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

TÜRK CEZA KANUNUNDA SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI (TCK m. 244/1, 2)

YÜKSEK LİSANS TEZİ

Sümeyra KARİPÇİN
164234001039

Danışman
Dr. Öğr. Üyesi Murat AKSAN

KONYA 2019

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Bilimsel Etik Sayfası

Öğrencinin	Adı Soyadı	Sümeyra Karipçin
	Numarası	164234001039
	Ana Bilim / Bilim Dalı	Kamu Hukuku
	Programı	Tezli Yüksek Lisans ☒ Doktora ☐
	Tezin Adı	Türk Ceza Kanununda Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244/1,2)

Bu tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını bildiririm.

Öğrencinin imzası
(İmza)

T. C.
SELÇUK ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü

Yüksek Lisans Tezi Kabul Formu

Öğrencinin	Adı Soyadı	Sümeyra Karipçin
	Numarası	164234001039
	Ana Bilim / Bilim Dalı	Kamu Hukuku
	Programı	Tezli Yüksek Lisans ☒ Doktora ☐
	Tez Danışmanı	Dr. Öğr. Üyesi Murat Aksan
	Tezin Adı	Türk Ceza Kanununda Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244/1,2)

Yukarıda adı geçen öğrenci tarafından hazırlanan "Türk Ceza Kanununda Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244/1,2)" başlıklı bu çalışma 9/9/2019 tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak, jürimiz tarafından yüksek lisans tezi olarak kabul edilmiştir.

Ünvanı, Adı Soyadı	Danışman/Üye	İmza
Dr. Öğr. Üyesi Murat Aksan	Danışman	
Prof. Dr. Berrin Akbulut	Üye	
Dr. Öğr. Üyesi M. Onursal Cin	Üye	

İÇİNDEKİLER

İÇİNDEKİLER ..... İ
KISALTMALAR VE SİMGELER ..... İV
ŞEKİLLER TABLOSU V
GİRİŞ 1

BİRİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

I. Bilişim Teknolojileri 4
II. Bilişim Sisteminin Unsurları 8
A. Temel Bilişim Teknolojileri 10
1. Bilgisayar 11
a. Donanım 13
b. Yazılım 15
2. İnternet 17
3. Cep Telefonu 20
B. Veri ve Veritabanı 21
C. Elektronik Delil 25
III. Bilişim Suçu 34
A. Kanunda Yer Alan Temel Kavramlar 37
B. Adli Bilişim 38
IV. Bilişim Suçlarının İşlenmesinde Kullanılan Yöntemler 40
A. Siber Ortam ve Siber Saldırılar 41
B. Bilgisayar/ Bilişim Sistemi Virüsleri 42
C. Sistem Güvenliğinin Kırılarak Veri İçeriğine Erişilmesi (Hacking) 43
D. Truva Atı (Trojan) 44
E. İstem Dışı Alınan Elektronik Postalar (Spam) 45
F. Ağ Solucanları 45
G. Casus Yazılımlar (Pishing) 46
H. Zararlı Yazılımlar (Malware) 46

İKİNCİ BÖLÜM

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

I. Suç Tipi Hakkında Genel Bilgiler 48

II. Korunan Hukuki Değer 52

III. Suçun Unsurları 55

A. Maddi Unsurlar 55

1. Fail 55

2. Mağdur 58

3. Suçun Konusu 60

4. Fiil ve Netice 62

a. Bilişim sisteminin işleyişinin engellenmesi veya bozulması 65

b. Bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi 68

B. Manevi Unsur 78

C. Hukuka Aykırılık Unsuru 79

IV. Suçun Nitelikli Hali 80

V. Suçun Netice Sebebiyle Ağırlaşmış Hali 81

VI. Suçun Özel Görünüş Şekilleri 82

A. Teşebbüs 82

B. İştirak 83

C. İçtima 84

VII. Suça Yönelik Yaptırım 87

VIII. Suçu Soruşturma ve Kovuşturm 88

A. TCK'da Yer Alan Hususlar 88

B. CMK'da Yer Alan Hususlar 91

1. CMK 134'üncü Maddesinin 1. Bendi 91

2. CMK 134'üncü Maddesinin 2. Bendi 93

3. CMK 134'üncü Maddesinin 3. Bendi 94

4. CMK 134'üncü Maddesinin 4. Bendi 94

5. CMK 134'üncü Maddesinin 5. Bendi..... 95
IX. BİLİŞİM SUÇLARININ ÖNLENMESİNE YÖNELİK TEDBİRLER 95
A. Bireylerin Alması Gereken Tedbirler 96
B. Kurum ve Kuruluşların Alması Gereken Tedbirler..... 99
C. Devletlerin Alması Gereken Tedbirler..... 102

KISALTMALAR ve SİMGELER

ADSL	: AsymmetricDigitalSubscriberLine (Asimetrik Sayısal Abone Hattı)
ANSI	: AmericanNational Standart Institute (Amerikan Ulusal Standart Enstitüsü)
ATM	: Automated Teller Machine (Otomatik Para Makinesi)
CMK	: Ceza Muhakemeleri Kanunu
CPU	: Central ProcessingUnit (Merkezi İşlem Ünitesi – İşlemci)
ENIAC	: Electronic NumericalIntegratorAndComputer (Elektronik Sayısal Entegreli Hesaplayıcı – İlk Bilgisayar)
GPRS	: General PacketRadio Service(Cep Telefonu Şebekeleri Üzerinden Paket Anahtarlamalı Veri Aktarımı)
GPS	: Global PositioningSystem (Küresel Konumlama Sistemi)
GSM	: Global Systemfor Mobile Communications (Küresel Mobil İletişim Sistemleri)
LAN	: LocalArea Network (Yerel Bilgi Ağı)
ODTÜ	: Orta Doğu Teknik Üniversitesi
PC	: PersonalComputer (Kişisel Bilgisayar)
POS	: Point Of Sale (Kredi Kartı İşlem Cihazı)
RAM	: Read Access Memory (Kaydedilebilir Bellek)
ROM	: Read Only Memory (Sadece Okunabilir Bellek)
SIM	: Subscriber Identity Module (Abone Kimlik Modülü)
SMS	: Short Message Service (Kısa Mesaj Servisi)
SQL	: Structured Query Language (Yapılandırılmış Sorgulama Dili)
TCK	: Türk Ceza Kanunu
TCP/IP	: Transmission Control Protocol/Internet Protocol (Ağ İletişim Portokolü)
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USB	: UniversialSerialBus (Seri Haberleşme Portu)
WAN	: WideArea Network (Uzak Bilgi Ağı)
YCGK	: Yargıtay Ceza Genel Kurulu

ŞEKİLLER TABLOSU

Şekil-1: Bilişim teknolojilerinin gelişimi7

Şekil-2. Bilişim sisteminin engellenmesi veya bozulması65

Şekil-3. Bilişim sisteminde verilerin bozulması veya değiştirilmesi68

Şekil-4. Bilişim sisteminde verilerin yok edilmesi, erişilmez kılınması veya sisteme veri yerleştirilmesi70

Şekil-5. Bilişim sitemindeki mevcut verilerin başka yere gönderilmesi75

ÖNSÖZ

Bilişim alanında yaşanan gelişmelerin insanlık tarihine olan katkısı kuşkusuz tartışılamaz. Ancak bu gelişmeler sonucu her zaman olumlu durumlar ile karşılaştığımız söylenemez. Teknolojinin ve buna bağlı olarak bilişim sektörünün gelişmesiyle ve insanların hayatlarının bir parçası olması ile birlikte değişik suç tipleri de ortaya çıkmaya başlamıştır. Bu suçlar bilişim sistemlerine karşı işlenebildiği gibi bilişim sistemlerinin araç olarak kullanılmasıyla da işlenebilmektedir. Ülkemizde de bilişim alanında yaşanan gelişmeler sonucu bu suç tipleriyle karşılaşılmaya başlanılmış ve mevzuatta düzenlemeler yapılması kaçınılmaz hale gelmiştir. İlk olarak 3756 sayılı Kanun ile 765 sayılı Türk Ceza Kanunu'nun 11. Babı'na "Bilişim Alanında Suçlar" başlığı altında 525. maddesinde düzenlemeler yapılmıştır. 5237 sayılı Türk Ceza Kanunu'muzda ise, "Topluma Karşı Suçlar" başlıklı üçüncü kısmında "Bilişim Alanında Suçlar" başlığını taşıyan onuncu bölümünde düzenlemeler yapılmıştır.

Bu tezde Türk Ceza Kanununda Bilişim Alanında Suçlar başlığı altında 244. maddede düzenlenen "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçları incelenmiştir. Yargıtay kararları ile birlikte doktrindeki görüş ayrılıklarına yer verilmiştir. Çalışmanın son kısmında ise bilişim suçlarının önlenmesine yönelik olarak alınacak tedbirlere değinilmiştir.

Tezimin hazırlık sürecinde, bilgisi ve tecrübesi ile her daim yardımcı olan ve yol gösteren tez danışmanım değerli hocam Dr. Öğr. Üyesi Murat AKSAN'a, tez savunma jürimde bulunan, bilgi ve tecrübeleri ile tezimi düzenlememde bana ışık tutan değerli hocalarım Prof. Dr. Berrin AKBULUT'a ve Dr. Öğr. Üyesi Onursal CİN'e sonsuz şükranlarımı sunarım.

Çalışmalarım sırasında bana destek olan, tezimi tamamlamam için benden daha çok çabalayan, beni cesaretlendiren canım ablam Sosyolog Hatice KARİPÇİN TEKE'ye, tez düzenlemelerim sırasında annesi ile olan kıymetli vakitlerini çaldığım biricik yeğenim Seçkin TEKE'ye ve her kararımda arkamda duran değerli babam Derviş KARİPÇİN'e, cefakar annem Şerife KARİPÇİN'e, pek kıymetli kardeşim Zehra KARİPÇİN'e, bilişim alanındaki bilgisiyle bu süreçte bana yardımcı olan, değerli arkadaşım Siber Güvenlik Uzmanı Abdullah Batuhan YILMAZ'a teşekkürü bir borç bilirim.

T. C.

SELÇUK ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin	Adı Soyadı	Sümeyra Karipçin	Numarası: 164234001039
	Ana Bilim / Bilim Dalı	Kamu Hukuku Ana Bilim Dalı	
	Tez Danışmanı	Dr. Öğr. Üyesi Murat Aksan	
Tezin Adı		Türk Ceza Kanunu'nda Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m.244/1,2)	

ÖZET

Modern çağın vazgeçilmez unsurları konumunda olan bilgisayar, cep telefonu ve tablet gibi gelişmiş teknolojik ürünler, bireylerin iş ve sosyal hayatının her alanında kullanılmaktadır. Hayatın olağan akışı içinde gün geçtikçe daha fazla ihtiyaç duyulan ses, resim, video, metin, banka bilgileri vb. verilerin işlemden geçirilmesini, depolanmasını veya başka kişi ya da sistemlere aktarılmasını sağlayan tüm bu gelişmiş teknolojik cihazlara kısaca Bilişim Sistemleri denilmektedir.

Bilişim sistemleri hayatı kolaylaştırdığı gibi, barındırdığı maddi ve manevi değerlerin yüksek ekonomik, sosyal ve politik getirisi sebebiyle, art niyetli ve suç işleme meyilli kişiler için de cazip hale gelmektedir. Bu sistemlerde suç işlenmesi kolay ancak, bu suçun ve faillerin tespiti bir o kadar zor olmaktadır. Yapılan yasal düzenlemelerle gerekli cezai müeyyidelerin uygulanarak bilişim suçlarıyla mücadele edilmesi hedeflenmektedir.

Yapılan bu çalışmada, Bilişim Suçları ile ilgili olarak TCK'nunda ifade edildiği şekliyle "sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu" na yönelik kavramlar, bu kapsamda yapılan yasal düzenlemeler ve suçun önlenmesi ya da maruz kalınmaması için birey ve kurumsal anlamda alınabilecek tedbirler incelenmiştir.

Anahtar Kavramlar: Bilişim Sistemi, Bilişim Suçu, Bilgisayar, Cep Telefonu, Veri.

T. C.

SELÇUK ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü

Öğrencinin	Adı Soyadı	Sümeyra Karipçin	Numarası: 164234001039
	Ana Bilim / Bilim Dalı	Department of Public Law	
	Danışman	Dr. Öğr. Üyesi Murat Aksan	
Tezin İngilizce Adı		Crimes Preventing, Disrupting,Destroying or Changing the System in the Turkish Penal Code (TPC Art. 244/1,2)	

ABSTRACT

Advanced technological products such as computers, mobile phones and tablets, which are the indispensable elements of the modern era, are used in every aspect of the individuals' business and social life. In the usual flow of life more and more needed sound, image, video, text, bank information and so on, all these advanced technological devices that allow data to be processed, stored or transferred to other people or systems are briefly referred to as Informatics Systems.

Information systems make life easier and are attractive for people who are malevolent and inclined to commit a crime because of the high economic, social and political return of their material and spiritual values. In these systems, crime is easy to commit, but the detection of this crime and the perpetrators becomes more difficult. It is aimed to combat cybercrime by applying the necessary penal sanctions through legal regulations.

In this study, in relation to IT Crimes, as stated in the Turkish Penal Code, the system is designed to prevent, disrupt, destroy or modify data, concepts, the legal arrangements made in this context, and the measures that may be taken in order to prevent or prevent the crime are examined.

Key Concepts: Information System, Informatics, Computer, Cell Phone, Data.

GİRİŞ

İnsanlık tarihi, insanlığın gelişimi, gelişim sürecindeki sorun ve bunlara çözüm üretme, yeni teknolojik gelişmeler ile hızla ilerlemeye devam etmektedir. Bu ilerleme içerisinde internetin hızla yayılması birçok kavramının tartışılması ihtiyacını doğurmuştur. Bilişim alanındaki gelişmeler, bir yandan insan hayatını kolaylaştırırken diğer yandan birtakım problemlere yol açmaktadır. Bilginin hızla yayılması, ekonomik, sosyal, siyasal değerinin artması ve bu değerler üzerine kolay yoldan hak sahibi olmak isteyenleri bilişim araçları vasıtasıyla suç işler hale getirmiştir[1].

