun işlenip işlenmediği, işlenmişse kimin tarafından işlendiği ve yaptırımın ne olacağı sorularına cevap aranmaktadır. Bu ortak işlemi oluşturan alt faaliyetler ise iddia, savunma ve yargılamadır. Diğer bir ifadeyle tez (iddia), anti-tez (savunma) ve bu ikisinin değerlendirilmesi ile neticeye varılmasını ifade eden sentez (yargılama) bu faaliyetin omurgasını teşkil etmektedir. Ceza muhakemesi faaliyeti sonrasında kişinin hürriyetini kaybetmesi ihtimali ile karşı karşıya kalacak olması ve maddi gerçeğin aranması bu faaliyetin amacı haline gelmiştir. Yargıtay'a göre, "ceza muhakemesinin amacı, maddi gerçeğin hiç bir duraksamaya yer vermeden ortaya çıkarılmasıdır." Bu amaca ulaşılması ise geçmişte olup bitmiş bir olayın deliller aracılığıyla ortaya konulmasını gerekli kılar. Zira zamanı geri döndürmek imkân dâhilinde olmadığına göre, maddi gerçeğin ortaya çıkartılabilmesi için olayla ilgisi bulunan tanıkların, belgelerin ve olaydan arta kalan izlerin tespit edilerek ceza muhakemesi sürecinde kullanılması gerekmektedir.[357]

Bilişim ve internet suçlarıyla mücadele kavramı, özellikle Türkiye için oldukça yeni bir kavramdır. Bu yüzden de mücadele anlamında, gerek hukuki gerekse teknik sıkıntılar bulunmaktadır. Bu sıkıntıların en önemli kaynağı ise; bilişim suçlarının tespiti ve değerlendirilmesinde, hem teknik hem de hukuki bilgilerin entegre bir şekilde kullanılmasıdır. Bu bir nevi sanal bir ortamı fiziksel bir ortam gibi ele almak anlamına gelmektedir. Bu anlamda söz konusu suçların tespiti ve yargılanmasındaki en önemli husus, delillendirmedir. Delillendirme kısaca, bir suç ile ilgili olarak o suçun kim tarafından ve ne şekilde islendiğini ispat edici nitelikte bilgiler elde edilmesi ve bunun adli mercilere sunulması şeklinde tanımlanabilir.[358] Türkiye'de delillendirme olarak adlandırabileceğimiz görev, kolluk tarafından yerine getirilmektedir.

---

[356] Koç, Serhat ve Kaynak, Selva, "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik", ***Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri,*** Muğla Üniversitesi, 10 - 12 Şubat 2010, s. 14.

[357] Sarsıkoğlu, Şenel, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", ***Türkiye Adalet Akademisi Dergisi***, Yıl:6, Sayı:22, Temmuz 2015, s. 429.

[358] Uzunay, Yusuf ve Koçak, Mustafa, "Bilişim Suçları Kapsamında Dijital Deliller", ***7. Akademik Bilişim Konferansı,*** Gaziantep, 2-4 Şubat 2005, s.2.

Türkiye, Emniyet Teşkilatı'nda internet ve bilişim ile ilgili temeller, Emniyet Genel Müdürlüğünde 1982 yılında Bilgi İşlem Daire Başkanlığının kurulmasıyla atılmış, daha sonra merkez teşkilatı içinde bir Bilgisayar Suçları ve Bilgi Güvenliği Kurulu ve Üst Kurul oluşturulmuştur.[359]

2001 yılında Kaçakçılık ve Organize Suçlar Daire Başkanlığı ile Birleşmiş Milletler tarafından ortaklaşa, TADOC (Turkish Academy Against Drug and Organised Crime) kurulmuş ve Bilişim Suçları Araştırma Merkezi oluşturulmuştur. Bu merkez faaliyetlerini daha çok bu suçlar ile mücadelede, ilgili birimlere yön göstermek amacıyla akademik destek niteliğinde çalışmalar yapmakla sürdürmektedir. Bilişim ve internet alanında karşılaşılan sorunlarla ciddi anlamda bir mücadele başlatılmıştır.[360]

Kaçakçılık ve Organize Suçlar Daire Başkanlığı, Emniyet Genel Müdürlüğü bünyesinde Koordinatör Daire Başkanlığı olma özelliğini kazanarak, internet ve bilişim suçlarıyla mücadelesini sürdürmüştür. 2011 yılında Emniyet Genel Müdürlüğü bünyesinde, Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Bu başkanlığın ismi 2013 yılında Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir.[361] Jandarma Genel Komutanlığında ise bu faaliyet Bilişim ve Teknik İstihbarat Daire Başkanlığı ile Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı tarafından yürütülmektedir.

İşte bilişim teknolojileri sonrasında suç mahallinin genişleyerek fiziksel alandan sanal alana kayması, muhakeme faaliyetine katılan kişilerin dikkatini bilgisayar, veri taşıma araçları, taşınabilir telefonlar, bulut bilişim sistemleri gibi elektronik bilgilerin bulunduğu ortamları keşfe yöneltmiştir. Söz konusu durum ise maddi gerçeği ortaya çıkartacak ispat vasıtası olan delil kavramının klasik delillerle birlikte elektronik delilleri (e-delil) de içerecek şekilde kabulünü gerekli kılmıştır. Zira, 5271 sayılı Ceza Muhakemesi Kanunu da klasik deliller ile e-delil arasında herhangi bir ayrıma gitmemiştir.[362]

Bilgisayarlardan veya diğer bilişim sistemlerinden toplanan verilerin ceza muhakemesinde delil değeri taşıyabilmesi için, bu verilerin teknik gerekliliklere

[359] Tekeli, Ömer, "Bilişim Suçlarıyla Mücadelede Polisin Yeri", ***Sayder Dış Denetim Dergisi***, Sayı 183, 2011, s. 185.
[360] Taşçı ve Can, a.g.e., s. 7.
[361] Taşçı ve Can, a.g.e., s. 237.
[362] Sarsıkoğlu, a.g.e., s. 430.

uygun olarak toplanması hayati derecede önem arz etmektedir. Bu bağlamda, bilgisayar ortamında delil toplamak, yalnızca şüphelinin bilgisayarının tamamen kopyalanması ve buradaki içeriğinin adli makamlara sunulmak üzere çıktısının alınması değildir. Bu delil toplama işlemi, teknik gerekliliklerin çok sayıda olduğu hassas bir süreçler bütünü olarak kabul edilmelidir. Bu süreç işletilirken, el konulacak bilgisayarlardan veri alınmasından, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarın kapatılması ve laboratuvara götürülmesine kadar bütün süreçler çok titiz bir biçimde yerine getirilmeli ve eldeki delillerden hiçbirinin kaybolmaması veya zarar görmemesi sağlanmalıdır.[363]

Elektronik delillerin latent, yani gizil yapıda olması, onların incelenmesinin uygun cihazlar ve ölçüm aletleri yardımıyla yapılmasını gerektirir. Çünkü, içerdiği bilgiler yalnızca insanın duyu organları ile algılanamaz. Örneğin, olay yerinde bulunan bir bıçağın, gerçekten bir bıçak olup olmadığını anlamak amacıyla nitel gözlem yapmak yeterlidir. Ancak, yasa kapsamına girip girmediğini anlamak için bıçağın boyu ölçülmelidir. Yani, nicel gözlem yapılmalıdır. Buna karşın, elektronik delillerin içerisindeki dijital verileri anlayabilmek için mutlaka bir uzman tarafından, alet ve cihazlar ile nicel gözlemler yapılmalıdır. Çünkü, genellikle makine dili ile kodlanmış olan bilgiler yine bir makine tarafından yorumlanmalıdır. Ceza muhakemesinde kullanılan klasik deliller gözle görülebilir nitelikte, üzerinde el koyma ve muhafaza altına alma kararları verilerek kolayca elde edilebilir deliller iken, bilişim suçlarında söz konusu olan elektronik deliller, klasik delillerden farklı olarak soyut bir yapıya sahiptirler. Şüphesiz ki, elektronik delillerin içerisinde yer aldığı somut bir donanım aygıtı bulunmakta ise de, ceza yargılaması bakımından esas delil teşkil edenler bu donanım aygıtının kendisi değil, içerisinde yer alan dijital nitelikteki delillerdir.[364]

Elektronik delil olarak ifade edilebilecek delilleri genel olarak şu başlıklar altında toplamak mümkündür:[365]

- "Video görüntüleri,
- Fotoğraflar,
- Yazı dosyaları (Word, Excell, Open Office vb. dosyaları),

[363] Özen ve Özocak, a.g.e., s. 51.
[364] Sarsıkoğlu, a.g.e., s. 441.
[365] Özen ve Özocak, a.g.e., s. 60.

- Çeşitli bilgisayar programları,
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları),
- Gizli ve şifreli dosyalar veya klasörler,
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları,
- Son girilen ve sık kullanılan İnternet siteleri,
- İnternet ortamından indirilen (download) dosyalar,
- Ve bu türden olup, silinmiş dosya veya klasörler"

Bir başka kaynakta ise dijital deliller şu şekilde sıralanmaktadır.

- "Veri dosyaları
- Kurtarılmış silinmiş dosyalar
- Kayıp alanlardan kurtarılmış veriler
- Dijital fotoğraf ve videolar
- Sunucu kayıt dosyaları
- E-posta
- Chat Kayıtları
- İnternet Geçmişi
- Web Sayfaları
- Kayıt Logları
- Abone Kayıtları" [366]

Elde edilme ve değerlendirme süreçleri hassas nitelikte olan elektronik delillere teknolojinin hızlı gelişimine bağlı olarak çok çeşitli ortamlarda rastlanabilmekte ve bu teknolojik yenilikler insanların elektronik ortamlarda muhafaza ettikleri bilgileri depolamadaki alışkanlıklarını sürekli değişime uğratmaktadır. Önceleri kişiler tarafından sabit diskler gibi bilgisayarda bulunan veri saklama birimlerinde tutulan bilgiler, sonrasında taşınabilir bilişim sistemlerinin hayatımıza girmesi ile her zaman erişilebilir olmasını istediğimiz bilgiler akıllı telefonlar ve taşınabilir bilgisayarlar

[366] Uzunay ve Koçak, a.g.e., s. 3.

gibi taşınabilir aletlerde tutulmaya başlamıştır. Gelinen noktada taşınabilir sistemlerin kapasitelerindeki yetersizlikler nedeniyle ve kişilerin taşımak istediği bilginin de çoğalması sonrasında bir ağa ulaşmak koşulu ile bilgilerini ortak sunumcu bilgisayarlarda depolama imkânı olarak bulut bilişim sistemleri kullanılmaktadır. Elektronik deliller saklanma biçimlerine göre iki farklı hafızada bulunmaktadır. Birincisi sabit diskler, CD (Compact Disc)'ler ve taşınabilir hafızalar gibi elektronik delillerin kalıcı olarak saklandığı hafızalardır. İkincil olarak ise ağ sunumcuları, geçici depolama birimleri, ram hafızalar gibi elektronik delillerin geçici olarak depolandığı birimler zikredilebilir.[367]

Dijital delillerin keşfedildiği alanlardan en çok göze çarpanları ise şunlardır:

- "Kuruluş kaynakları
- Geniş Alan Ağları
- Bilgisayarlar (Masaüstü, Laptop, Personal Data Assistant - Kişisel Sayısal Yardımcı, Sunucu, işlemci)
- Elektronik Aygıtlar
- Veri Havuzları
- Bir sistemde yapılan işlemleri gösteren kayıtlar, geçmiş bilgileri, erişim listeleri
- Yedekleme Üniteleri
- Yazılımlar
- E-Postalar
- İnternet ile ilgili dosyalar" (Ör: çerezler)"[368]
- Bulut sistemi[369]

Bilişim suçunun vuku bulduğu yerden dijital delillerin toplanıp mahkemeye sunulmasına kadar geçen süreçte belirli basamaklardan söz edilebilir. Döngü modeli olarak adlandırılabilecek modeldeki ilk safha, olay yerine gidildiğinde dijital delillerin teşhis edilmesidir. Bu safhada bilişim suçları uzmanları tarafından

[367] Sarsıkoğlu, a.g.e., sa.445.
[368] Uzunay ve Koçak, a.g.e., s. 3.
[369] Sarsıkoğlu, a.g.e., s. 445.

nerelerde delil olabileceği saptanır. En önemli konulardan birisi, özellikle delil niteliği taşıyabilecek uçucu bilgilerin (veri) bozulmadan korunmaya alınmasıdır. Uçucu veriler, bilgisayar sistemleri üzerinde, geçici kayıt bölgelerinde tutulan ve elektrik gücü kesildiğinde içeriği sıfırlanan verilerdir.[370]

Bilişim suçlarında delil toplamada başarılı olunabilmesi için dijital delillerin toplanmasına yönelik belirlenen standartlar şunlardır:[371]

- Orijinal deliller ilk bulundukları durum ve şartlara benzer şartlarda korunmalıdır.

- Orijinal delillerin bütünlüğünü bozmamak için mümkünse bire bir kopyası alınmalıdır.

- Kopyanın üzerine alınacağı medya "Adli Tıp yönünden steril" olmalıdır, yani üzerinde daha önceden herhangi bir veri bulunmamalıdır ile virüs ve diğer zararlı kodlara karşı kesinlikle temiz olmalıdır.

- Deliller mutlak suretle etiketlenmeli, korunmalı ve belgelendirilmelidir.

- Adli inceleme esnasındaki bütün basamaklar ve yapılan işlemler yazılı hale getirilmelidir.

Deliller belirtilen kurallar doğrultusunda toplandıktan sonra, toplanan delillerin dijital ve fiziksel olarak korunması gerekmektedir. Dijital olarak koruma; delillerin ilk alındığı andan itibaren değişmediğini, bütünlüğünün bozulmadığını ispatlayacak çeşitli mekanizmaları kapsamaktadır. En çok kullanılan tekniklerden bir tanesi verilerin kriptografik olarak özetlerinin alınmasıdır. Fiziksel olarak koruma ise; delillerin incelenecek yere bozulmadan taşınması, mahkeme esnasına kadar uygun ortamlarda saklanması ve yine mahkemeye gidiş esnasında her hangi bir bozulmaya uğramamasını içermektedir. Deliller mümkün olduğunca toplandığı ortam koşullarına benzer ortamlarda taşınmalı veya saklanmalıdır. Unutulmaması gereken başka bir nokta ise toplanan bütün delillerin etiketlenerek, uygun şekilde paketlendikten sonra mühürlenmesidir.

Dijital delillerin analiz safhası genellikle bilgisayar adli tıbbı uzmanları tarafından gerçekleştirilir. Elde edilen bütün deliller uygun ortam koşullarında açılıp

[370] Uzunay ve Koçak, a.g.e., s. 4.
[371] Çakır, Hüseyin ve Sert, Ercan, "Bilişim Suçları ve Delillendirme Süreci", ***Örgütlü Suçlar ve Yeni Trendler***, Polis Akademisi Yayınları, 2011, s. 150.

bir araya toplandıktan sonra eğer daha önceden yapılmamışsa ilk yapılacak şey, bire bir kopyalarının alınıp orijinallerinin korunmaya alınmasıdır. Genellikle kopyalar dörder adet olmaktadır. Bir tanesi mahkeme için, ikincisi analiz için, üçüncüsü savcı için dördüncüsü de savunma tarafı için çoğaltılır. Yapılacak bütün işlem ve analizler önceden planlanmalı, hangi kişinin hangi deliller üzerinde ne gibi işlemler yaptığı mutlaka belgelendirilmeli ve aynı zamanda uzmanları doğrulayacak sistemler ile oluşturulacak imzalar (Dijital imza) belgelere eklenmelidir. Analiz safhası, en fazla teknik bilgi gerektiren ve en uzun sürecek safhadır.

Bütün incelemeler bittikten sonra, son aşama bu delillerin mahkemeye sunulmasıdır. Hazırlanan bütün rapor ve belgeler bir araya toplanıp, delillerin mahkemeye sunumu için uygun formatta dokümanlar oluşturulur. Bütün işlemler titizlikle yapılmalı ve bütün süreçler açık bir şekilde dokümanda ifade edilmelidir. Delillerin bütünlüğü ve doğrulamasını sağlamak için kullanılmış olan bütün sistemler ayrıntılı bir şekilde açıklanmalıdır.[372]

Ceza muhakemesinde, muhakeme makamları öncelikle önlerine gelen somut olayın maddi yönünü çözmekte, maddi gerçeğin ne olduğunu tespit ettikten sonra bunun hukuki yönünü değerlendirmektedir. Bu nedenle, öncelikli görevi maddi gerçeğe ulaşmak olan ceza mahkemeleri, işlendiği iddia olunan fiilin işlenip işlenmediğini, işlenmişse bu fiilin kanunlar nezdinde bir suç teşkil edip etmediğini ve suç teşkil ediyorsa bunun sanık tarafından işlenip işlenmediğini belirlemek durumundadır. Bu değerlendirme sonucunda hüküm verecek olan hâkim, eğer fiilin işlendiğine, suç olduğuna ve sanık tarafından işlendiğine kanaat getirirse, hükmü "sabit görme"; ancak bu kriterlerden birinin mevcut bulunmaması durumunda "sabit görmeme" biçiminde tezahür edecektir. O halde, birinci durumda maddi gerçek ispatlandığından suçu sabit görülen sanık cezalandırılacak, ikinci durumda ise suç sübut bulmadığından cezalandırılmayacaktır. İşte, hâkimin ceza yargılaması esnasında yapacağı maddi olayı çözmek ve bunun için olayın sabit görülüp görülmemesine karar verilmesi olduğundan, yapılacak olan muhakemenin temelinde bu yargıyı oluşturacak delillerin değerlendirilmesi yer almaktadır.[373]

[372] Uzunay ve Koçak, a.g.e., s. 5.
[373] Özen ve Özocak, a.g.e., s. 56.

3.2.2. 5237 Sayılı TCK'ya Göre İnternet Suçları

Türk Ceza Hukukunda uygulanacak hukukun tespitine ilişkin ölçütler Alman Hukukuyla paralellik göstermektedir. Uygulanacak hukukun tespiti açısından Türk hukukunda geçerli olan ilkeleri;[374]

−TCK Madde 8-9: Mülkilik Prensibi,

−TCK Madde 10-11: Faile Göre Şahsilik Prensibi

−TCK Madde 12 (fıkra 1-2): Koruma İlkesi

−TCK Madde 123 (fıkra 3): Evrensellik İlkesi şeklinde sıralamak mümkündür.

Bu ilkeler içerisinde mülkilik prensibi alman hukukunda olduğu gibi temel prensip olarak dikkati çekmektedir. TCK Md. 8'e göre suç teşkil eden bir fiilin kısmen veya tamamen Türkiye'de islenmesi veya neticenin Türkiye'de gerçekleşmesi durumunda Türk hukukunun geçerli olduğu prensibi kabul edilmiştir. Bu yaklaşımdan hareketle suçun islendiği yerin tespiti hususunda Türk hukukunun da Alman hukuku gibi karma sistemi benimsediği anlaşılmaktadır. Başka bir ifade ile, suçun işlendiği yerin tespiti bakımından ne salt harekete ne de salt neticeye ağırlık verilmekte, hem netice hem de hareket dikkate alındığı için karma bir sistemden sözedilebilmektedir. Ancak, alman ceza hukukunun uygulanabilirliği konusunda ortaya konan çekincelerin Türk ceza hukuku bakımından da geçerli olduğu görülmektedir.[375] Karma yaklaşımın doğal sonucu olarak uygulanabilirliğin çok geniş anlaşılması ve CMK'dan kaynaklanan kovuşturma mecburiyetinin varlığı söz konusu durumu özellikle internet ortamında islenen suçlar konusunda oldukça zorlamaktadır. İnternet ortamında işlenen suçlar bakımından netice ve hareket ilişkisine İkinci Bölümde değinilmişti.

3.2.2.1. Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Sistemde Kalma Suçu

Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalma suç haline getirilmiştir (md 243). Suçun meydana gelmesi için verilerin ele geçirilmiş olması gerekli değildir. Bilişim güvenliğinin ihlal edilerek sadece sisteme girmek suçun meydana gelmesi için yeterlidir. Hükmün amacı başkasının

[374]Tepe, a.g.e., s. 190.
[375] Yetim, a.g.e., s. 186.

bilişim sitemine hukuka aykırı olarak girme ve orada kalmayı cezalandırmaktadır. Aslında bilişim sitemine girilmekle aynı zamanda orada kalınmaktadır da. Bu nedenle "ve orada kalmaya devam eden " ibaresine gerek yoktu. Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçuna karşılaştırmalı hukukta birçok ülke mevzuatında yer verilmektedir. Ancak söz konusu suç genellikle verilerin ele geçirilmesi ile düzenlenmektedir. Örneğin, Fransız Ceza Kanununun 323/1, Alman Ceza Kanununun 202/a, İtalyan Ceza Kanununun 616/2, 617 querter maddelerinde olduğu gibi.[376]

Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu TCK'de aşağıdaki gibi düzenlenmiştir.

"Madde 243- *(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.*

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(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 ile cezalandırılır."*[377]

Sanal Ortamda İşlenen Suçlar Sözleşmesinin 3'üncü maddesiyle, üye ülkeler, yasadışı araya girme eylemini cezalandırmaya davet edildiğinden, 5237 sayılı Kanunun 243'üncü maddesinde değişiklik öngörülmüştür. Böylece bilişim sistemlerinin bütününe veya bir kısmına hukuka aykırı olarak girmekle birlikte belirli bir süre kalmak da suçun unsuru olarak düzenlenmiş olmasına rağmen Sözleşmeye uyum amacıyla sadece sisteme/sistemlere girmek fiili suç olarak düzenlenmektedir. Verilerin izlenmesi eylemi, bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini ifade etmektedir. Bütün elektronik veri transferleri, bu çerçevede korunması amaçlanan veri transferinin gizliliği kapsamında kalmaktadır. Yasadışı araya girme eylemleri, temelde bilişim sistemlerine girilmeksizin işlenen fiillerdendir. Bu doğrultuda Sözleşmeye uyum amacıyla yine aynı maddenin birinci fıkrasına hüküm eklemek suretiyle, bir bilişim sisteminin kendi içinde veya bilişim

[376] Soyaslan, Doğan, Ceza Hukuku Özel Hükümler, Yetkin Yayınları, Ankara, 2014, s.692.
[377] 5237 Sayılı Türk Ceza Kanunu, s. 9027.

sistemleri arasında gerçekleşen veri nakillerini sisteme girmeksizin teknik araçlarla izleyen kişinin bir yıldan üç yıla kadar hapis cezası ile cezalandırılması öngörülmüştür. Ayrıca, 243 üncü maddeye 24.03.2016 tarihinde çıkarılan 6698 Sayılı kanunla eklenen 4. fıkrayla, kamu kurum veya kuruluşlarına karşı işlenenler hariç olmak üzere, suçun soruşturulması ve kovuşturulması şikâyete tabi hale getirilmektedir. Böylelikle, somut olayın özelliklerine göre mağdurun iradesi dâhilinde suçun soruşturulup soruşturulmayacağına karar verilecek ve mağdur bakımından ortaya çıkması muhtemel zararlar engellenecektir.[378]

Bilişim sistemine girme suçu ile bir nevi "engelleme suçu" yaratılmak istenmektedir. Zira, bilişim suçlarının büyük bir çoğunluğu sisteme girilmek suretiyle başlamaktadır. Bilişim sistemine girme suçu, failin hedef dosya ya da programlara izinsiz giriş yapması halinde ortaya çıkmaktadır. Diğer bir deyişle, "girmek" kavramından, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesi anlaşılmaktadır. "İzinsiz erişim" Avrupa Komisyonu tarafından da, bilgisayar sistemlerinin bir bölümüne ya da tümüne yapılan izinsiz erişimleri tanımlamak için kullanılmıştır. Bu bakımdan sisteme erişim yöntemi önemli değildir. Birleşmiş Milletler kitapçığına göre, giriş ya da erişim genellikle ağ bağlantıları boyunca uzak bir bölgeden pek çok farklı yollarla yapılmaktadır. Fail, erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanabileceği gibi, var olan güvenlik önlemlerindeki boşlukları da kullanabilir. Ağ üzerinden sisteme girmek için birçok yöntem kullanabilir; bir virüs kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir.[379]

Suçun maddi konusu, bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek ve orada kalmaya devam etmektir. Sisteme hukuka aykırı olarak girip orada kalmaya devam etmekle suç oluşur. Bilişim sistemine girme suçu, davranışın şekli bakımından yapılacak bir sınıflamada şekli suçlar arasında yer alır. Diğer bir anlatımla bu suçun oluşumu suç tipinde öngörülen davranışların gerçekleştirilmesi ile tamamlanmış sayılır. Bunun dışında ayrıca bir zarar veya başkaca bir takım sonuçların gerçekleşmesi gerekmez. Bununla birlikte, davranışın

---

[378] TBMM Mevzuat Bilgi Sistemi, ***6698 Sayılı Kişisel Verilerin Korunması Kanunu*** Madde 30 (Yürürlük Tarihi: 07.04.2016), Alt Komisyon Gerekçesi, (Erişim) http://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?_afrWindowMode=0&_afrLoop=2428696326380301&psira=122834&_adf.ctrl-state=uecwm0504_34, 20.01.2017.

[379] Erdoğan, Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu**",** ***Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi***, Cilt: 12, Özel Sayı, 2010, s. 1365.

devamlılığı bakımından da suç kesintisiz (mütemadi) bir suçtur. Yani davranış gerçekleştirildiğinde suç oluşur; ancak hemen sona ermez. Örneğin fail bilişim sistemine girip orada kalmakla suçu işlemiş olur. Ama sisteme girip orada kalmasıyla suç sona ermez. Fail sistemde kalmaya devam ettiği müddetçe suç da devam eder.[380]

Yargıtay 8. Ceza Dairesinin 24.06.2014 tarih ve 2013/1777 E, 2014/16144 K. Sayılı ilamı şu şekildedir:

"*Şikâyetçi şirketin sistemine hukuka aykırı olarak girerek, sistemin işleyişini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka yere gönderme şeklindeki TCK'nun 244/1-3. Maddesi ve fıkralarında yazılı hallerin gerçekleşmemesi nedeniyle, anılan maddenin 4. Fıkrasının uygulanamayacağı, şikâyetçi şirkete ait sisteme hukuka aykırı olarak girme ve orada kalmaya devam etme şeklindeki eylemin TCK'nun 243/1. madde ve fıkrasında düzenlenen suçu oluşturacağının gözetilmemesi*"

Şeklindeki karar yerel mahkeme kararını bozarak hukuka aykırı olarak girmeyi ve orada kalmaya devam etmeyi suçunun oluşumu için yeterli görmüştür.[381]

Benzer şekilde Yargıtay 11. Ceza Dairesi 26.03.2009 tarih ve 2008/18190 E, 2009/3058 K sayılı ilamında 243. Maddeye gönderme yapılarak şöyle denilmiştir:[382]

"Sanığın, katılanın yetkilisi olduğu Z T İmalat Pazarlama Sanayi ve Ticaret Limited şirketinin Türkiye E. Bankası Denizli şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK'nun 243/1. maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 sayılı TCK'nun 244/4, 35. maddeleri gereği) hüküm tesisi yasaya aykırı olup (Bozmayı gerektirmiştir.) suçun hareket suçu olduğu görülmektedir."

5237 sayılı TCK'nin 243'üncü maddesinde düzenlenen bilişim sistemine girme suçuyla bu tür fiiller ilk defa cezai müeyyideye bağlanmış ve Türk hukuk sistemi açısından önemli bir eksiklik de ortadan kaldırılmıştır. Bu maddede yer alan suç ile Avrupa Siber Suç Sözleşmesi'nin 2'nci maddesinde öngörülen "hukuka aykırı erişim" düzenlemesine paralellik sağlanmaya çalışılmıştır. Sözleşmenin 2. maddesi *"Her Taraf, iç hukukuna uygun olarak, bir bilişim sisteminin tamamına veya bir*

[380] Karakehya, Hakan, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", ***Türkiye Barolar Birliği Dergisi***, Sayı: 81, 2009, s. 13.
[381] Bikirli, a.g.e., s. 2.
[382] Bikirli, a.g.e., s. 3.

kısmına kasten ve haksız olarak erişimi suç haline getirmek için gerekli görülen yasal tedbirleri almayı kabul eder" şeklinde düzenlenmiştir. [383]

Bilişim sistemine girme ve sistemde kalmaya devam etme suçu açısından TCK'nin 243/2. Madde ve fıkrasında yalnızca cezayı hafifletici nitelikli hale yer verilmiştir. Buna göre, hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma eylemleri "bedeli karşılığı yararlanılabilen sistemler" hakkında işlenmesi yasa koyucu tarafından cezayı hafifletici bir neden olarak öngörülmüştür.[384]

Ancak TCK'nin 243/2. Madde ve fıkrasındaki bilişim sistemine girme ve sistemde kalmaya devam etme suçunun terör amaçlı olarak işlenmesi durumunda, 3713 sayılı Terörle Mücadele Kanunu'nun 29.06.2006 tarih ve 5532 sayılı Yasa ile değişik 4. Maddesi gereği ceza yarı oranında artırılarak hükmedilebilir.[385]

Bir bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme suçunun cezalandırılması için "veri" ele geçirilmesi koşulu yoktur. TCK'nin 136. maddesinde, kişisel verilerin elde edilmesi ayrı bir suç tipi olarak düzenlenmiştir. Bu fiil ile bir kişi veya kuruluşun çıkarlarına zarar verilmese dahi, bilişim sisteminin erişilmezliğine yönelik güven ortadan kaldırılmaktadır. Böylece bilişim sisteminin güvenliği özellikle hacker olarak tabir edilen şahıslara karşı korunmak istenmiştir. Bilişim sistemine hukuka aykırı erişim suçu, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilecek olan dolandırıcılık veya hırsızlık gibi suçlara ya da doğrudan bilişim suçları olan TCK'nin 244 ve 245'inci maddelerinde belirtilen suçlara zemin hazırlamakta ve bir araç olarak kullanılmaktadır. Bir bilişim sistemine haksız erişim, bilişim sistemlerinin ve kapsamındaki verilerin gizlilik, bütünlük, kullanılabilirlik gibi hususları kapsayan güvenliğine yönelen tehdit ve saldırılar biçimindeki hukuka aykırı fiilleri anlatmaktadır. Bilişim sistemlerinin korunma ihtiyacının yanında, ister ferdi ister kurumsal düzeyde kullanıcıların rahatsız edilmemesi ve engellenmemesi gereklidir. Yalnızca sistemine haksız erişimin dahi başlı başına bir suç olarak düzenlenmesi bir ihtiyaç olarak görülmektedir.[386]

Ayrıca, bu suç birleşik hareketli bir suç olup hukuka aykırı olarak bilişim sistemine girilmesi ve sistemde kalınmaya devam edilmesi hareketlerinin

---

[383] Apaydın, Cengiz, "Bilişim Sistemine Girme Suçu**",** ***Türkiye Adalet Akademisi Dergisi***, Yıl:7, Sayı:24, Ocak 2016, s. 252.
[384] Bikirli, a.g.e., s. 5.
[385] Bikirli, a.g.e., s. 6.
[386] Apaydın, a.g.e.,s.253-254.

yapılmasıyla suç gerçekleşmiş olacaktır. Bu nedenle, sisteme girilmesi ancak sistemde kalmaya devam edilmemesi halinde suç oluşmaz. Yargıtay 11. Ceza Dairesi, 19.03.2012 tarih ve 2012/3683 K tarihli ilamında;

"Sanığın katılan şirkette çalıştığı sırada kendisine görevi nedeniyle verilen internet şifresini, iş yerinden ayrıldıktan sonra hakkı bulunmadığı halde kullanmak suretiyle katılan şirkete ait bilişim sistemine hükümsüz kalan şifresi ile girip, buradaki şirket çalışanlarına ait maillerin kendi kurduğu siteye yönlendirmesini yapabilecek kadar süre ile kaldığını savunması karşısında; yüklenen TCK'nin 243/1. maddesindeki suçun bilişim sistemine hukuka aykırı olarak girmek ve orada kalmaya devam etmek unsurlarının gerçekleştiğinin kabulü ile mahkûmiyetine karar verilmesi yerine yazılı şekilde beraatı yönünde hüküm kurulması …"

Gerekçesiyle hükmü bozmuş ve bilişim sistemine hukuka aykırı olarak girmeyi ve orada kalmayı suçun unsurları olarak saymıştır.[387]

3.2.2.2. Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi Suçu

Türk Ceza Kanununun 244. maddesinde, "*bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır"* denilmektedir. Bu madde *"Avrupa Siber Suç Sözleşmesi"*nin *"sistem engellemeleri"* başlıklı 5. maddesine paralel bir iç hukuk düzenlemesidir. Mülkiyet hakkı bu düzenleme ile korunmaktadır.[388] 5237 sayılı TCK'nin 244. maddesinde, sisteme ve veriye müdahale iki fıkra halinde düzenlenmiş; maddenin birinci fıkrasında sistemin işleyişine müdahale, ikinci fıkrasında ise sistem içerisindeki veriye yönelik fiiller düzenlenmiştir. Şu var ki,TCK 244. maddenin 1. ve 2. fıkralarındaki suçlarla korunan hukuki değer konusunda görüş birliği bulunmamaktadır. Bir görüşe göre, burada korunan hukuki değer, karma nitelikte olup ve bilişim sistemi ve/veya bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisi bulunan kişinin verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. gibi değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarıdır. Diğer bir görüşe göre, genel olarak TCK 244. maddede, bilişim sisteminin ve bu sistem içerisindeki verilerin dokunulmazlığı korunan hukuki değerdir. 1. fıkrada, bilişim sistemi sahibinin mülkiyet hakkı, zilyedinin bilişim sisteminin dokunulmazlığı, iletişim kurma, teknolojik gelişim özgürlüğü korunmaktadır. 2. fıkrada göre ise, bazen mülkiyet hakkı, bazen de verilerin içeriğine göre fikri

[387] Bikirli, a.g.e., s. 3.
[388] Avşar ve Öngören, a.g.e., s. 135.

mülkiyet hakkı, özel hayatın gizliliği, ticari sırlar korunmaktadır. Bir başka görüş, TCK 244. maddenin 1. ve 2. fıkralarında korunan hukuki değerin, madde gerekçesinde de belirtildiği üzere, sistemlere yöneltilen ızrar fiillerini özel bir suç haline getirme düşüncesiyle bağlantılıdır. Aslında burada hem bilişim sisteminin ve hem de bu sistem içerisinde yer alan veriler veya diğer unsurların zarar görmemesi amaçlanmaktadır.[389]

Kanun'un 244. maddesinin ikinci fıkrası "bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır" şeklinde düzenlenmiştir. Maddenin ilk fıkrasında bilişim sistemdeki "işleyiş" özne alınmışken bu suçta "veri unsuru" özne alınmaktadır. Avrupa Siber Suç Sözleşmesi'nin "veriye müdahale" başlıklı 5. maddesine paralel bir iç hukuk düzenlemesi bununla sağlanmaktadır. Suçun maddi unsuru verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması gibi 244/1 düzenlemesine benzer eylemlerdir. Bunlardan birinin gerçekleşmiş olması cezalandırma için yeterlidir. Bu fıkra uyarınca sisteme veri yerleştirme bir başka suç oluşturmaktadır.[390] Örnek vermek gerekirse; Yargıtay 8. Ceza Dairesi 17.09.2014 tarih ve 2014/14716-20052 E-K sayılı;

"Sanığın katılana ait elektronik posta adresi ve Facebook sayfasının şifresini değiştirerek katılanın erişimine engel olması şeklindeki eyleminin TCK'nin 244/2. maddesine uygun bulunduğu gözetilmeden, yazılı şekilde uygulama yeri bulunmayan TCK'nin 244/1. maddesi gereğince hüküm kurulması,"

şeklindeki ilamla yerel mahkemenin kararını bozmuştur.[391]

Türk Ceza Kanunu 244. maddesinin 1.ve 2. fıkralarında düzenlenen suça bir başka örnek şu şekilde verilebilir: Kişiler arasındaki internet ortamında e-mail, telefon, chat veya haber grupları aracılığıyla yapılan haberleşmenin yahut bir internet web sayfasından yapılan basın ve yayın faaliyetinin birtakım virüsler göndererek ya da sisteme müdahale edilerek engellenmesi veya verilerin erişilmez kılınmasıdır. Burada önemli bir konu ise web sitesi içindeki bilgilerdir. Kişiler, kendileri hakkında hakaret içeren ya da suçlayıcı beyanlar bulunan web sitelerine karşı harekete geçerek kendileri hakkındaki verileri bozarlarsa veya değiştirirlerse suç işlemiş olmazlar. Çünkü, bu suç açısından da meşru müdafaa hali hukuka uygunluk sebebidir. Bu

[389] Yılmaz, Sacit, a.g.e., s. 67.
[390] Avşar ve Öngören, a.g.e., s. 137.
[391] Bikirli, a.g.e., s. 8.

maddede sayılan eylemlerin hukuka aykırı olması cezalandırma için gerekli bir şarttır. Bu suç için ayrıca suçun manevi unsuru olan genel kasıt yani eylemi bilme ve isteme de gereklidir.[392]

Suçun oluşması açısından verilerin erişilmez kılınmasının geçici süreyle ya da sürekli olması arasında fark bulunmamaktadır. Her iki halde de suç oluşundan söz edilmektedir. Nitekim Yargıtay 8. Ceza Dairesinin 08.04.2014 tarih ve 2013/2731 E, 2014/8912 K sayılı şu ilamı da bunu destekler niteliktedir.