Bilişim sistemleri ve bu kapsamdaki suçların, gerek işlenme gerekse sonuçları bakımından hukuki değerlendirmesi geniş bir alanı kaplamaktadır. Bu bakımdan, çalışma kapsamında bizzat bilişim sistemlerinin kendisinin kullanılarak işlenen suç tipi, diğer bir ifadeyle bilişim sisteminin "araç" değil "amaç" olduğu suç tipi incelenmiştir.

Teknoloji alanındaki gelişmeler her alanda olduğu gibi bilişim sektörünü de etkilemiş ve bu ortamda işlenen suçların niteliği sebebiyle tekrar gözden geçirilmesine ihtiyaç duyulmuştur. Ülkemizde bilişim suçlarıyla mücadele kapsamında ilk olarak, 3756 sayılı Kanun ve 765 sayılı Ceza Kanununun 11.Babı'na eklenen "Bilişim Alanında Suçlar" başlıklı 525/a, b, c ve d maddelerinde, sonrasında ise 01.06.2005 tarihli 5237 sayılı yeni Türk Ceza Kanunu'nun hazırlanmasıyla, bilişim sistemlerine karşı işlenen ya da bilişim sistemlerinin araç olarak kullanıldığı suç tipleriyle ilgili yasal düzenlemeler yapılmıştır[2].

Modern hayatımızdaki önemli sektörler olan enerji, ulaşım, iletişim, bankacılık, sağlık vb. kamu hizmetlerinde, verimlilik ve etkinliğin arttırılması amacıyla bilgi ve iletişim teknolojilerine olan bağımlılığı her geçen gün artırmaktadır. Fakat gelişen teknolojinin suçlular tarafından da kullanılması

---

1 Keskin, İbrahim, "Bilişim Suçları", *Adalet Dergisi*, Y: 99, S: 29, 2007, s.105.

2 Mahmutoğlu, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", İÜHFM, 2013, C.LXXI, S.1,s.870.

sebebiyle, bahse konu sektörler risk altına girmiş durumdadır. Kurum ve kuruluşlar mali kayıpların yanında, imaj zedelenmesi, müşteri güven kaybı vb. önemli sonuçlarla karşılaşmaya başlamışlardır. Uzun dönemde bu gibi faktörler bilişim suçları sebebiyle ortaya çıkacak zararın hesaplanmasını zorlaştırmaktadır[3].

Günümüzde bilişim suçlarıyla ilgili fail ve mağdur yelpazesi genişlemekte, mağduriyet düzeyleri artmaktadır. Örneğin; kişisel tatmin, suç kastı, siyasi ve ekonomik çıkar, bilgi toplamak, terörizm ya da psikolojik harekât vb. amaçlarla, kişi, devlet, hükümet, şirket, yönetici, suç örgütü, muhalif, terörist, casus gibi unvanlarla bilişim sistemlerine ilişkin fail ya da mağdur görebilmekteyiz[4].

Bilişim teknolojilerinin yaşadığımız hayatı etkilemesi, suçluların daha az bilgi ve tecrübeyle suç işleme fırsatı yakalamalarını doğurmuş ve bu nedenle de mahkemelerde elektronik (dijital) delil dönemi başlamıştır. Bu yeni dönemde suçla daha etkili mücadele edebilme adına ülkemizde standardizasyonu sağlanmış ve sertifikalı adli bilişim laboratuvarı kurulması ihtiyacı ortaya çıkmıştır. Gelişmiş ülkelerde bu suç türüyle mücadelede uygulanan yöntemlere nazaran, Türkiye Adli Bilişim'de henüz yeterli ilerlemeyi gösterememiştir. Halen akredite adli bilişim laboratuvar ve uzmanlarına ihtiyaç duyulmaktadır. Yalnızca hukuki düzenlemelerle bilişim suçları konusunda hedeflenen başarının elde edilemeyeceği bir gerçektir. Adli bilişim laboratuvarları sayesinde ülkemizdeki adli bilişim uzmanları kabiliyetlerini geliştirecek ve mahkemelere daha inandırıcı deliller sunulabilecektir. Adli bilişim kabiliyetlerinin geliştirilmesi ve akredite edilmiş adli bilişim laboratuvarının kurulması, bilişim suçlarıyla uluslararası geçerlilikte bir mücadele mekanizması kurulmasını da sağlayacaktır. Bilişim suçlarıyla mücadelede, ulusal bilgi güvenliği sistemlerinin geliştirilmesi ve e-devlet uygulamalarının güçlendirilmesi de önem arz etmektedir[5].

---

3 Çiçek, İlker, *Ülkemizde Adli Bilişim Laboratuvarı Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları*, Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, 2008, s.1-5.

4 Öztürk, Mustafa İ., *Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri*, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2007, s.9.

5 Çiçek, s.3.

Elektronik delil, suçun tüm yönleriyle kayıt altına alınması ve hangi boyutta işlendiğinin tespit edilmesi açısından çok önemlidir. Özellikle bilişim suçlarında, suça konu olan metanın dijital verilerden oluşması, elektronik delillerin, hukuka uygun olarak elde edilmesi, saklanması ve uygun metotlarla incelenmesi bakımından giderek önemini artırmaktadır.

Son zamanlarda ülkemizde de sık olarak görülmeye başlanan bilişim suçları konusunda yasal mevzuatta güncellenme çalışmaları yapılmakta, ancak hukuki süreci destekleyen yeterli seviyede teknik altyapı çalışmaları eş zamanlı olarak yapılamamaktadır. Ayrıca bilişim suçlarıyla mücadelede, yalnızca kolluk kuvveti değil, kamu ve özel kurumlar ile üniversiteler işbirliği içerisinde çalışmalıdır. Bu hususta, siber çağın yöntemleriyle işlenen suçların tespit edilmesi ve kanıtlarıyla ortaya konması sürecinde, yasal düzenlemelerle uyumlu, üniversitelerle işbirliği içerisinde, standartlara uygun, uzman personele ve uluslararası sertifikalara sahip adli bilişim laboratuvarlarının kurulması önemlidir[6].

Bu kapsamda hazırlanan çalışmada, bilişim suçları sürecinin hukuki boyutu ile uygulamaya ve teknik alana yönelik, adli bilişim laboratuvarlarının kurulması vb. sorunlar incelenmiştir. Hazırlanan çalışma iki bölümden oluşmaktadır;

Birinci bölümde konunun daha iyi anlaşılması için bilişim suçlarıyla ilgili kavramsal tanımlar ve bu kavramların bilişim suçları ve yapılan hukuki düzenlemelerle olan ilişkisi ve suçun işlenme şekilleri üzerinde durulmuştur.

İkinci bölümde, bilişim suçlarıyla ilgili yasal düzenlemelerin bulunduğu 5237 sayılı Türk Ceza Kanununda yer alan "bilişim suçları" açıklanmıştır ve bilişim suçlarının aydınlatılması ve önlenmesi amacıyla, kişi, kurum ve devlet ölçeğinde alınabilecek tedbirlere yer verilmiştir.

---

[6] Çiçek, s.4.

BİRİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

I. Bilişim Teknolojileri

Geniş anlamda bilişim teknolojileri; verilerin kaydedilmesi, depolanması, belli bir işlemden geçirilerek yeni bilgiler üretilmesi, üretilen bu bilgilere erişilebilmesi, tekrar saklanması veya aktarılması gibi işlemlerin etkin ve verimli olarak gerçekleştirilmesine olanak tanıyan teknolojileri tanımlamak amacıyla kullanılan terimdir. Bilişim teknolojileri, ses, resim, metin vb. sayısal verilerin elde edilmesini, işlenmesini, saklanmasını ve dağıtımını sağlayan mikro-elektronik teknolojilerine dayanan hesaplama ve iletişim sistemleridir. Bu bağlamda, öncelikle bilgisayarlar ve bunlara destek sağlayan girdi ve çıktı donanımları olmak üzere, iletişim, telekomünikasyon, belge hazırlama ve basım makineleri gibi tüm bilişim sektörlerinde kullanılan donanımlar da bu terimin kapsamına girmektedir[7].

Bilişim; kelime olarak, bilginin aktarılması, organize edilmesi, saklanması, yeniden elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler şeklinde tanımlanmaktadır. Bilişim sistemi ise, 5237 sayılı TCK'nın 243. maddesinin gerekçesinde; verilerin toplanıp yerleştirilmesinden sonra bunların otomatik işlemlere tabi tutulması olanağını veren manyetik sistemler şeklinde tanımlanmaktadır. Avrupa Konseyi Siber Suç Sözleşmesi 1. maddesine göre ise bilişim sistemi; bir programın işleyişi vasıtasıyla bir ya da daha çok unsurla ilgili verilerin otomatik olarak işleme tabi tutulmasını sağlayan, birbiriyle bağlantılı ya da benzer bir veya toplu birimi ifade etmektedir[8].

Bilişim, insanlar tarafından teknik, finansal ve toplumsal alanlarda iletişim için kullandığı ve bilimin dayanağı durumundaki bilginin, özellikle elektronik sistemler

---

[7] Kaya, Bensghir T., *Bilgi Teknolojileri ve Örgütsel Değişim*, Ankara, TODAİE Yayınları, 1996, s.38-39.

[8] Atamer, Yeşim, *İnternet ve Hukuk*, İstanbul, Bilgi Üniversitesi Yayınları, No: 51, 2004, s.363-368.

vasıtasıyla düzenli ve mantıklı biçimde elde edilmesi, elektronik cihazlarda toplanması ve işlenmesi bilimidir[9].

Bilgi-iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, yeniden elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ile bilginin kaynağından alınarak kullanıcıya aktarılmasını sağlayan genel sistem bilimidir. Bireylerin çalışma ortam ve zamanında kullandığı teknolojileri temel alan bilgi sistemlerini, şebekelerini, işlevlerini, süreçlerini ve etkinliklerini sibernetik ve otomasyonla düzenleyen unsurlardır[10].

Tanımlardan da anlaşılacağı üzere bilişim kavramının açıklanması yapılırken, "bilginin işlenmesi, aktarılması ve saklanması" sürecine vurgu yapılmaktadır[11].

Türk Dil Kurumu "Güncel Türkçe Sözlük"te bilişim kavramı; "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, informatik, enformatik." şeklinde ifade edilmiştir. Bilişim özetle, bilginin elektronik cihaz ve sistemlerle işlenmesi, iletilmesi ve depolanması şeklinde ifade edilebilir[12].

Bilişim sözcüğünün İngilizcesi "informationtechnology" olan bilgi (enformasyon) teknolojisi anlamına gelmektedir. Bilgiyi alan, işleyen ve sonuç veren cihazların yaptığı işlemlerle ilgili olarak ise İngilizce; *informatics*, Fransızca; *informatique,* Almanca; *informatik* ve İtalyanca *informatica*kelimeleri kullanılmaktadır. Yine bilişim sözcüğünün orijinali, Fransızca "informatique" kelimesinden Türkçeye geçmiştir. Dilimize ilk olarak "enformasyon" şeklinde geçen kelime, daha sonra "bilişim" sözcü olarak kullanılmaya başlanmıştır. Fakat günümüzde her iki kelime de kullanılmaktadır. Bilişim, "teknik, mali, sosyal, hukuk

---

9 Özel, Cevat, *Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*; Atamer, Yeşim (Ed.), *İnternet ve Hukuk*, İstanbul, Bilgi Üniversitesi Yayınları No: 51, 2004, s.341.

10 Aydın, Emin D., *Bilişim Suçları ve Hukukuna Giriş*, Ankara, 1992, s.92.

11 Kurt, Levent, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Ankara, Seçkin Yayıncılık, 2005, s.123.

12 Aydoğan, Hakan, *Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri*, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2009, s.6.

vb. alanlarda kullanılan verinin saklanmasını, saklanan bu verinin otomatik olarak işlenmesini, organize edilmesini, değerlendirilmesini ve aktarılmasını kapsayan bir bilim dalıdır." biçiminde ifade edilebilir[13].

Bilişim sistemlerinde bilgisayardan faydalanılmaktadır. Bilişim, bilginin daha sonra kullanılmak üzere depolanmasını, iletilmesini veya işlenerek kullanılır hale getirilmesini sağlayan akademik ve mesleki disiplindir[14].

Bilişim kavramı, hayatın içerisinde önemli bir yeri bulunan ve her türlü iş alanında ayrı bir disiplin olarak ortaya çıkan "belgeleme" ve "rapor hazırlama" tekniklerinin gelişmesiyle birlikte, insanların her konuyla ilgili veriyi muhafaza etmesini, işlemesini, düzenlemesini, analiz etmesini ve yüksek hızlı veri, ses ya da görüntü aktaran iletişim araçlarıyla bir başka yere aktarmasını içermektedir. Bu haliyle bilişim kavramı, hem verilerin işlenmesini (veri-işlem) hem de süreçten elde edilen sonuçlarının aktarılmasını (veri-iletişim) kapsar. Bu tanıma göre yalnızca veri-işlem ile veri-iletişim unsurlarını kapsayan sistemler bütünü *bilişim sistemi* niteliğinde olmaktadır. Genel olarak, bilişim kavramı ile sadece *veri-işlem* unsuru temel alınmakta, *veri-iletişim* unsuru ise göz ardı edilmektedir. Bu açıdan bakıldığında hukuk sisteminde yapılan bilişim sistemi tanımı ile bilişim sisteminden çok, bilgisayar sistemi tarifine yakın bir tanımlama yapıldığı söylenebilir[15].

Bilişim ve bilgisayar kavramlarının sıklıkla birbirinin yerine kullanılmasının nedeni olarak, bilişim kavramının bilgisayarın geliştiği dönemde kullanılmaya başlanmasına ve bilgisayarın bilgi işlemede en fazla kullanılan cihaz olmasına bağlamaktadır. Bu noktada bilişim ve bilgisayar kelimeleri arasındaki ayrımın belirtilmesi önemlidir. Bilişim kelimesi "bilgisayara göre daha geniş bir alanı kapsayıp, bu haliyle üst bir kavramdır"[16].Her bilgisayarın bir bilişim sistemi olduğunu, her bilişim sisteminin ise bilgisayar olmayabileceğini belirtmiştir.

---

13 Yenidünya, Caner A./Değirmenci, Olgun, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, İstanbul, 2003, s.27.

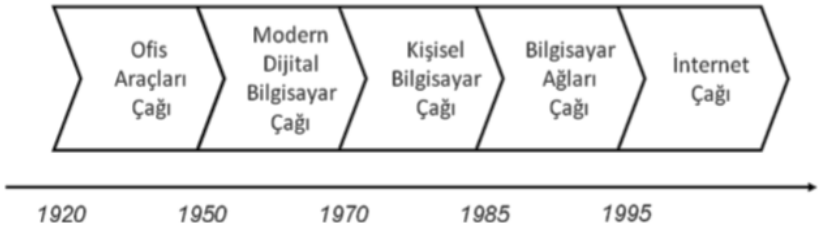
14 Yazıcıoğlu, Yılmaz, *Bilgisayar Suçları: Kriminolojik, Sosyolojik Ve Hukuki Boyutları ile*, İstanbul, 1997, s.131.

15 Erdağ, İhsan A., "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)". *Gazi Üniversitesi Hukuk Fakültesi Dergisi* C. XIV, S. 2, 2010, s.16.

16 Yenidünya/Değirmenci, s.31.

Günümüzde sık yaygınlaşan cep telefonları (akıllı telefonlar), araç bilgisayarları, tablet bilgisayarlar vb. birçok cihaz da birer bilişim sistemi durumundadır. Bilgisayarlar bilişim faaliyetlerinin gerçekleştirildiği en önemli aygıt olmaktadır[17].

Şekil-1: Bilişim teknolojilerinin gelişimi



Kaynak: Albayrak, 2007:16.

Bilişim teknolojilerinin gelişimi yukarıdaki tablodan da görüleceği gibi 1920'lerde ofis araçları çağı ile başlamıştır. 1950 ve 1970'ler arasında modern dijital bilgisayar çağı ile gelişimine devam etmiştir. 1970'den sonra 1980'lerin ortasına kadar kişisel bilgisayar çağı ile gelişimini sürdürmüştür. Daha sonra ise 1980'lerin ortasında bilgisayar ağları çağı başlamış ve gelişimini 1990'ların ortasında internet çağına bırakmıştır. Bilişim teknolojilerinin gelişimi bu şekilde olmuştur.[18]

Bilişim teknolojileri kavramına yönelik doktrinde farklı tanımlamalar yer almaktadır.

Bilginin toplanması, işlenmesi, saklanması ve gerektiğinde herhangi bir yere iletilmesi ya da herhangi bir yerden bu bilgiye erişilmesi işlemlerini, günümüzde elektronik ve optik tekniklerle otomatik olarak mümkün kılan teknolojileri bilişim teknolojilerinin kapsamına girmektedir.[19]

---

[17] Gözüşirin, Mesih, *5237 Sayılı Türk Ceza Kanununda Bilişim Suçları Ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi*, Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara, 2011, s.5.

[18] Albayrak, Ruşen A., Bilişim Sistemleri Gelişmişlik Düzeyi ve Yönetim Önceliklerinin Bilişim Sistemleri Üst Düzey Yöneticisinin Rollerine Etkisi: Finans, Sanayi, Kamu Sektörlerinde Bir İnceleme, Doktora Tezi, İstanbul Teknik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul,2007, s.16.

[19] Ceyhun, Yurdakul/Çağlayan, Ufuk M. *Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta*, Türkiye iş Bankası Kültür Yayınları, Ankara, 1997, s.96.

Bilişim teknolojilerinin organizasyonlarda bilgi toplaması, dönüştürülmesi ve dağıtılması işlevlerini icra eden insan kaynakları, bilgisayarlar ve prosedürler dizisi olduğu belirtilmektedir.[20]

Bilişim sistemleri, veri, bilgi ya da işlenmiş bilginin rakam, sayı, yazı, resim, ses ve görüntü biçiminde elde edilmesi, saklanması, düzenlenmesi, geri getirilmesi, istenilen formata dönüştürülmesi veya bir yerden başka yere aktarılmasını sağlayan teknoloji, yazılım ve insan kaynaklarının bir araya gelmesiyle oluşan bir bütündür.[21]

1960'lardan sonra teknolojide yaşanan hızlı gelişmeler, toplum hayatında köklü değişikliklere yol açmıştır. Özellikle bilginin iletilmesinde geliştirilen yeni cihazlarla, süreçler hızlanmış ve mekânın önemi azalmıştır. Bilginin önemli bir değer olması ve işlemci temelli cihazların hayat içerisinde çok yaygınlaşmasıyla yeni dönem bilişim teknolojileri çevresinde şekillenmiştir[22].

II. Bilişim Sisteminin Unsurları

Bilişim sistemleri ile ilgili farklı kaynaklarda farklı tanımlar bulunmaktadır. Tek bir tanımı bulunmasa bile tanımların ortak yönü bulunmaktadır. Bilişim "teknik, ekonomik, sosyal hukuki alanlardaki verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirmesi ve aktarılması"dır. Türk Dil Kurumu bilişimi sözlüğünde "insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi" olarak tanımlamıştır.[23]

Bilişim tanım olarak, bilgisayardan faydalanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetini,

---

20 Öğüt, Adem, *Bilgi Çağında Yönetim*, 2. Baskı, Ankara, 2003, s.156.

21 Güleş, Hasan K/Özata, Musa, *Sağlık Bilişim Sistemleri*, Ankara, 2005, s.86.

22 Tanşu, Okan, *Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler*, Atamer, Yeşim (Ed.), *İnternet ve Hukuk*, İstanbul, Bilgi Üniversitesi Yayınları No: 51, 2004, s.139-157.

23 Doğan, Ramazan, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Ankara,2014, s.6; Taşkın, Şaban Cankat, Bilişim Suçları, Bursa, 2008,s.3-4; Kurt, Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara,2005, s.23-24; Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku 6518, 6526 ve 6552 sayılı Yasa Değişiklikleri ile, Ankara, 2014, s.70-71.

bilgisayar ise bu faaliyetin gerçekleştirilmesinde en önemli etken olan cihazı ifade etmektedir[24].

Bilişim teknolojileri bütüncül bir sistemi kapsamaktadır. Bilişim sistemleri, araç ve cihazlarından oluşan donanımlar ile bu donanımlarda kullanılmak üzere özel olarak geliştirilmiş yazılım veya programları ihtiva etmektedir. Yazılım ve donanım şeklindeki iki temel unsur aracılığıyla bilgiye erişim, kullanım ve paylaşım faaliyetleri yürütülmektedir. Bilişim teknolojileri tek bir uygulamadan, belirli bir donanım ya da yazılımdan değil, birbiriyle uyumlu bir şekilde çalışan ve birleşik iş görme yeteneğine sahip unsurlardan oluşmaktadır[25].

Kurt bilişim alanının unsurlarını bilgisayar ve internet olarak ele almıştır. Bilgisayarın unsurları da donanım ve yazılım olarak ikiye ayrılmıştır.[26]

Bilişim sistemlerinin genel çalışma metodolojisi, girdi, çıktı, dönüt ve tüm bunların yer aldığı süreç gibi unsurlardan oluşmaktadır. Bu bağlamda bilişim sistemleri için girdi (input), organizasyon içi ya da dışından elde edilen ham verilerin bütününü oluşturmaktadır. Ham verilerin toplanmasından sonra işlenmesi, analiz edilmesi ve anlamlı bilgiler haline getirilmesine verinin işlenmesi (transaction) denilmektedir. Çıktı (output) ise, işlenmiş olan bilginin (information), ihtiyaç duyulan yer ya da kişilere dağıtılmasıdır. Genel sistem içinde, üretilen çıktıların organizasyon dâhilinde ilgili birimler tarafından yapılan analizler sonucunda oluşan dönütler, doğru girdilerin yeniden yapılmasına ve çıktıların elde edilmesine yardımcı olmaktadır.[27] Bu kapsamda bilişim teknolojileri, organizasyon içi ve dışı ile ilgili insanlar için önemli bilgileri içermektedir[28].

---

24 Taşkın, Şaban Cankat, s.4.

25 Karadal, Himmet/Savaş, Orhan/Kazan, Halim, *Bilişim Teknolojilerinin Yönetim Sürecine Etkileri: Aksaray'da Bir Araştırma*, Bilgi Teknolojileri Kongresi Bildiri Özetleri, 2002, s.71-76

26 Kurt, Levent, s. 27-40.

27 Şener, Selçuk, *Karar Destek ve Üst Yönetim Bilişim Sistemleri ve Türkiye'de Bilişim Sektöründe Bir Analiz*, Yüksek Lisans Tezi, Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006, s.45.

28 Karahoca, Adem/Karahoca, Dilek, *İşletmeciler, Mühendisler ve Yöneticiler İçin Yönetim Bilişim Sistemleri ve Uygulamaları*, İstanbul, 1998, s.8.

Bilişim suçlarının işlenmesi açısından değerlendirilme yapıldığında, bu suç türünün yukarıda bahsedilen girdi ve çıktı arasındaki döngü içerisinde veya çıktının kaydedildiği ortamda yer alan veri üzerinde gerçekleştirildiği değerlendirilmektedir.

A. Temel Bilişim Teknolojileri

Bilgi yönetiminde önemli donanım teknolojilerinin bilgisayar, telefonlar (özellikle akıllı cep telefonları), internet ve elektronik sistemler olduğu söylenebilir.

Bilişim sistemlerinin kapsamına bilgisayarlarla ilgili tüm donanım ve yazılımların yanı sıra, mikro elektronik, bütünleşik devreler, iletişim teknolojileri, multimedya ve bioteknoloji sistemleri de girmektedir[29].

Günümüzde bilgisayarların son derece gelişmiş olması nedeniyle iletişim teknolojisinde de buna paralel bir gelişme yaşanmıştır. İletişim sistemleri elektronik mesaj oluşturmak, göndermek, gönderilen bu mesajları almak ve kaydetmek için kullanılan sistemlerdir. İletişim sistemlerinde veri, elektronik sinyal olarak işlem görür, iletişim kanalları aracılığıyla gönderilir ve alınır. İletişim alanındaki en önemli gelişmelerden biri, veri iletiminde analog teknolojiden dijital teknolojiye geçişle sağlanmıştır. Dijital sistemler, bilgisayar destekli iletişim unsurlarının kullanımını büyük oranda artırmıştır. Bu sayede çok büyük orandaki bilgiler hızlı ve hatasız biçimde hareket edebilmektedir. Bir diğer önemli gelişme ise iletişim kanallarının değişimidir. Fiber optik hatlar ve uydu sistemleri kullanılmaya başlanmış geleneksel iletişim araçlarında karşılaşılan sorunlar ortadan kalkmıştır. Organizasyonların büyük verileri iletmek için gereksinim duydukları sürat ve kapasite önemli miktarda artış göstermiştir[30].

Bilişim teknolojilerindeki değişimlerin hızla ortaya çıkması iş çevrelerinin bilişim sistemlerine olan talebini ve desteğini artırmıştır. Küresel rekabet ortamında kurumlar ve şirketler farklı amaçlar ve beklentilerle bilişim teknolojilerinin desteğine

---

29 Ege, İlhan/Sezer, Sevgi, *Bilgi Teknolojileri Kullanımı İle Akademik Verimlilik İlişkisi: Erciyes Üniversitesi Örneği,2004,* https://ilhanege.com, Erişim tarihi: 20.12.2018.

30 Bülbül, Hasan, *Rekabet Üstünlüğü Sağlamada Ürün ve Süreç Yeniliği: Bilişim Teknolojileri Uygulaması*, Basılmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2003, s.119.

ihtiyaç duymaktadır. Bu kapsamda bilişim sistemleri örgütlere stratejik avantajlar sunmaktadır. Bilginin doğru karar vermede kullanılması ve gelecekle ilgili belirsizliğin azaltılmasında en önemli unsur olduğu kabul edilmektedir[31].

Bilgi ve iletişim teknolojileriyle, iletişim hızı artmış, maliyetler düşmüş, daha hızlı ve ucuz etkileşim sağlanmış, birçok ürün ve faaliyetin entegre ağlar sayesinde dağıtımı kolaylaşmış ve küreselleşme olgusu gelişmiştir. Yine bilişim sistemleri doğrudan ve hızlı iletişim bağlantısı kurulmasını, ekonomik uzaklıkların azaltılmasını, iş dünyasının faaliyetlerinin koordinasyonu için gereken zamandan tasarruf edilmesini, transfer maliyetlerinin düşmesini ve ekonomik pazarın uluslararası boyutta günün her saati yapılabilmesini sağlamıştır[32].

1. Bilgisayar

Son 50 yıla damgasını vuran bilgisayarlar günümüzdeki gelişmiş haline ulaşıncaya kadar ilk olarak hesaplamalara destek olan makineler şeklinde ortaya çıkmıştır[33].

Bilgisayar kelimesi dilimize İngilizce "computer" (hesaplayıcı) kelimesinden geçmiş ve ilk olarak kompütür ve elektronik beyin gibi kelimelerle ifade edilmiştir. Zamanla *bilgisayar* kelimesi benimsenmiştir[34]. Bilgisayar, programlar aracılığıyla verilen komutlara göre işlem yapmakta, verileri aritmetik veya mantıksal işlemlerle işlemekte, işlediği verilerden elde edilen bilgileri depolamakta veya yeni sonuçlar üretebilen dış cihaz ve sistemlerle veri haberleşmesi yapabilmektedir[35].

---

31 Ay, Mustafa, *Bilişim Teknolojilerinin Muhasebe Denetiminde Kullanılması ve Türkiye'de Faaliyet Gösteren Bağımsız Denetim Firmalarında Bilişim Teknolojilerinin Kullanım Düzeyi Üzerine Bir Araştırma,* Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2007, s.49.

32 Akdoğdu, Pınar/Şahin, Mehmet, *Bilişim Teknolojilerindeki Gelişmenin Turizm Sektörüne Etkisi ve Kullanım Alanları*, 2004, https://www.Bilgiyonetimi.org , Erişim Tarihi: 07.01.2019.

33 Bülbül, Hasan, *Rekabet Üstünlüğü Sağlamada Ürün ve Süreç Yeniliği: Bilişim Teknolojileri Uygulaması*, Basılmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2003, s.117.

34 Topaloğlu, Mustafa, *Bilişim Hukuku*, Adana, 2005, s.145; Karagülmez, Ali, Bilişim Suçları ve Soruşturma ve Kovuşturma Evreleri,5. Baskı, Ankara, 2014, s.48.