"Sanığın, katılana ait e-posta adresinin şifresini değiştirmek suretiyle erişilmez kılmaktan ibaret eyleminin TCK'nin 244/2. madde ve fıkrasında düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi," yine Yargıtay 8. Ceza Dairesi 01.11.2013 tarih ve 2012/33557 E, 2013/25987 K sayılı ilamında da "Oluşa, katılanın aşamalardaki anlatımlarına, sanığın da çalıştığı aile şirketine ait telefona bağlı internet hesabından katılana ait elektronik posta hesabına girildiğine ilişkin Microsoft şirketinden gelen yazı yanıtları ve kolluk araştırması sonuçlarına, katılanın 22.12.2010 tarihli dilekçesi ekinde ibraz ettiği fotoğraflara ve tüm dosya kapsamına göre; katılana ait elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabında yazışmalar yapan ve şifreyi değiştirmek suretiyle katılanın anılan hesaplara erişimini engelleyen sanığın, eylemine uyan TCK'nin 244/2. maddesi uyarınca cezalandırılmasına karar verilmesi gerekirken yazılı gerekçeyle beraat hükmü kurulması,"

Böylece; Yargıtay yukarıdaki gerekçeyle yerel mahkemenin kararını bozarak e-posta adresine ve facebook hesabına erişilmez kılmayı TCK'nin 244/2. maddesindeki suçu oluşturduğuna karar vermiştir.[393]

TCK'nin 244. maddesinin 3. ve 4. fıkralarında suça etki eden nedenler açısından iki düzenlemeye yer verildiği görülmektedir. Üçüncü fıkra ise, TCK'nin 244. maddesinin 1. ve 2 fıkrasında düzenlenen fiillerin bir kamu kurum ya da kuruluşuna ya da banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmesi halini düzenlemiştir. Son fıkrada yer alan hüküm de genel olarak bilişim ya da bilgisayar sistemleri aracılığıyla yarar sağlama fiillerinin cezalandırılmasına ilişkindir. Yine, TCK'nin 244. maddesinin 3. fıkrasında suçun ağırlaştırıcı nedeni de düzenlenmiştir. Buna göre, bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek ceza arttırılacaktır. Böylelikle Tüm kamu kurum veya kuruluşlarına ait bilişim sistemleri 3. fıkra kapsamında değerlendirilebilecektir. Özel kurumlardan ise

[392] Avşar ve Öngören, a.g.e., s. 138.
[393] Bikirli, a.g.e., s. 10.

banka veya kredi kurumu niteliği olan tüm özel kurum veya şirketler TCK 244/3 kapsamında değerlendirilecektir.[394]

5237 sayılı TCK'nin 244. maddesinin 1. fıkrasında, düzenlenen eylemler açısından bir yıldan beş yıla kadar hapis cezası, 2. fıkrasında düzenlenen eylemler açısından ise altı aydan üç yıla kadar hapis cezası öngörülmüştür. 5237 sayılı TCK'nin 244. maddesinin 3. fıkrasında düzenlenen durumun gerçekleşmesi halinde, yukarıda belirtilen cezalar yarı oranında arttırılacaktır. TCK'nin 244. maddesinde düzenlenen suçlar şikâyete bağlı olmayıp Cumhuriyet Başsavcılığı tarafından doğrudan soruşturma yapılır. Yargılama yetkisi ise asliye ceza mahkemelerine aittir.[395]

Dikkat edilecek olursa; 244. madde sekiz adet suç tipini içermektedir. Bir eylemle bu suçlardan birden fazlası mesela üç tanesi gerçekleşebilir. Bu durumda Ceza Hukuku genel teorisine göre, karma suç kapsamında birden fazla suç oluşmayacağından, en ağır cezası olan suç işlenmiş sayılır ve bu suçun cezası verilir; yani, "her bir suç ayrı ayrı işlendi" denilerek ayrı cezalar verilmez.[396]

3.2.2.3. Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu

Benzeri bir düzenleme Siber Suç Sözleşmesinin 8. maddesinde yer almıştır. Buna göre, bilgisayarlarla ilişkili sahtecilik fiillerinin, bir diğer kişinin malvarlığında doğrudan bir zarara yol açmış ve suçu işleyen kimse kasıtlı olarak kendisi veya bir başkası için yasadışı ekonomik yarar sağlamak amacıyla hareket etmişse suçunu oluşturduğu kabul edilmiştir. Mukayeseli hukuktaki gelişmelere paralel olarak, Anılan maddesinin son fıkrasında bilişim sistemi aracılığıyla haksız yarar sağlamaya ilişkin bir düzenlemeye yer verilmiştir. TCK'nin 244. Maddesinin 4. fıkrasında düzenlenen bu suç, maddenin 1 ve 2. fıkralarına göndermede bulunmaktadır. Bu fıkrada, bir bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemdeki verilerin bozulması, yok edilmesi, değiştirilmesi, başka yere gönderilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi suretiyle kişinin kendisinin veya başkasının

[394] Yılmaz, Sacit, a.g.e., s. 84.
[395] Yılmaz, Sacit, a.g.e., s. 85.
[396] Avşar ve Öngören, a.g.e., s. 138.

yararına haksız çıkar sağlaması gibi fiiller "başka bir suç oluşturmadığı" takdirde cezalandırılmaktadır.[397]

244/4'teki suçun yasa maddesindeki tanımına göre, failin bilişim sistemi aracılığıyla gerçekleştirdiği eylemler neticesinde suçun oluşması için failin hukuka aykırı bir yarar elde etmesi gerekmektedir; ancak bunun nasıl bir yarar olduğu açıklanmamıştır. Yararın türü bakımından bir ayrım yapılmadığına göre fail tarafından elde edilen maddî ya da manevî yarar suçla korunan hukuksal değeri oluşturmaktadır. Burada söz edilen fail, herkes olabilir. Söz konusu edilen hukuka aykırı yarar ise, ekonomik değeri olan mali bir yarar olabileceği gibi ekonomik bir getirisi ve değeri olmayan tamamen duyguları tatmine yönelik manevi bir yarar da olabilecektir.

Bu suç tipi 244. maddenin 4. fıkrasından aynı maddenin 1. ve 2. fıkralarına yapılan atıfla düzenlendiği için; 244. maddenin 1. ve 2. fıkralarında düzenlenen bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu ile verilerin yok edilmesi veya değiştirilmesi suçunun maddî unsurunu oluşturan eylemler, bu suçun da eylem unsurunu oluşturmaktadır. Buna göre bu suçun oluşabilmesi için failin bilişim sisteminin işleyişini engellemek, bilişim sistemin işleyişini bozmak, verileri bozmak, bilişim sistemine veri yerleştirmek, bilişim sisteminde var olan verileri başka bir yere göndermek, verileri erişilmez kılmak, verileri değiştirmek ve verileri yok etmek hareketlerinden birini ya da bir kaçını gerçekleştirmesi gerekmektedir. Dolayısıyla bu suç da seçimlik hareketli bir suç olarak düzenlenmiştir.[398]

ATM'lere fiziksel etkide bulunmak suretiyle ATM makinelerinin içindeki paranın alınması eylemi de TCK'nin 244/4. Madde ve fıkrasındaki suçu oluşturmaktadır. Örneğin, Yargıtay 11. Ceza Dairesinin 14.03.2012 tarih ve 2010/6346 E, 2012/3544 K sayılı ilamındaki gerekçesi şu şekildedir.

"Sanıkların Oyakbank ATM'nin çalışmasındaki aksaklığı fark ederek, çeşitli zamanlarda para çekme işlemi sırasında ATM'ye fiziki müdahalede bulunmak suretiyle cihazın para bloke edilmiş gibi işlem görmesini sağlayıp, çektikleri paranın hesaptan düşmesini engelleyerek menfaat elde ettiklerinin iddia ve kabul olunması karşısında eylemlerinin 5237 sayılı TCK'nun 244/4 maddesindeki "bilişim sistemini engellemek veya yanlış biçimde çalışmasını sağlamak suretiyle yarar sağlamak"

[397] Yılmaz, Sacit, a.g.e., s.86.
[398] Dülger ve Modoğlu, a.g.e., s. 48-49.

suçuna uygun bulunduğu gözetilmeden yazılı şekilde 765 sayılı TCK'nun 525/b-2. maddesinden hüküm kurulmak suretiyle eksik ceza tayini"

Yargıtay bu gerekçeyle eylemin 244/4. Maddesindeki suçu oluşturduğunu kabul etmiştir. Burada herhangi bir banka kartı kullanımı söz konusu olmayıp doğrudan fiziksel etki ile hukuka aykırı yarar elde edilmiştir.[399]

Yasa koyucu bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçunun gerçekleşmesi için failin gerçekleştirdiği eylemler neticesinde yasanın ifadesiyle "haksız bir çıkar sağlamasını" aramıştır. Haksız çıkar ifadesiyle kastedilen "hukuka aykırı yarardır". Bu yarar yukarıda da açıklandığı üzere mali haklara yönelik bir yarar olabileceği gibi manevi haklara yönelik bir yarar da olabilecektir. Bu durum her eylem açısından değerlendirilecektir. Failin gerçekleştirdiği eylemin sonucunda yarar elde edememesi durumunda bu suç oluşmayacaktır. Bu durumda 244/1–2 fıkralarında yer alan suçların gerçekleşmesi söz konusu olabilecektir.

TCK m. 244/4'te düzenlenen suç açısından teşebbüs özellik göstermektedir. Çünkü bu suç tipinin hareket unsuru 1. ve 2. fıkralarda düzenlenmiştir, suçun neticesi ise 4. fıkrada yer almaktadır. Failin kastının, gerçekleştirdiği eylemin neticesinde hukuka aykırı yarar elde etmek olduğunun tespit edilebildiği ancak 244. maddenin 1. ve 2. fıkralarında tanımlanan eylemin tamamlanıp neticenin failin elinde olmayan nedenlerle gerçekleşmediği durumda fail 244. maddenin 4. fıkrasına teşebbüsten dolayı cezalandırılmalıdır. Buna karşın failin kastının hukuka aykırı yarar elde etmek olduğunun ortaya konulamadığı ancak 1. veya 2. fıkradaki eylemlerin tamamlandığı durumlarda fail artık 4. fıkradaki suça teşebbüsten değil, 1. veya 2. fıkradaki suçun tamamlanmış hâlinden cezalandırılmalıdır.[400]

TCK'nin 244. maddesinin 4. fıkrasında yer alan bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçunu işleyen failler için hem hürriyeti bağlayıcı ceza hem de Adlî para cezası öngörülmüştür. Yasada bu suçun cezası olarak 2 yıldan 6 yıla kadar hapis cezası ve 5000 güne kadar Adlî para cezası düzenlenmiştir. Maddede işlenen suç şikâyete bağlı olmayıp, Cumhuriyet Başsavcılığı tarafından doğrudan soruşturma yapılır. Yargılama yapma yetkisi ise asliye ceza mahkemelerine aittir.[401]

[399] Bikirli, a.g.e., s. 15.
[400] Dülger ve Modoğlu, a.g.e., s. 50.
[401] Yılmaz, Sacit, a.g.e., s. 95.

3.2.2.4. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, TCK'nin ikinci kitabının, topluma karşı suçlara yer veren üçüncü kısmının, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde, Md. 245'te düzenlenmiştir. Bu hükme, 29.06.2005 tarih ve 5377 sayılı Kanunun Md. 27 ile iki fıkra ve 06.12.2006 tarih ve 5560 sayılı Kanunla 5. fıkranın eklenmesiyle, iki kez değişiklik yapılarak, maddeye bugünkü şekli verilmiştir. Temel olarak söz konusu hükümle, banka ve kredi kartlarını hukuka aykırı kullanma, sahte banka veya kredi kartı üretme, satma, devretme veya kabul etme, sahte banka veya kredi kartları oluşturma ve kullanma fiilleri, yaptırım altına alınmıştır.

Türkiye'de en sık karşılaşılan bilişim suçlarından biri olan banka veya kredi kartlarının kötüye kullanılması suçuyla ilgili TCK'nin 245. Maddesi şu şekildedir:[402]

"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) ***(Ek: 6/12/2006 – 5560/11 md.)*** *Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."*

TCK'nin 245. Maddesi başlığı altında 1. 2. ve 3. fıkralarda üç farklı suç tipi düzenleme konusu yapılmıştır.

1. Fıkrada; "gerçek bir banka veya kredi kartının kötüye kullanılmasıyla hukuka aykırı yarar sağlama",

[402] 5237 Sayılı Türk Ceza Kanunu, s. 9024-1.

2. Fıkrada "sahte banka veya kredi kartı üretme",

3. Fıkrada ise "sahte banka veya kredi kartı kullanma suretiyle hukuka aykırı yarar sağlama" suçları düzenlenmektedir. Bu maddeyle söz konusu kartların haksız, hukuka aykırı olarak kullanılması yoluyla bankaların ve kart sahiplerinin zarara uğraması ve bu surette hukuka aykırı yarar sağlanması önlenmek istenmiştir.[403]

TCK Md. 245/1'de 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 kullandırtarak kendisine veya başkasına yarar sağlaması cezalandırılmıştır. Başka bir deyişle başkasına ait kredi kartının ele geçiriliş şekline bakılmaksızın, kartın, sahibinin rızası hilafında kullanılması veya kullandırılması suç haline getirilmiştir. Madde metninde "her ne suretle olursa olsun" ibaresine yer verildiğinden, failin kartı ne şekilde ele geçirdiğinin ise bir önemi yoktur. Başka bir deyişle kartın hamilinin rızasıyla veya rıza dışı ya da çalınarak, hileyle, tehditle ele geçirilmesi bakımından bir fark bulunmamaktadır.[404]

Başkasına ait banka veya kredi kartıyla hukuka aykırı sağlama eyleminin meydana getiriliş sekli açısından yasada bir kısıtlama bulunmamaktadır, önemli olan bu eylemlerin sonucunda hukuka aykırı yararın elde edilmesidir. Gelişen teknolojiye bağlı olarak, bu suçun yeni işlenme şekilleri ortaya çıkabilecektir. Günümüz açısından işlenme şekillerine örnek verecek olursak; ATM'lerden para çekilmesi, alışveriş yapılabilmesi, internet üzerinden sipariş verilmesi örnek olarak gösterilebilir.[405]

245. maddenin 2. fıkrasında başkalarına ait banka veya kredi kartıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, satılması devredilmesi, satın alınması veya kabul edilmesi hareketleri ayrı bir suç olarak düzenlenmiştir. Banka veya kredi kartlarının tamamen sahte olarak üretilmesi mümkün olduğu gibi, bu kartların gerçek olmasına rağmen üzerinde çeşitli işlemler yapılarak sahteleştirilmesi de mümkündür. Bu durum yasa koyucu tarafından iyi bir şekilde tespit edilerek suç tipine yansıtılmıştır. Suç tipi seçimlik hareketli olarak düzenlenmiştir, bu

[403] Bikirli, a.g.e., s.17.
[404] Mahmutoğlu, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", ***Dergi Park, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,*** Cilt: 71, Sayı: 1, 2013, s. 872.
[405] Gözüşirin, a.g.e., s.73.

hareketlerden her hangi birinin yapılması ya da bazı hareketlerinin birlikte yapılması halinde 245/2. maddenin ihlali söz konusu olacaktır. Örneğin, failin önce sahte kartı üretmesi ve sonrasında satması halinde tek bir suç oluşacaktır. Ancak üreten ve akabinde satan ile satın alan ayrı kişiler olduğunda bunların herbiri açısından ayrı ayrı 245/2. maddenin ihlali söz konusu olacak, bunlar arasında suça iştirak hâli söz konusu olmayacaktır.[406]

245'inci maddenin 3'üncü fıkrasında sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartıyla hukuka aykırı yarar sağlama suçunun gerçekleştirilmesi durumu düzenlenmiştir. Sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartları ile otomatik para çekme makinelerinde, alışveriş amacıyla ticari işletmelerde veya veri iletim ağlarında kullanılması mümkün olabilecektir.

Failin gerçeğe aykırı beyan ve sahte belgelerle, kart çıkaran banka ya da kurumdan elde ettiği banka kartı veya kredi kartını kullanarak otomatik para çekme makinesinden para çekmesi, bankacılık işlemi yapması, bunu ticari işletmelerde ya da sanal alanda alışveriş amacıyla kullanması halinde oluşan suç tipi TCK'nin 158. maddesinde düzenlenen nitelikli dolandırıcılık suçudur. Çünkü yasa maddesinde "sahte oluşturulan veya üzerinde sahtecilik yapılan kartı kullanmak" ifadesi yer almaktadır. Hâlbuki sahte belgeler ve hukuka aykırı beyanlarla çıkartılan kart sahte oluşturulan veya üzerinde sahtecilik yapılan bir kart değildir.[407]

Banka ve Kredi Kartlarının Kötüye Kullanılması Suçu, bir suç işleme kararının icrası kapsamında, değişik zamanlarda, aynı kişiye karşı, birden fazla kez işlenirse, fail, zincirleme suç hükümlerine göre tek bir suçtan cezalandırılacaktır. Daha açık bir deyişle, fail tarafından başkasına ait kredi kartı, değişik zamanlarda birden fazla kez kullanıldığında, tek bir suçtan sorumluluk doğacak, ancak TCK Md. 43/1 gereğince failin cezasında artırım yoluna gidilecektir.[408]

Kanunun 245. Maddenin 1. ve 3.'ncü fıkralarında suçun tamamlanabilmesi amacıyla failin hareketleri gerçekleştirdikten sonra ayrıca bir "yarar" sağlaması gerekmektedir. Söz konusu "yarar" elde edilmediği müddetçe suç teşebbüs aşamasında kalacaktır. 245. Maddenin 2. fıkrası için yukarıda anlatılanlar geçerli

[406] Dülger ve Modoğlu, a.g.e., s. 52.
[407] Gözüşirin, a.g.e., s. 75-76.
[408] Mahmutoğlu, a.g.e., s. 876.

değildir. 245. maddenin 2‟inci fıkrasında belirtilen fiillerin gerçekleşmesi ile suç tamamlanmış olur ayrıca bir yararın elde edilmesine gerek yoktur. İnceleme konusu suç tipi, seçimlik hareketli bir suç olduğu için, yasada belirtilen seçimlik hareketlerden herhangi birinin icra edilmesi ve zararın meydana gelmesi durumunda diğer eylemler teşebbüs derecesinde kalmış olsalar da suç tamamlanmış sayılacak ve faile tamamlanmış suçun cezası verilecektir.[409]

245. Maddenin 3. fıkrasında yer verilen eylem açısından ise benzer hukuksal değeri koruyan suç tipleri arasında fikri içtima vb. suçların birleşmesi durumunun bulunması ise mümkün değildir. Çünkü maddenin metninde açık bir şekilde “fiil daha ağır cezayı gerektiren bir başka suç oluşturmadığı takdirde” ifadesine yer verilerek, söz konusu eylemlerin başka bir suç oluşturması halinde diğer suç tiplerinin gerçekleştirilen eylemin uygulanacağı, inceleme konusu suç tipinin uygulanmayacağı belirtilmektedir.

5237 sayılı TCK’nin 245. Maddesinin 4. fıkrasında, suçun failinin, zararına işlenen kişi ile akraba olması durumunda faile ceza verilmeyeceği düzenlenmiştir. Buna göre, 245. maddenin birinci fıkrasında yer alan “başkasına ait banka veya kredi kartıyla hukuka aykırı yarar sağlama suçunun, haklarında ayrılık kararı verilmemiş eşlerden birinin, üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, aynı konutta beraber yasayan kardeşlerden” birinin, zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmayacaktır.

TCK Md.245/5’e göre, 1. fıkra kapsamındaki fillerle ilgili, malvarlığına karşı suçlara ilişkin etkin pişmanlığın düzenlendiği TCK Md.168 uygulanacaktır. Uygulanacak bu maddeye göre; kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin, bizzat pişmanlık göstererek, mağdurun rızasıyla birlikte, mağdurun zararının tamamını tazmin etmesi durumunda cezası üçte ikisine kadar indirilmektedir. Kovuşturmanın başlaması durumunda ceza yarısı oranında indirilmektedir. Failin iradesi dışında zarar karşılanmışsa örneğin kolluk

[409] Gözüşirin, a.g.e., s. 77.

kuvvetlerince mağdurun zararı karşılanmışsa uygulamada fail artık etkin pişmanlık hükmünden yararlanamaz.[410]

Bu madde kapsamında failin etkin pişmanlıktan faydalanabilmesi için;[411]

-Suçun tamamlanmış olması,

-Failin azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi, kısmen giderme söz konusuysa mağdurun buna rıza göstermesi,

-Kovuşturmadan önce veya kovuşturma başlamışsa hüküm verilmeden önce aynen iade veya tazminin sağlanması gerekmektedir.

Yer bakımından yetkili mahkemeyi "suçun işlendiği yer" mahkemesi olarak belirleyen, CMK'nın 12. Maddesi gereğince, bu suçta neticenin meydana geldiği yer, yani suça konu kart ile haksız yarar sağlanan yer mahkemesidir. Haksız yarar sağlanan yer ise, banka veya kredi kartı ile paranın çekildiği, ATM makinesinin bulunduğu yer veya kredi kartı ile alışveriş yapıldığı işyerinin bulunduğu yer mahkemesidir. Ele geçirilen kredi kartı numarası kullanılmak suretiyle internet üzerinden alışveriş yapılması halinde ise alışveriş yapılan siteye bağlanılan yer mahkemesi yetkili mahkeme olarak belirlenecektir. TCK Madde 245. Madde de düzenlenen banka ve kredi kartının kötüye kullanılması suçunda görevli mahkeme; 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 10, 11 ve 12. Maddeleri gereğince, Asliye Ceza Mahkemesidir. Ancak işlenen suçun banka yetkili ya da görevlileri tarafından işlenmesi durumunda yetkili mahkeme, Ağır Ceza Mahkemesidir.[412]

3.2.2.5. Zararlı Yazılım ve Yasak Cihazlar

5237 sayılı Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlıklı onuncu bölümüne 24.03.2016 tarihinde yapılan değişiklik ile 245/A numaralı "Yasak Cihaz ve Programlar" başlıklı yeni bir madde eklenmiştir. Bu madde, yine aynı tarihte kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ile birlikte bu alanda

[410] Bilgen, Tülay, ***Türk Ceza Kanununda Banka veya Kredi Kartlarının Kötüye Kullanılması***, Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, 2010, s. 115.
[411] Mahmutoğlu, a.g.e., s. 879.
[412] Bilgen, a.g.e., s. 71.

ek koruma getirilmesini amaçlamaktadır. Genel olarak madde, izleme ve izinsiz şekilde veri edinme amacı taşıyan sistemlerin maddede sayılan eylemler dâhilinde kullanılması durumunda bir ceza öngörmektedir. Buna ilaveten asıl önemli düzenleme, herhangi bir bilişim güvenlik sisteminin aşılmasına ilişkin araçlar, yazılımlar geliştirme ve kullanma noktasında toplanmaktadır. İşte bu tam anlamıyla bir zararlı yazılım suçudur. Bugüne kadar hukukumuzda bu suç ayrıca ve açıkça düzenlenmemişti. Bu durum uygulamada bazı güçlükler ve karışıklıklar yaratmaktaydı. Bu açıdan bakıldığında Zararlı Yazılım ve Yasak Cihazlar suçu önemli bir uygulama alanı bulması beklenen önemli bir düzenlemedir ve ilgili madde metni aşağıdaki şekildedir;[413]

Madde 245/A- (Ek: 24/3/2016-6698/30 md.)

Zararlı Yazılım

(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.

Maddenin saydığı ilgili yazılımları sızma/zafiyet testi yapan herkes imal de ediyor, satın da alıyor. Test yapan şirketler bu araçları bilişim sistemi sahibi ile imzalanan sözleşme çerçevesinde kullandığı için hukuka aykırılık ortadan kalkıyor. Yine de şimdiye kadar sözleşme ilişkisine girmeden bu testleri yapanlar varsa ispat açısından bundan sonra sözleşme yapmaları yerinde olur. Maddede suçun işlenmesi için yapılması gereken hareketler oldukça geniş bir kapsamda ele alınmış ve yazılmış bulunmaktadır. Uygulamada en fazla gündeme gelecek olan kısmı zararlı yazılım veya cihaz bulundurma şeklinde beklenmektedir.

Yer sağlayıcı ve barındırma şirketleri bakımından bu tür yazılımların depolanması yeni bir şikâyet konusu olmaya adaydır. Yeni yasal düzenlemede hackleme yöntemleri ile ilgili herhangi bir ayrım yapılmadığı dikkat çekmektedir. Buna göre suç işlemek için oluşturulan bütün yazılımlar madde uygulamasına konu olabilecektir. Burada en çok uygulanacak olan durum: şifreli uydu kanalları için üretilen şifrelerinin kırılmasını sağlayan yazılım veya cihazlar olacaktır. Yine bilgisayar oyunlarında kullanılmak üzere üretilen hack / hile yazılımları da bu madde

[413] 5237 Sayılı Türk Ceza Kanunu, Md. 245/A, s. 9024-1.

kapsamında ele alınmaya uygun bulunmaktadır. Aslında bu madde uygulamada en çok yazılımları kısmen veya tamamen devre dışı bırakan ve uygulamalarını değiştiren third party software denilen hack / hile yazılımları için uygulanmaya adaydır.

Madde metni incelendiğinde, eylem dâhilinde kullanılabilecek olan araçların sayıldığı görülmektedir. Bunlar bir cihaz, bilgisayar programı, şifre veya sair güvenlik kodudur. Günlük hayatta bunlardan en çok karşımıza çıkan, "keylogger" adı verilen yazılımlardır. Keyloggerlar, kurulduğu bilgisayardaki klavye vuruşlarını kaydetmek ve harici bir ortama aktarmak suretiyle o bilgisayarda basılmış bütün klavye tuşlarının başkaları tarafından elde edilmesi imkânını sağlayan yazılımlardır. Buna göre, keyloggerlar vasıtasıyla kişilerin şifreleri, hatta ve hatta online alışveriş yaptıkları vakitlerde kredi kartı bilgilerine kadar bütün her şeyine erişilebilmektedir. Bunu önlemek maksadıyla senelerdir bankalar, internet sitelerindeki giriş kısımlarının bazılarını klavye eşliğinde değil de fare ile tıklayarak yazılabileceği arayüz yazılımları geliştirmektedir. An itibariyle, bilgisayara keylogger kurulması durumunda bu yazılımı kuran, oluşturan, bundan bilgi elde eden dâhil bu yazılım ile ilişki içerisinde olan her birey, bu madde nezdinde bir suç oluşturmaktadır. Ancak tabi ki bu şahısların cezalandırılabilmeleri için bu keylogger yazılımını maddede atıf yapılmış suçları işlemek adına oluşturmuş veya yapmış olmaları gerekmektedir.

TCK madde 245/A, şahısların bu suçu işlemiş olması için gerçekleştirmesi gerekli olan eylemler numerus clausus olarak sayılmıştır. Bunlar sırasıyla, imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişilerdir. Keylogger örneğinden devam edersek, öncelikle keylogger yazılımını oluşturan, daha sonra bunu başkalarına veren/satan, bu yazılımı alan, bu yazılımı bulunduranlar bu hüküm gereğince suç işlemektedirler.

Maddede belirtilen aracı kullanmak suretiyle suç işleyen kişiler hakkında herhangi bir yaptırım bu maddede öngörülmemiştir. Bunun sebebi, zaten bu araçları kullanmak suretiyle suç işleyen kişiler hakkında zaten onuncu bölüm hükümleri gereği farklı cezaların öngörülmüş olmasıdır.

Ceza Hukuku Genel Hükümlerindeki Kast/Taksir ayrımı önem arz etmektedir. Türk Ceza Kanunu'nun taksiri düzenleyen 22. Maddesinde, ancak kanunun açıkça

belirttiği hallerde taksirle bir suçun işlenebileceği düzenlenmiştir. Buna göre, 245/A'da bu suçun taksirle işlenebileceği hüküm altına alınmadığından, anılan suç yalnızca kast ile işlenebilecektir.

Yasadaki bu maddeye göre; belirtilen şahıslar tarafından ancak ve ancak kanunun onuncu bölümünde yer alan suçlar ile "bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi" kastı ile bu araçların imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması suç olarak nitelendirilmektedir. Örneğin bir ağ yöneticisinin vazgeçilmezi olan bir ağ izleme programının oluşturulması, ancak ve ancak suç işleme kastı ile yapıldığı takdirde suç olmaktadır. Bir ağ izleme programı, suç işlemek maksadıyla oluşturulmadıysa, ancak bunu bir şekilde elde eden kişi suç işlemek için satmaktaysa bu durumda salt bunu suç işleme maksadıyla satan kişi cezalandırılabilecektir, programı oluşturanın kastı olmadığı için o cezalandırılamayacaktır.

Ceza Hukuku Genel Hükümlerindeki iştirak durumu da önemlidir. İştirak, bir suçu farklı açılardan birlikte işleyen kişilerin bulunduğu vaziyettir. Bir suç birden fazla kişi tarafından elbirliği ile işlendiği zaman iştirak hükümleri uygulanır. Konumuz olan suçta ise, her bir eylem ayrı ayrı sayılmış ve bunlar "veya" ile birbirlerinden ayrılmış olduğu için, esasen bu suçları işleyen her bir kimse bunlardan ayrı ayrı sorumlu olacaktır.