35 Kurt, s.28-29.

Kişisel bilgisayarların üretimi için milat 1981 yılı olmuştur. IBM firması tarafından Ağustos 1981'de ev ve ofis kullanımı için kişisel bilgisayarlar niteliğindeki PC5150 bilgisayarı üretilmeye başlanmıştır. Günümüzde bilgisayarlara Kişisel Bilgisayar (PersonalComputer - PC) denilmesinin kökeninde, IBM firmasının ilk kişisel bilgisayar olarak piyasaya sunduğu PC5150 modelindeki "PC" ibaresinin etkisi çok büyüktür[36].

Bilgisayarlar temel olarak giriş-çıkış aygıtları ve belleklerden oluşmaktadır. Bunun yanında, her türlü sembolleştirilmiş işlemi yapabilen ve bu işlemleri belleğine kaydedilmiş programlarla gerçekleştiren bir ana işlemcisi bulunmaktadır. Veriler üzerinde dönüştürme işlemi yapan işletim sistemi ile verileri belirli bir düzende saklayabilmektedir. Üzerine farklı yazılımlar yüklenerek aynı yöntemle verileri çıkartılabilmekte, veri iletişimi yapabilmekte, her türlü işlemi yapabilmek için genel amaçlı olarak üretilmişlerdir[37].

Bilgisayar en basit haliyle "girdi", "süreç" ve "çıktı" işlemlerini gerçekleştiren bir yapıya sahiptir. Bilgisayara girdi işlemi, program ve giriş değerleri ile gerçekleştirilir. Daha sonra girdiler hafıza denilen alanda tutularak işlem ve komutlarla istenilen çıktı elde edilebilir.[38]

Bilgisayar sistemleri ilk üretildiği yıl olan 1940'lardan itibaren çalışma mantığı bağlamında temel olarak hiç değişmemiş, ancak en basit modelden günümüze kadar işlemci hızları, işlem yapabilme kapasiteleri ve veri depolama büyüklükleri gibi birçok alanda inanılmaz gelişmeler yaşanmıştır.

Bilgisayarları bir araya getiren parçalar somut ve soyut unsurlar olarak ikiye ayrılmaktadır. Somut unsurlara İngilizce "hardware" sözcüğünün karşılığı olan "*donanım"* ve soyut unsurlarına İngilizce "software" karşılığı olan "*yazılım"* adı verilmiştir[39].

---

36 Aydoğan, s.29.

37 Dülger, Murat V., *Bilişim Suçları*, Ankara, 2004, s.43.

38 Karagülmez, Ali, Bilişim Suçları ve Soruşturma ve Kovuşturma Evreleri,s.48.

39 Dülger, s.39.

a.Donanım

Temel olarak bir bilgisayarda teknik açıdan bulunması gereken asgari donanım üniteleri; merkezi işlem birimi (Central ProcessingUnit - CPU), kalıcı hafıza (Read Only Memory - ROM), geçici hafıza (Read Access Memory - RAM) ve çevre giriş-çıkış birimlerinden oluşmaktadır[40].

Merkezi işlemci birimi ya da *mikro işlemci* olarak tanımlanan CPU, giriş ünitelerinden gelen verileri mantık (logic) işlemlerinden geçirir, bu işlemleri denetler, işlem sonuçlarını bilgisayar kullanıcısına sunar ve geçici veya kalıcı olarak saklar[41].

Merkez işlem birimi, belirli mantık ve matematik işlemlerini elektronik olarak yapabilecek şekilde gelişmiş entegre devrelerden (yonga) oluşmuştur[42]. Bilgisayarların içinde gerçekleşen bütün işlemlerin temelinde CPU bulunmakta ve işlemler burada yapılmaktadır[43].

Salt okunur bellek şeklinde tanımlanan ROM, bilgisayarlarda yapılan temel işlemler için gerekli olan verilerin depolandığı bellek ünitesidir[44]. Adından da anlaşılacağı üzere yalnızca veri okuma işlemi yapılabilmekte, bilgisayar kullanıcısı tarafından veri yazma ya da veri değiştirme işlemi yapılamamaktadır. Bu hafıza birimini mikro işlemci ünitesi sadece veri okumak amacıyla kullanmakta, veri kaydetmek için kullanmamaktadır[45]. ROM'a üretici firmalar tarafından bilgisayarın ilk açılması esnasında yürütülecek işlemleri gerçekleştiren ve çalışması sırasında da gerekli olacak kalıcı program ve veriler kaydedilmektedir. ROM'daki bilgiler elektrik beslemesinin kesilmesi ile silinmezler ve her zaman kalıcıdır. ROM bilgisayar üretimi esnasında üretici tarafından yerleştirilmiş programları içerir.

---

40 Yenidünya/Değirmenci, s.21.

41 Kurt, s.31.

42 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.9.

43 Yaycı, Esra, *Bilişim Suçları*, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2007, s.6.

44 Dülger, s.40.

45 Kurt, s.32.

Bilgisayarın en temel işlevleri yapabilmesini sağlayan bu programlara temel giriş çıkış sistemi BIOS (Basic InputOutputSystem) adı verilmiştir[46].

Geçici hafıza birimi olan RAM, bilgisayarın üzerinde işlem yaptığı bellek ünitesidir. Bilgisayar elektriğinin kesilmesi durumunda RAM bellekteki bilgiler silinmekte, diğer bir ifadeyle kaybolmaktadır[47]. Bilgisayar işlem yaparken verileri bu bellek üzerinde tutmaktadır. Giriş birimlerinden gelen veriler önce RAM belleğe gelmekte ve daha sonra CPU tarafından bu veriler ihtiyaç duyuldukça alınarak işlenmektedir. CPU içinde işlenen veriler yine RAM belleğe gitmekte, sonuçta ise RAM bellekten çıkış ünitelerine aktarılmaktadır[47].

Bir diğer donanım ünitesi olan çevre giriş birimleri, bilgisayara veri girişi yapılmasını sağlayan sistemlerdir. Bunlar; klavye, mouse (fare), disket sürücü, CD ve DVD sürücü, tarayıcı (scanner) ile depolama üniteleri olan USB Flash bellek, taşınabilir hard disk, kart okuyucu vb. sistemlerdir. Çıkış birimleri ise bilgisayarda üretilen verilerin kullanıcıya sunulmasını sağlamaktadır. Çıkış birimleri; yazıcı (printer), ekran (monitör), USB Flash bellek, taşınabilir hard disk ve kart okuyucular vb. sistemlerden oluşmaktadır. Teknolojik gelişmeler paralelinde yeni ve üstün özelliklerde çevre giriş-çıkış birimleri üretilmektedir. Göz kapağı hareketlerini izleyen veya göz bilgilerinden insanları tanıyan sensörler, insan sesini doğrudan bilgisayara aktararak komut verilmesini sağlayan cihazlar veya beyin dalgaları ile bilgisayarları kontrol edebilen teknolojik sistemler örnek verilebilmektedir[48].

Bilgisayarlarda işlem yapabilmek için öncelikle bazı verilerin girilmesi gerekmektedir. Bilgisayarlarla veri ve bilgi alışverişi yapmamızı sağlayan ünitelerin tamamına çevre birimleri denilmektedir[49]. Bu birimler sayesinde kullanıcılar bilgisayarla iletişim kurabilmektedir.

---

46 Yenidünya/Değirmenci, s.24.

47 *Bilgisayar Nedir?* http://w3.gazi.edu.tr/~akaraci/bilgkull.htm, Erişim Tarihi: 13.12.2018.

48 Gözüşirin, s.14.

49 Çekiç, Burak, *İnternet Aracılığı İle İşlenen Suçlar*, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006, s.9.

b. Yazılım

Bilgisayarı oluşturan fiziksel parçalar durumundaki donanımlarda yaşanan gelişmelerden tam anlamıyla yararlanılması, kısaca donanım işlemlerini harekete geçiren ve yönlendiren komutlar olarak ifade edilen yazılım yani programların da geliştirilmesini sağlamıştır. Yazılım alanında kullanıcılar için iki alternatif bulunmaktadır. Bunlardan birincisi, profesyonel programcılar yazılım satıcılarından elde edilen hazır yazılım paketlerini tercih etmektedir. Bu sayede bilgisayarlar için ucuz, kullanımı kolay ve her sektöre hitap edebilen yazılım paketleri geliştirilmiştir. Yazılım paketleri diğer bir ifadeyle bilgisayar programları eğitim, mühendislik, hukuk gibi çok farklı alanlarda ses, grafik ve mekanik özelliklerde kullanıcıların hizmetine sunulmuştur[50].

Bilişim cihazlarında her türlü veri yazılımlar sayesinde elektronik biçimde toplanabilmekte, saklanabilmekte ve işlenebilmektedir[51]. Yazılımlar, bilgisayarlarla iletişim kurulmasına yardımcı olan dil durumundadır[52]. Yazılımların işlevleri genel anlamda, bilgisayar donanımının iş yapabilmesi için belirli bir mantık çerçevesinde hazırlanmış komutlardır[53].

Bilgisayar programları kullanıcıların istediği her türlü işlemi yapabilmesine imkan tanımaktadır. Bilgisayar programları üç ana grupta toplanmaktadır[54]. Bunlardan ilki, bilgisayar sistemine kendi kendisini nasıl çalıştıracağını tarif eden ve işletim sistemi denilen sistem programları, ikincisi diğer yazılım geliştirme araçları ile hazırlanan ve bilgisayarın anlamadığı programları, anlayabileceği bir dile dönüştüren çevirici programlarıdır. Üçüncü grup programlar ise, kullanıcılara ait özel bir işin yapılması amacı ile kullanılan uygulama programlarıdır[55].

---

50 Bülbül, s.35.

51 Akıncı, Hatice/Alıç, Emre/Er, Cüneyd, Türk Ceza Kanunu ve Bilişim Suçları, Atamer, Yeşim (Ed.), İnternet ve Hukuk, *Bilgi Üniversitesi Yayınları*, İstanbul No: 51, 2004, s.171.

52 Yazıcıoğlu, s.31.

53 Yaycı, s.7.

54 Topaloğlu, Mustafa, *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması*, İstanbul, 1997, s.25-28.

55 Yenidünya/Değirmenci, s.47.

Bilgisayar kullanıcısı ile bilgisayar arasında köprü vazifesi gören sistem yazılımına *işletim sistemi* (operatingsystem) denilmektedir. İşletim sistemleri bulundukları bilişim sisteminin çalışmasını ve temel fonksiyonların yerine getirilmesini sağlayan yazılımlardır. Kullanıcılar bilgisayarda yapmak istedikleri işleri işletim sistemi ve işletim sistemi üzerinde çalışan yazılımlar vasıtasıyla gerçekleştirirler[56].

Yazılımlar algoritmalardan oluşmaktadır[57]. Algoritmalar geniş anlamda, verilerden hareketle istenen sonucun nasıl alınacağını gösteren bir uygulama metodudur. Farklı sektörler için hazırlanan uygulama yazılımları ise, işletim sistemi ile uyumlu çalışarak bilgisayarın belirli bir görevi yerine getirmesini sağlayan programlardır. Örneğin; Kelime İşlemci Programı (Microsoft Word), Veri Tabanı Programı (Microsoft Access), Sunu Hazırlama Programı (Microsoft Power Point), Web Sayfası Hazırlama Programı (Microsoft Front Page) gibi programlar birer uygulama yazılımıdır[55]. Bu alanda neredeyse sınırsız sayı ve özellikte program geliştirilmiş durumdadır.

Bilgisayar teknolojileri son yıllarda ivme kazanmıştır. Yeni nesil bilgisayarlar, eski nesil bilgisayarlardan daha hızlı, daha yüksek miktarda veri işleme kapasitesine sahip ve daha düşük maliyettedirler[58].

Basit bir ifadeyle, yazılımlar donanımlara "nasıl davranacağını" ve "hangi işlemleri yapacağını" anlatmaktadır. Bilgisayar açıldığında CD-DVD sürücülerini, sabit sürücüleri ve diğer donanımları tanıyan BIOS, Windows, Linux ve Android gibi işletim sistemleri ile kelime işlemci programları, web tarayıcıları, antivirüs programları vb. tüm uygulama programları birer yazılımdır. Ayrıca yazılımların çalışması için gereksinim duyacağı değişik donanımlar olabilmekte ve bu donanımı bulunmayan bilgisayarlarda bu yazılım çalışmamaktadır.

---

56 Kurt, s.35.

57 Dülger, s.41.

58 Süzer, H.D., "Yükselen 4 Teknoloji", *Digital Dergisi*, No.11, 2004, s.28-31.

2. İnternet

Bilgisayar ağı olarak adlandırılan internet, bilgisayarların birbiri ile iletişim kurmasını sağlayan fiziki ortam ve bu ortamın fonksiyonunu gerçekleştirebilmesini sağlayan donanımlardan oluşmaktadır. Ağların ağı olarak da adlandırılan internet, "international" ve "network" kelimesinin bir araya gelmesinden oluşmaktadır[59]. Bilgisayarların birbirleri ile iletişime geçmesi için, öncelikli olarak aralarında fiziksel bir altyapının kurulması ve iletişimin gerçekleşebilmesi için bu bilgisayarların aynı dili kullanıyor olması gerekmektedir[60]. Bilgisayarlar arasındaki bağlantı bakır teller, fiber optik kablolar, radyo-link sistemleri, haberleşme uyduları, kızılötesi iletişim sistemleri, radyo dalgaları ile haberleşen sistemlerden herhangi birisi ile yapılabilmektedir[61].

İnternet dünya çapındaki küçük büyük bilgisayar ağlarının aralarında bağlantı kurmalarıyla gelişen ağlar arası bir ağdır[62]. Bu ağların toplamından oluşan internet, bilgiye ve bilişim kaynaklarına küresel boyutta erişimi sağlamaktadır[63].

Küresel rekabet ve bilişim teknolojisindeki gelişmelerle birlikte, örgütlerde bilgisayarların bağımsız terminaller yerine birbiriyle bağlantılı iş istasyonları olarak kullanılması doğmuştur. İlk olarak 1969 yılında telefon hatları üzerinden birbirine bağlanan dört bilgisayarla ARPANET isimli bir ağ bağlantısı kurulmuş ve günümüzde tüm dünyayı birbirine bağlayan internet ortamının gelişmesi sağlanmıştır. Önceleri sadece işlemlerin otomatik yapılması için yararlanılan internet ağlarından çağımızda, bilginin hızlı ve güvenilir biçimde iletilmesi ve paylaşılması, organizasyon içinde ve organizasyonlar arasında ortaklaşa cevaplar bulunması gibi stratejik konularda yararlanılmaktadır[64].