Anılan hükümde, açık bir şekilde yukarıda belirtilen durumlara uyan şahıslar hakkında bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür. "Ve" ile bağlandıkları için bunlara birlikte hükmedilebilmektedir. Dikkat edilmesi gereken husus, cezanın iki seneyi aşması durumunda sanıklar hakkında tutuklama kararı verilebileceğidir. Nihayetinde izleme, gözlemleme ve kaydetme yazılımları/araçları, bilişim hayatının vazgeçilmezleri olduklarından ötürü bunların bir düzenleme altına alınması, Kişisel Verilerin Korunması Kanunu ile birlikte bir zorunluluk halini almış durumdadır.[414]

[414] Elit Hukuk, ***Yeni Bir Bilişim Suçu: Zararlı Yazılım ve Yasak Cihaz***, (Erişim) http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/, 20.01.2017

3.2.2.6. Kanuni Yazılımların İzinsiz Kullanımı

Bilgisayar programlarının hukuken korunması ihtiyacı ve korumanın önemi, bunların hayatın her alanında kullanımının yaygınlaşması ve daha önemlisi kolay ve ucuz çoğaltılabilme özelliğine dayanmaktadır. Bilgisayar programlarının bu özelliği ve günden güne hızla gelişen bilgisayar teknolojilerinin getirdiği imkânların yanı sıra bilgisayar programlarını üretenlerin harcadığı masraf ve emeğin hukuki güvence altında olmamasının sektörde meydana getirmesi muhtemel olumsuz etkiler de bilgisayar programlarının korunmasının gerekliliğini ve önemini açıkça ortaya koymaktadır. Bilgisayar programları, nitelikleri ve kapasitelerine göre farklılık arz etmekle birlikte, genellikle piyasaya sunuldukları son aşamaya gelinceye kadar yoğun emek ve uzun zamana ihtiyaç duymaktadır. Bununla birlikte, bu nitelikteki programların son kullanıcıları tarafından çoğaltılması ise birkaç CD'ye ve dakikalarla ölçülebilecek kadar az bir zamana mal olmaktadır. Bu bakımdan bilgisayar programının hukuka aykırı olarak çoğaltılması ve kullanılmasının önüne geçmek amacıyla hak sahiplerinin bu bilgisayar programlarının ancak lisanslı kullanıcılar tarafından kullanılmasına olanak veren ve kullanımını bu yönde kontrol altına alan ve kısıtlayan bazı mekanizmaları geliştirdikleri görülmektedir.[415]

Türk hukuk sisteminde bilgisayar yazılımlarının korunması Fikri Hukuk alanında eser kategorisinde mümkün olabilmektedir. 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'na (FSEK) göre korumadan yararlanılabilmesi için, iki unsurun varlığı aranmaktadır. Bunlar;

- FSEK'te belirtilen eser kategorilerinin içerisinde yer almak,
- Sahibinin özelliğini taşımaktır.

Bilgisayar yazılımları ve sonucunda yazılımın ortaya çıkması şartı ile hazırlık tasarımları 5846 Sayılı Fikir ve Sanat Eserleri Kanunu'na göre ''ilim ve edebiyat eserleri'' kategorisinde korunmaktadır.

Hak sahibi olduğunu belgeleyebilen yazılım sahibi gerçek kişi yahut tüzel kişi çoğaltma, dağıtma, ticaretini yapma gibi hususların engellenmesini talep edebileceği gibi Fikir ve Sanat Eserleri Kanunu'nun 38. maddesinde yer alan düzenlemeye

[415] Başlar, Yusuf, "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri Suçu", **Dergi Park, Uyuşmazlık Mahkemesi Dergisi**, Cilt 1, Sayı 1, 2015, s. 245.

istisna olarak şahsi kullanımın ve şahsi kullanım amacıyla çoğaltılmasının engellenmesini de talep edebilmektedir.[416]

Kanun koyucu FSEK Madde 72'de düzenlemiş olduğu suç ile dolaylı da olsa fikir ve sanat eseri olarak kabul edilen bilgisayar programlarını ve bu programlar üzerinde hak sahibinin çoğaltma ve kamuya sunma haklarını korumak istemiştir. Buna göre "korsanla mücadele" kavramı altında yapılan düzenleme sonucunda madde metnindeki eylemleri yaptırım altına alarak "korsan" diye adlandırılan hukuka aykırı eylem ve sanat eserlerinin çoğaltılması ve bu suretle eser veya bundan kaynaklanan hak sahibinin Kanunda öngörülen manevi ve daha ziyade mali haklarının korunması amaçlanmaktadır.[417]

Fikir ve Sanat Eserleri Kanunu'na göre bilgisayar yazılımının haksız olarak kullanılması, çoğaltılması, satışı vb. hakkın özüne zarar verici uygulamalarda telif hakkı sahibince cezai soruşturma talep edilebileceği gibi tazminat davası da açılabilecektir. Diğer bir ifadeyle bilgisayar yazılımının lisans bedeli ödemeksizin bilabedel kullanımı hususunda haksız kullanıcının ceza davası ve tazminat davası ile karşılaşma ihtimali söz konusudur. Fikir ve Sanat Eserleri Kanunu'na göre bilgisayar yazılımının hak sahibi olan gerçek kişi yahut tüzel kişi, haksız yararlanandan lisans bedelinin 3 katına kadar tazminat ödenmesini talep edebilmektedir. Spesifik bir zümreye hitap eden mesleki bilgisayar yazılım bedellerinin günümüzde ciddi rakamlar olduğu kabul edildiğinde tazminat davalarında ciddi tutarlar ortaya çıkabilmektedir. Söz konusu mesleki yeterlilik gerektiren programların hedef kitlesi genelde ticari faaliyet gösteren kurum ve kuruluşlar olduğundan lisans bedelinin 3 katına kadar tazminat ödenmesi yerine uygulamada uzlaşma iradelerinin ön plana çıktığı görülmektedir.[418]

Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçunu oluşturan çeşitli fiillerin tümü FSEK Madde 72'de düzenlendiğinden bu fiillerin tamamı koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçunun seçimlik hareketini oluşturmaktadır. Bu hareketlerden hangisi gerçekleşirse gerçekleşsin, birden fazla hareketin bir arada gerçekleştiği durumlarda dahi, seçimlik

[416]Yılmaz, Tuğsan, ***Bilgisayar Yazılımlarının İzinsiz ve Yetkisiz Olarak Kullanımı***, (Erişim) http://www.tugsanyilmaz.av.tr/fikri-haklar-ve-bilisim-hukuku/bilgisayar-yazilimlarinin-izinsiz-ve-yetkisiz-olarak-kullanimi, 22.01.2017.
[417] Başlar, **a.g.e.**, s. 246.
[418] Yılmaz, Tuğsan, **a.g.e.**

hareketli suçun niteliği gereği ortada daima tek bir suçun varlığı kabul edilmektedir. Bununla birlikte FSEK Madde 72 uyarınca bir bilgisayar programının hukuka aykırı olarak çoğaltılmasını engellemek amacıyla üretilen bir bilgisayar programını bertaraf etmek için;

- Bir bilgisayar programı üretilse ve
- Bu program kullanılmak suretiyle bir bilişim sistemine izinsiz olarak girilse
- Yahut bilişim sistemindeki veriler bu program sayesinde değiştirilse ya da yok edilse,
- Bu takdirde FSEK Madde 72'deki suç dışında 5237 sayılı TCK'nin 243 ve 244'üncü maddelerinde yer alan "bilişim sistemine girme suçu" ve/veya "sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu"da ayrıca söz konusu olabilecektir.[419]

5237 sayılı TCK'da etkin pişmanlık kurumu, suç sonrası pişmanlık olarak düzenlenmiştir. Etkin pişmanlık fiilin haksızlık vasfını ortadan kaldırmayıp, haksızlığın meydana getirdiği neticeleri azaltması dolayısıyla failin cezasında indirime gidilmesini veya hiç ceza verilmemesini sağlayan bir şahsi sebeptir. Etkin pişmanlık suçun işlenmesi anında mevcut olmayıp suçun işlenmesinden sonra ortaya çıkar. FSEK Madde 71'in sonunda bir etkin pişmanlık düzenlemesine yer verilmiştir.[420] Bu hükme göre;[421]

"Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir"

Buradaki etkin pişmanlık hükmü 71. Maddede yer verilen tüm suçlar için geçerli olmayıp; sadece hukuka aykırı olarak başkası tarafından üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayınlanmış bir eseri, icrayı, fonogramı veya yapımı satın alan, satışa arz eden veya satan kişileri kapsamaktadır.[422]

Yetkili mahkeme konusunda FSEK'te bir düzenlemeye gidilmemiştir. Bu nedenle bu suçta yetkili mahkeme genel hüküm niteliğinde olan CMK Madde 12 ve devamı maddelerine göre belirlenecektir. CMK Madde 12 uyarınca davaya bakma

[419] Başlar, **a.g.e.**, s. 252.
[420] Bayındır, Sinan, "Eser Sahibinin İzni Olmaksızın Eseri Umuma İletim Suçu", ***Türkiye Barolar Birliği Dergisi***, Sayı: 113, 2014, s. 330.
[421] 5846 Sayılı FSEK, Madde 71 son paragraf, s.2413.
[422] Bayındır, **a.g.e.**, s. 330.

yetkisi suçun işlendiği yer mahkemesine aittir. Kanunun 76. maddesinde görevli mahkemeye ilişkin düzenlemeye yer verilmiştir. FSEK Madde 76/1'de;

"Bu Kanunun düzenlediği hukukî ilişkilerden doğan davalarda, dava konusunun miktarına ve Kanunda gösterilen cezaya bakılmaksızın, görevli mahkeme Adalet Bakanlığı tarafından kurulacak ihtisas mahkemeleridir. İhtisas mahkemeleri kurulup yargılama faaliyetlerine başlayıncaya kadar, asliye hukuk ve asliye ceza mahkemelerinden hangilerinin ihtisas mahkemesi olarak görevlendireceği ve bu mahkemelerin yargı çevreleri Adalet Bakanlığının teklifi üzerine Hâkimler ve Savcılar Kurulunca belirlenir" denilmiştir.

5846 sayılı FSEK Madde 76 uyarınca hak sahibinin manevi haklarına tecavüz hallerinde davaya bakmakla görevli mahkeme Adalet Bakanlığınca kurulacak ihtisas mahkemeleridir. Bununla birlikte ihtisas mahkemelerinin kurulmadığı yerlerde Adalet Bakanlığının teklifi üzerine Hâkimler ve Savcılar Yüksek Kurulunca yetkilendirilecek Asliye Ceza Mahkemeleri davaya bakmakla görevlidir.[423]

3.2.2.7. Yasadışı Yayınlar

TCK'ya göre incelenebilecek suçlar, kamu barışına karşı suçlar olarak adlandırılan ve 213, 214, 215, 216, 217 ile 218'de düzenlenen suçlardır. Bu suçların bilişim sistemi aracılığıyla gerçekleştirilme olasılığı yaşanmışlıklarla sabittir.

Türkiye'de terör örgütlerinin bilgisayar ve internet teknolojisini yakından takip ettikleri, haberleşme, propaganda yapma, eğitim amaçlı CD'ler ve bildiriler hazırlama şeklinde faaliyetler içinde oldukları bilinmektedir. Bunların yanı sıra bilişim teknolojisinden yararlanarak bilgi işlem ve veri merkezlerine, bakanlıklara, PTT-Telekom, Emniyet Genel Müdürlüğü ve Türk Silahlı Kuvvetleri gibi birimlerin sistemlerine sanal saldırılarda bulunabilecekleri ve bu sistemleri çökertmek için çaba harcadıkları istihbari bilgiler arasındadır.

Emniyet kaynaklarına göre Türkiye aleyhine faaliyet gösteren zararlı internet sitesi sayısı yaklaşık 8000 civarındadır. Bu sitelerden 150 tanesi aktif olarak faaliyette olup, bu siteleri her gün ortalama 500-1000 kişi ziyaret etmektedir. Genellikle com, org ve net uzantı isimli olan bu siteler Amerika, Almanya, Hollanda ve diğer Batı Avrupa ülkeleri üzerinden yayın yapmaktadır. 2000 yılında Elazığ Emniyet Müdürlüğü'nün internet sitesinin e-posta servisine, öğretmenevine bomba koyacağına yönelik e-posta gönderen bir kişi Terörle Mücadele Şube Müdürlüğü

[423] Aynı, s. 330.

tarafından yakalanarak adli birimlere sevk edilmiştir. 1999 yılında İstanbul Emniyet Müdürlüğü tarafından İBDA-C terör örgütüne yönelik olarak düzenlenen operasyonda 33 örgüt üyesi, hedef kişilere ait fotoğraflar ile yakalanarak gözaltına alınmıştır. Yapılan sorgulamada örgütün internet sitesinde "İBDA-C Hedef Listesi" başlığı altında ele geçirilen fotoğrafları yayınladıkları tespit edilmiştir. 1998 yılında DHKP-C'ye yönelik olarak Denizli'de gerçekleştirilen operasyonlarda yakalanan teröristlerin ifadelerinde, komşu bir ülkede bulunan örgüt evinde eğitildikleri, kampta askeri ve siyasi eğitimin yanında uydu telefonu ile internet üzerinden haberleşme ve şifreli konuşmalar yapma konusunda da eğitildikleri anlaşılmıştır. Emniyet Teşkilatı bünyesinde sadece siber suçlarla mücadele için oluşturulan "siber polis" (cybercop) ekipleri tarafından, 2001 yılında tespit edilen siber suç sayısı 11 iken, bu sayının 2002'de 47'ye, 2003'de 98'e ve 2004 yılının 11 aylık diliminde de 224'e kadar yükseldiği görülmektedir. Ayrıca Ocak Haziran 2006 dönemini kapsayan 6 aylık sürede 86 siber suç tespit edildiği ve bu suçlara ilişkin olarak 148 kişinin de yakalandığı bilinmektedir.[424]

TCK'nin 213. Maddesi, halk arasında korku ve panik yaratmak amacıyla tehdit başlığında iki bent halinde düzenlenmiştir.

Halk arasında korku ve panik yaratmak amacıyla tehdit

Madde 213- *(1) Halk arasında endişe, korku ve panik yaratmak amacıyla hayat, sağlık, vücut veya cinsel dokunulmazlık ya da malvarlığı bakımından alenen tehditte bulunan kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.*

(2) Suçun silahla işlenmesi halinde, verilecek ceza, kullanılan silahın niteliğine göre yarı oranına kadar artırılabilir.

Bilişim sistemi aracılığıyla ve internet yoluyla yapılan terör amaçlı yasadışı yayınları bu bağlamda değerlendirmek mümkündür. TCK'da suç işlemeye tahrik, suçu ve suçluyu övme, haklı kin ve düşmanlığa tahrik veya aşağılama, kanunlara uymamaya tahrik başlıklarında düzenlenen sırasıyla 214, 215, 216, 217. Maddelerle bu tür suçların önüne geçilmeye çalışılmaktadır.

Suç işlemeye tahrik

Madde 214- *(1) Suç işlemek için alenen tahrikte bulunan kişi, altı aydan beş yıla kadar hapis cezası ile cezalandırılır.*

(2) Halkın bir kısmını diğer bir kısmına karşı silahlandırarak, birbirini öldürmeye tahrik eden kişi, on beş yıldan yirmi dört yıla kadar hapis cezası ile cezalandırılır.

[424] Özkan, **a.g.e.**, s. 87.

(3) Tahrik konusu suçların işlenmesi halinde, tahrik eden kişi, bu suçlara azmettiren sıfatıyla cezalandırılır.

Suç işlemeye tahrik başlıklı 214 üncü maddede iki ayrı suç düzenlenmektedir: Suç işlemeye tahrik (Md.214/1) ve halkı birbirini öldürmeye tahrik (Md. 214/2). 214 üncü maddede yer alan her iki suç tipi de, tehlike suçu olup, tamamlanmaları için tahrik konusu suçların işlenmiş olması gerekmez. Bu suçlar, kamu barışı açısından büyük bir tehlike ifade ettiği için, iştirak ilişkisinden bağımsız, müstakil suç olarak düzenlenmiştir. Burada önemli olan, belirli olmayan kimselerin suç işlemeye tahrik edilmesidir. Eğer muayyen kişiler, belli bir suçu işlemek için teşvik veya azmettirilmiş ise, meselenin iştirak kuralları çerçevesinde değerlendirilmesi gerekir. Suç işlemeye tahrik fiilinin maddi unsurunu, suç işlemek için alenen tahrikte bulunmak oluşturmaktadır.

İkinci fıkrada düzenlenen suçun maddi unsuru, halk kesimlerinin silahlı şekilde birbirlerine karşı öldürmeye tahrik edilmesidir. Suç halkın bir kısmını diğer bir kısmına karşı silahlandırarak, birbirini öldürmeye tahrik etmekle tamamlanır. Suçun tamamlanabilmesi için öldürmenin ya da fiili saldırının başlaması gerekmez. Belirli kişilerin öldürülmesinin istenmesi, tahrikin bu doğrultuda yapılmış olması hâlinde; fıkra hükmü uygulanmaz. Bu hâlde de konunun iştirak kuralları çerçevesinde çözülmesi gerekir.[425]

Suçu ve suçluyu övme başlığı altında düzenlenen Madde 215 şu şekilde ifade edilmektedir. "*İşlenmiş olan bir suçu veya işlemiş olduğu suçtan dolayı bir kişiyi alenen öven kimse, bu nedenle kamu düzeni açısından açık ve yakın bir tehlikenin ortaya çıkması hâlinde, iki yıla kadar hapis cezası ile cezalandırılır."*[426]

Suçun oluşması için, kişinin işlenmiş olan bir suçu veya işlemiş olduğu bir suçtan dolayı bir kişiyi alenen övmesi gerekmektedir. Yapılan bu düzenleme ile işlenmiş olan bir suçun failini, sırf suç işlemesi sebebiyle övme hâli de cezalandırılmıştır. Bu ihtimalde aslında, kişi aracılığıyla işlenmiş olan suç övülmektedir.[427]

216. Madde Halkı kin ve düşmanlığa tahrik veya aşağılama başlığı altında üç bent halinde düzenlenmiştir.

---

[425] Gökçen, Ahmet, Kamu Barışına Karşı Suçlar, ***Yeni Türk Ceza Adaleti Tanıtım Sitesi***, (Erişim), www.ceza-bb.adalet.gov.tr/makale/118.doc, 22.01.2017.
[426] 5237 Sayılı Türk Ceza Kanunu, Suçu ve Suçluyu Övme, Madde 215, s. 9016.
[427] Gökçen, **a.g.e.**, s. 6.

Madde 216- *(1) Halkın sosyal sınıf, ırk, din, mezhep veya bölge bakımından farklı özelliklere sahip bir kesimini, diğer bir kesimi aleyhine kin ve düşmanlığa alenen tahrik eden kimse, bu nedenle kamu güvenliği açısından açık ve yakın bir tehlikenin ortaya çıkması halinde, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.*

(2) Halkın bir kesimini, sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge farklılığına dayanarak alenen aşağılayan kişi, altı aydan bir yıla kadar hapis cezası

(3) Halkın bir kesiminin benimsediği dini değerleri alenen aşağılayan kişi, fiilin kamu barışını bozmaya elverişli olması halinde, altı aydan bir yıla kadar hapis cezası ile cezalandırılır.

Maddenin 1. fıkrasındaki suç, halkın sosyal sınıf, ırk, din, mezhep veya bölge bakımından farklı özelliklere sahip bir kesimini, diğer bir kesimi aleyhine kin ve düşmanlığa alenen tahrik etmek suretiyle işlenir. Suçun oluşması bakımından bu tahrikin "kamu güvenliği açısından açık ve yakın bir tehlike ortaya çıkarması" gerekmektedir.

Suçu oluşturan "tahrik", soyut saygısızlık ve reddin ötesinde, bir halk kesimine karşı düşmanca tavırlar gösterilmesini sağlamaya veya bu tür tavırları pekiştirmeye objektif olarak elverişli olmalıdır. Fail subjektif olarak da bu amacı gütmeli, halk kesimini kin ve nefrete tahrik etmelidir. Bu kapsamda salt yüz çevirme, soyut bir ret veya saygısızlık ifade eden bir davranışta bulunma veya bu yönde sözler sarf etme, suçun gerçekleşmesi bakımından yeterli değildir. Fiilin suç teşkil etmesi için bunların ötesinde, ağır ve yoğun bir tarzda kin ve düşmanlığa tahrikin bulunması gerekir. Failin fiili, adet ve şahıs olarak muayyen olmayan toplum kesimi üzerinde kin ve nefret duygularının oluşumuna veya mevcut duyguların pekişmesine etkide bulunacak nitelikte olmalıdır.

Kin, "öç almayı gerektirecek şiddetli düşmanlık hareketlerin zeminini oluşturan psikolojik bir hâl"; düşmanlık ise, "husumet beslenen konuya karşı düşünerek, tasarlayarak zarar vermeye, onu mağlup etmeye yönelmiş kin duygusu" olarak tanımlanabilir. Şu hâlde kin ve düşmanlık; "husumet beslenen konuya karşı tasarlayarak zarar vermeye, öç almayı gerektirecek şiddette nefret duymaya yönelik hareketlerin zemini oluşturan psikolojik bir hâl" olarak açıklanabilir.

Fiil dolayısıyla kamu güvenliği açısından açık ve yakın bir tehlikenin ortaya çıkması arandığı için, suç; soyut değil, somut tehlike suçu niteliğindedir. Bu düzenleme sayesinde "kin ve düşmanlık" ibaresinin anlamı da dikkate alındığında sadece "şiddet içeren ya da şiddeti tavsiye eden tahrikler" madde kapsamında

değerlendirilebilecektir.

TCK'nin 216/2. maddesinde halkın sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge bakımından farklı bir kesiminin alenen aşağılanması suç sayılmıştır. Suçla korunan hukuki yarar kamu barışıdır. Bu suç, halkın bir kesiminin, sosyal sınıf, ırk, din, mezhep, cinsiyet veya bölge farklılığına dayanarak alenen aşağılanması suretiyle işlenebilir. Suçun oluşması için fıkrada belirtilen özelliklere sahip ve halkın bir kesimini oluşturan gayrimuayyen sayıdaki kişilerin aşağılanması, tahkir edilmesi gerekir.

Maddenin 3. fıkrasında bir halk kesiminin benimsediği dinî değerlerin alenen aşağılanması, suç hâline getirilmiştir. Fiilin cezalandırılabilmesi için, "kamu barışını bozmaya elverişli" olması gerekir.[428]

TCK'nin 217. Maddesinde düzenlenen kanunlara uymamaya tahrik suçuyla ilgili kanun metni; "*Halkı kanunlara uymamaya alenen tahrik eden kişi, tahrikin kamu barışını bozmaya elverişli olması halinde, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır."* Şeklinde söz konusu suçu işleyen kişi veya kişilere verilecek ceza açık bir şekilde ifade edilmektedir.

218. Madde ortak hüküm başlığıyla düzenlenmiş ve 29.06.2005 tarihinde 5377 sayılı Kanun'un 25. Maddesiyle değişikliğe gidilmiştir. 218. Madde, 213. Maddeden 217. Madde dahil bütün maddeleri kapsamakta; "*Yukarıdaki maddelerde tanımlanan suçların basın ve yayın yoluyla işlenmesi hâlinde, verilecek ceza yarı oranına kadar artırılır. Ancak, haber verme sınırlarını aşmayan ve eleştiri amacıyla yapılan düşünce açıklamaları suç oluşturmaz."* Denilerek söz konusu maddelerin kapsadığı eylemler hakkında sınırların olduğunu göstermektedir.[429]

3.2.2.8. Çocuk Pornografisi

TCK'nin 226. Maddesinin 3. Fıkrasında yer alan çocuk pornografisiyle ilgili düzenleme şu şekildedir:[430]

"...(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, 5 yıldan 10 yıla kadar hapis ve 5000 güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan

[428] Gökçen, **a.g.e.**, s. 8-9.
[429] Dülger, 2015, **a.g.e.**, s. 109.
[430] 5237 Sayılı Türk Ceza Kanunu, Müstehcenlik, Madde 226/3, s.9019.

kişi, 2 yıldan 5 yıla kadar hapis ve 5000 güne kadar adlî para cezası ile cezalandırılır."

Kanun'un 3.fıkrasında, müstehcenliğe karşı çocukları korumaya yönelik iki ayrı suç tanımına yer verildiği görülmektedir. Bunlardan birincisi; müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların kullanılması suretiyle oluşmaktadır. İkinci suç ise, bu ürünlerin ülkeye sokulması, çoğaltılması, satışa arzı, satışı, nakli, depolanması, ihracı, bulundurulması ya da başkalarının kullanımına sunulması fiillerinden birinin işlenmesiyle oluşmaktadır. Yani, maddenin 3. fıkrası ile çocuk pornosu suç haline getirilerek, çocukların müstehcen ürünlerin üretiminde kullanılması ve çocukların kullanıldığı müstehcen ürünlerin ülkeye sokulması, çoğaltılması, satışa arz edilmesi, satılması, nakledilmesi, depolanması, ihraç edilmesi, bulundurulması ya da başkalarının kullanımına sunulması bu suç kapsamına alınmıştır. TCK'nin 226/3. maddesiyle, çocuk pornosu tabiri kullanılmadan müstehcen içerikteki ürünlerin üretiminde, meydana getirilmesinde çocukların kullanılması suç olarak düzenlenmiştir. Burada geçen müstehcen ürün tabiri ile anlatılmak istenen çocuk pornografisidir.

Çocuk pornosunda dikkate edilmesi gereken husus, suça konu olan nesnenin, görüntü, yazı veya söz içermesidir. Yani bu tür özelliğine sahip olmayan örneğin, tahrik edici bir koku bu suçun konusu olmayacaktır.

Çocuk pornosunu içeren görüntü, ses veya sözlerin genellikle bilişim sistemleri vasıtasıyla işlendiği görülmektedir. Örneğin, yurt dışı kaynaklı bir internet sitesi üzerinden bu tür görüntünün mail yoluyla bilgisayarınıza gönderilmesi, sosyal paylaşım sitelerinden olan facebook.com adresi üzerinden bu tür bir görüntü veya ses kaydının paylaşılması, sanal ortamdan bu tür görüntülerin satılması, sanal ortamda görüntülerin oynatılması, sanal ortamda bu tür filmlerin arşivlenerek depo edilmesine uygulamada sıkça rastlanılmaktadır.

Bu suçla (çocuk pornosu) korunan hukukî yarar, çocukların bedensel, zihinsel, ahlaki, ruhsal ve duygusal tamlığının korunması olduğu kadar, çocukların psikolojik yapılarının zarar görmesinin önlenmesidir. Cinsel istismarın bir türü olan çocuk pornografisinin cezalandırma konusu olması, çocuğun ruhsal ve fiziksel gelişimini henüz tamamlamamış olması ve onun kendi cinsel davranışı üzerinde özerk bir karar verme yeteneğinin henüz gelişmemiş olmasından kaynaklanmasındandır. 3. fıkrada düzenlenen suçun mağduru 18 yaşını tamamlamamış kimseler olan çocuklardır. 18

yaşını doldurmamış, ancak resmi olarak evlenmiş kimseler, suçun mağduru olamayacaktır. Müstehcen ürünün konusunun gerçek bir çocuk olması şart değildir, burada önemli olan ürünün algısal içeriğidir.

Pornografik görüntü konusunda birçok tanım yapılsa da, çocuk haklarını korumaya yönelik Birleşmiş Milletler tarafından oluşturulan Çocuk Hakları Sözleşmesi'ne üye devletlerarasında 25.05.2000'de imzalan 4755 sayılı Yasa ile uygun bulunarak kabul edilen Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi ile İlgili İhtiyari Protokolün 2. maddesinin c bendinde çocuk pornosu tanımlanmıştır.

Buna göre çocuk pornografisi, *"Çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesidir."* şeklinde tanımlanmıştır.

Bir eserin pornografik sayılabilmesi için, bir bütün olarak objektif açıdan önemli ölçüde cinsel dürtüleri tahriki amaçlaması, insani ilişkilere yer vermemesi, insanı cinsel bir obje haline indirgemiş olması, daha açık bir deyişle cinselliği mutlak hale getirmiş olması, cinsel davranışları estetikten uzak, tahrike yönelik bir şekilde ve sadece ayrıntılı bir biçimde cinsel organları göstermesi gerekir. Bu özellikleri kendinde toplayan eser pornografik bir eserdir.

TCK'nin 226/3. maddesinde düzenlenen suç seçimli hareketli bir suçtur. Bu nedenle eylemin anılan suçu oluşturması için maddede sayılan hareketlerden birisinin yapılması gerekir. Bu eylemlerden hepsinin yapılması ile değil, yalnız birisinin yapılması ile anılan suç oluşacaktır.

Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların kullanıldığı sırada, çocuklara karşı cinsel istismar suçu da işlenmekte ise, TCK'nin 44. maddesinden düzenlenen fikri içtima hükümlerinin uygulanması gerekecektir. Bu durumda TCK'nin 103/2. maddesi hükmünde öngörülen ceza daha ağır ceza hükümleri içerdiğinden TCK'nin 226/3. maddesi değil, TCK'nin 103/2. maddesi gereğince ceza verilecektir.[431]

[431] Dülger ve Modoğlu, **a.g.e.**, s. 73-75.

3.2.2.9. İntihara Yönlendirme

İntihara yönlendirme suçu 5237 sayılı TCK md. 84 düzenlenmektedir. Madde ilk önce "İntihar" olarak düzenlenmiş ancak yapılan eleştirilerden sonra 29.06.2005 tarih ve 5377 sayılı Kanunun 10. maddesi ile "İntihara Yönlendirme" olarak değiştirilmiştir.[432]

Maddenin birinci fıkrasında bir başkasını intihara azmettirme, teşvik etme, başkasının intihar kararını kuvvetlendirme ya da başkasının intiharına herhangi bir şekilde yardım etme fiilleri, seçimlik hareketli bir suç olarak tanımlanmaktadır.

Canlı türü olarak insan, hayatını sürdürme konusunda bir içgüdüye sahiptir. Ancak, algılama yeteneğinin olmaması nedeniyle veya yakalandığı hastalıktan kaynaklanan acı ve ızdırabın etkisiyle kişide hayatını sona erdirmeye yönelik bir eğilim ortaya çıkabilir ve bunu bir irade açıklamasıyla ortaya koyabilir. Belirtmek gerekir ki, kişinin bu şartlar altında hayatını sona erdirme yönündeki iradesinin hukukî geçerliliği söz konusu değildir. Başka bir deyişle, belirtilen durumlarda hukuken muteber bir iradeden söz etmek mümkün değildir.

Ahlaken tasvip edilmeyen bir tasarruf olan intihar veya intihara teşebbüs olgusu, bizatihi cezalandırılabilir bir davranış niteliği taşımamaktadır. Buna karşılık, bir başkasını intihara azmettiren, teşvik eden, başkasının intihar kararını kuvvetlendiren ya da başkasının intiharına herhangi bir şekilde yardım eden kişinin bu fiilleri cezalandırılabilir niteliktedir.

Başlı başına cezalandırılabilir bir fiil olarak intihara yardım, esas itibarıyla icraî davranışla gerçekleştirilebilir. Ancak, intiharı önleme konusunda hukukî yükümlülük altında bulunan kişinin, bir intihar olgusuyla karşı karşıya olmasına rağmen, bu intihar girişimini engellememesi, bu girişim karşısında kayıtsız davranması; intihara ihmali davranışla yardım olarak nitelendirilmek gerekir. Ancak, bunun için, kişinin intiharı önleme konusunda hukukî bir yükümlülüğünün olması gerekir.

Maddenin ikinci fıkrasında, intihara teşvik veya yardım suçunun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. İntihara teşvik veya yardımın cezalandırılabilmesi için, kişinin intihar etmesi şart değildir. Teşvik veya yardım

[432] 5237 Sayılı Türk Ceza Kanunu, İntihara Yönlendirme, Madde 84, s.8988.

sonucunda intiharın gerçekleşmesi durumunda, söz konusu fıkraya göre cezanın artırılması gerekmektedir.

Üçüncü fıkrada, başkalarını intihara alenen teşvik edilmesi, ayrı bir suç olarak tanımlanmıştır. Bu suçun oluşabilmesi için, belli bir kişinin muhatap alınması gerekmemektedir. Aleniyet için aranan temel ölçüt, fiilin, gerçekleştiği koşullar itibarıyla belirli olmayan ve birden fazla kişiler tarafından algılanabilir olmasıdır. Keza, aleniyetin basın, yayın veya internet yoluyla gerçekleşmesi durumunda artırma oranı ayrıca düzenlenmektedir.