İnternet üzerinden ağ sayesinde iletişim kuran bilgisayar sistemleri olan askeri iletişim sistemi SAGE (Semi-Automatic Ground Environment) ve ticari havayolu

---

59 Yenidünya/Değirmenci, s.34-36.
60 Demirkol, Zafer, *İnternet Teknolojileri*, İstanbul, 2001, s.2.
61 Çekiç, s.45.
62 Sınar, Hasan, *İnternet ve Ceza Hukuku*, İstanbul, 2001, s.23.
63 Yaycı, s.14.
64 Bülbül, s.87.

rezervasyon sistemi olan SABRE (Semi-Automatic Business Research Environment 1950'lerin başında başlamıştır. 1960'larda ise ARPA (the Advanced Research Projects Agency, ABD'nin savunma sistemi ARPANET'in (the Advanced Research Projects Agency Network) tasarım finansmanı olmaya başladı. Bu projelerin sayesinde 1969 da internet o dönemin zirvesine ulaşmış ve bu tarihten sonra ARPANET, İNTERNET olarak hayatımıza girmiştir. 70'li yıllarında başında ise Amerika üniversitelerine bu projeden yararlanmaları için imkan verilmesinden sonra e-posta (SMPT) ve NNTP uygulamaları yaygınlık kazanmaya başlamış ve ardından da FTP ve HTTP uygulamaları izlemiştir.[65]

Amerikan Yüksek Mahkemesi Kararına göre, "internet ve birbiri ile bağlı bulunan bilgisayarlardan oluşan uluslararası ağdır. İnternet, bireylerin dünya çapında haberleşmesi için tamamen yeni ve benzeri olmayan bir ortamdır" [66].

Modern yaşam ile birlikte internet kullanımı yaygınlaşıp, her alanda ihtiyaç duyulan bir sistem haline gelmiştir. İnternet üzerinden bankacılık işlemleri yapılabilmekte, canlı görüntülü konuşma yapılabilmektedir, elektronik ileti aracılığıyla hızlı, ucuz ve basit haberleşme sağlanabilmektedir, bireylerin fikirlerini paylaştıkları forumlar ve haber grupları aracılığıyla da, dosya, fotoğraf ve görüntü paylaşımı yapabilmektedir. Ayrıca haberler internetten alınabildiği gibi bazı internet sayfaları aracılığıyla bilimsel araştırmalar yapılabilmekte olup, bilimsel yazılara ve kitaplara ulaşılabilmektedir[67].

Sistem içerisindeki farklı özellikteki bilgisayarların birbirlerini tanımasına ve aralarındaki uyuşmazlıkları çözmeye yarayan, günümüzde ise dünyadaki bilgisayarların ve yerel ağların birbiriyle iletişim kurmasını sağlayan kurallar bütünü olan TCP/IP (Transport Control Protocol/İnternet Protocol) kuralları gibi kurallar

---

65 Doğan,Ramazan, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları,s.11.

66 Karagülmez, Ali, s.53; aynı görüşte Doğan, Ramazan, s.11.

67 Taşkın, Şaban Cankat, s.14.

geliştirmiştir. Bu kuralların olduğu sistem sonradan sivil bilgisayarların kullanımına açılmıştır ve 1990'da sistem daha da geliştirilerek bugünkü halini almıştır.[68]

Ülkemizde ise internetin kurulmasını ODTÜ (Orta Doğu Teknik Üniversitesi) sağlamıştır. İlk kez Nisan 1993'te TÜBİTAK tarafından desteklenen bir projeye bağlı olarak ODTÜ'de gerçekleştirilen ağ bağlantısının amacı, akademik ortamda bilimsel veri iletişimi yapmak şeklinde olmuştu[69].

İnternet'te gerçekte bir merkez bulunmamaktadır. Ara merkezlerde bulunan bilgisayarların elektronik araçlar vasıtası ile birbirine bağlanmasıyla internet ağı oluşmaktadır[70].

İnternet birden fazla haberleşme ağından oluşan, ses, video ve veri içeren tüm bilgilerin paylaşıldığı ve bilgisayarlar arasında karşılıklı olarak iletildiği bir ağ sistemidir. Bilgisayar ağları genel olarak LAN ve WAN olmak üzere ikiye ayrılmaktadır. LAN (LocalArea Network) türü ağ bağlantılarında temel özellik, sistemlerin aynı ortamda ve birbirlerine yakın mesafede bulunmasıdır. Bir ofisteki bilgisayarların birbirleri ile bağlantı içinde olması LAN sistemlerine örnektir[71]. WAN (WideArea Network) ise, uzak mesafelerdeki bilgisayarların birbirleriyle bağlantılı olarak veri alışverişi yapabilecekleri ağ sistemleridir[72].

---

68 Taşkın, Şaban Cankat, s.13; Dülger'e göre ağ içindeki bilgisayarların birbiriyle iletişim kurabilmeleri ve veri aktarımında bulunabilmeleri için bir takım kurallara uygun hareket etmeleri gerekmektedir. Bu kurallar iletişimdeki veri trafiğinin kurallarını oluşturduğundan dolayı etkin bir iletişim sağlarlar. Bu kurallara "TCP/IP Protokolü" denilir. Bu protokol iki ayrı protokolün bir araya gelmesiyle oluşmaktadır. Bunlardan "TCP" iletilerin doğru yere aktarılmasına, "IP" adresleme sisteminden sorumludur (Dülger, Murat V., Bilişim Suçları ve İnternet İletişim Hukuku 6518,6526,6527 ve 6552 sayılı Yasa Değişiklikleri ile, Ankara, 2014,s.83), Kurt'a göre askeri amaçlarla oluşturulan internetin bilimsel amaçlarla kullanılmak istenmesiyle ve bir kısım ticari hesapların etkili olmasıyla herkesin kolaylıkla dahil olabildiği bir protokol diliyle (TCP/IP) umuma açılmıştır (Kurt, Levent,Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,Ankara,2005,s.42).

69 Dülger, s.61.

70 Dilber, Caner, *Bilişim Teknolojilerinin Bilgi Yönetimi Üzerine Etkisi: İstanbul'da Bilişim Sektörü Üzerine Bir Uygulama*, Yüksek Lisans Tezi, Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Kütahya, 2008, s.39.

71 Özdilek, Ali O., *İnternet ve Hukuk*, Ankara, 2002, s.14.; Karagülmez, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s.52.

72 Gözüşirin, s.19.; Karagülmez, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s.52.

İnternet, çok sayıda bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında yaygınlaşmış ve sürekli büyüyen bir iletişim ağıdır. Internet, insanların her geçen gün gittikçe artan üretilen bilgiyi saklama, paylaşma ve ona kolayca ulaşma istekleri sonrasında ortaya çıkmış bir teknolojidir. Bu teknoloji yardımıyla pek çok alanla ilgili bilgiye insanlar erişebilmektedir. Bu özelliğiyle internet, büyük bir bilgi hazinesi, büyük bir kütüphane, günümüzde eşsiz bir bilgi denizine benzetilmektedir[73].

Bilgi yönetimi bakımından intranet, internet araç ve teknolojilerini kullanarak işletme içi bilgi dağıtım sistemi şeklinde tanımlanmıştır. İşletmeler bilgi paylaşımı, kurum içi iletişimin arttırılması, departmanlar arası işbirliklerinin desteklenmesi gibi sebeplerle intranet sistemlerini kurma yoluna gitmektedirler[74].

Bilişim teknolojilerinin günümüzde temelini oluşturan internetin geçmişi çok eski olmasa da büyük bir hızla gelişmiş ve bunun sonucunda yeni bir dünya yapısı ortaya çıkartmıştır. Sanal ortamla oluşan bu yapı engel tanımadan büyümüş ve ülkelerin arasındaki sınırları kaldırmıştır. Bilişim ve iletişim alanında günümüzde en popüler araç bilgisayar ve internet teknolojileri olmuştur[75].

3. Cep Telefonu

Bilişim teknolojisi olarak telefon sistemleri, kendi içinde sabit telefon ve kablosuz telefon (GSM) olmak üzere ikiye ayrılmaktadır. Sabit telefon hatları özellikle sözlü ve yazılı bilgi yönetiminin önemli parçasıdır. Son yıllarda GSM şirketlerinin hizmet ağlarını geliştirmeleri, Android vb. geliştirilen yeni yazılımlar ve akıllı telefonlar gibi yeni donanımlarla cep telefonlarının bilişim alanında kullanılması çok yaygınlaşmıştır. Telefonun bilgi yönetimindeki temel fonksiyonu bilgi elde edilmesi, saklanması ve iletilmesi olmuştur. Bu sistemlerle hem açık bilgi üretilmekte hem de kapalı bilgiler elde edilmektedir. Örneğin; cep telefonu ile bir

---

73 Sevim,Şerafettin/Öncel, Mesut, *İşletmelerde Bilişim Teknolojilerinin Kullanım Düzeyinin Belirlenmesine Yönelik Bir Saha Çalışması*, İNET. TR. 02 Konferans Sunusu,2002, s.56.

74 Karagül, Aziz, *Bilgi Yönetim Sürecinde Kurumsal Kaynak Planlaması Uygulamalarının Muhasebe Bilgi Sistemine Etkisi*, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s.25.

75 Sevim/Öncel, s.45.

müzik sitesinden açık bilgi olarak müzik dinlenmesi yapılırken kapalı bilgi durumundaki kullanıcının bilgileri de bu hizmeti sağlayan servis sağlayıcısı tarafından kayıt altına alınmaktadır[76].

Cep telefonlarının GSM şebekesinden hizmet alabilmesi için abone kartı olan SIM kartlara ihtiyaç duyulmaktadır. SIM kartlar dahili bir belleğe sahiptirler ve bu bellekte adli bilişim açısından kıymetli bilgiler bulunabilmektedir. Bu bilgilere örnek olarak telefon rehber bilgileri, son arama bilgileri (arayan, aranan ve cevapsız çağrı bilgileri), kısa mesajlar (SMS) ve GSM şebekesine ait bilgiler verilebilmektedir[77].

B. Veri ve Veri tabanı

Veri, olaylara ilişkin nesnel gerçekler olup, kurumsal anlamda işlemlerin belirli bir yapıda kaydedilmesidir. Modern kurum ve şirketlerde veriler, teknolojik ve elektronik ortamlarda saklanmaktadır[78].

Veri, bilgi hiyerarşisinin en alt basamağında bulunmaktadır. Ham sembol ve gerçekler birer veridir. Veri tek basına bir anlam ifade etmemekte, olaylar hakkında birbirinden bağımsız nesnel gerçekleri temsil etmektedir[79].

Bir diğer tanıma göre veri, bilgilerin belirli bir formata dönüştürülmüş halidir. Bilişim sistemleri tarafından depolanabilen, üzerinde işlem yapılabilen her şey veridir.[80] Avrupa Siber Suçlar Sözleşmesinde ise veri "bilgisayar sisteminin belirli bir işlemi yerine getirmesini sağlayan, yazılımlar da dahil olmak üzere, bilgisayar sisteminde işlenmek için en uygun özellikleri bulunan her türlü bilgidir"[81].

---

76 Karabağ, Solmaz F., "Bilgi Yönetiminde Donanım ve Yazılım Teknolojileri", *Çukurova Üniversitesi Sosyal Bilimler Derisi*, Cilt:14 Sayı:1, 2005, s.302.

77 Aydoğan, s.65.

78 Evcimen, I.V./Evcimen, T.T. (2008) Bir Yüksek Öğretim Kurumunun Sıfır Noktasından Kavramsal Tasarımı: Özyeğin Üniversitesi Akademik Tasarımı ve Geliştirme Süreci, *2008 Oxford Business &Economics Conference (OBEC)*,St. Hugh'sCollege, Oxford, İngiltere, s.25.

79 Barutçugil, İsmet, *Bilgi Yönetimi*, İstanbul, Kariyer Yayınları: 24, Yönetim Dizisi: 7, 2002, s.58.

80 Yenidünya/Değirmenci, s.47; Yazıcıoğlu, s.29

81 Atamer, Yeşim, *İnternet ve Hukuk*, İstanbul, Bilgi Üniversitesi Yayınları, No: 51, 2004, s.705.

Veri tanımdan anlaşılan husus; verinin bir bilgisayar veya bilişim sistemi tarafından işlenebilecek formda olmasıdır[82].

Veri; rakam, alfabe ve simge özellikleri taşımaktadır. Sonuçta bilgisayarlar bu bilgileri veri olarak kodlamakta ve işlemektedir[83].

Bir başka tanıma göre ise veri, bilgilerin, bilgisayarların işlem yapabileceği, sonuçlar üretebileceği, saklayabileceği ve gerekli görüldüğünde yeniden okunabileceği biçimde sayısal birimlere dökülmüş halidir.[84]

Verilere farklı yollarla değer eklenmesi ve verilerin bu yolla bilgiye (enformasyon) dönüştürülmesi söz konusudur. Verilere değer eklemeyle ilgili bazı yöntemler aşağıda gösterilmiştir[85];

- Amaçlama: Verinin hangi amaç için toplandığını bilmek.
- Kategorize etme: Verinin analizine uygun birimlerinin veya temel bileşenlerinin neler olduğunu öğrenmek.
- Hesaplama: Veriyi matematiksel veya istatistiksel olarak analiz etmek.
- Düzeltme: Verideki hataları ayıklamak.
- Özetleme: Veriyi kısa ve öz olarak sunmak.

Bu bağlamda bilgi kelimesinin de açıklanmasına ihtiyaç duyulmaktadır. Bilgi; genellikle bir araya gelmiş sayı, söz ve önermelerden oluşmaktadır. Çoğunlukla, sayı

---

82 Helvacıoğlu, Deniz A., *Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi*, Atamer, Yeşim (Ed.), İnternet ve Hukuk, İstanbul, Bilgi Üniversitesi Yayınları, No: 51, 2004, s.277-301.

83 Kurt, s. 39; Dülger, s.49.

84 Doğan,s.9; Ayrıca Doğan'ın aktardığına göre Avrupa Siber Suç Sözleşmesi'nde veri şu şekilde tanımlanmıştır: " Belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünü"dür. (bkz.: Doğan, s.9).

85 Davenport, Thomas H./Prusak, Laurence, *İş Dünyasında Bilgi Yönetimi*, 1. Basım, Çeviren: Günhan Günay Rota Yayınları, 2001, s.25

ve önermeler özet olarak birleştirilir. Bu özet bilgi, ham verinin tek başına taşıdığından çok daha fazla anlam taşımaktadır[86].

Veriler dağınık bir yapıya sahipken, enformasyonda biçim vermek, düzenlemek, belli bir amaca hizmet etmek, fayda sağlamak olguları öne çıkmaktadır[87].

Özetle bilgi, verinin işlenmiş halidir[88]. Bilgiler, girdilerden otomatik olarak çıktılara dönüşmeyebilir. Bunun için bilginin ayrıca bilişsel bir süreçten geçirilmesi ve rekabet avantajı elde etmeyi sağlayacak yargıya dönüşmesi de gerekmektedir. Bilginin oluşmasını sağlayan bu bilişsel süreci etkileyen tecrübe, kabiliyet, kültür, karakter, kişilik, duygu, sezgi, algı, güdü, eğitim, ortam ve niyet gibi birçok faktör bulunmaktadır[89].

Veri ve bilgilerin nitelikli olmasını sağlayan temel özellikler açık ve anlaşılabilir olması, doğru zamanlı, eksiksiz ve devamlılık arz etmesidir. Bu amaçla bilginin niteliğine ilişkin temel standartlar oluşturulmalı ve güvenirliğin sağlanmasındaki en temel yöntem olarak bu standartlara uyulup uyulmadığı uluslararası kuruluşlar, denetçiler veya standartları oluşturan kurumlar tarafından takip edilmelidir[90]. Ayrıca veri ve bilgi doğru, güncel ve standart olmalı, istenilen formda ve esnek olabilmeli, ihtiyaçlara yetişebilmeli ve paylaşılabilmeli, ancak mükerrer olmamalıdır[91].

Veriler bilişim sistemleri sayesinde bilgi, ses, yazı, görüntü gibi formatlarda bilgisayar ağları tarafından iletilmektedir. Günümüzde büyük miktarlardaki veriler

---

86 Cambazoğlu, Türker, *Yararlı Bilgi Yönetiminde İnsan Faktörü*, Türkiye Bilişim Vakfı Eğitim Seminerleri, 2000, s. 17

87 Dervişoğlu, Gökçe H., *Stratejik Bilgi Yönetimi*, Dışbank Kitapları Bilgi Yönetim Dizisi, 2004, s.23.

88 Yalçıner, Filiz/Şahin, Fikret, *Açıklamalı Bilgisayar Terimleri Sözlüğü*, İstanbul, 1993, s.86.

89 Barca, Mehmet, Yeni Ekonomide Bilgi Yönetiminin Stratejik Önemi, I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi, *Kocaeli Üniversitesi İİBF*, Hereke-Kocaeli, 2002, s.10-11.

90 Arbak, Yasemin, "Örgütlerde Bilgisayar Destekli Bilgi Sistemlerinin İncelenmesine Yönelik Kurumsal Bir Yaklaşım", *Verimlilik Dergisi*, 1995, s.73

91 Erdi, Ali/Durduran, Savaş, Türkiye Coğrafi Bilgi Sistemi Çalışmalarında Kurumsal Politikalar ve Bir Öneri, *3.Coğrafi Bilgi Sistemleri Bilişim Günleri Bildirileri*, Fatih Üniversitesi, İstanbul, 2003, s.22.

son derece hızlı, ucuz ve güvenilir bir şekilde alıcılarına ulaşabilmektedir. Bu kapsamda, cep telefonları, taşınabilir bilgisayarlar vb. cihazlar yaygın olarak kullanılmaktadır[92].

Dijital kavramı dilimizde sayısal kelimesi ile ifade edilmektedir. Elektronik cihazlar içinde bulunan dijital veriler temelde ikili sayı sistemi ile kaydedilmektedir. İkili sayı sistemi 1 ve 0 değerlerinden oluşmaktadır. Bu sayı sistemi dijital verilerin temelini oluşturmaktadır. Örneğin bilgisayarda yazılan ve kaydedilen bir metin aslında temel olarak arka arkaya gelen birler ve sıfırlardan oluşmaktadır. Bilgisayar ekranında görülen metin arka arkaya kaydedilen bu bir ve sıfırların anlamlandırılmasını sağlayan programlar sayesinde okunabilir duruma gelmektedir. Bilişim sistemlerinde dijital verinin nasıl işlem gördüğünü bir örnekle açıklamak gerekirse; bilgisayarın geçici hafıza ünitelerinde ya da kalıcı depolama ünitelerinde bulunan "01100010 01101001 01101100 01101001 11000101 10011111 01101001 01101101 00100000 01110011 01110101 11000011 10100111 01110101" şeklindeki veri seti ilk bakışta hiçbir anlam ifade etmemektedir. Ancak, arka arkaya gelen "1" ve "0" değerlerinden oluşan bu veri seti, bilgisayarın merkezi işlem ünitesi (CPU) tarafından önceden belirlenen algoritmalardan geçirilerek dönüştürülmekte ve kullanıcıya bu verinin "bilişim suçu" kelimesine karşılık geldiği gösterilmektedir[93]. Diğer bir ifadeyle, bilgisayar için "b" harfi "01100010", "i" harfi "01101001" anlamına gelmekte ve metnin tamamının kodlaması bu şekilde devam etmektedir. Bu kodlama işlemi dünya genelinde her ülkenin alfabesini ve matematiksel rakamları kapsayacak şekilde belirli bir standart oluşturularak belirlenmiştir.

Veri ve bilgi işleme ile yakın ilişkisi bulunan "veri tabanı" bir yazılımdır. Veri tabanı bilginin hammaddesinin depolandığı yerdir. Bilgiyi oluşturan bileşenleri sınıflara ayırarak aralarındaki ilişkileri de dikkate alarak depolanmakta ve istenilen zamanda birleştirilerek sunulmaktadır. Bilişim sistemleriyle ilgili hemen her konunun bileşenlerden birisini veri tabanları oluşturmaktadır. En bilinen veri tabanı

---

92 Özgüler, Canbey V., "Yeni Ekonomi Anlayışı Kapsamında Gelişmiş ve Gelişmekte olan Ülkeler: Türkiye Örneği", *Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Yayınlar,* Eskişehir, 2003, s.86-89.

93 ASCII totextconverter, , Erişim Tarihi: 10.05.2019.

işleme yazılımı 1986 yılında ANSI (AmericanNational Standart Institute) tarafından kabul edilen SQL(Structure Query Language-Yapısal Sorgulama Dili) programıdır. SQL yazılımı tüm veri tabanları için ortak bir dil olmasına rağmen günümüzde sadece belirli veri sorgulama işlemleri için kullanılmaktadır. Karmaşık uygulamalarda, veri tabanı şirketleri kendi yazılım geliştirme araçlarını ve kendi programlama dillerini kullanarak ses, resim, harita, video, hesap tabloları gibi pek çok veri bilgisini işlemekte ve depolamaktadır. Veri tabanı işlemleri için kullanılan diğer yaygın uygulamalara, dBase, FoxProve kısmen MS-Office Excel örnek olarak verilebilir. Günümüzde veri işleme kavramı, ortamdan bağımsız bir şekilde her geçen gün internet ortamında gerçekleştirilmektedir[94].

Veri tabanı denilince sadece verilerin depolandığı bir kavram algılanmamalıdır. Veri tabanı, verilerin bilgiye dönüştürüldüğü ve diğer verilerle birlikte işlendiği bir fabrika niteliğindedir. Veri tabanı mimarileri, algoritmaları, bellek ve kaynak kullanımı gibi konular oldukça detaylı bilgi birikimi gerektirmektedir. Veri tabanı kullanarak kurumlar hangi katma değeri sağlayabileceklerini çok iyi bilmelidirler. Kurumların kullandıkları veri tabanları bazen gömülü bazen de açık olabilmektedir. Kuruluşun ihtiyaçlarına göre veri tabanı üzerinde yeni yazılımların da geliştirilmesi mümkündür[95].

C. Elektronik Delil

Elektronik delil konusu bilişim alanındaki suçların tespiti ve incelenmesi açısından önemli bir konudur. Özellikle bilişim alanındaki suçların, elektronik veriler üzerinden işlenmesi nedeniyle, bu suçun hangi boyutta ve ne şekilde işlendiği gibi kritik önemdeki huşuların tespitlerin yapılması ve suça karşılık olarak öngörülecek cezanın belirlenmesi noktasında elektronik delil konusu gündeme gelmektedir.

Bu bağlamda, suça konu olan elektronik delillerin uygun yöntemlerle elde edilmemesi veya elektronik çözümleme sürecinde olası bir hata veya suiistimal yapılması, yeni bir suç vakasını gündeme getirebilecek ve telafisi mümkün olmayan

---

[94] Bayraktar,R., *Veritabanı ve Akılcı Düşünce Üzerine,* http://bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=127, Erişim Tarihi: 17.01.2019.

[95] Dilber, s.69.

mağduriyetlere de sebebiyet verilebilecektir. Bu gibi durumların önlenmesi amacıyla elektronik delil konusunun da çalışma kapsamında irdelenmesinin önemli olduğu düşünülmektedir.

Hukuk açısından delil, uyuşmazlık konusu olayın gerçekleşip gerçekleşmediği ya da nasıl gerçekleştiği hususunda hakim üzerinde genel bir kanaat oluşturmaya yarayan araç şeklinde değerlendirilmektedir. Delil kavramı, uyuşmazlığa neden olan fiilin suç olup olmadığı hususunda kolluk, savcı veya hakimin dolayısıyla mahkemelerin bir kanaate varmasını sağlayan, bir hukuki ihtilafı çözmeye yarayan veya ikamesi hukuk tarafından yasaklanmamış canlı, cansız, yazılı veya sözlü metalar olarak ifade edilmektedir[96].

Ceza muhakemesinin temel amacı, muhakeme konusu olan mevcut olayda maddi gerçeğin araştırılması ve hiçbir kuşkuya yer bırakmayacak biçimde ortaya çıkarılmasının sağlanmasıdır. Maddi gerçek, ancak akla uygun ve doğru deliller aracılığıyla ortaya çıkarılabilmektedir[97].

Ceza muhakemesi hukuku açısından delil; bir fiilin gerçekleşip gerçekleşmediği; gerçekleşti ise sanığın kimliği, suçun manevi unsurları gibi tartışmalı noktaların ispatı için kullanılan araçlardır[98]. Diğer bir ifade ile delil; yaşanmış, bitmiş, geçmişte kalmış bir olayın parçalarını bugüne taşıyan ve bahse konu olayın nasıl cereyan ettiğini gösteren araçlardır[99].

Günümüzde yaygın olarak kullanılan bilişim teknolojilerinin gelişmesi ile birlikte, işlenen suç çeşitleri arasına bilişim suçları da eklenmiştir. İşlenen suçların içeriğinin ve yöntemlerinin değişmesi, bu suçların soruşturulması ve kovuşturulmasında da bazı yeni kıstas ve düzenlemelerin ortaya çıkmasına neden olmuştur.

Bilişim sistemlerinde suça konu olan delil türlerinden elektronik delil olgusu;

---

96 Kaygusuz, Mustafa, *Adli Bilimler*, Ankara, 2005, s.29.

97 Parlar, Ali/Hatipoğlu, Muzaffer/Yüksel Güngör E., *Ceza Muhakemesi Hukukunda Deliller, Çapraz Sorgu ve İspat*, Ankara, 2008, s.1.

98 Şafak, Ali/Bıçak, Vahit, *Ceza Muhakemesi Hukuku ve Polis*, 6'ncı Baskı, Ankara, 2005, s.277.

99 Koca, Mahmut, *Ceza Muhakemesi Hukukunda Deliller*, Özbek Özer V., (Ed.), *Ceza Hukuku Dergisi*, Ankara, 2006, s.207.

> "*Elektronik delil, temel delil şartlarını sağlamanın yanında suça delil niteliği sağlayan ve mahkemelere sunulabilecek sayısal veri depolayabilen, disk, disket, CD, bilgisayar, cep telefonu, tablet cihazları, flash bellekler, SIM kartlar ile bilgisayarlara ait dahili veya harici donanımlar gibi çeşitli elektronik cihazlardır"* biçiminde tanımlanmaktadır[100].

Adli bilişim çalışmalarında bir suçun veya olayın aydınlatılmasını sağlayacak delilleri elde etme çalışmaları dijital ortamdaki verilerin okunmasına dayanmaktadır. Diğer bir ifadeyle olay mahallinde bulunan bir USB bellek yerine, bu belleğin içindeki sayısal veriler olayın esasını teşkil etmektedir. Kolluk kuvvetlerinin olay mahalline gittiğinde ilk müdahale sırasında toplayacağı ve fiziksel olarak temas edeceği elektronik deliller, içerisinde sayısal verileri barındıran elektronik cihazlar olacaktır. Bu bağlamda ilk müdahale sırasında toplanan bir USB belleğin kendisi de bir elektronik delil olmaktadır. İlk müdahale esnasında suç ya da olayla ilişkisi araştırılacak meta USB belleğin kendisidir. Elektronik delil ifadesi hem elektronik cihazı hem de bu cihaz içerisindeki dijital verileri kapsamaktadır. Bu şekilde elektronik delil kavramı dijital (sayısal) delil kavramını içine almaktadır. Bu sebeple dijital delil yerine elektronik delil ifadesinin kullanılması yaygınlaşmıştır[101].

Bilişim suçlarında olay yerinin incelenmesi uzmanlık gerektiren bir konudur. Adli Önleme ve Aramaları Yönetmeliği'ne dayanarak olay yeri incelemesi; suçun aydınlatılması amacıyla her türlü iz, emare ve delil niteliği taşıyabilecek bulgular uzman personel tarafından, çeşitli bilimsel yöntemler kullanarak araştırılmakta ve elde edilen bulgular tespit edilerek kayıt altına alınmaktadır. Sonrasında ise muhafaza ve incelenmek üzere ilgili yerlere gönderilmektedir. Elektronik delil elde edilmesi amacıyla yapılan "Olay Yeri İncelemesi"ndeki amaç[102];

- Meydana gelen bir olayın adli bir suç olup olmadığının tespit edilmesi,

---

[100] Dokurer, Semih, *Bilişim Suçları ve Adli Bilişim*, https://docplayer.biz.tr/8768747-Semih-dokurer-semih-dokurer-kpl-gov-tr.html, Erişim Tarihi: 14.05.2019.