Maddenin son fıkrasında, işlediği fiilin anlam ve sonuçlarını algılama yeteneği gelişmemiş olan veya ortadan kaldırılan kişileri intihara sevk edenlerle, cebir veya tehdit kullanmak suretiyle kişileri intihara mecbur edenler, kasten öldürme suçundan sorumlu tutulacağı kabul edilmiştir. Aslında, bu durumda kasten öldürme suçu, mağdurun kendisinin araç olarak kullanılması suretiyle, yani dolaylı faillik şeklinde işlenmektedir.[433]

İntihara yönlendirme suçu internet açısından değerlendirilecek olursa; öncelikle suçun fail ve mağduru bakımından 5237 s. TCK Md. 84'de yapılan düzenleme dikkate alınmalıdır. Genel anlamda gerek fail gerekse mağdur için özel bir durum yaratılmadığı görülmektedir. Bu bakımdan intihara yönlendirme suçunda herkesin fail veya mağdur olması mümkündür. Tek özellikli durum olarak maddenin son fıkrasında kasten adam öldürme suçuna yapılan gönderme gösterilebilir. Buna göre intihara yönlendirme suçu, işlediği fiilin anlam ve sonuçlarını algılama yeteneği gelişmemiş olan ya da ortadan kaldırılmış bir kişiye karşı işlenecek olursa veya mağdur cebir ya da tehditle intihara mecbur bırakılırsa fail intihara yönlendirmeden değil kasten adam öldürmeden dolayı sorumlu tutulacaktır (Md. 84/4). Dolayısıyla failin intihara yönlendirme suçunun değil kasten adam öldürme suçunun faili olarak kabul edilmesi söz konusu olacaktır. Haliyle mağdur da kasten adam öldürme suçunun mağduru olarak kabul görecektir. Bu durum suçun internette işlenebilirliği bakımından oldukça önemlidir. Keza bugün internet her yaş ve seviye grubundan kişi tarafından kullanılmaktadır. Özellikle yaş grubu itibariyle algılama ve muhakeme yeteneği gelişmeyen çocuklara karşı intiharı özendirecek nitelikte iletiler

[433]5237 Sayılı Ceza Kanunu Madde 84, ***İntihara Yönlendirme***, (Erişim) http://www.turkhukuksitesi.com/mevzuat.php?mid=5174 , 12 Aralık 2016.

gönderilmesi, sohbetlerde bulunulması ya da yayınların yapılması neticesinde söz konusu fıkranın uygulanabilirliği gündeme gelecektir.[434]

Suçun internet aracılığıyla işlenebilirliği bakımından kusurluluğu etkileyen herhangi bir durumun söz konusu olup olmadığı ele alınacak olursa; failin 5237 sayılı TCK Md. 28 ve 29 hükmünce cebir, şiddet, korkutma ve tehdit altında veya haksız tahrik etkisiyle bu suçu işlemesi durumu pek mümkün görünmemektedir, ancak özellikle internet teknolojisinin kullanımında sıklıkla hatalara düşülmesi dolayısıyla failin eyleminde TCK Md. 30 anlamında bir hatadan bahsedilip bahsedilemeyeceği üzerinde durulabilir. Özellikle internet üzerinden kurulan iletişimde kullanıcı isimleri, milyonlarca kullanıcı ile karışmaması için "nick name" denilen takma isimler, normal isimlerden farklı şekillerde veya sembollerle desteklenerek oluşturulmaktadır. Ayrıca internette iletişim olanağı sunan birçok varlığı da kişileri hata yapmaya sevk etmektedir. Dolayısıyla internet ortamında girişilen hareketlerde hata yapma olasılığı artmaktadır. Bu anlamda internette en çok karşılaşılan hata türü olan şahısta hataya örnek olarak bir kişiye e- posta aracılığıyla hakaret etmek isteyen bir başka kişinin, hedef kişinin e-posta adresinde bir harf veya sembolü yanlış bilmesi veya girmesi neticesinde başka bir kişiye hakaret içerikli e-postayı göndermesi gösterilebilir. Ancak kanaatimizce uygulamada gözden kaçırılması muhtemel bir hata türünün bu suç açısından gerçekleşmesi mümkündür. Daha önce üzerinde durulduğu gibi internette aleniyet sadece herkes için doğrudan erişilebilirliğinin söz konusu olduğu durumlarda değil, aynı zamanda belli koşullar altında dolaylı veya aşamalı erişilebilirliğin söz konusu olduğu durumlarda da geçerlidir. Örnek verilecek olursa, bir web sitesinde yorum sayfasına yorum eklemek için üyeliğin şart koşulmasını, o içeriğin aleniyetini engelleyen bir faktör olarak algılayan bir kişi, söz konusu sayfaya üyelik başvurusu yapan ve bilgileri eksiksiz dolduran herkesin üye olabileceğini, dolayısıyla buradaki üyelik prosedürünün aleniyeti engelleyen bir prosedür olmadığını atlaması sonucu o siteye intiharı teşvik eden bir yorum yazarsa bu durum suçun nitelikli halinde yapılan hata kapsamında (TCK Md. 30/2) değerlendirilmelidir. Çünkü Md. 84/3 de suçun aleni işlenmesi ağırlaştırıcı bir nedendir.

[434]Tepe, İlker, ***Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları***, Yayımlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya, 2009, s. 199.

Suça etki eden nedenler arasında interneti en yakından ilgilendiren düzenleme maddenin üçüncü fıkrasındaki düzenlemedir. Buna göre, başkalarını intihara alenen teşvik eden kişi üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılacaktır. Maddenin ilk halinde anılan ağırlaştırıcı nedene ek olarak suçun basın yayın yolu ile işlenmesi de yer almıştı. Ancak 29.06.2007 tarih ve 5377 sayılı kanunla yapılan değişiklikle bu hüküm madde metninden çıkarılmıştır. Bu değişikliğin gerekçesi de aynen şöyle yapılmıştır.

"Suçun basın ve yayın yoluyla işlenmesi hali de, aleniyetin gerçekleşiş şekillerinden birini oluşturmaktadır. İntihara teşvik suçuyla ilgili olarak aleniyet bir nitelikli unsur olarak belirlendiği için, söz konusu suçun basın yayın yoluyla işlenmesi, bu suç açısından ayrı bir nitelikli unsur olarak görülmemiştir."

Bu değişiklik internet açısından irdelendiğinde, suçun internet aracılığıyla işlenmesi bakımından herhangi bir farklılığa sebebiyet verilmediği görülmektedir. Çünkü gerekçede de aktarıldığı üzere bir suçun işlenmesinde aleniyet unsurunun aranması kaplamsal bir bakış açısını beraberinde getirecektir. Bu yüzden suçun basın yayın yolu ile işlenmesi bu bağlamda ele alınacaktır.[435]

İntihara yönlendirme suçunda verilecek cezalar, madde metninde açıkça belirtilmektedir.

"Başkasını intihara azmettiren, teşvik eden, başkasının intihar kararını kuvvetlendiren ya da başkasının intiharına herhangi bir şekilde yardım eden kişi, 2 yıldan 5 yıla kadar hapis cezası ile cezalandırılır. İntiharın gerçekleşmesi durumunda, kişi 4 yıldan 10 yıla kadar hapis cezası ile cezalandırılır. Başkalarını intihara alenen teşvik eden kişi, 3 yıldan 8 yıla kadar hapis cezası ile cezalandırılır. İşlediği fiilin anlam ve sonuçlarını algılama yeteneği gelişmemiş olan veya ortadan kaldırılan kişileri intihara sevk edenlerle cebir veya tehdit kullanmak suretiyle kişileri intihara mecbur edenler, kasten öldürme suçundan sorumlu tutulurlar."[436]

3.2.2.10. Cinsel Taciz

5237 sayılı TCK Md. 105'de düzenlenen cinsel taciz suçunun da internet aracılığıyla işlenebileceği kuşkusuzdur. İlgili maddenin 1. Fıkrasında, "Bir kimseyi cinsel amaçlı olarak taciz eden kişi hakkında, mağdurun şikâyeti üzerine, üç aydan iki yıla kadar hapis cezasına veya adlî para cezasına fiilin çocuğa karşı işlenmesi hâlinde altı aydan üç yıla kadar hapis cezasına hükmolunur."[437] İfadesi kullanılarak

[435] Tepe, **a.g.e.**, s. 202.
[436] 5237 Sayılı Türk Ceza Kanunu, İntihara Yönlendirme, Madde 84, s.8988.
[437] 5237 Sayılı Türk Ceza Kanunu, Cinsel Taciz, Madde 105, s. 8995.

böyle bir suçun işlenmesi durumunda verilecek ceza belirtilmiştir. Cinsel taciz suçunun işlenmesi için, sanal ortamların kullanılabileceği de aşikârdır. Özellikle e-posta yoluyla veya diğer kişisel iletişim kanalları kullanılmak suretiyle cinsel amaçlı rahatsızlık verici ifadeler kullanılabilir. Özellikle internetin, bir multimedya aracı olarak aynı anda hem görsel hem işitsel, hem yazıyla hem resimle bu suçta kullanılması mümkündür.

Suçun fail ve mağduru bakımından kanun koyucu herhangi özel bir belirlenime gitmemiş ve dolayısıyla cinsel taciz suçunun her erkek veya kadın tarafından işlenebileceğini kabul etmiştir. Bu anlamda suçun mağduru herkes olabilir. Kanunda "bir kimseyi cinsel amaçlı olarak taciz eden" denildiğinden, mağdur açısından da herhangi bir sınırlamaya gidilmemiştir. Bununla birlikte mağdur faille farklı cinsten olabileceği gibi aynı cinsten de olması mümkündür. Özellikle internette kişilerin kimliklerini olabildiğince gizlemeye çalışmaları ve hangi cinsiyetten olduklarının anlaşılamamaları karşısında kanun koyucunun cinsel taciz suçlarında mağdur ve fail açısından cinsiyet temelli bir ayrıma gitmemesi normal karşılanmalıdır. Bunların yanında Yargıtay cinsel taciz suçunun oluşabilmesi için eylemin doğrudan doğruya mağdura karşı işlenmesi gerekliliğini aramaktadır. Anılan suç tipinin tipe uygun eylem unsuruna yönelik internet aracılığıyla işlenebilirliğini de kapsayacak şekilde bir değerlendirme yapmak gerekirse; Md. 105/1'e göre cinsel taciz suçunun maddi unsuru bir kişiyi cinsel amaçlı olarak taciz etmektir.[438] Gerekçede, "cinsel taciz, kişinin vücut dokunulmazlığının ihlâli niteliği taşımayan cinsel davranışlarla gerçekleştirilebilir. Cinsel taciz, cinsel yönden, ahlâk temizliğine aykırı olarak mağdurun rahatsız edilmesinden ibarettir."[439] denilmektedir.

Suçun; kamu görevinin veya posta veya elektronik haberleşme araçlarının sağladığı kolaylıktan faydalanmak suretiyle ya da koruma, bakım ve gözetim yükümlülüğü altında bulunan kişiler tarafından işlenmesi hâlleri de, bu suç bakımından daha ağır cezayı gerektiren nitelikli unsur olarak kabul edilmektedir.[440]

TCK Md. 105 anlamında cinsel tacizin internet aracılığıyla sıklıkla işlenen bir suç tipi olduğu bilinmektedir. Çünkü internetin, isabetli olmamasına rağmen kanunun

---

[438] Tepe, **a.g.e.**, s. 206.

[439] 5237 Sayılı Ceza Kanunu Madde 105, ***Cinsel Taciz***, (Erişim) http://www.turkhukuksitesi.com/mevzuat.php?mid=5174 , 12 Aralık 2016.

[440] Yurtcan, Erdener, ***Yargıtay Kararları Işığında Cinsel Suçlar***, Türkiye Barolar Birliği Yayınları: 304, Ankara, 2015, s. 223.

ifadesiyle ahlak temizliğinin kirletilmesine müsait bir ortam olduğu bilinmektedir. Özellikle internetin kullanıcılarına sunduğu gizlilik ve anonimlik güvencesinin tespit edilebilmeyi engelleyen güvenceler olduğu zannıyla, sıklıkla sohbet odalarında, forumlarda veya e-posta ya da kişisel iletişim programları aracılığıyla gönderilen iletilerle cinsel taciz suçunun unsurlarının gerçekleşmesi mümkündür. Ancak kanaatimizce madde gerekçesinde kullanılan "ahlak temizliğine aykırı olarak" ifadesinin özellikle internet aracılığıyla işlenebilen bir suç olması dolayısıyla cinsel taciz suçunda müstakbel genişlemelerin habercisi olduğu, bunun da tehlikeli neticeleri beraberinde getireceği açıktır. Şöyle ki; yukarıda da ifade edildiği gibi internet kanun koyucunun kullandığı ifadeyle "ahlak temizliğinin" en rahat kirletilebildiği ortamların başında gelmektedir. Şayet ahlak temizliğine aykırılık gibi muğlak, göreceli bir kriter bir internet içeriğinin değerlendirmesinde kullanılacak olursa internet kullanımı ciddi anlamda engellenir. Çünkü daha önce de dile getirildiği üzere internet küresel bir ağdır ve burada küresel değerlerin hâkim olduğu bir düzlem yaratılmıştır.[441]

Maddenin ikinci fıkrasında cinsel taciz suçunun nitelikli hâlleri belirlenmiştir. Buna göre, hiyerarşi veya hizmet ilişkisinden kaynaklanan nüfuz kötüye kullanılmak suretiyle ya da aynı işyerinde çalışmanın sağladığı kolaylıktan yararlanılarak kişiye karşı cinsel tacizde bulunulması, suçun temel şekline göre daha ağır ceza ile cezalandırılmayı gerektirmektedir. Cinsel taciz suçunun soruşturulması ve kovuşturulması, mağdurun şikâyetine bağlı tutmuştur.[442]

3.2.2.11. Nitelikli Hırsızlık

TCK'nin 142. maddesinin ikinci fıkrasının "e" bendinde düzenlenmiştir. Hırsızlığın bilişim sistemi aracılığıyla işlenmesi "nitelikli" hırsızlık sayılmıştır.[443] 141. maddede hırsızlık, zilyedin rızası dışında başkasına ait taşınır malı failin kendisine veya başkasına yarar sağlamak için bulunduğu yerden alması şeklinde ifade edilmektedir. Bu suçun bilişim sistemleri yoluyla işlenmesi nitelikli hırsızlık sayılmış örneğin failin mağdura ait banka hesaplarından kendisinin veya başkalarının

[441] Tepe, **a.g.e.**, s. 208.
[442] Yurtcan, **a.g.e.**, s.222.
[443] 5237 Sayılı Türk Ceza Kanunu, Nitelikli Hırsızlık, Madde 142, s. 9002.

hesabına mağdurun rızası dışında para aktarması TCK'nin 142/2.e maddesinden cezalandırılabilmesine olanak tanımaktadır.[444]

Bu suç parçalara bölünebildiğinden teşebbüs aşamasında kalması mümkündür. Çünkü suçun tamamlanması için malın alınması ya da veri halindeki paranın transfer edilmesi yetmeyip failin egemenlik alanına girmesi de gerekmektedir. Bu ise belli bir zaman gerektirdiğinden, bu zaman esnasında hareketin yarıda kalması halinde suç teşebbüs aşamasında kalmış olacaktır. Ancak hemen belirtelim ki, suçun bilişim sistemleri suretiyle işlenmesi hâlinde veri şeklindeki paranın transferi ile failin hâkimiyet alanına girmesi arasında saniyelerle ölçülebilecek bir zaman dilimi olacağından suçun teşebbüs aşamasında kalmasına sıklıkla rastlanmamaktadır.

Hırsızlık suçu iştirak bakımından bir özellik göstermemektedir, dolayısıyla bu suça iştirakin her türlüsü mümkündür. İnternet üzerinden yetkisiz erişimle bankanın online sistemine girilerek müşterilerin mevduat ya da kredi hesaplarından para transferi yapılması 142/2-e maddesi içinde değerlendirilmektedir. Bu durumda failin parayı temsil eden veri hırsızlığını yapmadan önce bankanın bilişim sistemine girmesi ve sistemde kalması gerekmektedir. Dolayısıyla fail 142/2-e maddesindeki suçu işlemeden önce 243. maddede tanımlanan eylemi de gerçekleştirmektedir.

Dolayısıyla bu iki madde arasındaki ilişkinin ortaya konulması gerekir. Burada ilk akla gelen bu suçlar açısından geçit suçunun söz konusu olup olmadığıdır. Geçit suçu, bir suçun işlenmesi için öncelikle cezası daha hafif olan bir suçun işlenmesinin, bu suçtan geçilmesinin gerekmesidir. Ancak geçit suçunun söz konusu olabilmesi için işlenen ilk suçun ve sonraki daha ağır suçun aynı hukuksal değeri koruması gerekir. Oysa 243. maddede bilişim sisteminin güvenliği korunmakta iken 244/2-e'de mağdurun malvarlığı korunmaktadır. Dolayısıyla bu iki suç arasında korunan hukuksal değerlerin farklı olması nedeniyle geçit suçunun gerçekleşmesi mümkün değildir. Diğer yandan geçit suçunun söz konusu olabilmesi için ilk suçtan geçilmeksizin ikinci suçun işlenememesi gerekir (örneğin kasten yaralama suçu işlenmeden kasten öldürme suçunun işlenmesi mümkün değildir). Her iki suç bu açısından incelendiğinde bilişim sistemi aracılığıyla hırsızlık suçunun işlenmesi için, mutlaka sisteme girme ve orada kalmaya devam etme suçunun işlenmesi

[444]Nacar, Fatma Burcu, ***Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları***, Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010, s. 121.

gerekmemektedir. Zira 243. maddedeki eylemin suç oluşturması için bunun hukuka aykırı olarak gerçekleştirilmesi gerekir, bu eylemlerin mağdurunun rızasıyla işlenmesi halinde ise hukuka aykırılık unsuru ortadan kalkacağı için suç da gerçekleşmeyecektir.

Örneğin bankanın bilişim sisteminin test edilmesi ya da bakım yapılması için bilişim güvenliği uzmanlarına yetki verilmesi halinde sisteme giriş ve sistemde kalma hukuka uygun olmakta ve suç oluşmamaktadır. İşte bu kişilerin sistem içindeki verilerin transferi yoluyla hırsızlık yapmaları hâlinde (bu kişilerin banka çalışanı olmağı da dikkate alındığında) 142/2-e'de tanımlanan suç gerçekleşmiş olacak ancak 243. maddedeki suç işlenmemiş olacaktır. Dolayısıyla bilişim sistemleri aracılığıyla hırsızlık suçunun işlenmesi için mutlak surette bilişim sistemine girme ve sistemde kalmaya devam etme suçunun işlenmesine gerek bulunmamaktadır.

Sonuç olarak bu açıdan da her iki suç arasında geçit suçu ilişkisinin bulunmadığı görülmektedir. Bu eylemlerin birlikte gerçekleştirilmesi hâlinde faile her iki suçun da cezası verilmelidir. Hırsızlık suçunun temel hali için bir yıldan üç yıla kadar hapis cezası öngörülmüşken, 142/2-e'deki suçun nitelikli hali için üç yıldan yedi yıla kadar hapis cezası öngörülmüştür. Bu suçun temel hali açısından da nitelikli hali açısından da aslîye ceza mahkemeleri yargılama yapmakla görevlidir.[445]

3.2.2.12. Nitelikli Dolandırıcılık

5237 Sayılı TCK'nin malvarlığına karşı suçlar başlıklı onuncu bölümünün 158. maddesinin 1. fıkrasının f bendinde düzenlenmiştir. 158. madde dolandırıcılık suçunun nitelikli hallerini düzenlemiştir.[446]

Dolandırıcılık suçunda failin sorumlu tutulabilmesi için gerçek bir kişiye karşı hileli davranışlarda bulunulması gerekir. 158. maddenin 1. fıkrasının f bendinde birden fazla nitelikli hal belirtilerek bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi halinde 2 yıldan 7 yıla kadar hapis ve 5000 güne kadar adli para cezasına hüküm olunur denmektedir. Bu suçla hem bireylerin malvarlıkları, hem irade özgürlükleri, hem de toplumsal yaşam içinde diğer insanlara duydukları güven korunmaktadır. Dolandırıcılık suçu fail ve

[445] Dülger ve Modoğlu, **a.g.e.**, s. 54-55.
[446] 5237 Sayılı Türk Ceza Kanunu, Nitelikli Dolandırıcılık, Madde 158, s. 9005.

mağdur açısından bir özellik göstermemektedir, herkes bu suçun faili ve mağduru olabilir.[447]

Günümüzde bilişim yoluyla dolandırıcılığına en çok görüldüğü yer internet üzerinde gerçekleştirilen elektronik ticaret dolandırıcılıkları ve internetteki müzayede sitelerinde yaşanan olayları örnek verebiliriz.

Örneğin kişi sahte ticari bir web sitesi oluşturup mağdurların güvenini kazanıp onlara satacağını vaat edip para havale etmelerini sağlayarak dolandırıcılık suçu işlenebilir yine para çekme cihazlarında önceden hazırladıkları tertibatla bankamatik kartının sıkışmasını sağlayıp banka görevlisi ile telefonda görüşüyormuş gibi yapıp mağdurdan kartın şifresini öğrenip bankadan para çekilmesi eylemi de TCK'nin 158/1-f maddesi kapsamında kalır.[448]

Uygulamada en sık karşılaşılan bilişim sistemleri aracılığıyla dolandırıcılık eylemleri, failin bir kişiye ait sosyal medya (MSN messenger, facebook vb.) ya da elektronik posta giriş şifrelerini ele geçirerek şifresini ele geçirdiği kişilerin arkadaşlarına kendisini profil sahibi gibi tanıtıp para istemesi ya da belli bir telefona kontör yüklenmesini talep etmesi ve istemlerinin kabul edilmesi suretiyle gerçekleştirilmektedir. Fail burada, profilin arkadaşları ya da yakınları olan mağdurların iyi niyetinden, güveninden ya da bazen saflığından faydalanarak haksız yarar elde etmektedir. Bilişim suçları dünyasında bu yönteme "phishing" denilmektedir ve ülkemizde de yabancı ülkelerde de en sık görülen dolandırıcılık yöntemlerinden biridir.

Dolandırıcılık suçunun oluşması için, haksız yarar sağlanması, suçun teşebbüs aşamasında kaldığının kabul edilebilmesi için, hazırlık hareketlerinin sona erip haksız yararın elde edilmesine yönelik icra hareketlerine başlanması gerekmektedir. Bilişim sistemleri kullanılmak suretiyle işlenen dolandırıcılık suçunun cezası 3 yıldan 7 yıla kadar hapistir. Ayrıca bu suçun cezası olarak hapis cezasının yanında adlî para cezasına hükmedilmesi gerekmektedir. Nitelikli dolandırıcılığın bu türü için 5000 güne kadar adlî para cezası öngörülmekle birlikte adlî para cezasının miktarının suçtan elde edilen yararın 2 katından az olamayacağı belirtilmiştir.[449]

[447] Karagülmez, **a.g.e.**, s. 182.
[448] Nacar, **a.g.e.**, s. 121.
[449] Dülger ve Modoğlu, **a.g.e.**, s. 57.

3.2.2.13. Müstehcenlik

5237 Sayılı TCK'nin topluma karşı suçlar başlıklı üçüncü kısmının genel ahlaka karşı suçlar başlıklı yedinci bölümünün 226. maddesinde düzenlenmiştir. Maddenin metninde müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına yönelik düzenlemeler yer almaktadır. Veri iletim ağları ile zararlı yayınların yayılması ve paylaşılması eylemlerine uygulanan bir maddedir. Son zamanlarda çocuk pornografisi giderek artmakta ve Türkiye'de de bu suçlarla mücadele devam etmektedir. Benzeri düzenlemeler karşılaştırmalı hukukta da yer almaktadır.

ABD'de çocukların online yayınlardan korunması yasası yine Amerika'da Çocuk Pornografisinin Önlenmesi Yasası, Fransa'da Ceza Kanununda, İngiltere'de Müstehcen Yayınlar Yasasında ve Telekomünikasyon Yasasında yapılan değişikliklerle sanal âlemde yapılan pornografik içerikli yayınlar engellenmiştir.

Avrupa Konseyi Siber suç sözleşmesinde çocuk pornografisine ilişkin materyalin elektronik olarak üretimi dağıtımı ve bu materyale sahip olunması fiilleri cezalandırılmaktadır. Burada dikkati çeken sözleşme ile yalnızca çocuk pornografisi ile küçüklerle ilgili müstehcen görüntülerin yasaklanmış olduğudur. Siber suç sözleşmesinde 9. Maddenin kapsamına çocuk erotizmi dâhil edilmediğinden birçok ülkede bu konudaki yasal boşluktan yararlanılarak bu materyalin satılması suç sayılmamıştır.[450]

TCK'nin 226. maddesinde çocuklara ve yetişkinlere ilişkin müstehcenlik arasında bir ayrım yapılmadığından bizde de yasal bir boşluk bulunmaktadır. Bu da uygulamada sorunlara sebep olabilir. TCK'de hangi eylemlerin pornografik hangi eylemlerin müstehcen sayıldığının sınırları çizilmemiştir. Maddenin ikinci fıkrasındaki müstehcenlik ifadesinin neyi kastettiği belirtilmemiş, hâkime yasa koyucu burada takdir yetkisi vermiştir. 226. maddenin 4. fıkrasında doğal olmayan yoldan yapılan cinsel ilişki ifadesinde net somut bir açıklama yoktur. Her türlü yazı, görüntü ve ses olabilir yasa koyucu geniş yoruma açık bir alan bırakmıştır.[451] Yine dördüncü fıkrada suç teşkil eden görüntü, ses ve yazıların bulundurulması suç olarak düzenlenmiş. Devlet eliyle kişinin özel bilgisayarında bulundurduğu bu verilere

[450] Nacar, **a.g.e.**, s. 122.
[451] Karaca, Ayşe ve Beyaznar, Bahar, "İnternette Müstehcenlik: Nerede başlar ve nerede biter?", **Akademik Bilişim'10**, s. 3.

müdahale edilebilecektir. Bu da anayasanın 20. maddesine (özel yaşama müdahale) ve Anayasanın 13. maddesine (hakkın özüne aykırılık) teşkil edebilecektir. Bu suçun mağduru çocuktur. Kasten işlenen bir suçtur. İçtima bakımından özellik göstermez. TCK'nin genel hükümleri uygulanır. Teşebbüs mümkündür. İştirak bakımından da TCK'nin genel hükümleri uygulanır.

TCK'nin 226. maddesinde 2., 3. ve 4. fıkralarında suçun alenen işlenmesine ilişkin bir düzenleme yer almamıştır.[452]

3.2.2.14. Fuhuş

TCK 227. Maddeyle düzenlenen fuhuş konusunda söz konusu düzenleme şu şekildedir:[453]

"Madde 227- (1) Çocuğu fuhşa teşvik eden, bunun yolunu kolaylaştıran, bu maksatla tedarik eden veya barındıran ya da çocuğun fuhşuna aracılık eden kişi, dört yıldan on yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır. Bu suçun işlenişine yönelik hazırlık hareketleri de tamamlanmış suç gibi cezalandırılır.

(2) Bir kimseyi fuhşa teşvik eden, bunun yolunu kolaylaştıran ya da fuhuş için aracılık eden veya yer temin eden kişi, iki yıldan dört yıla kadar hapis ve üç bin güne kadar adlî para cezası ile cezalandırılır. Fuhşa sürüklenen kişinin kazancından yararlanılarak kısmen veya tamamen geçimin sağlanması, fuhşa teşvik sayılır.

(3) (Mülga: 6/12/2006 – 5560/45 Md.; Yeniden düzenleme: 24/11/2016-6763/18 Md.) Fuhşu kolaylaştırmak veya fuhşa aracılık etmek amacıyla hazırlanmış görüntü, yazı ve sözleri içeren ürünleri veren, dağıtan veya yayan kişi bir yıldan üç yıla kadar hapis ve iki yüz günden iki bin güne kadar adli para cezası ile cezalandırılır.

(4) Cebir veya tehdit kullanarak, hile ile ya da çaresizliğinden yararlanarak bir kimseyi fuhşa sevk eden veya fuhuş yapmasını sağlayan kişi hakkında yukarıdaki fıkralara göre verilecek ceza yarısından iki katına kadar artırılır.

(5) Yukarıdaki fıkralarda tanımlanan suçların eş, üstsoy, kayın üstsoy, kardeş, evlat edinen, vasi, eğitici, öğretici, bakıcı, koruma ve gözetim yükümlülüğü bulunan diğer kişiler tarafından ya da kamu görevi veya hizmet ilişkisinin sağladığı nüfuz kötüye kullanılmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(6) Bu suçların, suç işlemek amacıyla teşkil edilmiş örgüt faaliyeti çerçevesinde işlenmesi halinde, yukarıdaki fıkralara göre verilecek ceza yarı oranında artırılır.

(7) Bu suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(8) Fuhşa sürüklenen kişi, tedaviye veya psikolojik terapiye tâbi tutulabilir."

[452] Nacar, **a.g.e.**, s. 122-123.
[453] 5237 Sayılı Türk Ceza Kanunu, Fuhuş, Madde 227, s. 9020.

3.2.2.15. Kumar Oynanması İçin Yer ve İmkân Sağlama

Online kumardan bahsedilirken TCK 228. maddesine göre aşağıdaki yasal metninden de anlaşılacağı üzere bu maddenin normal kumar oyunlarında yer temin edeni cezalandırdığı aşikardır. Normal kumar oynama eylemi ise, suç ve ceza kapsamında değil, kabahat kapsamında ve 5326 sayılı kabahatler kanununun 34. maddesine göre idari yaptırımla cezalandırılmıştır.[454]

"Kumar Oynanması İçin Yer ve İmkân Sağlama TCK Madde 228[455]

(1) Kumar oynanması için yer ve imkân sağlayan kişi, bir yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(2) Çocukların kumar oynaması için yer ve imkân sağlanması hâlinde verilecek ceza bir katı oranında artırılır.

(3) Bu suçtan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(4) Ceza Kanununun uygulanmasında kumar, kazanç amacıyla icra edilen ve kar ve zararın talihe bağlı olduğu oyunlardır

5326 Sayılı Kabahatler Kanunu Madde 34[456]

(1) Kumar oynayan kişiye, yüz Türk Lirası idari para cezası verilir. Ayrıca, kumardan elde edilen gelire el konularak mülkiyetin kamuya geçirilmesine karar verilir.

(2) Bu kabahat dolayısıyla idari para cezasına ve el koymaya kolluk görevlileri, mülkiyetin kamuya geçirilmesine mülki amir karar verir."

Suçun hukuki konusu; suçla ihlal edilen hukuki varlık veya menfaattir. Suçun ihlal ediciliği kaynağını hukuki konudan alır. Her suçta nasıl bir fail varsa, bir de hukuki konu vardır. Bu bağlamda incelemekte olduğumuz suç, TCK'nin özel hükümler başlıklı 2. kitabının, topluma karşı suçlar başlıklı 3. kısmının, genel ahlaka karşı suçlar başlıklı 7. bölümünde düzenleme altına alınmıştır. Kanun koyucu kanunun sistematiğine bakıldığında söz konusu fiili genel ahlaka aykırı olduğu gerekçesiyle cezalandırmaktadır. Dolayısıyla kanun koyucunun mantığına göre suç tipinin koruduğu hukuki menfaat ağırlıklı olarak genel ahlaktır.[457]

Kumar için sağlanan yerin muhakkak somut bir mekân olması gerekli değildir. Bunun dışında sanal ortamda sağlanacak yer ve uygun ortam da yer sağlama kapsamına girer. Dolayısıyla internet ortamında kumar sitesi kurmak suretiyle ki-

[454] Dülger ve Modoğlu, **a.g.e.** , s. 71.

[455] 5237 Sayılı Türk Ceza Kanunu, Kumar Oynanması İçin Yer ve İmkan Sağlama, Madde 228, s. 9020.

[456] 5236 Sayılı Kabahatler Kanunu, II. Kısım: Çeşitli Kabahatler, "Kumar", s. 9344.

[457] Karakehya, Hakan, "Kumar Oynanması İçin Yer ve İmkân Sağlama Suçu", ***Marmara Üniversitesi Hukuk Araştırmaları Dergisi***, 2014, s. 705, (Erişim) e-dergi.marmara.edu.tr/maruhad/issue/download/5000001567/5000000627, 24.01.2017.

şilere kumar oynama alanı ve imkânı sağlayan kimseler de bu madde kapsamında cezai sorumluluğa sahip olacaklardır. Yurt dışında kurulmuş kumar sitelerinde kumar oynanmasına imkân sağlayanlar bakımından ise 7258 s. Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun'un 5/2. maddesinde özel düzenleme yapılmıştır. Buna göre; "Yurt dışında oynatılan her çeşit bahis veya şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, iki yıldan beş yıla kadar hapis cezasıyla cezalandırılır." Aynı maddenin 3. fıkrasında ise; "Her türlü bahis veya şans oyunlarıyla bağlantılı olarak para nakline aracılık eden kişiler, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezasıyla cezalandırılır." denilmek suretiyle kumar ve bahis oyunlarında para nakline aracılık edenlere de cezai sorumluluk öngörülmüştür.[458]

Online kumar ise özel olarak 7258 sayılı yasa düzenlenmiştir. 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis Ve Şans Oyunları Düzenlenmesi Hakkında Kanun'un 5. Maddesinde yer alan özel düzenlemeler şu şekildedir:[459]

"Kanunun verdiği yetkiye dayalı olmaksızın, spor müsabakaları ile ilişkili olarak sabit ihtimalli veya müşterek bahis oynatanlar, oynanmasına yer veya imkân sağlayanlar, 1 yıldan 3 yıla kadar hapis ve 10000 güne kadar adlî para cezasıyla cezalandırılır.

Yurt dışında oynatılan her çeşit bahis veya şans oyunlarının internet yoluyla ve sair suretle erişim sağlayarak Türkiye'den oynanmasına imkân sağlayan kişiler, 2 yıldan 5 yıla kadar hapis cezasıyla cezalandırılır.

Her türlü bahis veya şans oyunlarıyla bağlantılı olarak para nakline aracılık eden kişiler, 1 yıldan 3 yıla kadar hapis ve 5000 güne kadar adlî para cezasıyla cezalandırılır.

Kişileri, reklam vermek ve sair surette, her türlü bahis veya şans oyunlarını oynamaya teşvik edenler, 6 aydan 2 yıla kadar hapis ve 3000 güne kadar adlî para cezasıyla cezalandırılır.

Bu maddede tanımlanan suçlarla bağlantılı olarak, her türlü bahis veya şans oyunlarının oynanmasına tahsis edilen veya oynanmasında kullanılan ya da suçun konusunu oluşturan eşya ile bu oyunların oynanması için ortaya konulan veya oynanması suretiyle elde edilen her türlü mal varlığı değeri, 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununun eşya ve kazanç müsaderesine ilişkin hükümlerine göre müsadere edilir.

Bu maddede tanımlanan suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bu maddede tanımlanan suçlarla ilgili olarak, 4/5/2007 tarihli ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen

[458] Karakehya, 2014, **a.g.e.**, s. 707.

[459] 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun, Madde 5, s. 3202-1.

Suçlarla Mücadele Edilmesi Hakkında Kanunun erişimin engellenmesine ilişkin hükümleri uygulanır."

Ayrıca 21/5/1986 tarihli ve 3289 sayılı Gençlik ve Spor Genel Müdürlüğünün Teşkilat ve Görevleri Hakkında Kanunun 10 uncu maddesi ile 29/4/1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun hükümlerine dayanılarak spor müsabakalarına dayalı sabit ihtimalli ve müşterek bahis oyunları uygulama yönetmeliği 28.02.2009 tarihli Resmî Gazete'de yayınlanmıştır.

3.2.3. Fikir ve Sanat Eserleri Kanunu'nda Düzenlenen İnternet Yoluyla İşlenen Suçlar

5846 sayılı FSEK'te "hukuk ve ceza davaları" üst başlıklı beşinci bölümde; hukuk davaları, ceza davaları ve çeşitli hükümler olmak üzere üç husus düzenlenmiştir. Bunlardan ceza davalarını düzenleyen B kısmında suçlar, mülga edilen "diğer suçlar" hükmüne karşılık olarak iki alt başlıkta düzenlenmiştir. Bunlardan 71. madde, "manevi, mali veya bağlantılı haklara tecavüz"ü, 72. madde ise "koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri"ni kapsamaktadır.[460]

Bunlardan 71. madde hükmü;

"(Değişik: 23/01/2008-5728/138 md.)

Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek:

1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

2. Başkasına ait esere, kendi eseri olarak ad koyan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz.

3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

---

[460] Yaman, Dilara, "Fikir ve Sanat Eserleri Kanunu'nda Düzenlenen Bir Eserden Kaynak Göstermeksizin İktibasta Bulunma Suçu (M. 71/1-III)", ***Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi***, Cilt: 12, Özel Sayı, 2010, Basım Yılı: 2012, s.1552.

4. Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır.

5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır.

6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur.

Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir."[461] şeklindedir.

Neticede FSEK m. 71'in bugünkü düzenlemesinde yer alan suçlar;

- Manevi haklara tecavüz suçları (71/1-I)
- Mali haklara tecavüz suçları (71/1-II)
- Bağlantılı haklara tecavüz suçları (71/1-III)
- Başkasının eserini sahiplenmek suçu (71/1-II)
- İntihal suçları (71/1-III ve V)
- Eser içeriğini ifşa suçu (71/1-IV)
- Başkasının adından istifade suçu (71/1-VI) olarak sınıflandırılabilir. Bu sayılanlardan eser sahibinin manevi haklarına yönelik olan suçlar; "başkasının eserini sahiplenmek (71/1-II)", "kaynak göstermeksizin alıntı yapmak (71/1-III)", "eserlerle ilgili gerçeğe aykırı kaynak göstermek (71/1-V)", "eserin içeriğini ifşa (71/1-IV)" düzenlemelerinde yer almaktadır ve bu sayılanlar haricindeki düzenlemeler mali haklar ile bağlantılı haklara tecavüz suçlarıdır.[462]

Manevî haklara tecavüz suçu açısından; Yasanın 71/1-1. maddesindeki *"henüz alenileşmemiş bir eseri hak sahibi kişilerin yazılı izni olmaksızın her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten veya yayımlayan"*, 71/4. maddesindeki *"henüz alenileşmemiş bir eserin içeriğini ifşa eden"*, 71/1. maddesindeki *"bir eseri yazılı izin olmaksızın değiştiren"*, 71/2. maddesinde

[461] 5846 Sayılı Fikir ve Sanat Eserleri Kanunu, Madde 71, s. 2413.
[462] Yaman, **a.g.e.**, s. 1554.

"başkasının eserini sahiplenen", 71/3 ve 71/5. Maddelerindeki *"intihal eylemlerini gerçekleştiren"* kişiler bu suçun faili olacaklardır.

Maddî haklara tecavüz açısından ise fail; hak sahibi kişilerin yazılı izni olmaksızın eseri işleyen, çoğaltan, yayan, temsil eden, kamuya elektronik aletlerle ileten, ticari amaçla satın alan, ithal eden veya ihraç eden ve kişisel ihtiyacı dışında elinde bulunduran veya depolayan kişidir. [463]

Eserin İşlenmesi: Bir yazılımın hak sahibinin yazılı izni olmaksızın işlenmesi eylemi maddî haklara yönelik suç tipini oluşturmaktadır. Bu eylemle FSEK'in 21. maddesinde düzenlenen yazılımı işleme hakkı ihlal edilmektedir. Bir yazılımı işleme yetkisi yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımın işlenmesi yoluyla, "işleme bir yazılımın" oluşturulmasıyla suç gerçekleşmiş olacaktır.

Eserin Çoğaltılması: Bir yazılımın, hak sahibinin yazılı izni olmaksızın çoğaltılması eylemi maddî haklara yönelik diğer bir suç tipini oluşturmaktadır. Çoğaltma, topluma sunulan bir yazılımın, ekonomik getiri amacıyla herkese ulaştırılması için sayılarının arttırılmasını sağlayan ve bilişim sistemleriyle yapılan teknik bir işlemdir. Bu eyleme uygulamada çok sık rastlanmakta ve bu nedenle yazılım endüstrisinde milyon dolarla ifade edilen kayıpların olduğu belirtilmektedir. Çünkü bilişim yazılımlarının yaratılması için gerekli olan emek ve ekonomik maliyet büyük boyutlardayken, kopya nüshaların hazırlanması için oldukça az zaman ve masraf yeterli olmaktadır. Bu eylemle FSEK'in 22. Maddesinde düzenlenen yazılımı çoğaltma yetkisi ihlal edilmektedir. Bir yazılımı çoğaltma yetkisi yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımının her ne şekilde olursa olsun çoğaltılmasıyla suç gerçekleşmiş olacaktır. Çoğaltma eyleminin asıl yazılım ya da işleme niteliğindeki yazılım üzerinde olması suçun oluşmasını etkilemeyecektir. Eserden ekonomik olarak yararlanmanın en eski ve yaygın yolu olan çoğaltma hakkı, günümüz fikri haklarının temelini de oluşturmaktadır.

Eserin Failin Kendisi Tarafından Çoğaltılmış Kopyalarının Satışa Çıkarılması: Bir yazılımın ya da işlemelerinin hak sahibinin yazılı izni olmaksızın failin kendisi tarafından çoğaltılmış kopyalarının satışa çıkarılması eylemi de maddî haklara yönelik suç oluşturacaktır. Satışa çıkarmayla kastedilen yazılımların her türlü

[463] Dülger ve Modoğlu, **a.g.e.**, s. 93.

pazarlama yöntemiyle tüketicilere ulaştırılması eylemidir. Nitekim Yargıtay da buradan hareket ederek kiralamayı da tüketicilere ulaştırma kabul ederek suçun oluştuğunu kabul etmiştir. Bu eylemle FSEK'in 23. Maddesinde düzenlenen yazılımı yayma hakkı ihlal edilmektedir. Bir yazılımı satışa çıkarma hakkı yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımın satışa çıkarılmasıyla suç gerçekleşmiş olacaktır.

Bir yazılımın hak sahibinden izinsiz kiralanması veya kamuya ödünç verilmesi suretiyle yayılması hareketi de maddî haklara yönelik suç tipini oluşturacaktır. Bu eylemle FSEK'in 23. Maddesinin 3. fıkrasında düzenlenen yazılımı kiraya verme ve kamuya ödünç verme hakkı ihlal edilmektedir. Bir yazılımı kiralama ve ödünç verme hakkı yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden izin alınmadan yazılımın kiralanması veya kamuya ödünç verilmesiyle suç gerçekleşmiş olacaktır.

Eserin İthal Edilmesi: Bir yazılımın hak sahibinin izni olmaksızın ithal edilmesi eylemi de maddî haklara yönelik suç tipi olarak düzenlenmiştir. Bir yazılımın ithalatı yalnızca yazılım üzerinde hak sahibi olan kişinin izniyle olabilir. Yazılım üzerinde hak sahibi olan kişiden izin alınmadan yazılımın ithal edilmesiyle suç gerçekleşmiş olacaktır. İthalat vergilerinin ödenmesi suçun oluşumunu etkilemeyecektir. İthal edilen yazılımları pazarlayan ve şahsî kullanım amacı dışında satın alan veya kullanan kişiler de aynı eylemi gerçekleştirmiş gibi kabul edilecektir.

Eserin Temsil Edilmesi: Maddî haklara tecavüz suçunu oluşturan eylemlerden bir diğerini de "temsil etme" eylemi oluşturmaktadır. Zira FSEK'in "temsil hakkı" başlıklı 24. Maddesinin 1. fıkrasında *"Bir eserden, doğrudan doğruya yahut işaret, ses veya resim nakline yarayan aletlerle umumî mahallerde okumak, çalmak, oynamak ve göstermek gibi temsil suretiyle faydalanma hakkı münhasıran eser sahibine aittir."* denilmek suretiyle bu hak düzenlenmektedir. Temsil hakkı, bir eserin yayım dışında başka yöntemlerle duyulara hitap edecek şekilde kamuya sunulma yetkisidir. Temsilde bir eserin sabit olmayan bir araçla kamuya sunulması söz konusu olmaktadır. Temsil, bir eserin insan duyularına hitap etmek üzere doğrudan doğruya insan algılamasına yönelirken, yayım ise eserin sabit bir ortamda kamuya sunulması şeklidir. Buna göre bir eserin topluma okunması, bir musiki eserinin icrası, bir tiyatro ya da opera eserinin seyirciler önünde oynanması ya da bir sinema eserinin izlettirilmesi temsilin içinde yer almaktadır. İşte bu tür hareketler de

FSEK'in 71. Maddesinin 1. fıkrasında *"bir eserin hak sahibi kişilerin yazılı izni olmaksızın temsil edilmesi"* ile suç hâline getirtilmiştir.

Maddî haklara yönelik suçu oluşturan eylemlerden biri de bir yazılımı hak sahibinin yazılı izni olmaksızın veri iletim ağı üzerinden yaymak ya da yayımına aracılık etmektir. Bu hareketle FSEK'in 25. Maddesinde düzenlenen yazılımı işaret, ses ve/veya görüntü nakline yarayan araçlarla topluma iletim hakkı ihlal edilmektedir. Bir yazılımı satışa bu şekilde iletme hakkı yalnızca yazılım sahibine aittir, bu konuda yazılım sahibinden yazılı izin alınmadan yazılımın iletilmesiyle suç gerçekleşmiş olacaktır. Bu hak, fikir ve sanat eserlerinin radyo, televizyon, uydu ve kablo gibi telli telsiz yayın yapan kuruluşlar ile internet gibi sanal ağlar aracılığıyla kamuya sunulmasını ifade etmektedir.[464]

Maddî haklara yönelik suçu oluşturan eylemlerden biri de bir yazılımın hak sahibinin yazılı izni olmaksızın ticari amaçla satın alınmasıdır. Suç tipinde yer alan bu hareketle eser sahibinin herhangi bir mali hakkı doğrudan koruma altına alınmamaktadır. Ancak bu hareketin suç hâline getirilmesi ile hak sahibi kişilerin eserden kaynaklanan mali haklardan yararlanabilme ve bu hakları ne suretle olursa olsun belirleyebilme hakkının dolayısıyla da olsa korunması amaçlanmaktadır. Bu hareketin ticari amaçla olmayıp kişisel amaçla alınması hâlinde(ki günlük yaşamda genel olarak görülen ve eserlerden hak sahiplerinin maddî yarar elde etmesini sağlayan işlem budur) ise suç oluşmayacaktır.

Kişisel amaç dışında elinde bulundurmak ya da depolamak hareketlerinin suç olarak düzenlenmesi ile özellikle 4110 sayılı Yasa ile amaçlanan fikir ve sanat eserlerinin hukuk dışı ticareti veya buna neden olacak eylemler sonucunda hak sahiplerinin mali haklarına yönelik tecavüz eylemlerinin önlenmesi amaçlanmaktadır. Yasa koyucu kişisel amaç dışında bulundurmak ya da depolamak hareketi ile fikir ve sanat eserlerinin hukuk dışı ticarete konu olmasını kast etmektedir. Nitekim ticari amaç dışında bulundurmak veya depolamak dışındaki bütün bulundurma veya depolama hareketleri kişisel amaç içinde yer alacak ve suç oluşturmayacaktır. Ayrıca bilişim teknolojilerinin gelişimine paralel olarak depolama

[464] 5846 Sayılı Fikir ve Sanat Eserleri Kanunu, Madde 25, s. 2400.

hareketi, mp3, mp4, DVD, DivX ve benzeri formatlardaki verilerin toplanmasını yani kaydedilebilir, depolanabilir bir ortamda bulunmasını da kapsamaktadır.[465]

Mali haklara tecavüz suçunun yaptırımı *"1 yıldan 5 yıla kadar hapis veya adlî para cezası"*[466] olarak belirlenmiştir.

Manevî haklara tecavüz suçu açısından ise farklı hareketler için farklı yaptırımlar öngörülmüştür. 71. Maddenin 1. fıkrasında *"bir eseri hak sahibi kişilerin yazılı izni olmaksızın her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma iletmek veya yayımlamak"* ve *"hak sahibi kişilerin yazılı izni olmaksızın eseri değiştirme"* hareketleri açısından "*bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur"* denerek eylem ve ceza birlikte belirtilmiştir.

71. Maddenin 4. fıkrasında bir eserin muhtevası hakkında kamuya açıklamada bulunma hareketi açısından *"altı aya kadar hapis cezası"* verileceği ifade edilmiştir. Aynı maddenin 2. fıkrasında yer alan *"başkasına ait esere kendi eseri olarak ad koyma"* hareketi için *"6 aydan 2 yıla kadar hapis veya adlî para cezası"*; bu suçun dağıtmak veya yayımlamak suretiyle işlenmesi halinde ise hapis cezasının üst sınırının 5 yıl olacağı ve adlî para cezasına karar verilemeyeceği belirtilmiştir. Yine aynı maddenin 3. fıkrasında *"bir eserden kaynak göstermeksizin iktibasta bulunma hareketi"* için *"6 aydan 2 yıla kadar hapis cezası veya adlî para cezası"* verileceği belirtilmiştir. 5. fıkradaki *"bir eserle ilgili yetersiz, yanlış veya aldatıcı mahiyette kaynak gösterme"* hareketi için *"6 aya kadar hapis cezası"* öngörülmüştür.

Bu suçun soruşturulması ve kovuşturulması FSEK Madde 75'in 1. Fıkrasına göre şikâyete bağlıdır. Yasada suçtan zarar gören kişi ya da kurumun doğrudan doğruya şikâyet etmesinin yeterli olmadığı, şikâyetin geçerli olabilmesi için, hak sahiplerinin veya üyesi oldukları meslek birliklerinin haklarını kanıtlayan belge ve sair delilleri Cumhuriyet Başsavcılığına vermeleri gerektiği belirtilmiştir. Eğer gerekli belge ve sair delillerle süresi içinde başvuru yapılmazsa, şikâyet geçerli olmayacak, kovuşturmaya yer olmadığına karar verilecektir.

5846 sayılı Yasanın 75. maddesinin 2. fıkrası gereğince bu yasada yer alan soruşturması ve kovuşturması şikâyete bağlı suçlar için, başta Milli Eğitim Bakanlığı, Kültür ve Turizm Bakanlığı yetkilileri olmak üzere ilgili gerçek ve tüzel

[465] Dülger ve Modoğlu, **a.g.e.**, s. 95-99.
[466] 5846 Sayılı Fikir ve Sanat Eserleri Kanunu, Madde 71/1, s. 2413.

kişiler tarafından, eser üzerinde manevî ve mali hak sahibi kişiler, şikâyet haklarını kullanabilmelerini sağlamak amacıyla durumdan haberdar edileceklerdir.

FSEK'in 71. maddesinde düzenlenen bu eylemlerin suç olarak düzenlenmesi ve yaptırıma bağlanması yanında, bu eylemler için FSEK'in 66/1. maddesi gereğince tazminat davası da açılabilecektir.

FSEK'in 76. maddesinin 1. fıkrasında "Bu Kanun'un düzenlediği hukukî ilişkilerden doğan davalarda, dava konusunun miktarına ve Kanunda gösterilen cezaya bakılmaksızın, görevli mahkeme Adalet Bakanlığı tarafından kurulacak ihtisas mahkemeleridir." denilmek suretiyle bu hususta ihtisas mahkemeleri kurulacağı belirtilmiştir. İstanbul, Ankara ve İzmir başta olmak üzere büyük şehirlerde bu konuda ihtisas mahkemeleri "Fikri ve Sınai Haklar Ceza Mahkemesi" olarak kurulmuş ve yasadan kaynaklanan ceza davalarına ilişkin yargılamalara bu mahkemelerde devam edilmektedir. Diğer kentlerde ise HSK tarafından belirlenen bir aslîye ceza mahkemesi o yerde ihtisas mahkemesi olarak görev yapmaktadırlar.[467]

3.2.4. Elektronik İmza Kanunu'nda Düzenlenen İnternet Suçları

Elektronik İmza Kanunu'nda düzenlenen internet suçları, İmza Oluşturma Verilerinin İzinsiz Kullanımı (Madde 16) ve elektronik sertifikalarda sahtekârlık (Madde 17) şeklinde düzenlenmiştir. İlgili kanuna göre Madde 16 ve Madde 17 şu şekildedir;[468]

Madde 16- (Değişik: 23/1/2008 – 5728/525 Md.)
Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar.
Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Elektronik Sertifikalarda Sahtekârlık
Madde 17- (Değişik: 23/1/2008 – 5728/526 md.)
Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.

---

[467] Yaman, **a.g.e.**, s. 1565.
[468] 5070 Sayılı Elektronik İmza Kanunu, Madde 16 ve Madde 17.

Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."

Bu suçlar ile korunan hukuksal değer, belgede sahtecilik suçlarıyla korunmak istenilen hukuksal değerle büyük benzerlik göstermektedir. Dolayısıyla devlet tarafından oluşturulan hukuk alanında inandırıcılığı olan bu tür verilere karşı güven ve bunun karşılığı olarak bireylerin de bu verilerin inandırıcılığına ve geçerliliğine olan güvenleri korunmak istenmektedir.

Elektronik imza oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekârlık yapılması suçlarında fail açısından yasa maddelerinde herhangi bir özellik aranmamıştır. Bu nedenle bu suçları herkes işleyebilecektir. Ancak yasada her iki suç açısından da failin çalıştığı işe bağlı olarak suçun cezasını artırıcı nitelikli hal öngörüldüğü için failin çalıştığı işin tespiti önemlidir. Buna göre eylemi meydana getiren failin elektronik sertifika hizmet sağlayıcısı çalışanı olması durumunda ceza yarısına kadar arttırılarak verilecektir.

Bu suçların mağduru daima toplumdur. Elektronik imza oluşturma verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekârlık yapılması suçları nedeniyle zarara uğrayan kimse mağdur olmayıp "suçtan zarar gören kimse" konumundadır.

Her iki suçun da konusunu genel olarak veriler oluşturmaktadır. Çünkü hem elektronik imza hem de elektronik sertifika sayısal verilerden oluşmaktadır. Ancak bu veriler 5237 sayılı TCK'nin 244. maddesinin konusunu oluşturan verilerden farklı olarak bilişim sisteminde bulunan her türlü veri değil, EİK'da belirtilen elektronik imza ve sertifikanın oluşturulmasında kullanılan verilerdir.

EİK'nın 16. maddesinde belirtilen suçun konusunu elektronik imza oluşturma verileri ve araçları, 17. maddesinde düzenlenen suçun konusunu ise elektronik sertifikalar oluşturmaktadır. Her ne kadar yasal düzenlemede de belirtildiği gibi bunlar farklı araçlar olsa da aslında birbirini tamamlayan ve elektronik imzayı geçerli bir onay sistemi haline getiren araçlardır. Failin kendi oluşturduğu sahte sertifikayı kullanmasının suçun oluşumu açısından her hangi bir özelliği yoktur. Tek suç tipi içinde hem sertifikanın oluşturulması hem de oluşturulan sertifikanın kullanılması, suçu oluşturan seçimlik hareketler olarak düzenlendikleri için suçun oluşumunu etkilememektedir.

EİK'nın 16. ve 17. maddelerinin 2. fıkralarında her iki suç için de aynı ağırlatıcı nitelikli hal öngörülmüştür. Buna göre *"yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar arttırılır"* denilmek suretiyle fail açısından elektronik hizmet sağlayıcısı çalışanı olunması durumu, cezanın yarısına kadar arttırılmasını gerektirecektir.

EİK'in 16. ve 17. maddelerinde düzenlenen suçlar yukarıda da belirtildiği üzere hareket dışında ayrıca neticenin aranmadığı, sırf hareket suçlarıdır. Bu nedenle bu suçlara teşebbüs ancak eylem unsurunu oluşturan hareketlerin parçalara bölünebilmesi halinde söz konusu olabilecektir. Ancak failin elinde olmayan nedenlerden ötürü yasada belirtilen suçun işleniş şekillerinin örneğin elektrik kesilmesi ya da sistemin kapatılması gibi bir nedenle yarıda kalması gibi durumlarda suç teşebbüs aşamasında kalabilecektir.

EİK'in 16. ve 17. maddelerinde düzenlenen suçlarda iştirak açısından bir özellik söz konusu olmayıp, ortaya çıkacak iştirak halleri TCK'nin 37, 38, 39, 40 ve 41. maddelerine göre değerlendirilecek ve ortaya çıkacak sorunlar çözülecektir.

EİK'in 16. maddesinde düzenlenen imza oluşturma verilerinin izinsiz kullanımı suçunun, TCK'nin 244/1-2. maddesinde düzenlenen "Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması Suçu ile Verilerin Yok Edilmesi veya Değiştirilmesi Suçu", 244/4'te düzenlenen "Bilişim Sistemi Aracılığıyla Hukuka Aykırı Yarar Sağlama Suçu", 135. maddede düzenlenen "Kişisel Verilerin Kaydedilmesi Suçu" ve 136. maddede düzenlenen "Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu" ile içtima hâlinde bulunması mümkündür.

Ancak EİK yalnızca elektronik imzayla ilgili düzenlenmiş bir yasa olduğu için içerdiği suç tipleri de özel olarak elektronik imzayla ilgilidir. Her ne kadar elektronik imzalar da verilerden oluşmakta ve bunlar üzerinde gerçekleştirilen eylemler yukarıda anılan TCK'de düzenlenen suç tiplerini de ihlal eder nitelikte olsalar da, EİK'nın TCK karşısında özel bir yasa olması nedeniyle EİK'da düzenlenen ceza normları da TCK'nin ceza normlarına göre özel hüküm niteliğindedir. Bu nedenle EİK'in 16. maddesinin TCK'da düzenlenen bilişim suçlarıyla içtima ilişkisinde bulunması durumunda EİK'in 16. maddesi uygulama alanı bulacaktır. Dolayısıyla EİK, TCK karşısında da özel yasa niteliğinde olduğu için çıkabilecek içtima sorunları özel hüküm – genel hüküm ilişkisi çerçevesinde çözülecektir.

EİK'in 17. maddesinde düzenlenen elektronik sertifikalarda sahtekârlık suçunun diğer bilişim suçlarıyla içtima halinde olması halinde de yukarıda belirttiğimiz üzere EİK'in özel yasa olması nedeniyle "genel hükümler" dışında kalan suç tiplerine ilişkin düzenlemelerde öncelikle bu yasada yer alan suç normları uygulama yeri bulacaktır.

EİK'in 16. ve 17. maddelerinde düzenlenen suçları işleyen failler için hem hürriyeti bağlayıcı ceza hem de adlî para cezası öngörülmüştür. Yasa'nın 16. maddesinde yer alan suç için bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezası öngörülmüştür. Yasa'nın 17. maddesinde yer alan suç için ise iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezası öngörülmüştür. TCK'nin 52. maddesinde adlî para cezasının yasada aksine bir hüküm bulunmaması halinde yedi yüz otuz günden fazla olamayacağı belirtildiği için adlî para cezasının gün sayısının tespitinde üst sınır olarak bu sayı esas alınacaktır.[469]

3.2.5. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

Anayasamızın 41. maddesinde yer alan ailenin korunması ve 58. maddesinde yer alan gençliğin korunması hükümlerinin bir gereği olarak Türkiye'de internetin düzenlenmesi konusunda ilk esaslı düzenleme 2007 yılında yürürlüğe giren, 4/5/2007 tarihli ve 5651 sayılı internet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile yapılmıştır.

Bu Kanun ile belli kişilere internet alanında bazı yükümlülük ve sorumluluklar yüklenmiştir. Kanunda bu kişiler içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcı olarak belirlenmiş ve bu kişiler tek tek tanımlamıştır (Md. 2). Kanunun amacı bu kişiler üzerinden, yani bu kişilere belli yükümlülük ve sorumluluklar yüklenerek, internet ortamında işlenen suçlarla mücadele etmek olarak belirlenmiştir (Md. 1). 5651 sayılı Kanunun yürürlüğe girmesinden önce birçok yazar

[469] Dülger ve Modoğlu, **a.g.e.**, s. 66-71.

internet ortamında yapılan yayınlar ve sorumluluk rejimi hakkında acilen yasal düzenlemeye ihtiyaç bulunduğunu ifade etmiştir.[470]

Bilgilendirme yükümlülüğü "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" 3.maddesinde düzenlenmiştir. Ticari veya ekonomik amaçlı içerik sağlayıcılar, yer sağlayıcıları ve erişim sağlayıcılar, tanıtıcı bilgilerini, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür. Belirtilen yükümlülüğü yerine getirmeyen içerik, yer veya erişim sağlayıcısına Başkanlık tarafından iki bin Yeni Türk Lirasından on bin Yeni Türk Lirasına kadar idari para cezası verilir.

Yeni düzenleme ile ilgili maddeye 3. fıkra eklenmiş ve "Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir." şeklinde bir hüküm getirilmiştir. Bu madde ile bilgilendirme yükümlülüğü açısından BTK'ye bir kolaylık sağlanmış ve içerik, yer ve erişim sağlayıcılara madde metninde belirtilen yollar ile bildirim yapılabileceği hükme bağlanmıştır. Bu noktada, ilgili kişinin bildirimden haberdar olup olmadığı konusu gündeme gelecektir. Nitekim bildirimin muhatabına yapılmasının amacı, muhatabın bildiriden haberdar edilerek aksiyon almasını sağlamaktır. Bildirimin doğru bir şekilde muhatabına ulaşmaması hak kaybına yol açabilecektir. Dolayısıyla özellikle "ve benzeri kaynaklardan" ile "diğer iletişim araçları" şeklindeki ibarelerin açık olması ve bu şekilde ilgililerin hangi yollardan kendilerine bildirim yapılacağını bilmeleri gerekmektedir. [471]

Kanunun genel yaklaşımı internet alanında sorumluluk esaslarını belirleme şeklinde sübut bulmuştur. 5651 sayılı Kanun, interneti cezai, idari ve hukuksal sorumluluk açısından düzenleyen bir kanundur. Kanun ile cezai, idari ve hukuksal sorumluluğun internetteki aktörleri belirlenmiştir. Diğer taraftan, cezai sorumlulukla ilgili olarak internet servis sağlayıcılarını muhatap alan birkaç siber suç ve bir

[470] Söyler, Yasin, ***Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi***, Yayımlanmamış Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2013, s. 261.
[471] Dülger ve Modoğlu, **a.g.e.**, s. 121.

koruma tedbiri olarak erişimin engellenmesi tedbiri; idari sorumlulukla ilgili olarak bazı idari para cezaları ve bir idari tedbir olarak erişimin engellenmesi tedbiri; hukuksal sorumlulukla ilgili olarak ise kişilik haklarını ihlal eden içeriğin yayından çıkarılması ve cevap hakkı müessesesi düzenlenmiştir. Bu nedenle Kanunun ceza hukuku ile ilgili bir boyutu bulunduğu gibi, idare hukuku ve medeni hukuk ile ilgili bir boyutu da bulunmaktadır. Kanun, bu özelliğinden dolayı doktrinde kimi yazarlarca "sui generis" bir kanun olarak nitelendirilmiştir.

5651 sayılı Kanun özel bir ceza kanunu niteliği taşımamaktadır. Kural olarak bu Kanun ile suç ve ceza tanımlaması yapılmamıştır. Ancak, Kanun İçel'in de belirttiği gibi ceza sorumluluğunun belirlenmesinde yardımcı bir kaynak olarak değerlendirilebilir. Örneğin, içerik sağlayıcı, erişim sağlayıcı ve yer sağlayıcı tanımlamaları kişilerin ceza sorumluluğunun belirlenmesinde göz önünde bulundurulması gereken önemli bir husustur ve bu tanımlamalar 5651 sayılı Kanun ile yapılmıştır. 5651 sayılı Kanun internete özgü sadece iki tane suç oluşturmuştur. Bunun dışında bu Kanun ile başka bir bilişim suçu öngörülmemiştir. Zaten bu Kanunun amacı bilişim suçlarını düzenlemek de değildir. 1. maddede Kanunun amacı, "internet ortamında işlenen suçlarla içerik, yer ve erişim sağlayıcılar üzerinden mücadele" olarak; bir diğer deyişle "suç unsuru içeren internet siteleri ile mücadele" olarak belirlenmiştir.

5651 sayılı Kanuna doktrinde birçok eleştiri yöneltilmektedir. Kanunun geneline yönelik olarak bir sansür yasası olduğu ve ifade hürriyetini Anayasaya aykırı bir şekilde sınırlandırdığı ileri sürülmektedir. Bu görüşün karşısında yer alan görüş ise 5651 sayılı Kanunun internet alanında kişilerin sorumluluklarını belirlemesi ve erişimin engellemesi nedenlerini tek tek sayması ve sınırlandırması yönü ile demokratik açıdan ileri düzeyde bir kanun olduğunu savunmaktadır. Bu görüşü savunan yazarlar özellikle çoğu Batı ülkesinde erişimi engelleme nedenlerinin özel olarak ve sınırlı sayıda belirlenme yerine, genel kanun hükümlerine ve sınırsız nedenlere dayanılarak yapıldığını ileri sürmektedir.[472]

BTK tarafında internet üzerinde yapılacak izleme, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun 10. maddesinin dördüncü fıkrasında düzenlenmiştir. Buna göre BTK, internet ortamında yapılan yayınların içeriklerini

[472] Söyler, **a.g.e.**, s. 262-263.

izleyerek, bu Kanun kapsamına giren suçların işlendiğinin tespiti halinde, bu yayınlara erişimin engellenmesine yönelik olarak bu Kanunda öngörülen tedbirleri alma (b bendi), internet ortamında yapılan yayınların içeriklerinin izlenmesinin hangi seviye, zaman ve şekilde yapılacağını belirleme (c bendi), internet ortamındaki yayınların izlenmesi suretiyle Kanunun 8. maddesinin birinci fıkrasında sayılan suçların işlenmesini önlemek için izleme ve bilgi ihbar merkezi dâhil, gerekli her türlü teknik altyapıyı kurma veya kurdurma, bu altyapıyı işletme veya işletilmesini sağlama (d bendi) ve internet ortamında herkese açık çeşitli servislerde yapılacak filtreleme, perdeleme ve izleme esaslarına göre donanım üretilmesi veya yazılım yapılmasına ilişkin asgari kriterleri belirleme (e bendi) yetkisini haiz kılınmıştır. Bu düzenlemeler BTK'ye geniş bir çerçevede internet iletişimini izleme yetkisi vermektedir.

BTK'nin, bu düzenlemelere dayanarak kişisel haberleşme niteliğindeki "e-posta" ve "Facebook" gibi sosyal paylaşım siteleri üzerinden yapılan iletişimi de izleyebileceği ileri sürülmekte ve bu husus eleştirilmektedir. Ancak, BTK'ye internet iletişiminin izlenmesi açısından verilen bu yetki kişisel iletişimin izlenmesine ilişkin bir yetki değildir. 5651 sayılı Kanunda "internet ortamı" kavramı tanımlanırken "haberleşme", kavramın kapsamı dışında bırakılmıştır. Haberleşme kavramı, hem internet dışında kalan hem de internet ortamında yapılan kişisel haberleşmeyi kapsamaktadır. Bu durumda örneğin, "msn" üzerinden yapılan bir görüşme veya e-mail ile yapılan haberleşme, 5651 sayılı Kanun kapsamında internet ortamını ifade etmeyeceği için bu tür kişisel haberleşmeler üzerinde izleme yapılması 5651 sayılı Kanun kapsamında mümkün değildir.

5651 sayılı Kanun kapsamında BTK'nin internet iletişimini izlemesi kişisel haberleşme dışında kalan herkese açık internet ortamında gerçekleştirilebileceği için bu izlemenin, önleme amaçlı internet iletişiminin denetlenmesi olarak düşünülmesi mümkün değildir. Zaten bu alan herkese açıktır ve kişisel haberleşme niteliğinde değildir. Bu nedenle BTK, suçların tespiti ve takibi açısından herkese açık olan internet iletişimini izleyebilir; hatta izlemesi gerekir.[473]

[473] Söyler, **a.g.e.**, s. 156-157.

3.2.6. 6518 Sayılı Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun

6518 Sayılı Kanunla 5651 Sayılı 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda bazı değişiklikler yapılmıştır. Bunlardan ilki; 5651 sayılı Kanunun 2. Maddesine yapılan tanım ekleridir.

Bunlar şu şekildedir:

"n) (Ek: 6/2/2014-6518/85 md.) Birlik: Erişim Sağlayıcıları Birliğini,

o) (Ek: 6/2/2014-6518/85 md.) Erişimin engellenmesi: Alan adından erişimin engellenmesi, IP adresinden erişimin engellenmesi, içeriğe (URL) erişimin engellenmesi ve benzeri yöntemler kullanılarak erişimin engellenmesini,

ö) (Ek: 6/2/2014-6518/85 md.) İçeriğin yayından çıkarılması: İçerik veya yer sağlayıcılar tarafından içeriğin sunuculardan veya barındırılan içerikten çıkarılmasını,

p) (Ek: 6/2/2014-6518/85 md.) URL adresi: İlgili içeriğin internette bulunduğu tam internet adresini,

r) (Ek: 6/2/2014-6518/85 md.) Uyarı yöntemi: İnternet ortamında yapılan yayın içeriği nedeniyle haklarının ihlal edildiğini iddia eden kişiler tarafından içeriğin yayından çıkarılması amacıyla öncelikle içerik sağlayıcısına, makul sürede sonuç alınamaması hâlinde yer sağlayıcısına iletişim adresleri üzerinden gerçekleştirilecek bildirim yöntemini, ifade eder."[474]

6518 sayılı Kanunun 85. Maddesiyle 5651 sayılı Kanunun 2. Maddesinde bulunan tanımlara birlik, erişimin engellenmesi, içeriğin yayından kaldırılması, URL adresi, uyarı yöntemi tanımları eklenmiştir.