[101] Aydoğan, s.30.

[102] Bayer, Metin/Kaygısız, Mustafa, *Olay Yeri İnceleme*, Emniyet Genel Müdürlüğü, Ankara, 2002, s.10.

• Olayın öngörülen şekil ve şartlarda meydana gelip gelmediğinin belirlenmesi,

• Olay yeri, fail, mağdur ya da maktul arasındaki ilişkinin kurulması için maddi suç delillerinin bulunması,

• İşlenen suçun aydınlatılması ve adli mercilerin doğru karar vermesinin sağlanması amacıyla olay yerinin belgelenmesi,

Bu amaçlara ulaşmak için olay yerinde bulunan delillerin ne oldukları ve nerelerde aranması gerektiği bilinmelidir. Elektronik deliller genel olarak[103];

• Sabit disk, CD, DVD ve disketlerden

• Harici disklerden (Taşınabilir Harddisk ve USB Flash diskler)

• ZIP, DAT, DLT vb. data-teyp türü veri yedekleme birimlerinden

• Hafıza kartlarında (SD, MMS, CF, Memory Stick vb.)

• Dijital kamera ve fotoğraf makinelerinden

• MP3 çalarlardan

• Taşınabilir bilgisayarlardan (Tablet, PDA vb.)

• Cep Telefonlarından

• Oyun konsollarından

• Bazı yazıcı ve faks cihazlarından

• Network ağ bağlantı cihazlarından

• İnternet ve server sistemlerinden elde edilmektedir.

Bunlara ilave olarak veri depolama kabiliyeti bulunan her türlü cihaz dijital delil içerme potansiyeline sahiptir[104]. Örneğin GPRS, GPS gibi sistemler, araçların nerede olduğunun tespiti için kullanıldığı gibi, araçların üzerine yüklenecek gömülü

---

[103] Çiçek, s.5.

[104] Ekizer, Hakan A., *Adli Bilişim Sertifikasyonları*, , Erişim Tarihi: 14.05.2019.

bilgisayar sistemine sahip modüller sayesinde aracın hızı, frenlerin durumu, olaydan önceki kısa süre içindeki fonksiyonlar gibi bir kaza esnasında kazayı aydınlatıcı oldukça faydalı bilgilere ulaşılabilmektedir[105].

Bilişim sistemlerinden elde edilecek elektronik delillerin içeriğinde aşağıda yer alan bilgiler bilişim suçlarının aydınlatılmasında kullanılabilecektir[106]:

- Elektronik cihaz ve bilgisayarın marka, model, seri numarası vb. bilgileri,
- Cihazın mevcut durumu (çalışır halde, arızalı, belirli bir işlemi gerçekleştiriyor vb.),
- Veri yedekleme biriminin teknik özellikleri,
- Yazılım ve veritabanlarınınversiyonu,
- Yazılımların lisans bilgileri,
- Yazılımların amacı,
- Yazılımların kurulum bilgileri ve yapılandırma ayar dosyaları,
- İşletim sistemi ya da yazılımlar tarafından tutulan geçici, kalıcı veya silinen tüm veriler (metadata),
- Programlarda tanımlı kullanıcı bilgileri,
- Programların yetkilendirme politikası,
- Programların erişim ve güvenlik politikası ve şifreler,
- Silinen dosyaların tarih, saat vb. bilgileri,
- Veri tabanı dosyaları, veri tabanı erişim kayıtları,
- E-Mail veya sosyal ağ kayıtları,
- İnternet geçmişi,
- Şifrelenmiş veya kriptolanmış dosyalar,

---

[105] Uzunay, Yusuf, Dijital Delil Araştırma Süreci, 2. *Polis Bilişim Sempozyumu*, Ankara, 2005, s.3.
[106] Çiçek, s.5-10.

- İşletim sistemi yapılandırma ayar dosyaları (config, registery, eventlogvb),
- Sistem tarafından sağlanan hizmetler,
- Virüs, Trojan, SpyWare vb. yazılımlar.
- Sanal Disk alanları ve RAM bilgileri,
- EPROM'dan elde edilen veriler,
- Ağ üzerinden uzaktan erişim özellikleri,
- İşletim sisteminin dosya sistemi türü (FAT32, NTFS, EXT3 vb.),
- İşletim sisteminde tanımlı olan harici donanım birimleri,
- İşletim sistemi erişim politikası ve açık port bilgileri,
- Görev yöneticisi vasıtasıyla tespit edilebilen uygulamalar ve işlemler,
- İşletim sistemi açılış ve kapanış politikası,
- İşletim sistemi açılırken ve kapanırken çalışan yazılımlar,
- Bir yazılım ile ağ üzerindeki başka bilgisayar veya cihazlara ait veri trafiği,
- Bilişim sistemine veri giriş-çıkışı amacıyla kullanılan yazıcı, tarayıcı, çizici, kesintisiz güç kaynağı, web kamerası, mikrofon, klavye, barkot okuyucu, küresel konum belirleme (GPS) cihazları vb. ek donanım bilgileri,
- Sabit disk, taşınabilir disk, disket, CD, DVD, bellek çubukları, bellek kartları, harici sürücüler, Data Teyp/Kaset/Kartuş yedekleme ünitelerinde veri tabanı dosyaları,
- Ağ cihazının türü (modem, yönlendirici, hub, switch vb.),
- Ağın konfigürasyonu,
- Donanım tabanlı cihaz bilgileri (MAC adresi vb.),
- Ağın performans ve kullanım bilgileri,
- Ağ üzerindeki yetkisiz erişim bilgileri,
- Teknik dinleme sonucu bilişim ağı üzerinden akan dijital verinin elde edilmesi ve çözümlenmesiyle elde edilen veriler,

• Cep telefonu, çağrı cihazı, sayısal kamera ve fotoğraf makinesi, özel amaçlı kameralar (ısıya duyarlı, kızıl ötesi vb.), fotokopi makinesi, ATM cihazı, elektronik ajanda, faks, elektronik veri bankası, akıllı kart, POS makinesi gibi tümleşik cihazlardaki elektronik verilerdir.

Bunlara ek olarak verilerin sürekli olarak akış gösterdiği internet ve ağ ortamlarında da dijital delil elde edilmesi mümkündür. Bilgisayar ortamlarında bulunması muhtemel birçok dijital veri, delil olarak internetten elde edilebilir. İnternet ortamından elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

• İnternete bağlantı şekli (kurumsal ağ, ADSL, kablosuz vb.)

• İnternet bağlantısı için kullanılan şifreler

• Üzerinden bağlantı sağlanan internet servis sağlayıcısı bilgileri

• Tespit edilebilen son bağlantı yapılan site adresleri

• Söz konusu sitelerin türleri (haber, eğlence, forum vb.)

•Bağlanılan sitelerin özellikleri (üyelik sistemi, başka bir adrese yönlendirmeli, bağlantı sonrası bir program yüklemeli vb.)

• Söz konusu sitelerin tespit edilen sayısal kimlikleri (IP adresi, etki alanı (domain), hizmetin verildiği ülke vb.)

• Kullanılan internet tarayıcısının aktif olan özellikleri

• İnternet ortamında iletişim ve sosyal ağ için kullanılan yazılımlar

• İletişim veya sohbet yazılımlarının ürettiği geçici veya kalıcı kayıtlar

• Kullanılan elektronik posta hizmet programları (Outlook, Gmail, MSN vb.)

• Elektronik posta hizmet programlarının kullandığı ve ürettiği kalıcı, geçici ve silinen kayıtlar

• Gelen ve giden elektronik posta sahipleri ve alıcıları

• İnternet ortamında kullandığı takma isim/isimler (nickname)

• Web kamerası tarafından kaydedilen görüntüler

• İnternet bağlantılarının denetlenmesi maksadıyla kullanılan içerik filtreleme yazılımları, ateş duvarı yazılımları ya da saldırı önleme yazılımları tarafından tutulan kayıtlar ve günlük ve tarihçeler

• İnternet servis sağlayıcıları tarafından internet bağlantıları ile ilgili tutulan kayıtlar

Bilgisayarlarda ve Cep telefonlarında yapılabilecek delil inceleme aşamasındaki işlemler[107];

1. Bilgisayar dosyalarının erişim ve oluşturulma tarihlerinin tespiti

2. Kullanılan internet web sitelerinin ve bu sitelere giriş zamanının tespiti,

3. İnternetten indirilen dosyaların tespiti,

4. Şifre korumalı dosyaların çözümünün yapılması,

5. Gizlenen ya da dosya türü (dosya uzantısı) değiştirilen dosyaların tespiti,

6. Yazıcıya gönderilen dosyaların tespiti,

7. Bilgisayar dosyaları içerisinde kelime araması yapılması,

8. Cep telefonuna kayıtlı bilgilerin tespiti,

9. SIM karta kayıtlı bilgilerin tespiti,

11. Son arama veya gelen aramaların listesinin tespiti,

12. Gelen/giden mesajların görüntülenmesi,

13. Silinen mesajların tekrar elde edilmesi,

14. Cep telefonun son hizmet aldığı konum bilgisinin tespit edilmesi,

15. Cep telefonuna kaydedilen doküman, resim, video vb. dosyaların tespiti şeklinde özetlenebilir.

---

[107] Aydoğan, s.16.

Elektronik Delillerin Özellikleri

Ceza muhakemesinde geçerli olan delil sisteminde, bir suçun aydınlatılması için her şey delil olarak kullanılabilir. Bir metanın delil olarak değerlendirilmesi tamamen mahkemenin kanaatine bağlıdır. Ancak bu durum mahkemenin keyfi hareket edebileceği anlamına gelmemektedir. Bu konuyla ilgili Yargıtay tarafından verilen çeşitli tarihli kararlarla; bir şeyin delil olabilmesi için hangi özelliklere sahip olması gerektiği ifade edilmiştir. Örneğin; YCGK 30.1.1984 E 1984/3-370 K 1984/43 sayılı kararında;

> "*Gerçek, akla uygun ve realist, olayın bütününü ya da bir parçasını temsil eden kanıtlardan veya kanıtların bütün olarak değerlendirilmesinden ortaya çıkarılmalıdır. Yoksa bir takım varsayımlara dayanılarak sonuca ulaşılması, ceza muhakemesinin amacına kesinlikle aykırıdır*" denilmektedir[108].

Ceza muhakemesinin amacı maddi gerçeğe ulaşmak olduğundan, delillerin hangi yollarla ya da nasıl elde edileceğini Ceza Muhakemeleri Kanunu (CMK), bir yandan devletin menfaatlerini göz önünde bulundurarak, diğer taraftan da temel hak ve özgürlüklerin zarar görmemesine özen göstererek düzenlemiştir[109].

Toplanan deliller öncelikle hukuki yollarla elde edilmelidir. Bu durum Ceza Muhakemeleri Kanununun m. 206/2 a bendinde belirtilmiştir. Ayrıca, CMK'nın m. 217/2. fıkrasında da "yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir" denilerek; ceza muhakemesi hukukunda delillerle ilişkin yaklaşım açıkça ifade edilmiştir. Delil kaynağının güvenilir olmaması, delilin kabulünün adil yargılama prensibine aykırı olması gibi durumlarda delilin kullanılması kanuna aykırılık oluşturmaktadır[110].

---

[108] Kunter, Nurullah/Yenisey, Feridun/Nuhoğlu, Ayşe, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, 16'ncı Baskı, İstanbul, 2008, s.619.

[109] Aksoy, İpekçioğlu P., "Gözaltında Alınan İfadenin Önemi ve Delil Değeri, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Ankara, Sayı: 3, Cilt: 57, 108-123, 2008, s.27.

[110] Şafak/Bıçak, s.281-282.

Deliller olayla ilgili bir durumu ispat etmeli ya da çürütmeli, olay hakkında bir kanaat uyandırmalıdır[111]. Olay ya da isnat edilen suçla ilgili delilin maddi gerçeğin ortaya çıkarılmasına katkı sağlaması ve ispat edici özellikte olması kanuni bir zorunluluktur. CMK'nın 206.maddesi 2/(b) bendinde "delil ile ispat edilmek istenilen olayın karara etkisi yoksa reddolunacağı hükme bağlanmıştır.

Bilimsel açıdan kabul edilebilir nitelikteki bulgular delil olarak değerlendirilmektedir[112]. Deliller akılcı olmalıdır. Diğer bir ifadeyle, ancak gerçeği akla uygun olarak ifade eden ve bilim tarafından kabul edilebilen şeyler delil olabilir. Örneğin bir olayla ilgili olarak, bir kişinin diğer kişiye beddua etmiş olması delil niteliği taşımamaktadır. Dedikodu, safsata, falcı ya da medyum kehaneti vb. akla, mantığa ve bilime aykırı bilgiler delil olamamaktadır. Ayrıca temeli ve kaynağı belirsiz verinin de delil olma özelliği bulunmamaktadır. Bunun yanında delillerin içeriğinin de güvenilir olması gerekmektedir. Örneğin devam eden bir yargılamanın farklı aşamalarında, birbiriyle çelişkili beyanlarda bulunan tanık beyanı güvenilir kabul edilememelidir[112].

Deliller, davanın taraflarınca ve yargı makamınca tartışılacağından, müşterek olmalı ve olay taraflarının salt özel bilgilerinden ibaret bulunmamalıdır[113]. CMK' nın 217'inci maddesi "hakim kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir" şeklinde ifade ederek, delil içeriğinin yalnızca hakim tarafından bilinmesinin yeterli olmadığını, bahse konu içeriğin ortaya konularak tartışılması gerektiğini vurgulamıştır. Böylece yargılamanın aleniyeti de sağlanmış olacaktır[114]. Böylece tarafların delillere itiraz edebilmesi ve etkin savunma yapabilmeleri mümkün olabilecektir.

III. Bilişim Suçu

Genel anlamda başarılı bir suçla mücadelede stratejisi, suça neden olan problemin boyutlarının tam olarak tespitine bağlıdır. Bir yerde yaşanan suçların

---

111 Şenocak, Cengiz, *Maddi Suç Delilleri ve Ateşli Silahlar*, Ankara, 1995, s.279.