6518 sayılı Kanunun 86. Maddesiyle 5651 sayılı Kanunun Bilgilendirme Yükümlülüğünün bulunduğu 3. Maddeye, *"Bu Kanun kapsamındaki faaliyetleri yurt içinden ya da yurt dışından yürütenlere, internet sayfalarındaki iletişim araçları, alan adı, IP adresi ve benzeri kaynaklarla elde edilen bilgiler üzerinden elektronik posta veya diğer iletişim araçları ile bildirim yapılabilir."*[475] Şeklinde 3. Fıkra eklenmiştir.

---

[474] "Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun", **Resmi Gazete**, Kanun No: 6518, Sayı: 28918, 19 Şubat 2014, s. 22, (Erişim) http://www.resmigazete.gov.tr/eskiler/2014/02/20140219.pdf, 25.01.2017.

[475] Aynı.

87. Maddeyle 5651 sayılı Kanunun 4. Maddesine aşağıdaki fıkra eklenmiştir. *"(3) İçerik sağlayıcı, Başkanlığın bu Kanun ve diğer kanunlarla verilen görevlerinin ifası kapsamında; talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim eder ve Başkanlıkça bildirilen tedbirleri alır."*

Madde 88'de 5651 sayılı Kanunun 5 inci maddesinin ikinci fıkrası aşağıdaki şekilde değiştirilmiş ve aynı maddeye aşağıdaki fıkralar eklenmiştir.[476]

"(2) Yer sağlayıcı, yer sağladığı hukuka aykırı içeriği bu Kanunun 8 inci ve 9 uncu maddelerine göre haberdar edilmesi hâlinde yayından çıkarmakla yükümlüdür.

"(3) Yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür.

(4) Yer sağlayıcılar, yönetmelikle belirlenecek usul ve esaslar çerçevesinde yaptıkları işin niteliğine göre sınıflandırılabilir ve hak ve yükümlülükleri itibarıyla farklılaştırılabilirler.

(5) Yer sağlayıcı, Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla yükümlüdür.

(6) Yer sağlayıcılık bildiriminde bulunmayan veya bu Kanundaki yükümlülüklerini yerine getirmeyen yer sağlayıcı hakkında Başkanlık tarafından on bin Türk Lirasından yüz bin Türk Lirasına kadar idari para cezası verilir."

Yapılan bu değişikliklerle yer sağlayıcıların yükümlülüklerinin sınırları belirlenmiştir.

6518'in 89. Maddesiyle ise, 5651 sayılı Kanunun 6. maddesinin 1. fıkrasının (a) bendindeki *"ve teknik olarak engelleme imkânı bulunduğu ölçüde"* ibaresi çıkartılmış, aynı fıkraya aşağıdaki (ç) ve (d) bentleri eklenmiş, üçüncü fıkrasında geçen "(b) ve (c)" ibaresi "(b), (c), (ç) ve (d)" şeklinde değiştirilmiştir.

"ç) Erişimi engelleme kararı verilen yayınlarla ilgili olarak alternatif erişim yollarını engelleyici tedbirleri almakla,

d) Başkanlığın talep ettiği bilgileri talep edilen şekilde Başkanlığa teslim etmekle ve Başkanlıkça bildirilen tedbirleri almakla,"[477]

Böylece erişim sağlayıcının yükümlülüklerine yukarıda belirtilen yükümlülükler eklenmiş ve 10.000 ile 50.000 Türk Lirası idari para cezasının verilebileceği durumlar genişletilmiştir.

[476] **Resmi Gazete**, Kanun No: 6518, **a.g.e.**, s. 23.
[477] **Resmi Gazete**, Kanun No: 6518, **a.g.e.**, s. 23.

90. Maddeyle 5651 sayılı Kanunun 6. maddesinden sonra gelmek üzere 6/A maddesi eklenmiştir. Bu maddeyle erişimin engellenmesi kararlarının uygulanmasını sağlamak üzere Erişim Sağlayıcıları Birliği kurulmuş ve birlikle ilgili amacından faaliyet alanına kadar uzanan bütün düzenlemeler belirlenmiştir.

Toplu kullanım sağlayıcıların yükümlülüklerinin belirlendiği 5651'in 7. Maddesine 6518'in 91. Maddesiyle eklenen fıkralarla internet aracılığıyla gerçekleştirilen suçların önüne geçmek amaçlanmıştır.

"(2) Ticari amaçla olup olmadığına bakılmaksızın bütün internet toplu kullanım sağlayıcılar, konusu suç oluşturan içeriklere erişimin engellenmesi ve kullanıma ilişkin erişim kayıtlarının tutulması hususlarında yönetmelikle belirlenen tedbirleri almakla yükümlüdür.

(3) Ticari amaçla toplu kullanım sağlayıcılar, ailenin ve çocukların korunması, suçun önlenmesi ve suçluların tespiti kapsamında usul ve esasları yönetmelikte belirlenen tedbirleri almakla yükümlüdür.

(4) Bu maddede belirtilen yükümlülükleri ihlal eden ticari amaçla toplu kullanım sağlayıcılarına, ihlalin ağırlığına göre yönetmelikle belirlenecek usul ve esaslar çerçevesinde uyarma, bin Türk Lirasından on beş bin Türk Lirasına kadar idari para cezası verme veya üç güne kadar ticari faaliyetlerini durdurma müeyyidelerinden birine karar vermeye mahalli mülki amir yetkilidir."[478]

6518'in 92. Maddesiyle; 5651 sayılı Kanunun 8. Maddesinin 2. fıkrasının 4. cümlesinden sonra gelmek üzere *"Erişimin engellenmesi kararı, amacı gerçekleştirecek nitelikte görülürse belirli bir süreyle sınırlı olarak da verilebilir."* cümlesi eklenmiş, dördüncü fıkrasında yer alan "(2) ve (5)" ibaresi "(2), (5) ve (6)" şeklinde değiştirilmiş, onuncu fıkrasındaki *"altı aydan iki yıla kadar hapis cezası"* ibaresi *"beş yüz günden üç bin güne kadar adli para cezası"* şeklinde değiştirilmiştir.

5651 sayılı Kanunun 9. Maddesinin başlığı "İçeriğin yayından çıkarılması ve cevap hakkı" iken 6518 sayılı Kanunun 93 üncü maddesiyle "İçeriğin yayından çıkarılması ve erişimin engellenmesi" şeklinde değiştirilmiştir. Başlıkla birlikte değiştirilen madde ve fıkraları şu şekildedir:

"MADDE 9 – (1) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden gerçek ve tüzel kişiler ile kurum ve kuruluşlar, içerik sağlayıcısına, buna ulaşamaması hâlinde yer sağlayıcısına başvurarak uyarı yöntemi ile içeriğin yayından çıkarılmasını isteyebileceği gibi doğrudan sulh ceza hâkimine başvurarak içeriğe erişimin engellenmesini de isteyebilir.

(2) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini iddia eden kişilerin talepleri, içerik ve/veya yer sağlayıcısı tarafından en geç yirmi dört saat içinde cevaplandırılır.

[478] **Resmi Gazete**, Kanun No: 6518, **a.g.e.**, s. 24.

(3) İnternet ortamında yapılan yayın içeriği nedeniyle kişilik hakları ihlal edilenlerin talepleri doğrultusunda hâkim bu maddede belirtilen kapsamda erişimin engellenmesine karar verebilir.

(4) Hâkim, bu madde kapsamında vereceği erişimin engellenmesi kararlarını esas olarak, yalnızca kişilik hakkının ihlalinin gerçekleştiği yayın, kısım, bölüm ile ilgili olarak (URL, vb. şeklinde) içeriğe erişimin engellenmesi yöntemiyle verir. Zorunlu olmadıkça internet sitesinde yapılan yayının tümüne yönelik erişimin engellenmesine karar verilemez. Ancak, hâkim URL adresi belirtilerek içeriğe erişimin engellenmesi yöntemiyle ihlalin engellenemeyeceğine kanaat getirmesi hâlinde, gerekçesini de belirtmek kaydıyla, internet sitesindeki tüm yayına yönelik olarak erişimin engellenmesine de karar verebilir.

(5) Hâkimin bu madde kapsamında verdiği erişimin engellenmesi kararları doğrudan Kuruma gönderilir.

(6) Hâkim bu madde kapsamında yapılan başvuruyu en geç yirmi dört saat içinde duruşma yapmaksızın karara bağlar. Bu karara karşı 4/12/2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre itiraz yoluna gidilebilir.

(7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır.

(8) Birlik tarafından erişim sağlayıcıya gönderilen içeriğe erişimin engellenmesi kararının gereği derhâl, en geç dört saat içinde erişim sağlayıcı tarafından yerine getirilir.

(9) Bu madde kapsamında hâkimin verdiği erişimin engellenmesi kararına konu kişilik hakkının ihlaline ilişkin yayının veya aynı mahiyetteki yayınların başka internet adreslerinde de yayınlanması durumunda ilgili kişi tarafından Kuruma müracaat edilmesi hâlinde mevcut karar bu adresler için de uygulanır.

(10) Sulh ceza hâkiminin kararını bu maddede belirtilen şartlara uygun olarak ve süresinde yerine getirmeyen sorumlu kişi, beş yüz günden üç bin güne kadar adli para cezası ile cezalandırılır."[479]

Yapılan değişiklikle içeriğin yayından kaldırılması ve erişimin engellenmesi için yapılacaklar belirlenmiş, izlenecek yol çizilmiş, konuyla ilgili kararı uygulamada sorumlulukları yerine getirmeyenlere verilecek cezalar belirlenmiştir.

6518 sayılı Kanunun 94. Maddesiyle 5651 sayılı Kanunun 9. Maddesinden sonra gelmek üzere 9/A Maddesi eklenmiştir. "özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi" başlığını taşıyan Madde 8 fıkradan oluşmaktadır.

5651 sayılı Kanunun 10. maddesinin 4. fıkrasının (a) bendinde yer alan "yayınları önlemeye" ibaresinden sonra ", internetin güvenli kullanımını sağlamaya, bilişim şuurunu geliştirmeye" ibaresi eklenmiş, 5. fıkrası aşağıdaki şekilde değiştirilmiş, maddeye aşağıdaki fıkralar eklenmiştir.

"*(5) Başkanlık; Bakanlık bünyesinde 26/9/2011 tarihli ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname hükümleri uyarınca oluşturulan İnternet Geliştirme Kurulunca internetin yaygınlaştırılması, geliştirilmesi, yaygın ve güvenli*

[479] **Resmi Gazete**, Kanun No: 6518, **a.g.e.**, s. 24-25.

kullanılması gibi konularda yapılacak öneriler ile ilgili gerekli her türlü tedbir veya kararları alır.

(6) Kurum, ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar.

(7) Kurum kanunlarla kendisine verilen görevlerin ifası amacıyla araştırma ve geliştirme merkezleri kurabilir."[480]

5651 sayılı Kanunun 11. Maddesinin 2. fıkrasında yer alan *"yer veya erişim sağlayıcı olarak faaliyet icra etmesi amacıyla yetkilendirme belgesi verilmesine"* ibaresi *"yer, erişim ve toplu kullanım sağlayıcıların yükümlülüklerine"* şeklinde değiştirilmiştir.

3.2.7. 6527 Sayılı Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun

6518 Sayılı Kanunla 5651 Sayılı 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunda bazı değişiklikler yapılmıştır. Bunlardan ilki; 5651 sayılı Kanunun 2. Maddesine j bendinde tanımlaman trafik bilgisi tanımının değiştirilmesi şeklindedir.

"j) (Değişik: 26/2/2014-6527/15 md.) Trafik bilgisi: Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,"

6527 sayılı Kanunun 17. Maddesiyle 5651 sayılı Kanunun 8. Maddesinin 15. Bendi *"Bu maddeye göre soruşturma aşamasında verilen hâkim kararı ile 9 uncu ve 9/A maddesine göre verilen hâkim kararı birden fazla sulh ceza mahkemesi bulunan yerlerde Hâkimler Savcılar Kurulu tarafından belirlenen sulh ceza mahkemeleri tarafından verilir."*şeklinde düzenlenmiştir.

6518 sayılı Kanunun 94. Maddesiyle 5651 sayılı Kanunun 9. Maddesinden sonra gelmek üzere eklenen 9/A Maddesi eklenmiştir. *"Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi"* başlığını taşıyan Maddeye *"Bu maddenin sekizinci fıkrası kapsamında Kurum tarafından verilen erişimin engellenmesi kararı, Başkanlık tarafından, yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar."* İfadesiyle 9. Fıkra eklenmiştir.

[480] **Resmi Gazete**, Kanun No: 6518, **a.g.e.**, s. 25.

3.2.8. 6698 Sayılı Kişisel Verilerin Korunması Hakkında Kanun

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun "Amaç" başlıklı 1. maddesinde Kanun ile elde edilmesi umulan amaç belirtilmiştir. Buna göre Kişisel Verilerin Korunması Kanunu'nun amacı, *"kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir."* Maddenin gerekçesinde, maddeyle Kanun'un amacının belirlendiği, bu amacın, kişisel verilerin işlenmesinin disiplin altına alınması ve Anayasa'da öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunması olduğu belirtilmiştir. Gerekçede ayrıca, Kanun ile son yıllarda önem kazanan kişinin mahremiyet hakkı ile bilgi güvenliği hakkının korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasların düzenlenmesinin amaçlandığı belirtilmiştir.

Kişisel Verilerin Korunması Kanunu'nun "Kapsam" başlıklı 2. maddesinde Kanun'un kapsamı düzenlenmiştir. Buna göre Kişisel Verilerin Korunması Kanunu *"kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanır."* Kanunun gerekçesinde de belirtildiği gibi, Kanun, kişisel verileri işlenen gerçek kişiler ile bu verileri işleyen gerçek ve tüzel kişiler hakkında uygulanacaktır. Kanunun uygulaması bakımından kamu ve özel sektör ayrımı yapılmamış olup, düzenlenen usul ve esaslar her iki sektör bakımından da uygulama alanı bulmaktadır. Kanun, kişisel verilerin otomatik veya herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesi durumunda uygulanacaktır.

Kişisel verilerin korunmasına ilişkin düzenlemelerde, verilerle ilgili yapılan işlemlerin insan onuru ve değerlerine uygun yapılması maksadıyla bazı ortak ilkeler belirlenmiştir. Bu ilkelerin birbirinden kesin çizgilerle ayrılması zordur. Bazı ilkeler diğerlerine kaynaklık ederken bazıları da tamamlayıcı rol oynamaktadır. Bu ilkelere riayet edilmemesi durumunda kişisel verilerin iyi niyetle, hukuka uygun olarak işlenmediği, ortada bir kötüye kullanımın bulunduğu kabul edilmektedir. Kişisel verilerin işlenmesi ile ilgili genel ilkeler Kişisel Verilerin Korunması Kanunu'nun 4. maddesinde yer almaktadır. Maddenin birinci fıkrasında kişisel verilerin ancak

Kanunda ve diğer Kanunlarda öngörülen usul ve esaslar çerçevesinde işlenebileceği belirtildikten sonra ikinci fıkrada kişisel verilerin işlenmesi ile ilgili ilkeler sayılmıştır. Bu ilkeler;

- Hukuka ve dürüstlük kurallarına uygun olma,
- Doğru ve gerektiğinde güncel olma,
- Belirli, açık ve meşru amaçlar için işlenme,
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma ve
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmedir.

Kişisel Verilerin Korunması Kanunu'nun 5. maddesinde kişisel verilerin işlenme koşulları düzenlenmiştir. Maddeye göre kural olarak kişisel verilerin ilgili kişinin açık rızasının bulunduğu durumlar veya maddede sayılan istisnalar dışında işlenmesi yasaktır.

Kişisel Verilerin Korunması Kanunu'nun 6. Maddesinde, kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri, özel nitelikli kişisel veri olarak sınıflandırılmıştır. Kanundaki düzenlemeye göre, özel nitelikli kişisel verilerin, ilgili kişinin açık rızası olmaksızın işlenmesi yasaktır.

Kişisel Verilerin Korunması Kanunu'nun 7. Maddesiyle, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi düzenlenmektedir. Buna göre, hukuka uygun olarak işlenmiş kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması durumunda, bu kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinecek, yok edilecek veya anonim hale getirilecektir.[481]

Veri sorumlusunun kişisel verilerin güvenliklerine ilişkin yükümlülükleri Kişisel Verilerin Korunması Kanunu'nun 12. maddesinde düzenlenmiştir. Maddeye göre veri sorumlusu, kişisel verilerin hukuka aykırı olarak işlenmesini ve verilere hukuka aykırı olarak erişilmesini önlemek, ayrıca verilerin muhafazasını sağlamak

[481] Turan, Metin, "Kişisel Verilerin Korunması", **Türkiye Kalkınma Bankası Yayını e-dergi**, Nisan- Haziran 2016, s. 4-5.

için uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Kişisel Verilerin Korunması Kanunu'nun 17. maddesinde, kişisel verilere ilişkin suçlar ve cezai yaptırımlar için 5237 sayılı Türk Ceza Kanunu'nun ilgili hükümlerine atıf yapılmaktadır. Maddenin ikinci fıkrasında, kişisel verileri silmeyen veya anonim hale getirmeyenlerin ise Türk Ceza Kanunu'nun 138. maddesi hükmü uyarınca cezalandırılmaları gerektiği düzenlenmiştir.

Kişisel Verilerin Korunması Kanunu'nun 19. maddesinde, Kanun'un verdiği görevleri yerine getirmek üzere kurulan, idari ve mali özerkliğe sahip, kamu tüzel kişiliğini haiz Kişisel Verileri Koruma Kurumunun kuruluşu düzenlenmektedir.

Kişisel Verilerin Korunması Kanunu'nun 28. maddesinde Kanun kapsamı dışında tutulan hususlar düzenlenmektedir. Maddenin birinci fıkrasında tamamen Kanun kapsamı dışında tutulan hususlar düzenlenmektedir. Maddenin düzenlemesine göre kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla, gerçek kişiler tarafından kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetleri kapsamında; resmi istatistik ile anonim hale getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında, milli savunmayı, milli güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında, soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi, Kanun'un tamamen kapsamı dışında tutulmuştur.[482]

[482] Korkmaz, **a.g.e.**, s.146.

DÖRDÜNCÜ BÖLÜM

İNTERNET SUÇLARINA İLİŞKİN ARAŞTIRMA YÖNTEMLERİ VE BULGULARIN ANALİZİ

Bu bölümde internet suçlarına ilişkin oluşturulan araştırma modeline, araştırma grubuna, çalışmada kullanılan veri toplama araçlarına, elde edilen verilerin analizinde kullanılan yöntem ve tekniklere yer verilmiştir.

4.1. ARAŞTIRMA YÖNTEMİ

Araştırma modeli olarak kişilerin internet suçlarına ilişkin görüşlerinin demografik bilgilerine göre farklılaşıp farklılaşmadığını test etmek amacıyla betimsel ve ilişkisel tarama modeli tercih edilmiştir. Betimsel ve ilişkisel tarama modeli sayesinde, katılımcıların verdikleri yanıtların betimlenmesi ve birbiriyle ilişkilendirilerek anlamlı bütünler haline getirilebilmesi mümkün olacaktır.

Böylece ankete katılım sağlayan bireylerin demografik özellikleri doğrultusunda internet suçlarına karşı algılarını ölçmek mümkün olacak, ulaşılan verilerden hareketle toplumun geneli hakkında bir kestirim yapabilme imkânı doğacaktır. Ayrıca internette meydana gelme olasılığı bulunan suça maruz kalma riskinden bireylerin korunmak adına ne gibi önlemler aldıkları konusunda fikir sahibi olunabilecektir.

4.2. VERİ TOPLAMA ARAÇLARI

Bu araştırmada veri toplama yöntemi olarak anket tekniği kullanılmıştır. İki bölümden oluşan bir anket formu geliştirilmiştir. Birinci bölümde anket katılımcılarının demografik özelliklerini belirleyici sorular, ikinci bölümde de internet algılarını ölçmeye yönelik sorular yer almaktadır. Bu bölümdeki sorularda temel amaç; katılımcıların internet suçlarına ilişkin algılarını ölçmektir. Bu amaçla araştırmada katılımcılara çeşitli ifadelere “Kesinlikle katılmıyorum, Katılmıyorum,

Kararsızım, Katılıyorum, Kesinlikle Katılıyorum" diyerek katılıp katılmadıkları sorulmuştur. Katılımcılara yöneltilen ifadeler şunlardır;

1. "İnternette alışveriş yapmaktan korkuyorum",
2. "Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum",
3. "İnternette sürekli gözetim altında olduğumu hissediyorum",
4. "Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum",
5. "Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum",
6. "Reklam çıkan siteleri bir daha kullanmıyorum",
7. "Kimlik bilgilerimi isteyen sitelerden uzak duruyorum",
8. "Kendimi güvendiğim siteler ile sınırlandırıyorum",
9. "İnternetten herhangi bir indirme işlem yapmıyorum",
10. "İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum".

Yukarıda belirtilen ifadelere katılımcıların verdikleri yanıtlar, demografik deşikenler doğrultusunda analize tabi tutulmuştur.

Cronbach alpha iç tutarlılık katsayısı 0.787 olarak bulunmuş olup, buna göre ölçeğin oldukça güvenilir olduğu tespit edilmiştir (Tablo 4).

Tablo 4. Güvenilirlik testi sonuçları

Cronbach's Alpha	N of Items
,787	10

4.3. BULGULARIN ANALİZİ

Araştırmada elde edilen veriler IBM SPSS 21 paket programı aracılığıyla istatistiki test ve analizler uygulanarak çözümlenmiştir. Çözümlenen veriler söz konusu istatistiksel test ve analizlerin bilimsel gerektirimleri doğrultusunda değerlendirilerek raporlanmıştır.

Araştırma bulgularının analizi aşamasına geçmeden önce verilerin dağılımının normal dağılımdan farklı olup olmadığı sınanmıştır. Kolmogorov-Smirnov test sonucuna göre veriler normal dağılıma uymaktadır (Tablo 5).

Tablo 5. Normallik testi sonuçları

	Soru 1	Soru 2	Soru 3	Soru 4	Soru 5	Soru 6	Soru 7	Soru 8	Soru 9	Soru 10
N	483	483	483	483	483	483	483	483	483	483
Kolmogorov-Smirnov Z	0,753	0,613	0,667	0,731	0,586	0,667	0,753	0,667	0,731	0,500
Asymp. Sig. (2-tailed)	0,623	0,847	0,765	0,659	0,882	0,768	0,627	0,765	0,659	0,800

Hedeflenen örnekleme ulaşıldığı da göz önünde bulundurulduğunda parametrik analizler uygulanması için gerekli varsayımlar sağlanmıştır. Verilerin analizinde kullanılan yöntemler aşağıdaki gibidir:

Bağımsız Örnekler T-Testi: İki aritmetik ortalama arasındaki farkın manidarlığını test etmede kullanılan parametrik bir analizdir.

Tek Yönlü Varyans analizi: İki ya da daha fazla ortalama arasında fark olup olmadığı ile ilgili önermeyi test etmek amacıyla kullanılan parametrik bir testtir.

4.4. DEMOGRAFİK BİLGİLERİN DAĞILIMI

Demografik bilgiler katılımcıların özelliklerini ortaya koymada kullanılan sorulardan oluşmakta ve Tablo 6'da görülmektedir.

Tablo 6'da da görüldüğü üzere çalışma doğrultusunda 483 kişi üzerinde gerçekleştirilen araştırmada, katılımcıların % 57'si kadın, % 43'ü erkeklerden oluşmaktadır.

Katılımcıların yaş dağılımlarına bakıldığında 18-25 yaş arası katılımcıların oranı %52, 26 yaş ve üzerinde olan katılımcıların oranı %48 olup yoğunlukları birbirine yakındır.

Katılımcıların günlük internet kullanım sürelerine bakıldığında, 3-5 saat günlük internet kullanımının % 52'lik oranla ilk sırada yer aldığı görülürken, 8+ saat günlük

internet kullananlar ise % 13'lük oranla son sırada olduğu görülmektedir. Günlük internet kullanım sıklığının daha çok 3 saat ile 8 saat aralığında değiştiği dikkat çekmektedir.

Tablo 6. Katılımcıların demografik bilgilerinin dağılımı

		n	%
Cinsiyet	Kadın	273	57%
	Erkek	210	43%
Yaş	18-25 yaş	249	52%
	26 ve üzeri yaş	234	48%
Eğitim Düzeyi	Lisans	261	54%
	Lisansüstü	222	46%
İnternet Kullanım Süresi	4-6 yıl	78	16%
	7-10 yıl	225	47%
	11-15 yıl	180	37%
Günlük İnternet Kullanım Süresi	1-2 saat	72	15%
	3-5 saat	252	52%
	6-8 saat	96	20%
	8+ saat	63	13%
İnternet Suçuna Maruz Kalma Durumu	Evet	57	12%
	Hayır	426	88%
İnternette sınırsız özgürlük olmalı mı?	Evet	99	20%
	Hayır	384	80%
İnternet suçları ile kişilik hakları ihlallerine karşı tüm dünyada geçerli ve uygulanabilir hukuk kuralları olmalı mı?	Evet	483	100%
	Hayır	0	0%
Bu konuda uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunabilir mi?	Evet	378	78%
	Hayır	105	22%
	Toplam	483	100%

İnternet kullanıcılarının sadece % 12'si yani 57 kişi internet suçuna maruz kalmıştır. 483 katılımcının 384'ü internette sınırsız özgürlük olmasına karşı çıkarken, 99'u internette sınırsız özgürlüğün olması gerektiği görüşündedir.

İnternet suçları ile kişilik hakları ihlallerine karşı tüm dünyada geçerli ve uygulanabilir hukuk kurallarının olması gerekliliği konusunda bütün katılımcılar, olumlu yönde görüş beyan etmişlerdir. Uluslararası uzlaşma sağlanmasının suçlarla mücadelede başarıyı etkileyip etkilemeyeceği yönündeki soruya 378 kişi olumlu yanıt verirken, 105 kişi olumsuz görüş bildirmiştir.

4.5. İNTERNET KULLANIMINA İLİŞKİN İFADELERİN İNCELENMESİ

Araştırmada kullanılan ve aşağıda sıralanan ifadeler katılımcıların anket sonucu ortaya çıkan özellikleri doğrultusunda incelenmiştir.

1. "İnternette alışveriş yapmaktan korkuyorum",
2. "Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum",
3. "İnternette sürekli gözetim altında olduğumu hissediyorum",
4. "Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum",
5. "Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum",
6. "Reklam çıkan siteleri bir daha kullanmıyorum",
7. "Kimlik bilgilerimi isteyen sitelerden uzak duruyorum",
8. "Kendimi güvendiğim siteler ile sınırlandırıyorum",
9. "İnternetten herhangi bir indirme işlem yapmıyorum",
10. "İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum".

Bu ifadeler katılımcıların; cinsiyetine, yaşına, eğitim düzeyine, internet kullanım süresine, günlük internet kullanım süresine, internet suçuna maruz kalma durumuna, internette sınırsız özgürlüğe bakış açısına ve suçlarla mücadeleye bakış açısına göre ayrı ayrı incelenmiştir.

4.5.1. İfadelerin Cinsiyete Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, cinsiyet açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin bağımsız örnekler t-testi sonucu Tablo 7'de sunulmuştur.

"n" ifadesi, araştırmaya katılımcılarının sayısını, "ort" ifadeye yanıt verenlerin incelenen özellikteki ortalamasını, "ss" standart sapmayı, "t" incelenen ifade ile özellik arasında ilişki olup olmadığını, "p" ifadesi ise incelenen ifade ile özellik arasında anlamlı bir fark olup olmadığını göstermektedir. "p" değerinin 0.05

düzeyinden küçük olması farklılığın olduğunu, 0.05 düzeyinden büyük olması ise ifade ile özellik arasında anlamlı bir farklılığın olmadığını gösterir.

Tablo 7. Katılımcıların ifadelere verdiği yanıtların cinsiyete göre incelenmesi

	Cinsiyet	n	ort.	ss.	t	p
İnternette alışveriş yapmaktan korkuyorum	Kadın	273	2,8	1,1	2,075	0,039
	Erkek	210	2,6	1,3		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	Kadın	273	2,8	1,2	4,347	0,000
	Erkek	210	2,3	1,2		
İnternette sürekli gözetim altında olduğumu hissediyorum	Kadın	273	3,3	1,3	0,516	0,606
	Erkek	210	3,3	1,4		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	Kadın	273	2,6	1,0	2,542	0,011
	Erkek	210	2,3	1,1		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	Kadın	273	3,1	1,1	6,357	0,000
	Erkek	210	2,5	1,1		
Reklam çıkan siteleri bir daha kullanmıyorum	Kadın	273	3,1	1,3	3,178	0,002
	Erkek	210	2,8	1,2		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	Kadın	273	4,2	1,0	3,419	0,001
	Erkek	210	3,8	1,2		
Kendimi güvendiğim siteler ile sınırlandırıyorum	Kadın	273	3,4	1,2	3,964	0,000
	Erkek	210	2,9	1,3		
İnternetten herhangi bir indirme işlem yapmıyorum	Kadın	273	1,8	,8	-1,368	0,172
	Erkek	210	1,9	1,1		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	Kadın	273	3,2	1,1	0,491	0,624
	Erkek	210	3,1	1,2		

Tablo 7'ye göre; "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla internette alışveriş yapmaktan korktuğu saptanmıştır.

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı saptanmıştır.

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla reklam çıkan siteleri bir daha kullanmadığı saptanmıştır.

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla kimlik bilgilerini isteyen sitelerden uzak durduğu saptanmıştır.

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Kadınların erkeklere kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır.

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin kadın ve erkekler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

4.5.2. İfadelerin Yaşa Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, yaş açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin bağımsız örnekler t-testi sonucu Tablo 8'de ve yorumu Tablo 8'in altında sunulmuştur.

Tablo 8. Katılımcıların ifadelere verdiği yanıtların yaşa göre incelenmesi

	Yaş	n	ort.	ss.	t	p
İnternette alışveriş yapmaktan korkuyorum	18-25 yaş	249	2,9	1,2	4,102	0,000
	26 ve üzeri yaş	234	2,5	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	18-25 yaş	249	2,8	1,3	5,161	0,000
	26 ve üzeri yaş	234	2,3	1,1		
İnternette sürekli gözetim altında olduğumu hissediyorum	18-25 yaş	249	3,3	1,2	-0,468	0,640
	26 ve üzeri yaş	234	3,3	1,4		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	18-25 yaş	249	2,6	1,1	3,250	0,001
	26 ve üzeri yaş	234	2,3	,9		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	18-25 yaş	249	3,1	1,1	4,204	0,000
	26 ve üzeri yaş	234	2,6	1,1		
Reklam çıkan siteleri bir daha kullanmıyorum	18-25 yaş	249	2,8	1,2	-2,407	0,016
	26 ve üzeri yaş	234	3,1	1,3		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	18-25 yaş	249	4,0	1,0	-0,911	0,363
	26 ve üzeri yaş	234	4,1	1,2		
Kendimi güvendiğim siteler ile sınırlandırıyorum	18-25 yaş	249	3,1	1,2	-0,869	0,385
	26 ve üzeri yaş	234	3,2	1,3		
İnternetten herhangi bir indirme işlem yapmıyorum	18-25 yaş	249	1,8	,9	-0,309	0,758
	26 ve üzeri yaş	234	1,8	1,0		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	18-25 yaş	249	3,3	1,1	2,238	0,026
	26 ve üzeri yaş	234	3,0	1,1		

Tablo 8'e göre; "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla internette alışveriş yapmaktan korktuğu saptanmıştır.

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı saptanmıştır.

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 26 ve üzeri yaş aralığındaki kişilerin, 18-25 yaş aralığındakilerden daha fazla reklam çıkan siteleri bir daha kullanmadığı saptanmıştır.

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p < 0,05$).

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin farklı yaş gruplarındaki kişiler arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla internetini ve bilgisayarını sürekli denetim altında tuttuğu saptanmıştır.

4.5.3. İfadelerin Eğitim Düzeyine Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, eğitim durumu açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin bağımsız örnekler t-testi sonucu Tablo 9'da, sunulmuştur.

Tablo 9'da da görüldüğü gibi, "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla internette alışveriş yapmaktan korktuğu saptanmıştır.

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$). 4-6 yıl kullananın 11-15 yıl kullanana kıyasla daha şüpheci olduğu saptanmıştır.

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla internette sürekli gözetim altında olduğumu hissettiği saptanmıştır.

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür (p > 0,05).

Tablo 9. Katılımcıların ifadelere verdiği yanıtların eğitim düzeyine göre incelenmesi

	Eğitim Düzeyi	n	ort.	ss.	t	p
İnternette alışveriş yapmaktan korkuyorum	Lisans	261	2,9	1,2	3,433	0,001
	Lisansüstü	222	2,5	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	Lisans	261	2,7	1,2	1,856	0,064
	Lisansüstü	222	2,5	1,2		
İnternette sürekli gözetim altında olduğumu hissediyorum	Lisans	261	3,5	1,2	4,650	0,000
	Lisansüstü	222	3,0	1,4		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	Lisans	261	2,6	1,0	2,226	0,026
	Lisansüstü	222	2,4	1,0		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	Lisans	261	2,8	1,1	-1,463	0,144
	Lisansüstü	222	2,9	1,2		
Reklam çıkan siteleri bir daha kullanmıyorum	Lisans	261	3,0	1,3	0,914	0,361
	Lisansüstü	222	2,9	1,2		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	Lisans	261	3,9	1,1	-2,231	0,026
	Lisansüstü	222	4,1	1,1		
Kendimi güvendiğim siteler ile sınırlandırıyorum	Lisans	261	3,2	1,2	0,073	0,942
	Lisansüstü	222	3,2	1,3		
İnternetten herhangi bir indirme işlem yapmıyorum	Lisans	261	2,0	1,1	5,179	0,000
	Lisansüstü	222	1,6	,7		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	Lisans	261	3,1	1,1	-1,820	0,069
	Lisansüstü	222	3,2	1,2		

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür (p > 0,05).

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür (p < 0,05). Lisansüstü mezunlarının, lisans düzeyindekilere kişilere kıyasla daha fazla kimlik bilgilerini isteyen sitelerden uzak durduğu saptanmıştır.

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı saptanmıştır.

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin lisans ve lisansüstü mezunları arasında anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

4.5.4. İfadelerin İnternet Kullanım Süresine Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, internet kullanım süresi açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin tek yönlü varyans analizi sonucu Tablo 10'da sunulmuştur.

Tablo 10'da da görüldüğü üzere "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 4-6 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla internette alışveriş yapmaktan korktuğu saptanmıştır.

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$).

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 4-6 yıl süre ile internet kullanan kişilerin, 11-15

yıl süre ile kullananlara kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 4-6 yıl süre ve 7-10 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

Tablo 10. Katılımcıların ifadelere verdiği yanıtların internet kullanım süresine göre incelenmesi

	İnternet Kullanım Süresi	n	ort.	ss.	F	p
İnternette alışveriş yapmaktan korkuyorum	4-6 yıl	78	3,0	1,2	3,064	0,048
	7-10 yıl	225	2,7	1,1		
	11-15 yıl	180	2,6	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	4-6 yıl	78	3,2	1,2	11,319	0,000
	7-10 yıl	225	2,4	1,2		
	11-15 yıl	180	2,5	1,2		
İnternette sürekli gözetim altında olduğumu hissediyorum	4-6 yıl	78	3,2	1,2	1,796	0,167
	7-10 yıl	225	3,2	1,3		
	11-15 yıl	180	3,4	1,3		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	4-6 yıl	78	2,8	1,2	11,062	0,000
	7-10 yıl	225	2,3	1,0		
	11-15 yıl	180	2,6	,9		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	4-6 yıl	78	3,3	1,3	7,575	0,001
	7-10 yıl	225	2,7	1,1		
	11-15 yıl	180	2,8	1,1		
Reklam çıkan siteleri bir daha kullanmıyorum	4-6 yıl	78	2,9	1,2	1,457	0,234
	7-10 yıl	225	2,9	1,3		
	11-15 yıl	180	3,1	1,2		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	4-6 yıl	78	4,1	,8	0,089	0,915
	7-10 yıl	225	4,0	1,0		
	11-15 yıl	180	4,0	1,2		
Kendimi güvendiğim siteler ile sınırlandırıyorum	4-6 yıl	78	3,5	1,1	3,284	0,038
	7-10 yıl	225	3,1	1,3		
	11-15 yıl	180	3,2	1,2		
İnternetten herhangi bir indirme işlem yapmıyorum	4-6 yıl	78	1,8	,7	0,165	0,848
	7-10 yıl	225	1,9	1,1		
	11-15 yıl	180	1,8	,9		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	4-6 yıl	78	2,9	1,2	1,824	0,162
	7-10 yıl	225	3,2	1,1		
	11-15 yıl	180	3,2	1,1		

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). 4-6 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır.

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

4.5.5. İfadelerin Günlük İnternet Kullanım Süresine Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, günlük internet kullanım süresi açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin tek yönlü varyans analizi sonucu Tablo 11'de sunulmuştur.

Tablo 11'de "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Günde 6 saat ve üzeri süre ile internet kullanan

kişilerin, 1-5 saat arası süre ile kullananlara kıyasla daha fazla internette sürekli gözetim altında olduğumu hissettiği saptanmıştır.

Tablo 11. Katılımcıların ifadelere verdiği yanıtların günlük internet kullanım süresine göre incelenmesi

Günlük İnternet Kullanım Süresi		n	ort.	ss.	F	p
İnternette alışveriş yapmaktan korkuyorum	1-2 saat	72	2,8	1,3	1,392	0,244
	3-5 saat	252	2,8	1,2		
	6-8 saat	96	2,8	1,2		
	8+ saat	63	2,4	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	1-2 saat	72	2,7	1,4	1,599	0,189
	3-5 saat	252	2,6	1,2		
	6-8 saat	96	2,7	1,2		
	8+ saat	63	2,3	1,1		
İnternette sürekli gözetim altında olduğumu hissediyorum	1-2 saat	72	3,0	1,2	7,210	0,000
	3-5 saat	252	3,2	1,3		
	6-8 saat	96	3,7	1,1		
	8+ saat	63	3,6	1,5		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	1-2 saat	72	2,6	,8	2,560	0,054
	3-5 saat	252	2,4	1,1		
	6-8 saat	96	2,6	1,1		
	8+ saat	63	2,2	1,2		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	1-2 saat	72	2,3	,9	7,567	0,000
	3-5 saat	252	3,0	1,1		
	6-8 saat	96	3,1	1,1		
	8+ saat	63	2,7	1,2		
Reklam çıkan siteleri bir daha kullanmıyorum	1-2 saat	72	3,2	1,4	0,928	0,427
	3-5 saat	252	3,0	1,3		
	6-8 saat	96	2,8	1,0		
	8+ saat	63	3,0	1,3		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	1-2 saat	72	4,0	1,3	0,712	0,545
	3-5 saat	252	4,0	1,1		
	6-8 saat	96	4,1	,8		
	8+ saat	63	4,1	1,0		
Kendimi güvendiğim siteler ile sınırlandırıyorum	1-2 saat	72	3,4	1,5	9,023	0,000
	3-5 saat	252	3,3	1,2		
	6-8 saat	96	3,1	,9		
	8+ saat	63	2,5	1,2		
İnternetten herhangi bir indirme işlem yapmıyorum	1-2 saat	72	2,3	1,2	8,901	0,000
	3-5 saat	252	1,8	1,0		
	6-8 saat	96	1,7	,8		
	8+ saat	63	1,5	,6		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	1-2 saat	72	3,0	1,3	3,457	0,016
	3-5 saat	252	3,1	1,1		
	6-8 saat	96	3,5	1,0		
	8+ saat	63	3,1	1,1		

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Günde 3 saat ve üzeri süre ile internet kullanan kişilerin, 1-2 saat arası süre ile kullananlara kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Günde 1-8 saat arası süre ile internet kullanan kişilerin, 8 saat üzeri süre ile kullananlara kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır.

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Günde 1-2 saat arası süre ile internet kullanan kişilerin, 3 saat üzeri süre ile kullananlara kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı saptanmıştır.

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin günlük internet kullanım süresine göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Günde 6-8 saat arası süre ile internet kullanan kişilerin, 3-5 saat arası süre ile kullananlara kıyasla daha fazla internetini ve bilgisayarını sürekli denetim altında tuttuğu saptanmıştır.

4.5.6. İfadelerin İnternet Suçuna Maruz Kalma Durumuna Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, internet suçuna maruz kalma durumu açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin bağımsız örnekler t-testi sonucu Tablo 12'de yorumu tablo altında sunulmuştur.

Tablo 12. Katılımcıların ifadelere verdiği yanıtların internet suçuna maruz kalma durumuna göre incelenmesi

İnternet Suçuna Maruz Kalma Durumu		n	ort.	ss.	t	p
İnternette alışveriş yapmaktan korkuyorum	Evet	57	2,7	1,1	-0,201	0,840
	Hayır	426	2,7	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	Evet	57	2,6	1,1	0,394	0,694
	Hayır	426	2,6	1,2		
İnternette sürekli gözetim altında olduğumu hissediyorum	Evet	57	3,3	1,4	-0,178	0,859
	Hayır	426	3,3	1,3		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	Evet	57	1,9	,8	-4,045	0,000
	Hayır	426	2,5	1,1		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	Evet	57	2,5	1,1	-2,376	0,018
	Hayır	426	2,9	1,1		
Reklam çıkan siteleri bir daha kullanmıyorum	Evet	57	2,9	1,3	-0,179	0,858
	Hayır	426	3,0	1,2		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	Evet	57	4,3	,9	1,743	0,082
	Hayır	426	4,0	1,1		
Kendimi güvendiğim siteler ile sınırlandırıyorum	Evet	57	3,1	1,3	-0,484	0,628
	Hayır	426	3,2	1,2		
İnternetten herhangi bir indirme işlem yapmıyorum	Evet	57	1,8	1,0	-0,360	0,719
	Hayır	426	1,8	1,0		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	Evet	57	3,3	1,0	0,863	0,389
	Hayır	426	3,1	1,1		

Tablo 12'de "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Daha önce internet suçuna maruz kalmamış kişilerin, maruz kalmış kişilere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Daha önce internet suçuna maruz kalmamış kişilerin, maruz kalmış kişilere kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin internet suçuna maruz kalma durumuna göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

4.5.7. İfadelerin İnternette Sınırsız Özgürlüğe Bakış Açısına Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, internette sınırsız özgürlüğe bakış açısı açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin bağımsız örnekler t-testi sonucu Tablo 13'de yorumu da tablonun altında sunulmuştur.

Tablo 13. Katılımcıların ifadelere verdiği yanıtların internette sınırsız özgürlüğe bakış açısına göre incelenmesi

İnternette sınırsız özgürlük olmalı mı?		n	ort.	ss.	t	p
İnternette alışveriş yapmaktan korkuyorum	Evet	99	2,5	1,2	-2,144	0,033
	Hayır	384	2,8	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	Evet	99	2,3	1,2	-2,176	0,030
	Hayır	384	2,6	1,2		
İnternette sürekli gözetim altında olduğumu hissediyorum	Evet	99	3,4	1,2	1,137	0,256
	Hayır	384	3,3	1,3		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	Evet	99	2,2	1,0	-3,387	0,001
	Hayır	384	2,5	1,0		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	Evet	99	2,4	1,2	-4,355	0,000
	Hayır	384	3,0	1,1		
Reklam çıkan siteleri bir daha kullanmıyorum	Evet	99	2,5	1,1	-3,901	0,000
	Hayır	384	3,1	1,3		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	Evet	99	3,8	1,2	-2,224	0,027
	Hayır	384	4,1	1,0		
Kendimi güvendiğim siteler ile sınırlandırıyorum	Evet	99	2,7	1,2	-4,424	0,000
	Hayır	384	3,3	1,2		
İnternetten herhangi bir indirme işlem yapmıyorum	Evet	99	1,5	,8	-3,757	0,000
	Hayır	384	1,9	1,0		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	Evet	99	3,2	1,1	0,992	0,322
	Hayır	384	3,1	1,1		

Tablo 13'de de görüldüğü gibi, "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla internette alışveriş yapmaktan korktuğu saptanmıştır.

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı saptanmıştır.

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla reklam çıkan siteleri bir daha kullanmadığı saptanmıştır.

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla kimlik bilgilerini isteyen sitelerden uzak durduğu saptanmıştır.

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini

düşünen kişilerin, düşünmeyenlere kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır.

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı saptanmıştır.

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin internette sınırsız özgürlüğe bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

4.5.8. İfadelerin Suçlarla Mücadeleye Bakış Açısına Göre İncelenmesi

Araştırmaya katılanların internet suçları ve internet kullanımına ilişkin görüşlerinin, suçlarla mücadeleye bakış açısı açısından incelendiğinde anlamlı bir farklılık olup olmadığı ile ilgili bulgulara ilişkin bağımsız örnekler t-testi sonucu Tablo 14'de sunulmuştur.

Tablo 14'e göre, "İnternette alışveriş yapmaktan korkuyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

Tablo 14. Katılımcıların ifadelere verdiği yanıtların suçlarla mücadeleye bakış açısına göre incelenmesi

Bu konuda uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunabilir mi?		n	ort.	ss.	t	p
İnternette alışveriş yapmaktan korkuyorum	Evet	378	2,7	1,2	-0,828	0,408
	Hayır	105	2,8	1,2		
Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum	Evet	378	2,6	1,3	0,540	0,590
	Hayır	105	2,5	1,1		
İnternette sürekli gözetim altında olduğumu hissediyorum	Evet	378	3,3	1,3	0,310	0,757
	Hayır	105	3,3	1,4		
Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum	Evet	378	2,5	1,0	1,999	0,046
	Hayır	105	2,3	1,0		
Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum	Evet	378	2,8	1,2	-1,673	0,095
	Hayır	105	3,0	,8		
Reklam çıkan siteleri bir daha kullanmıyorum	Evet	378	3,0	1,2	2,435	0,015
	Hayır	105	2,7	1,3		
Kimlik bilgilerimi isteyen sitelerden uzak duruyorum	Evet	378	4,0	1,1	-1,208	0,228
	Hayır	105	4,1	,9		
Kendimi güvendiğim siteler ile sınırlandırıyorum	Evet	378	3,3	1,3	2,493	0,013
	Hayır	105	2,9	1,1		
İnternetten herhangi bir indirme işlem yapmıyorum	Evet	378	1,9	1,0	2,485	0,013
	Hayır	105	1,6	,8		
İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum	Evet	378	3,1	1,1	-2,675	0,008
	Hayır	105	3,4	1,0		

"Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Reklam çıkan siteleri bir daha kullanmıyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla reklam çıkan siteleri bir daha kullanmadığı saptanmıştır.

"Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olmadığı görülmüştür ($p > 0,05$).

"Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır.

"İnternetten herhangi bir indirme işlem yapmıyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı saptanmıştır.

"İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesi ile ilgili görüşlerin suçlarla mücadeleye bakış açısına göre anlamlı olarak bir farklığa sahip olduğu görülmüştür ($p < 0,05$). Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünmeyen kişilerin, düşünen kişilere kıyasla daha fazla internetini ve bilgisayarını sürekli denetim altında tuttuğu saptanmıştır.

4.6. ANKETİN DEĞERLENDİRİLMESİ

Bu çalışmada kişilerin “İnternette alışveriş yapmaktan korkuyorum” ifadesine katılma dereceleri ölçülmüştür. Bulgulara göre kadınların erkeklere kıyasla daha fazla internette alışveriş yapmaktan korktuğu tespit edilmiştir. 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla internette alışveriş yapmaktan korktuğu tespit edilmiştir. Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla internette alışveriş yapmaktan korktuğu tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla internette alışveriş yapmaktan korktuğu tespit edilmiştir. 4-6 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla internette alışveriş yapmaktan korktuğu saptanmıştır.

Buna göre yaş ilerledikçe; eğitim düzeyi yükseldikçe; internet kullanım süresi azaldıkça kişilerin internette alışveriş yapmaya karşı kendilerini daha güvende hissettikleri söylenebilir.

Bu çalışmada kişilerin "Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum" ifadesine katılma dereceleri ölçülmüştür. Kadınların erkeklere kıyasla daha fazla bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı tespit edilmiştir. 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı tespit edilmiştir.

Buna göre yaş azaldıkça kişilerin bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaştığı söylenebilir.

Bu çalışmada kişilerin "İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesine katılma dereceleri ölçülmüştür. Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla internette sürekli gözetim altında olduğunu hissettiği tespit edilmiştir. Günde 6 saat ve üzeri süre ile internet kullanan kişilerin, 1-5 saat arası süre ile kullananlara kıyasla daha fazla internette sürekli gözetim altında olduğumu hissettiği saptanmıştır.

Buna göre eğitim düzeyi azaldıkça; günlük internet kullanım süresi arttıkça kişilerin internette sürekli gözetim altında olduğumu hissettiği söylenebilir.

Bu çalışmada kişilerin "Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesine katılma dereceleri ölçülmüştür. Kadınların erkeklere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü tespit edilmiştir. 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü tespit edilmiştir. Lisans mezunlarının, lisansüstü mezunu kişilere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü tespit edilmiştir. Daha önce internet suçuna maruz kalmamış kişilerin, maruz kalmış kişilere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü tespit edilmiştir. İnternette sınırsız özgürlük olmaması

gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü tespit edilmiştir. Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü tespit edilmiştir. 4-6 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla birçok siteyi engelleyerek kendini koruma altına aldığımı düşündüğü saptanmıştır.

Buna göre yaş azaldıkça; eğitim düzeyi azaldıkça; internet kullanım süresi azaldıkça kişilerin birçok siteyi engelleyerek kendini koruma altına aldığını düşündüğü söylenebilir.

Bu çalışmada kişilerin "Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum" ifadesine katılma dereceleri ölçülmüştür. Kadınların erkeklere kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü tespit edilmiştir. 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü tespit edilmiştir. Daha önce internet suçuna maruz kalmamış kişilerin, maruz kalmış kişilere kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü tespit edilmiştir. 4-6 yıl süre ve 7-10 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır. Günde 3 saat ve üzeri süre ile internet kullanan kişilerin, 1-2 saat arası süre ile kullananlara kıyasla daha fazla aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü saptanmıştır.

Buna göre yaş azaldıkça; internet kullanım süresi azaldıkça; günlük internet kullanım süresi arttıkça kişilerin aile korumasını aktifleştirerek yakınlarını koruyabildiğini düşündüğü söylenebilir.

Bu çalışmada kişilerin "Reklam çıkan siteleri bir daha kullanmıyorum" ifadesine katılma dereceleri ölçülmüştür. Kadınların erkeklere kıyasla daha fazla reklam çıkan siteleri bir daha kullanmadığı tespit edilmiştir. 26 ve üzeri yaş aralığındaki kişilerin, 18-25 yaş aralığındakilerden daha fazla reklam çıkan siteleri

bir daha kullanmadığı tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla reklam çıkan siteleri bir daha kullanmadığı tespit edilmiştir. Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla reklam çıkan siteleri bir daha kullanmadığı tespit edilmiştir.

Buna göre yaş ilerledikçe kişilerin reklam çıkan siteleri bir daha kullanmadığı söylenebilir.

Bu çalışmada kişilerin "Kimlik bilgilerimi isteyen sitelerden uzak duruyorum" ifadesine katılma dereceleri ölçülmüştür. Kadınların erkeklere kıyasla daha fazla kimlik bilgilerini isteyen sitelerden uzak durduğu tespit edilmiştir. Lisansüstü mezunlarının, lisans mezunu kişilere kıyasla daha fazla kimlik bilgilerini isteyen sitelerden uzak durduğu tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla kimlik bilgilerini isteyen sitelerden uzak durduğu tespit edilmiştir.

Buna göre eğitim düzeyi yükseldikçe kişilerin kimlik bilgilerini isteyen sitelerden uzak durduğu söylenebilir.

Bu çalışmada kişilerin "Kendimi güvendiğim siteler ile sınırlandırıyorum" ifadesine katılma dereceleri ölçülmüştür. Kadınların erkeklere kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı tespit edilmiştir. Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı tespit edilmiştir. 4-6 yıl süre ile internet kullanan kişilerin, 11-15 yıl süre ile kullananlara kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır. Günde 1-8 saat arası süre ile internet kullanan kişilerin, 8 saat üzeri süre ile kullananlara kıyasla daha fazla kendini güvendiği siteler ile sınırlandırdığı saptanmıştır.

Buna göre internet kullanım süresi azaldıkça; günlük internet kullanım süresi azaldıkça kişilerin kendini güvendiği siteler ile sınırlandırdığı söylenebilir.

Bu çalışmada kişilerin "İnternetten herhangi bir indirme işlem yapmıyorum" ifadesine katılma dereceleri ölçülmüştür. Lisans mezunlarının, lisansüstü mezunu

kişilere kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı tespit edilmiştir. İnternette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, düşünmeyenlere kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı tespit edilmiştir. Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, düşünmeyen kişilere kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı tespit edilmiştir. Günde 1-2 saat arası süre ile internet kullanan kişilerin, 3 saat üzeri süre ile kullananlara kıyasla daha fazla internetten herhangi bir indirme işlem yapmadığı saptanmıştır.

Buna göre eğitim düzeyi azaldıkça; günlük internet kullanım süresi azaldıkça kişilerin internetten herhangi bir indirme işlem yapmadığı söylenebilir.

Bu çalışmada kişilerin "İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum" ifadesine katılma dereceleri ölçülmüştür. 18-25 yaş aralığındakilerin, 26 ve üzeri yaş aralığındaki kişilerden daha fazla internetini ve bilgisayarını sürekli denetim altında tuttuğu tespit edilmiştir. Uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünmeyen kişilerin, düşünen kişilere kıyasla daha fazla internetini ve bilgisayarını sürekli denetim altında tuttuğu tespit edilmiştir. Günde 6-8 saat arası süre ile internet kullanan kişilerin, 3-5 saat arası süre ile kullananlara kıyasla daha fazla internetini ve bilgisayarını sürekli denetim altında tuttuğu saptanmıştır.

Buna göre yaş azaldıkça; günlük internet kullanım süresi arttıkça kişilerin internetini ve bilgisayarını sürekli denetim altında tuttuğu söylenebilir.

SONUÇ

Dünya üzerinde yaşayan bütün insan topluluklarının bilişim teknolojilerine artan bağlılığı, gündelik yaşama koşut bir yaşam şeklinin oluşmasına neden olmuştur. Bu bilinmeyen ve her gün yeni keşiflerin olduğu dünyada, kaçınılmaz olarak bazı sorunlar ortaya çıkmaktadır. Bu sorunlara zaman içinde yenileri eklenmekte, suçluyu bulma ve derdest etme konusunda sıkıntılar meydana gelmektedir. Teknolojinin sağladığı kolaylıklar sayesinde artık bilgi kolay ulaşılabilir, uzaktakiyle iletişim kolay kurulabilir hale gelmiştir. Bu durum kişilik haklarına karşı saldırıların artmasını beraberinde getirmiştir. Önceden sınırlı çerçevede karşılaşılan hak ihlalleri, sanal ortamlar sayesinde inanılmaz ölçüde genişlemiştir. Oluşan bu koşullar doğrultusunda da günümüzde bireyler, çeşitli saldırılarla karşı karşıya gelmekte, savunmasız kalmaktadırlar. Hukuk düzeni içinde devletler ve bireyler çeşitli önlemler almak durumundadırlar. Bu önlemler doğal olarak kuralları içerecek ve sanal ortamda ortaya çıkan sorunlara çözüm yolları sunacaktır. Hukuk sisteminin amacı da, bu kuralsızlıklara bağlı olarak bireyi kişi olarak koruma çabası çok eski çağlardan günümüze dek uzanan düzenlemeleri beraberinde getirmektedir. Bu düzenlemeler insan var olduğu ve teknoloji geliştiği sürece de devam edecek gibi görünmektedir.

Enformatik sistemler hayatın her alanında olduğu gibi hukuk alanında da ciddi sonuçlar yaratmakta ve çözümlenmesi gereken yepyeni hukuki sorunların dogmasına neden olmaktadır. Bu suçlar gün geçtikçe büyük aşamalar kaydederek ciddi zararlara yol açmaktadır. Dinamik bir yapıda olan bilişim dünyasında, ortaya çıkan sorunlara özellikle Türkiye gibi bürokrasinin fazla olduğu durağan bir yasama anlayışı ile karşılık ver(ebil)mek bir hayli zor gözükmektedir. Ayrıca çıkarılacak yasaların yeterince kapsayıcı olamaması durumunda karşılaşılabilecek sorunlara alternatif çözüm önerilerinin sunulması gerekmektedir.

Bugün internet kullanımının hızla artış eğilimi göstermesi doğrultusunda internet kullanıcılarının da sayısal olarak büyümesine ve kişilerin haklarına yapılan saldırıların da paralel şekilde artış göstermesine neden olmaktadır. Kişilik hakkı ihlalleri ya da saldırıları fiziksel temastan uzak, bilişim sistemine özgü virüsler, mailler yoluyla gerçekleştirilen saldırılardan oluşmaktadır. Türkiye'de ve dünyada

internet ortamındaki ihlallere karşı kişilik hakkı ihlal şekillerinde sürekli yeni durumların ortaya çıkması sebebiyle doktrinde umumi olarak yapılan düzenlemeler hususi düzenlemelere göre daha çok uygulanabilirliğe sahip olmaktadır. Bu anlamda internet yoluyla kişilik haklarına karşı yapılan saldırılardan korunmak amacıyla genellikle özel hukuk, Medeni Kanun ile Borçlar Kanunu yanında Türk Ceza Kanununun hükümlerine başvurulmaktadır.

Bilgisayar ve internet aracılığıyla işlenen suçlara ilişkin mevcut yasal mekanizmanın serbest gözlemlenmesi neticesinde ortaya söz konusu mekanizmanın kanun ihlalleri karşısında teknik anlamda yetersiz, bilişim suçlarının etkilerini kısa süre içerisinde sınırlandıramayan bir yapıda olduğu görülmektedir. Özellikle gerek yasal (TCK ve CMK) yetersizlikler, gerek oturmuş bir yapının olmaması, söz konusu sorunun ilerideki mahiyeti konusunda akıllara olumsuz senaryoları getirmektedir. Ancak son zamanlarda yapılan yasal düzenlemelerin oldukça faydalı yaklaşımlar içinde olduğunu söylemek mümkündür.

Avrupa Birliğine bağlı olarak çalışan konseyin oluşturduğu ve ülkelerin siber ortamda meydana gelen suçlarla etkin şekilde mücadele etmesini amaçlayan "Sanal Ortamda İşlenen Suçlar Sözleşmesi" Türkiye'de ilk başlarda bazı çekinceler yaratsa da, zaman içinde onaylanarak uluslararası işbirliğinin gündeme gelmesi, internet ve bilişim sistemleri aracılığıyla gerçekleştirilen suçlarla mücadelede önemli bir basamak oluşturduğu söylenebilir.

Bu doğrultuda Türkiye'de 5651 Sayılı Kanun çok tartışılmış olmakla birlikte özel hukuk kapsamında gerekliliği ve yerindeliği görülmektedir. Kanunda 6518 Sayılı Kanunla yapılan değişiklikle, kişilik hakkı ihlalleri ile ilgili "içeriğin yayından çıkarılması ve erişimin engellenmesi" başlığını taşıyan Madde 9 ile kişilik hakkı ihlale uğrayan kişilerin talepleri halinde saldırının en kısa sürede sona ermesini sağlayabilecekleri, 9A maddesinde de "özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi" konusunda ihlale uğrayan kişiler içeriğe erişimin engellenmesi tedbirinin uygulanmasını talep edebilmeleri olanağıyla mahkemeler yoluyla elde edilen sonuçlardan daha hızlı sonuç alınması sağlanmıştır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi hakkındaki kanun doğrultusunda, internet servis sağlayıcılarının sorumluluğu belirlenmiş ve içerik sağlama

konumunda bulunmadıkları müddetçe sorumluluklarının bulunmadığı görülmektedir. Başka bir ifadeyle içerik servis sağlayıcılar, mevcut abonelere yalnızca internete bağlanma hizmeti verdiğinde herhangi bir sorumluluk yüklenmeleri söz konusu olmayacaktır. Ancak internete bağlanma hizmeti dışında başka hizmetler de sunması durumunda içerik servis sağlayıcıların sorumlulukları artmaktadır.

Hem ulusal hem de uluslararası mevzuatla bilişim sistemindeki hak ihlallerinin önüne geçilmeye çalışılıyor olsa da, bilişim sistemleri söz konusu hak ihlallerinin oluşması açısından kolaylık sağlayan bir yapı sergilemektedir. Bu durum bilişim sisteminin sahip olduğu olumsuz etkilere karşı, sistemin kullanıcısı konumundaki tüm bireylerin uyanık olmasını gerekli kılmaktadır.

Günümüzde Türkiye'de yaşayan bireylerin internet suçlarına ilişkin algılarını ve farkındalıklarını ölçmeyi, internetle ilgili eğilimlerini ve internete yaklaşımlarını belirlemeyi amaçlayan bir anket araştırması yapılarak, bugünün somut durumunu seçilen örnekten hareketle bütün topluma genellemeye yönelik bir çalışma gerçekleştirilmiştir.

Tez çalışmasında seçilen örneklem 483 kişiden oluşmakta, yaş aralıkları en az 18 yaş olan örneklemdeki katılımcıların eğitim durumları da en az lisans düzeyinde bulunmaktadır. Bu profildeki bir katılımcı grubun düzenlenen anket çerçevesinde internet kullanım sıklıklarından, kullanım şekillerine kadar uzanan ve internette güvenlik kavramı ekseninde hissettiklerini belirlemeye yönelik olarak yapılan çalışmada elde edilen bulgular ışığında aşağıda belirtilen betimlemeleri yapmak mümkündür.

Çalışma doğrultusunda 483 kişi üzerinde gerçekleştirilen araştırmada, katılımcıların % 57'si kadın, % 43'ü erkeklerden oluşmaktadır.

Katılımcıların yaş dağılımlarına bakıldığında 18-25 yaş arası katılımcıların oranı %52, 26 yaş ve üzerinde olan katılımcıların oranı %48 olup yoğunlukları birbirine yakındır.

İnternet kullanım süresi açısından incelendiğinde ise; 4-6 yıl olarak belirlenen en düşük kullanım süresinde internet kullananların sayısı 78 ve bütün içindeki oranı %16'dır. 7-10 yıl ve 11-15 yıl aralığında internet kullananlar içinde de 7-10 yıl internet kullananların % 47 oranla ilk sırada yer aldığı belirlenmiştir.

Katılımcıların günlük internet kullanım sürelerine bakıldığında, 3-5 saat günlük internet kullanımının % 52'lik oranla ilk sırada yer aldığı görülürken, 8+ saat günlük internet kullananların ise % 13'lük oranla son sırada olduğu görülmektedir. Günlük internet kullanım sıklığının daha çok 3 saat ile 8 saat aralığında değiştiği dikkat çekmektedir.

İnternet kullanıcılarının sadece % 12'si yani 57 kişi internet suçuna maruz kalmıştır. 483 katılımcının 384'ü internette sınırsız özgürlük olmasına karşı çıkarken, 99'u internette sınırsız özgürlüğün olması gerektiği görüşündedir.

İnternet suçları ile kişilik hakları ihlallerine karşı tüm dünyada geçerli ve uygulanabilir hukuk kurallarının olması gerekliliği konusunda bütün katılımcılar, olumlu yönde görüş beyan etmişlerdir. Uluslararası uzlaşma sağlanmasının suçlarla mücadelede başarıyı etkileyip etkilemeyeceği yönündeki soruya 378 kişi olumlu yanıt verirken, 105 kişi olumsuz görüş bildirmiştir.

Araştırmada katılımcılara çeşitli ifadelere "Kesinlikle katılmıyorum, Katılmıyorum, Kararsızım, Katılıyorum, Kesinlikle Katılıyorum" diyerek katılıp katılmadıkları sorulmuştur. Katılımcılara yöneltilen ifadeler şunlardır;

- "İnternette alışveriş yapmaktan korkuyorum",
- "Bankacılık işlemlerimi internet yolu ile gerçekleştirmeye şüphe ile yaklaşıyorum",
- "İnternette sürekli gözetim altında olduğumu hissediyorum",
- "Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum",
- "Aile korumasını aktifleştirerek yakınlarımı koruyabiliyorum",
- "Reklam çıkan siteleri bir daha kullanmıyorum",
- "Kimlik bilgilerimi isteyen sitelerden uzak duruyorum",
- "Kendimi güvendiğim siteler ile sınırlandırıyorum",
- "İnternetten herhangi bir indirme işlem yapmıyorum",
- "İnternetimi ve bilgisayarımı sürekli denetim altında tutuyorum".

Katılımcıların bu ifadelere yanıt vermeleri bugün kullandıkları internete ne derece güvendiklerini ya da kendilerini ne kadar güvende hissettiklerini belirlemeye

yardımcı olması açısından ve internet üzerinde yaptıkları işlemlerde-eylemlerde ne derece özgür davrandıklarını ortaya koyması açısından önemlidir.

Araştırmada yukarıda belirtilen ifadelerden hareketle elde edilen bulgulara göre; bireylerin yaşının ilerlemesi, eğitim seviyesinin yükselmesi ve günlük internet kullanım süresinin azalmasıyla birlikte, internet üzerinden alışveriş yapma konusunda kendilerini daha güvende hissetme eğilimi göstermektedirler. Başka bir ifadeyle internet üzerinden alışveriş yapmaktan duyumsanan korku, yaş ve eğitim seviyesiyle doğru orantılı, günlük internet kullanma süresiyle ters orantılıdır denilebilir.

Katılımcıların bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe ile yaklaşma eğilimi incelendiğinde, kadınların internet üzerinden alışveriş yapma konusunda olduğu gibi bu konuda da, daha şüpheci oldukları dikkat çekmektedir. Bankacılık işlemlerini internet yoluyla gerçekleştirmeye şüpheci yaklaşanların daha çok 18-25 yaş aralığındaki bireyler ve internette sınırsız özgürlüğün olmaması gerektiğini düşünen katılımcılar olduğu önemli bulgular arasındadır. Katılımcıların yaşları küçüldükçe, bankacılık işlemlerini internet yolu ile gerçekleştirmeye şüphe arttığı için, ters orantılı olduğu söylenebilir.

"İnternette sürekli gözetim altında olduğumu hissediyorum" ifadesine katılanların daha çok lisans okuyan bireyler oldukları ve günlük internet kullanımlarının da 6 saatin üzerinde olduğu ilginç bulgulardandır. Çünkü bireyler gözetim altında olduğunu hissetmesine rağmen yine de, internet kullanımını kısıtlamamakta, 6 saat ve üzerinde günlük internet kullanımını devam ettirmektedir. Buradan hareketle, katılımcı bireylerin internette sürekli gözetim altında olduğunu hissetse de internet kullanımını kısıtlamamakta, devam ettirmektedir.

Katılımcıların "Birçok siteyi engelleyerek kendimi koruma altına aldığımı düşünüyorum" ifadesine katılma derecelerinin ölçümüne göre, kadınlar erkeklere göre daha korumacı davranmaktadırlar. Korumacı davranan katılımcıların özellikleri incelendiğinde, 18-25 yaş aralığındaki bireylerin, lisans düzeyindekilerin, daha önce internet suçuna maruz kalmamış kişilerin, internette sınırsız özgürlük olmaması gerektiğini düşünen kişilerin, uluslararası bir konsensus sağlansa suçlarla mücadelede başarılı olunacağını düşünen kişilerin, bu eğilimde oldukları belirlenmiştir.

Aile korumasını aktifleştirme yoluyla yakınlarını koruyabildiklerini düşünenlerin de, site engelleyerek kendini koruma altına aldığını düşünenlerin sergiledikleri eğilim içinde oldukları tespit edilmiştir. Kadınlar, 18-25 yaş aralığındaki katılımcılar, daha önce internet suçuna maruz kalmamış kişiler, internette sınırsız özgürlük olmaması gerektiğini düşünen kişiler, aile korumasını aktifleştirerek yakınlarını koruyabildiğini ifade etmektedir. Burada ortaya çıkan farklılık, internet kullanım süresi 4-6 yıl ve 7-10 yıl olan katılımcıların daha fazla bu yola başvurdukları belirlenmiştir.

Günlük kullanım süresi açısından ise, 1-2 saat internet kullananlar daha az aile korumasını aktifleştirerek korumayı tercih ettiği, daha çok günde 3 saat ve üzeri süre ile internet kullanan katılımcıların, daha fazla aile korumasını aktifleştirerek yakınlarını koruma eğiliminde olduğu saptanmıştır.

Yaş olarak daha ileri olan bireyler reklam amaçlı yazılımlara temkinli yaklaşırken, gençlerin koruma programlarıyla sezgisel değil, bilgiye dayalı farkındalık içinde olduğu görülmüştür.

Reklam çıkan siteleri kullanma eğilimi incelendiğinde ise; özellikle kadınların ve 26 yaş üzeri katılımcıların, internette sınırsız özgürlük olmaması gerektiğini düşünen bireylerin, uluslararası bir konsensus sağlanması durumunda suçlarla mücadelede başarılı olunacağını düşünen kişilerin, daha fazla reklam çıkan siteleri tekrar kullanmadığı ortaya konan bulgulardandır.

Ayrıca diğer ifadelerle elde edilen bulgulara göre, eğitim seviyesinin artmasıyla doğru orantılı olarak kimlik bilgilerini isteyen sitelerden uzak durma eğilimi sergilenmektedir. Güven duyduğu sitelerle kendini sınırlayan katılımcıların ise daha çok, yıl bazında ve günlük internet kullanım süresi az olan katılımcılar olduğu görülmektedir.

İnternetten herhangi bir indirme işlemi yapmadığını belirten katılımcıların eğitim düzeyinin daha düşük, aynı zamanda da internet kullanım sürelerinin daha az olduğu saptanmıştır. İnternetini ve bilgisayarını sürekli olarak denetim altında tutan katılımcıların da, yaş olarak daha küçük, daha sık internet kullanan katılımcılar olduğu belirlenmiştir.

Bugün olduğu gibi yarın da internet her daim çeşitli yollarla kişilik haklarının ihlal edildiği ortamlar olmaya devam edecek gibi görünmektedir. Bu nedenle hem

dünyada hem de Türkiye'de internet yoluyla işlenen suçların önüne geçebilmek için, hem bireysel hem de kurumsal olarak önlemler alınması gerekmektedir. Yapılan anket çalışmasında bireylerin kendilerini korumak için, aile koruması kullandıkları, reklam çıkan siteleri kullanmadıkları, kişisel bilgilerini isteyen sitelerden kaçındıkları, interneti alışveriş işlemlerinde mümkün mertebe kullanmama yolunu seçtikleri görülmektedir. Suça karşı alınan önlemler doğal olarak suçun oluşmasını engellemekte, karşı karşıya kalınan zararı da minimize etmektedir. Bu manada kurumsal açıdan düşündüğümüzde, bu tür suçları önleme mekanizmalarının geliştirilerek genişletilmesi, eğitim ve bilinçlendirmede farkındalığın arttırılması neticesinde daha iyi sonuçlar alınabileceği muhakkaktır.

Bireyler ve devlet kurumları teknolojinin kaçınılmaz yaşamın içindeliğinden kurtulmak mümkün olmadığına ve zararları yüzünden faydalarından vazgeçilemeyeceğine göre, internet ve bilişim sistemlerinin güvenliğini sağlamak için gerekli çabayı harcamak zorundadırlar. İnternet ve bilişim sistemleri içinde yer alan verilerin gizliliğinden güvenliğinin sağlanmasına kadar uzanan önlemler sayesinde yetkisi olmayan kişilerin bu sistemlere erişmesinin önüne geçmek ve hak ihlalleri daha oluşmadan önüne geçmek gereklidir.

Evrensel kurallar oluşturularak uygulamaya konmalı, ancak bu yapılırken etik ilkeler ve yasal süreçler birlikte değerlendirilmeli, bireylerin temel hak ve özgürlükleri gözetilerek, gerekli önlemleri alma yoluna gidilmelidir. Tüm dünyada uygulanabilir kurallar doğrultusunda, ülkeler arası işbirlikleri devreye sokularak sınırları olmayan internet ve bilişim dünyasında, suçun önüne geçme konusunda sınırlar ve sınırlamalar ortadan kaldırılmalıdır. Zira bütün bunların gerçekleştirilmesi dünya üzerindeki tüm bireyler için, artık vazgeçilmesi mümkün olmayan bir gereksinim durumundadır.

KAYNAKÇA

Akarslan, Hüseyin, ***Avrupa Konseyi Siber Suçlar Sözleşmesi (Türkçe),*** (Erişim) http://www.bhd.org.tr/dokumanlar/Avrupa%20Konseyi%20Siber%20Suclar%20Sozlesmesi%20TR.docx , 12.12.2016.

Akarslan, Hüseyin, ***Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı***, T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2011.

Akarslan, Hüseyin, ***Bilişim Suçları***, Seçkin, Ankara, 2012.

Akdeniz, Yaman, **Çağdaş İnternet Yönetimi**, Nisan 2004, (Erişim) http://www.policy.hu/akdeniz/beyaz_kitap_sura.pdf, 12 Aralık 2016.

Akıncı, Hatice – Alıç, Emre A. ve Er Cüneyt, "Türk Ceza Kanunu ve Bilişim Suçları", **İnternet ve Hukuk**, Ed. Yeşim Atamer, Bilgi Üniversitesi Yayınları, İstanbul, No: 51, 2004.

Akıntürk, Turgut - Karaman, Derya Ateş, ***Medeni Hukuk***, Beta Yayınları, İstanbul, 2011.

Akipek, Jale – Akıntürk, Turgut, ***Türk Medeni Hukuku, Birinci Cilt: Başlangıç Hükümleri, Kişiler Hukuku***, Beta Yayınları, İstanbul, 2007.

Alaca, Bahattin, **Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle),** Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2008.

Alikaşifoğlu, Müjgân, ***İnternet Kullanımı ve Çocuk ve Ergen Sağlığı*** Türk Pediatri Kurumu TBMM Sunusu, 2012, (Erişim) https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/Turk_Pediatri_Kurumu_.internet%20Kullanimi%20ve%20cocuk-Ergen-sagligi.pdf , 12 Aralık 2016.

Alkan, Mustafa, Canbay, Cafer, "İnternet Alan Adları Yönetimi, Mevcut Sorunlar ve Çözüm Önerileri", (Erişim) https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FArastirma_Raporlari%2FInternet_Alan_Adlari_Yonetimi_Mevcut_Sorunlar_ve_Cozum_Onerileri.pdf, 12 Aralık 2016.

Apaydın, Cengiz, "Bilişim Sistemine Girme Suçu**",** ***Türkiye Adalet Akademisi Dergisi***, Yıl:7, Sayı:24, Ocak 2016

Arpacı, Abdülkadir, ***Kişiler Hukuku Gerçek Kişiler***, Beta Yayınları, İstanbul, 2010.

Avcı, Artun, ***Türkiye'de İnternet ve İfade Özgürlüğü***, İstanbul, Legal, 2013.

Avşar, Zakir, Öngören, Gürsel, ***Bilişim Hukuku***, Türkiye Bankalar Birliği Yayınları, Yayın No:270, İstanbul, 2010.

Aydın, Ahmet Hamdi, **Suç Önlemenin Önemi ve Etkisi**, KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi, Sayı 16, Özel Sayı I, 2014.

Aydın, Sedat Erdem, ***AİHM İçtihatları Kapsamında Kişisel Verilerin Kaydedilmesi Suçu***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2014.

Bahtiyar, Ziya, ***Virüsler ve Güvenlik***, Pusula Yayınları, İstanbul, 2003.

Başalp, Nilgün, ***Kişisel Verilerin Korunması ve Saklanması***, Yetkin Yayınları, 2004.

Başlar, Yusuf, "Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri Suçu", **Dergi Park, Uyuşmazlık Mahkemesi Dergisi**, Cilt 1, Sayı 1, 2015.

Bayındır, Sinan, "Eser Sahibinin İzni Olmaksızın Eseri Umuma İletim Suçu", ***Türkiye Barolar Birliği Dergisi***, Sayı: 113, 2014.

Bikirli, Alper Yükselen, ***5237 Sayılı Türk Ceza Kanununda Düzenlenen Bilişim Suçları***, Ankara, (Erişim), https://www.google.com.tr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjwspOoo_PQAhVBaRQKHWA7DBUQFggrMAI&url=http%3A%2F%2Fwww.taa.gov.tr%2Findir%2Falper-yukselen-bikirli-yargitay-8-ceza-dairesi-uyesi-c2F5ZmF8NzhjNTMtOWRjZDAtMWZlNDItNGRhZDYuZG9jeHwyMTc%2F&usg=AFQjCNEE1ErXJyI_OAW_Mrll1PRm7qXkgw , 12 Aralık 2016.

Bilgen, Tülay, ***Türk Ceza Kanununda Banka veya Kredi Kartlarının Kötüye Kullanılması,*** Yayımlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, 2010.

Börteçin, Ege, "İnternet Nasıl Çalışıyor?", Bilim ve Teknik Dergisi, Ekim 2013.

Çakır, Hüseyin ve Sert, Ercan, "Bilişim Suçları ve Delillendirme Süreci", ***Örgütlü Suçlar ve Yeni Trendler***, Polis Akademisi Yayınları, 2011

Çekiç, Burak, ***İnternet Aracılığıyla İşlenen Suçlar***, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Çetin, Hakan, ***Türkiye'nin Otonom Sistem Seviyesinde İnternet Haritasının Çıkarımı ve İncelenmesi***, T.C. Muğla Üniversitesi Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2009.

Değirmenci, Olgun, ***Bilişim Suçları***, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2002.

Demir, Esra Peker, ***İnternet Aracılığı ile Kişilik Haklarına Saldırı***, T.C. İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2014.

Demir, Önder, " İnternet Servis Sağlayıcısının Cezai Sorumluluğu", ***İzmir Barosu Dergisi***, 2000, Sayı:3.

Deryal, Yahya, ***Medeni Hukuk Bilgisi***, Seçkin Kitabevi, Ankara, 2010.

Dilek, Halil İbrahim, ***Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri***, T.C. Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2007.

Doğan, Pınar Bahar, "Çatışan İki Değer: Haber Verme Hakkı ve Kişilik Hakkı", **Ankara Barosu Dergisi**, Sayı 4, 2014.

Dokurer, Semih, ***Bilişim Suçları Laboratuvarlarında Çocuk Pornografisi İncelemeleri***, s. 3, (Erişim) http://www.dokurer.net/files/documents/cocukpornincelemeleri.pdf , 12 Aralık 2016.

Durak, Yasemin, "İnternet Yoluyla Kişilik Haklarına Saldırı ve Hukuki Korunma", ***Selçuk Üniversitesi Hukuk Fakültesi Dergisi***, Cilt 22, Sayı 1, 2014, (Erişim) http://www.mutlakbutlan.com/2016/12/internet-yoluyla-kisilik-haklarina-saldiri-ve-hukuki-korunma.html , 12 Aralık 2016.

Dural, Mustafa – Öğüz, Tufan, ***Türk Özel Hukuku Cilt 2 Kişiler Hukuku***, Filiz Kitabevi, İstanbul, 2012.

Dülger, Murat Volkan – Modoğlu, Gözde, ***Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku Uygulama Rehberi***, Avrupa Birliği ve Avrupa Konseyi Ortak Yayını, Ankara, 2014.

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

Dülger, Murat Volkan, ***Bilişim Suçları ve İnternet İletişim Hukuku***, Seçkin Yayınları, 2012.

Dülger, Murat Volkan, **Bilişim Suçları ve İnternet İletişim Mevzuatı**, Ankara, 2015.

Dülger, Murat Volkan, ***Suçların Birleşmesine İlişkin Tanımlar, Sorunlar ve Çözüm Önerileri,*** 25 Mart 2015, (Erişim) http://www.hukukgunlugu.org/suclarin-birlesmesi/ , 12 Aralık 2016.

Elit Hukuk, ***Yeni Bir Bilişim Suçu: Zararlı Yazılım ve Yasak Cihaz***, (Erişim) http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/, 20.01.2017.

Erdoğan, Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu**",** ***Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi***, Cilt: 12, Özel Sayı, 2010.

Erdoğan, Yavuz, ***Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)***, Legal Yayıncılık, İstanbul, 2012.

Ergüç, Seher, **Türk Bankacılık Sisteminde İnternet Bankacılığı ile Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku,** Yayımlanmamış Yüksek Lisans Tezi, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2008.

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

Erkan, Boğaç - Murat, Songür, ***Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü***, 1999.

Fırat, Muhammed Sabır, "Hukuk Devleti Açısından İnternette İnsan Hakkı ve Kişilik Haklarına Saldırı Sorunu", ***Hacettepe HFD***, 5(2), 2015.

Gökçen, Ahmet, Kamu Barışına Karşı Suçlar, ***Yeni Türk Ceza Adaleti Tanıtım Sitesi***, (Erişim), www.ceza-bb.adalet.gov.tr/makale/118.doc, 22.01.2017.

Gözüşirin, Mesih, **5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi**, Yayımlanmamış Yüksek Lisans Tezi, Kara Harp Okulu, Savunma Bilimleri Enstitüsü, Ankara, 2011.

Güler, Niyazi – Bayzan, Şahin ve Güneş, Abdülhamit, ***İnternette Çocuklara Yönelik Riskler ve Ailelerin Bilinçlendirme Faaliyetlerindeki Rolü***, (Erişim) http://s3.amazonaws.com/academia.edu.documents/45841666/icits2016_makale_tam_metin_24NISAN.pdf?AWSAccessKeyId=AKIAJ56TQJRTWSMTNPEA&Expires=1481654665&Signature=7SpotRR40CmlcqnL15EIy%2BMkcOA%3D&response-content-disposition=inline%3B%20filename%3DInternette_Cocuklara_Yonelik_Riskler_ve.pdf, 12 Aralık 2016.

Güngör, Necmi Murat, **Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, İstanbul, 2007.

Güran, Sait – Akünal, Teoman – Bayraktar, Köksal – Erdener, Yurtcan – Kendigelen, Abuzer – Beller, Önder – Sezer, Bülent, ***İnternet ve Temel Hukuk Metni***, İstanbul 2002.

Hafızoğulları, Zeki – Güngör, Devrim, "Türk Ceza Hukukunda Suçların Tasnifi", **TBB Dergisi**, Sayı 69, 2007.

Haşıloğlu, Selçuk Burak, Elektronik Posta ile Pazarlama, Beta Basım Yayın Dağıtım, İstanbul, 2007.

Hekim, Hakan ve Başıbüyük, Oğuzhan, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", **Uluslararası Güvenlik ve Terörizm Dergisi**, C: 4, S: 2, 2013.

Helvacı, Serap, ***Gerçek Kişiler***, İstanbul, 2013.

Helvacıoğlu, Aslı Deniz, "Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi", Yeşim Atamer (Ed.), **İnternet ve Hukuk**, Bilgi Üniversitesi Yayınları No: 51, İstanbul, 2004.

http://bilisimci2007.blogcu.com/kamusal-alan-ve-kamusal-alan-olarak-internet/2652009

İçel, Kayıhan ve Ünver, Yener, Kitle İletişim Hukuku, Beta Basım Yayın Dağıtım, İstanbul, 2012.

İlbaş, Çığır ve Köksal, Mehmet Ali, **Türkiye'de Bilişim Suçları 1990-2011**, 2015, (Erişim) http://docplayer.biz.tr/15849702-Adli-bilisim-uzm-cigir-ilbas-av-mehmet-ali-koksal.html, 12.01.2017.

İnan, Aslan, ***İnternet El Kitabı***, İstanbul, 1999.

İnternette Zorbalık - Katlanmak zorunda değilsiniz, Şikâyet edin, (Erişim) http://www.guvenliweb.org.tr/guvenlik/node/154, 10.Ocak.2016.

İşgüzar, Hasan, "3444 Sayılı Kanunla Değiştirilen Borçlar Kanunun 49. Maddesine Göre Kişilik Hakkının İhlali Nedeniyle Manevi Tazminat Davasının Şartları", ***Ankara Barosu Dergisi***, S. 6, Aralık, 1990.

Kalkota, R and Whinston A.B., (1996), "Frontiers Of Electronic Commerce", Massachussets, Addision,Wesley. Kalkota ve Whinston, 1996, akt.,

Karaçetin, Murat, ***İnternet Üzerinden Alışverişe Yönelik Tutumlar: Bir Araştırma***, T.C. Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Burdur, 2015.

Karaca, Ayşe ve Beyaznar, Bahar, "İnternette Müstehcenlik: Nerede başlar ve nerede biter?", **Akademik Bilişim'10,** s.63.

Karakehya, Hakan, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", ***Türkiye Barolar Birliği Dergisi***, Sayı: 81, 2009.

Karakehya, Hakan, "Kumar Oynanması İçin Yer ve İmkân Sağlama Suçu", ***Marmara Üniversitesi Hukuk Araştırmaları Dergisi***, 2014, s. 705, (Erişim) e-dergi.marmara.edu.tr/maruhad/issue/download/5000001567/5000000627, 24.01.2017.

Kara Kılıçarslan, Seda, ***Kişilik Hakkına Saldırıda Üstün Nitelikte Özel ve Kamusal Yarar***, Yayımlanmamış Yüksek Lisans Tezi, T. C. Marmara Üniversitesi Sosyal Bilimler Enstitüsü, 2010.

Karagülmez, Ali, ***Bilişim Suçları ve Soruşturma Kovuşturma Evreleri***, Seçkin Yayınları, Ankara, 2011.

Karahasan, Mustafa Reşit, ***Tazminat Davaları***, İstanbul, 1976.

Kaymas, Serhat, İnternet ve Ulusal Kamu Politikaları: İnternet Yönetiminde Türkiye için Alternatif Öneriler, **İletişim: araştırmaları**, 5(2), 2007, (Erişim) http://dergiler.ankara.edu.tr/dergiler/23/1820/19198.pdf , 29.Eylül 2016.

Ketizmen, Muammer, ***Türk Ceza Hukukunda Bilişim Suçları***, Yayımlanmamış Doktora Tezi, T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Kılıçoğlu, Ahmet, ***Şeref ve Haysiyet ve Özel Yaşama Basın Yoluyla Saldırılardan Hukuksal Sorumluluk***, Ankara, 1993.

Kılıçoğlu, Mustafa, ***Sorumluluk Hukuku***, C.1, Sözleşme Dışı Sorumluluk, Ankara 2002.

Kızıltan, Burak, **5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları**, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006.

Koç, Serhat ve Kaynak, Selva, "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik", **Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri,** Muğla Üniversitesi, 10 - 12 Şubat 2010.

Korkmaz, İbrahim, "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme", ***TBB Dergisi***, Sayı 124, 2016.

Kurt, Levent, (2005b), ***Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması***, Seçkin Yayıncılık, Ankara, 2005b.

Kurt, Levent, ***Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanundaki Uygulaması,*** Seçkin Yayınları, Ankara, 2005a.

Leiner, M. Berry-Vinton G. Cerf-David D. Clark-Robert E. Kahn-Leonard Kleinrock -Daniel C. Lynch-Jon Postel-Larry G. Roberts-Stephen Wolff, "A Brief History of the Internet", ***ACM SIGCOMM Computer Communication Review***, 39/5, October 2009, (Erişim) http://www.cs.ucsb.edu/~almeroth/classes/F10.176A/papers/internet-history-09.pdf, 10 Kasım 2016.

Mahmutoğlu, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", ***Dergi Park, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,*** Cilt: 71, Sayı: 1, 2013.

Memiş, Tekin, "*Hukuki Açıdan Kitlelere E-posta Gönderilmesi"*, **AÜEHFD**, S. 1-4, 2001.

Milli Eğitim Bakanlığı, ***Bilişim Teknolojileri İnternet ve E-Posta Yönetimi***, Ankara, 2011.

Nacar, Fatma Burcu, ***Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları***, Yayımlanmamış Yüksek Lisans Tezi, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2010.

Noyan, Erdal, ***Ceza Hukuku 1***, Ankara, Şubat 2005.

Odabaşı, Arda, "*Bilgi Toplumu mu, Gözetim Toplumu mu?"*, **Bilim ve Ütopya**, İstanbul, 1999.

Oğuz, Habip, ***İnternet Ortamında Kişilik Haklarının İhlali ve Korunması***, Adalet Yayın Evi, Ankara, 2012.

Özcan, Mehmet, ***Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk***, Bilgi Üniversitesi Yayınları, İstanbul, 2002.

Özdilek, Ali Osman, ***İnternet ve Hukuk***, Papatya Yayıncılık, Ankara, 2002.

Özel, Cevat, ***Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı***, Yeşim Atamer (Ed.), İnternet ve Hukuk, İstanbul, Bilgi Üniversitesi Yayınları No: 51, 2004.

Özel, Sibel, ***Uluslararası Alanda Medya ve İnternette Kişilik Hakkının Korunması***, Seçkin Yayınları, Ankara, 2004.

Özen, Muharrem ve Özocak, Gürkan, "Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134***)***", ***Ankara Barosu Dergisi***, Sayı: 1, 2015.

Özen, Mustafa, "Hakaret Suçu ve İnternetle İşlenmesi", ***TBB Dergisi***, Sayı 75, 2008.

Özgenç, İzzet, ***Türk Ceza Kanunu Gazi Şerhi***, Genel Hükümler, Ankara, 2005.

Özkan, Tezcan, **Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi**, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Ağustos 2006.

Öztan, Bilge, **Medeni Hukukun Temel Kavramları**, Turhan Kitabevi, Ankara 2000.

Öztan, Bilge, ***Şahsın Hukuku Hakiki Şahıslar***, Filiz Kitabevi, Ankara, 1997.

Parlar, Ali – Hatipoğlu, Muzaffer, **"Türk Ceza Kanunu Yorumu'',** Cilt: 4, Seçkin Yayınevi, Ankara, 2008.

Peker Demir, Esra, ***İnternet Aracılığıyla Kişilik Haklarına Saldırı***, Yayımlanmamış Yüksek Lisans Tezi, Kültür Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2014.

Remzi, Mehmet, Aydın, Sezer ve Ispartalı, Murat, ***Medeni Hukuk,*** İkinci Sayfa Yayınları, İstanbul, 2010.

Sarsıkoğlu, Şenel, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", **Türkiye Adalet Akademisi Dergisi**, Yıl:6, Sayı:22, Temmuz 2015.

Sırabaşı, Volkan, ***İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz***, Adalet Yayınevi, Ankara, 2007.

Sokullu-Akıncı, Füsun, ***Avrupa Konseyi Sıber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi***, (Erişim) www.journals.istanbul.edu.tr/iuhfm/article/download/1023004153/1023003747 , 12.12.2016.

Soyaslan, Doğan, Ceza Hukuku Özel Hükümler, Yetkin Yayınları, Ankara, 2014.

Soysal, Tamer, "Elektronik Posta Yoluyla Kişilik Haklarına Elektronik Posta Yoluyla Kişilik Haklarına Müdahaleden Doğan Hukuki Sorumluluk", ***Ankara Barosu Dergisi***, Yıl: 65, Sayı: 1, Kış 2007.

Soysal, Tamer, "İnternet Servis Sağlayıcılarının Hukuki Sorumlulukları," ***TBB Dergisi***, 2005.

Soysal, Tamer, İnternet Alan Adları Sistemi ve Tahkim Kuruluşlarının UDRP Kurallarına Göre Verdikleri Kararlara Eleştirel Bir Yaklaşım-I**, Sosyal Bilimler Enstitüsü Dergisi**, Sayı: 21, Yıl: 2006/2.

Söyler, Yasin, ***Kamu Hukuku Açısından İnternet İçeriğinin Düzenlenmesi ve Bu Alanda Devletin İdari Yaptırım Uygulama Yetkisi***, Yayımlanmamış Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2013.

Şamlı, Rüya, "Türk ve Dünya Hukukunda Bilişim Suçları", **Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri**, Muğla Üniversitesi , 10 - 12 Şubat 2010.

Taner, Fahri Gökçen, Ceza Hukukunda Şantaj Suçu, ***TBB Dergisi***, 92, 2011.

Taşçı, Ufuk ve Can, Ali, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014", **Fırat Üniversitesi Sosyal Bilimler Dergisi**, Cilt: 25, Sayı: 2, Sayfa: 229-248, Elazığ, 2015.

Taşkın, Şaban Cankat, ***Bilişim Suçları***, Beta Yayınevi, Bursa, 2008.

tbmm.gov.tr, (2015), "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu (1/676).

TBMM Mevzuat Bilgi Sistemi, ***6698 Sayılı Kişisel Verilerin Korunması Kanunu*** Madde 30 (Yürürlük Tarihi: 07.04.2016), Alt Komisyon Gerekçesi, (Erişim) http://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?_afrWindowMode=0&_afrLoop=2428696326380301&psira=122834&_adf.ctrl-state=uecwm0504_34, 20.01.2017.

Tekeli, Ömer, "Bilişim Suçlarıyla Mücadelede Polisin Yeri", **Sayder Dış Denetim Dergisi**, Sayı 183, 2011.

Tepe, İlker, ***Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları,*** Yayımlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya, 2009.

Tepe, İlker, "Modern Ceza Hukuku Teorisinde İnternet ve İnternet Suçluluğunun Konumu", Veli Özer Özbek (Ed.), **Ceza Hukuku Dergisi**, Ankara, Yıl:4 Sayı:9, 2009.

Tunçbilek, Burak, *Bilişim Suçları ve Üniversite Lisans* ***Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri***, Gazi Üniversitesi Bilişim Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2012.

Turan, Metin ve Külcü, Özgür, "Türkiye'de Bilişim Suçlarının Tanımlanması ve Yaşanan İhlallere Yönelik İçerik Analizi", ***Türk Kütüphaneciliği Dergisi***, 28(1), 2014.

Turan, Metin, "Kişisel Verilerin Korunması", **Türkiye Kalkınma Bankası Yayını e-dergi**, Nisan- Haziran 2016.

Turhan, Oğuz**, Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar),** Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi, Ankara, 2006.

Tümerdem, Murat, ***İnternette Kişilik Hakkı İhlâlinden Kaynaklanan Manevi Tazminat***, Yayımlanmamış Yüksek Lisans Tezi, T.C. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2013.

Türk Ceza Kanunu Madde Gerekçeleri, ***Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar,*** İkinci Kitap, Dokuzuncu Bölüm, (Erişim) www.ceza-bb.adalet.gov.tr/mevzuat/madde**gerekce**.doc , 12 Aralık 2016.

Uğur, Hüsamettin, "Suçta ve Cezada Kanunîlik İlkesi ve Anayasa Mahkemesi Kararları Karşısında Yaptırımsız Kalan Bazı Suçlar", **TBB Dergisi**, 91, 2010, (Erişim) http://tbbdergisi.barobirlik.org.tr/m2010-91-662, 12 Aralık 2016.

Uslu, Tolga***, İnternet Güvenliği ve Risk Yönetimi***, Yayımlanmamış Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, 2007.

Uzunay, Yusuf ve Koçak, Mustafa, "Bilişim Suçları Kapsamında Dijital Deliller", **7. Akademik Bilişim Konferansı**, Gaziantep, 2-4 Şubat 2005.

Üzülmez, İlhan, ***Yeni Türk Ceza Kanunu'nun Hürriyete Karşı İşlenen Suçlar Sistemi Çerçevesinde Tehdit, Şantaj ve Cebir Kullanma Suçları***, Ankara, Turhan, 2007.

Yalçın, Filiz, ***İnternet Pazarlamasında Müşteri Memnuniyeti: Günün Fırsatları Üzerine Bir Uygulama***, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2012.

Yaman, Dilara, "Fikir Ve Sanat Eserleri Kanunu'nda Düzenlenen Bir Eserden Kaynak Göstermeksizin İktibasta Bulunma Suçu (M. 71/1-III)", ***Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi***, Cilt: 12, Özel Sayı, 2010, Basım Yılı: 2012.

Yargıtay 4. H.D. , 15.02.2001, 2000/10596 E. , 2001/1501 K. , **Yargıtay Kararları Dergisi**, C.27, S.8.

Yargıtay Ceza Genel Kurulu E. 2009/11-193, K. 2009/268, 17.11.2009, (Erişim) http://www.turkhukuksitesi.com/serh.php?did=6165 , 13 Aralık 2016.

Yargıtay Ceza Genel Kurulu E. 2009/11-193, K. 2009/268, 17.11.2009, (Erişim) http://www.turkhukuksitesi.com/serh.php?did=6165 , 13 Aralık 2016.

Yazıcıoğlu, Yılmaz, ***Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukukî Boyutları ile,*** 1997.

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

Yetim, Servet, "Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi", **Türkiye Adalet Akademisi Dergisi**, S: 17, 2014.

Yılmaz, Tuğsan, ***Bilgisayar Yazılımlarının İzinsiz ve Yetkisiz Olarak Kullanımı***, (Erişim) http://www.tugsanyilmaz.av.tr/fikri-haklar-ve-bilisim-hukuku/bilgisayar-yazilimlarinin-izinsiz-ve-yetkisiz-olarak-kullanimi, 22.01.2017.

Yılmaz, Davut, ***Hacking Bilişim Korsanlığı ve Korunma Yöntemleri***, Hayat Yayınları, 2005.

Yılmaz, Sacit, "5237 Sayılı TCK'nin 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", ***TBB Dergisi***, 92, 2011.

Yokuş Sevük, Handan, "Haberleşme Hakkının Kullanımının Türk Ceza Kanunu Hükümleri ile Korunması (TCK M.124, TCK M.298/1)", (Erişim) www.dicle.edu.tr/Contents/a3dba4dd-975a-47d3-98c3-76e3fd469268.pdf, (06.02.2017).

Yüksel, Mehmet, "Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi", ***Ankara Üniversitesi SBF Dergisi***, 58-1, 2003.

Zevkliler, Aydın - Acabey, M. Beşir, Gökyayla, M. Emre, ***Medeni Hukuk***, Türkmen Kitabevi, Ankara, 2000.

"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", **Resmi Gazete**, Kanun No: 5651, Sayı: 26530, 23 Mayıs 2007, (Erişim) http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm , 12.12.2016.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun, (Erişim) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5235.pdf , 12 Aralık 2016.

5236 Sayılı Kabahatler Kanunu, II. Kısım: Çeşitli Kabahatler, "Kumar", s. 9344.

5237 Sayılı Ceza Kanunu Madde 103, ***Çocukların Cinsel İstismarı***, (Erişim) http://www.turkhukuksitesi.com/mevzuat.php?mid=3934, 12 Aralık 2016.

5237 Sayılı Ceza Kanunu Madde 104, ***Reşit Olmayanla Cinsel İlişki***, (Erişim) http://www.ceza-bb.adalet.gov.tr/mevzuat/5237.htm , 12 Aralık 2016.

5237 Sayılı Ceza Kanunu Madde 226, ***Müstehcenlik***, (Erişim) http://www.turkhukuksitesi.com/mevzuat.php?mid=5174 , 12 Aralık 2016.

5237 Sayılı Türk Ceza Kanunu Madde Gerekçeleri Madde 107, s.51, (Erişim) www.ceza-bb.adalet.gov.tr/mevzuat/madde**gerekce**.doc , 12 Aralık 2016.

5237 Sayılı Türk Ceza Kanunu, Kumar Oynanması İçin Yer ve İmkan Sağlama, Madde 228, s. 9020.

5237 Sayılı Türk Ceza Kanunu, Madde 107, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237 , 12 Aralık 2016.

5237 Sayılı Türk Ceza Kanunu, Madde 124, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5237&MevzuatIliski=0&sourceXmlSearch&Tur=1&Tertip=5&No=5237, 12 Aralık 2016.

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.5651&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=5651 , 12 Aralık 2016.

5846 Sayılı Fikir ve Sanat Eserleri Kanunu, Madde 71, s. 2413.

6698 Kişisel Verilerin Korunması Kanunu, Madde 3: Tanımlar, (Erişim) http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf , 12 Aralık 2016, s. 12301.

6698 Sayılı Kişisel Verilerin Korunması Kanunu, Madde 2, (Erişim) http://www.mevzuat.gov.tr/Metin1.Aspx?MevzuatKod=1.5.6698&MevzuatIliski=0&sourceXmlSearch=&Tur=1&Tertip=5&No=6698 , 12 Aralık 2016.

"Aile ve Sosyal Politikalar Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun", **Resmi Gazete**, Kanun No: 6518, Sayı: 28918, 19 Şubat 2014, (Erişim) http://www.resmigazete.gov.tr/eskiler/2014/02/20140219.pdf, 25.01.2017.