112 Gözüşirin, s.84.

113 Kaygusuz, s.30.

114 Şahin, Cumhur, *Ceza Muhakemesi Kanunu Gazi Şerhi*, Ankara, 2005, s.679.

çözümü ancak suçun o coğrafyada yayılma nedenleri, etkileri ve sonuçlarının iyi bir şekilde analizi ile mümkün olmaktadır. Diğer suçlara nazaran bilişim alanında işlenen suçlar da bilgilerin derlenmesi ve sağlıklı bir değerlendirme yapılması güçtür. Çünkü ilk olarak bu suçlarla ilgili verilere ulaşmak zor olmaktadır. Bu durum bilişim sistemlerinin doğasından kaynaklanmaktadır[115].

Alan yazında bilişim suçlarının farklı tanımları bulunmaktadır. Bilgisayarın ilk kullanılmaya başladığı ülke olan ABD'de, ilk suç vakalarının ortaya çıktığı dönemde bu tür suçlara "bilgisayar suçları" (computercrimes) denilmiştir[116].

"Bilişim suçu" kavramıyla ilgili en geniş kabul gören nitelendirme Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu tarafından yapılan "Bilgileri otomatik isleme tabi tutan ya da verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır" şeklinde yapılmıştır.[117] Aynı zamanda üyesi olduğumuz kurumun kararında bilişim suçları beş kategoriye ayırmıştır. Bunlar[118];

1. Bilgisayarda mevcut olan kaynağa ya da herhangi bir veriye yasal olmayan biçimde ulaşarak transferini yapmak için kasten bilgisayar verilerine girilmesi, bunların bozulması, silinmesi, yok edilmesi,

2. Sahtekârlık yapmak amacıyla kasten bilgisayar verilerine ya da yazılımlarına girilmesi, bozulması, silinmesi, yok edilmesi,

3. Bilgisayar sistemlerinin çalışmasının engellenmesi amacıyla kasten bilgisayar verilerine ya yazılımlarına girilmesi, bozulması, silinmesi, yok edilmesi,

4. Ticari anlamda fayda sağlanması amacıyla bir bilgisayar programının yasal sahibinin haklarının zarara uğratılması,

---

115 Peker, Bekir, *Bilişim Suçları Ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu*, Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2010, s.68.

116 Yazıcıoğlu, s.125.

117 Kurt, s.50.

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

5. Bilgisayar sistemi sorumlusunun izni olmaksızın, güvenlik tedbirlerinin aşılması suretiyle sisteme kasten girilerek müdahale edilmesidir.

Bilişim suçları, "elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi, bu kayıtların değiştirilmesi, silinmesi, bu tür kayıtlara girilmesi veya bilgi tecavüzü için hazırlık yapılması" olarak tanımlanmaktadır[119].

Literatürde bilişim suçları farklı isimlerle anılmaktadır. Bunlar: "Bilgisayar Suçları", "Bilişim Suçları", "Siber Suçlar", "İnternet Suçları" gibi ifadelerle dile getirilmektedir[120]. Ülkemizde yeni Türk Ceza Kanunu kapsamında bu tür suçlar; "Bilişim Suçları" ve "Bilişim Sistemleri Aracılığıyla İşlenen Suçlar" şeklinde kabul edilmektedir.

Bilişim sistemlerinin en temel unsuru, verilerin saklanması, işlenmesi ve aktarılmasını sağlayan bilgisayarlardır. Ancak bilgisayarlar haricinde de, bilişim sistemi olarak nitelendirilen cihazlar bulunmaktadır. Bu nedenle, bilişim suçu olarak isimlendirilen fiiller, bilişim alanına dahil olan tüm unsurları kapsamaktadır[121].

Bilişim Suçları İle ilgili yasal düzenlemeler bilişim suçlarının niteliği, hızlı işlenebilmesi, uluslararası sonuçlar doğurması sebebiyle dünya genelinde farklı hukuki düzenlemeler şeklinde yapılmıştır. Bazı ülkeler mevcut düzenlemeler içindeki ayrı bir bölümde bilişim suçlarını düzenlerken, bazıları mevcut yasalar içerisinde ancak hangi hukuki yarar ihlal edildiyse, bu hukuki yararı ihlal eden suçun düzenlendiği bölümde incelenmiştir. Şili, Danimarka, Fransa, Yunanistan, İngiltere, İtalya, Japonya, Kanada, Avusturya, İsveç, Norveç vb. ülkeler mevcut ceza yasası içerisindeki bölümlerde düzenlemeler yapmıştır. Türk Ceza Kanununda da Fransız ceza mevzuatından esinlenilerek düzenlemeler yapılmıştır. Bazı ülkelerde ise mevcut ceza kanununda değişiklik yapılarak bilişim suçlarıyla ilgili düzenlemeler getirilmiştir. Örneğin, Almanya'da "mala karşı işlenen suçlar" başlıklı düzenlemenin ilgili maddesinin nitelikli hali bilgisayarla girilmek suretiyle mevcut yazılımların

---

119 Aydın, Emin D., *Bilişim Suçları ve Hukukuna Giriş,* Ankara, 1992, s.27.

120 Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Ankara, 2008, s.13.

121 Yenidünya, Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu", *Legal Fikri ve Sınaî Haklar Dergisi*, İstanbul, 2005, s.758.

bozulması hususunu kapsamaktadır. Sahtecilik, dolandırıcılık, hırsızlık gibi suçlar için de benzer düzenlemeler yapılmıştır[122].

Bilişim suçu olarak adlandırılan fiiller bilgisayarda veya bilgisayar olarak nitelendirilmemekle birlikte bilgilerin otomatik olarak işleme tabi tutulduğu veya veri iletişimi sağlayan diğer elektronik, manyetik ya da mekanik araçlarla bunları veri iletişimi için birbirine bağlayan ağlar üzerinde işlenebilmektedir[123].

A. Kanunda Yer Alan Temel Kavramlar

Bilişim teknolojilerinin gelişmesi ve yaygınlaşması, kendisini sadece olumlu manada göstermemiştir. Teknolojinin kötü niyetlerle kullanımı bu sahada düzenlemeler yapılmasını gerektirmiş, bilişim ögelerinin ceza hukuku sınırları içine dâhil edilmesi zorunluluğu ortaya çıkmıştır[124].

Bu kapsamda, 5237 sayılı Türk Ceza Kanununun bilişim sistemine girme suçu madde gerekçesinde bilişim sistemi; "verilerin toplanıp yerleştirilmesinden sonra bunların otomatik işlemlere tabi tutulma olanağını veren manyetik sistemler olarak tanımlanmıştır". Avrupa Siber Suç Sözleşmesinin tanımlar kısmında ise *bilgisayar sistemi* terimi kullanılmış olup, bu terimin tercih edilmesi bilişim sistemleri ve bu yolla işlenen suçlar için daha kapsayıcı görünmektedir[125].

26 Eylül 2004 tarihinde kabul edilen, 5237 sayılı Türk Ceza Kanunu kapsamında "Bilişim Suçları"na yönelik konu kapsamları aşağıda gösterilmiştir:

- TCK Md.158/1-f; Nitelikli Dolandırıcılık,
- TCK Md.243/1, 243/2, 243/3; Bilişim Sistemine Girme,
- ***TCK Md.244/1, 244/2, 244/3, 244/4; Sistemi Engelleme, bozma, verileri yok etme veya değiştirme,***
- TCK Md.245/1, 245/2; Banka ve Kredi kartlarının kötüye kullanılması,

---

122 Altunok, Ebru/Vural, Fatih A., "Bilişim Suçları", *Denetişim Dergisi*, 2011, s.8.

123 Erdağ, s.25.

124 Gözüşirin, s.24.

125 Pallı, Hayati, *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri, 2008, s.36.

- TCK Md.239/1, Md.239/2, Md.239/3; Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması,
- TCK Md. 327, Md. 328, Md. 329, Md.; Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgiler,
- TCK Md. 135; Verilerin kaydedilmesi,
- TCK Md. 138; Verilerin yok edilmesi,
- TCK Md. 132; Haberleşmenin gizliliğini ihlal,
- TCK Md. 124; Haberleşmenin engellenmesidir.

Bilişim sistemleri aracılığıyla işlenen suçlar;

- TCK Md. 125; Hakaret,
- TCK Md. 142; Bilişim sisteminin kullanılması yoluyla hırsızlık,
- TCK Md. 158; Bilişim sistemi yoluyla dolandırıcılık,
- TCK Md. 226; Müstehcenlik,
- TCK Md. 228; Kumar,
- TCK Md. 107; Şantaj,
- TCK Md. 28; Cebir şiddet, korkutma ve tehdit,
- TCK Md. 103; Çocukların cinsel istismarı,
- TCK Md. 191; Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırmadır.

B. Adli Bilişim

Etkin bir ceza yargılamasının yapılabilmesi amacıyla bilişim suçları kapsamındaki bir davanın mahkemeye ve karar verici hâkimin önüne tüm yönleri aydınlatılmış olarak gelmesi gerekmektedir. Bu tür suçlarda hâkimin objektif karar verebilmesi için, suça konu olarak elde edilen dijital delillerin alanında uzman bilirkişiler tarafından ayrıntılı ve doğru olarak incelenmiş olması kritik önemdedir.

Delil niteliğindeki elektronik verilerin uygun olmayan yöntemler ve şartlar altında çözümlenmiş olması, hem itirazlara sebep verecek, hem de haksız veya yanlış kararların doğmasına neden olabilecektir. Dolayısıyla, bağımsız ve teknik donanımı yüksek bir adli bilişim sisteminin tesis edilmesi bilişim alanındaki suçlar kapsamında son derece önemlidir.

Adli Bilişim (ComputerForensics) bilimi; suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli özelliklerdeki dijital materyaller üzerindeki, suçla ilgili dijital delillerin zarar görmeden yasal mercilere sunulmaya hazır hale getirilmesini sağlayan ve bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecini temsil etmektedir[126].

Bir yargılama esnasında kullanılabilecek potansiyel delillerin belirlenmesi için bilgisayar araştırma ve analiz teknikleri adli bilişim sürecinden geçirilmektedir. Bilgisayardaki verilerin çıkarılması, korunması, tanılanması, dökümü ve yorumunu içermekte, ancak bunun yanında hukuki kurallar, süreçler, delillerin bütünlüğü gibi konulara riayet ederek tespit edilen veriler hakkında rapor hazırlanmasını da kapsamaktadır[127].

Adli bilişim kavramı ilk olarak bilişim suçlarının gündeme gelmesinden sonra, bu suçların tespit edilmesi ve açığa kavuşturulmasını sağlamak için geliştirilmiştir. Fakat günümüzde elektronik delil sadece bilişim suçlarına özel bir olgu olmaktan çıkmıştır. Teknolojinin insan hayatında büyük rol oynadığı günümüzde, klasik suçlarda şüphelilerin kullanmış olduğu bilgisayar ve diğer bilişim cihazlarında olayla ilgisi olabilecek bilgiler de bulunabilmektedir. Adli bilişim, çoğunlukla bilgisayar bilimiyle uğraşan insanların ilgi alanına girmekle birlikte adli bilişim müstakil bir bilimdir ve daha çok güvenlik güçlerini ve savcıları ilgilendirmektedir. Bu işlemleri yapabilmek için, bilgisayarlar ve diğer cihazlara usulüne uygun şekilde el konulması, adli bilişim kurallarına uygun şekilde yedek alınması, alınan yedeklerin incelenmesi,

---

[126] Ekizer, Hakan A., *Adli Bilişim (ComputerForensics-Bilgisayar Kriminalistiği),* 2007, https://www.ekizer.net/adli-bilisim-computer-forensics/, Erişim Tarihi: 14.05.2019

[127] BT Hukuku (İ.Ü. Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi), http://bthukuku.bilgi.edu.tr/pages/top_05.asp?id=0&r=4%2F9%2F2008+8%3A57%3A24+AM &lid=tr, Erişim Tarihi: 20.12.2018.

mahkemeye sunulacak şekilde hazırlanması ve uygun şekilde paketlenerek, taşınması ve yedeklenmesi gerekmektedir. Bilgisayarlar ve diğer elektronik cihazlarda adli bilişim işlemleri, bu cihazların hem suçlular tarafından suçu işlemede araç olarak kullanıldığında hem de herhangi bir suçun işlenmesinde direkt olarak kullanılmasa dahi suçluların bilgisayarları kendi aralarındaki iletişimde veya işlemlerini kolaylaştırmak ve bilgileri yedeklemek için kullanmaları durumunda yapılmaktadır[128].

Bilişim suçları konusunda yaşanan problemler, delil elde etme ve analiz sürecindeki hukuki ve teknik boyut arasındaki koordinasyon eksikliğinden kaynaklanmaktadır. Suçla daha etkin mücadele edebilmek için daha iyi teşkilatlanma ve teknik altyapı gerekmektedir. Delillendirme ve faile ulaşmayı, diğer bir ifadeyle fiil ile fail arasındaki bağlantıyı sağlayacak temel etken, uluslararası standartlara sahip bir Adli Bilişim laboratuvarıdır[129].

Adli bilişimde kullanılan programlar, en temel seviyedeki donanım üniteleriyle iletişim kurma kapasitesine sahip karmaşık yazılımlardır. Normal bireylerin kullandığı yazılımlar olmadıkları için çoğunlukla kanun kuvvetlerinin ihtiyaçları ve talepleri doğrultusunda hazırlanmaktadırlar. Veri kurtarma, veri inceleme, veri depolama ve veri koruma programları vb. özelliklerde yerine getirdikleri fonksiyonlara göre gruplandırılırlar[130].

IV. Bilişim Suçlarının İşlenmesinde Kullanılan Yöntemler

Genel olarak bilişim suçlarının işlenmesi çok kısa bir süre içerisinde ve çok farklı şekillerde gerçekleşmektedir. Gün geçtikçe bilişim suçlarıyla ilgili yeni yöntemler ortaya çıkmaktadır. Bu bölümde açıklanan bilişim suçu isleme şekillerinin haricinde çok sayıda farklı yöntem de bulunmaktadır. Bunlar arasında Web Sayfası Yönlendirme, Sırtlama, Yazılım Bombaları, Mantık Bombaları, Yerine Geçme,

---

128 Aydoğan, s.2-9.

129 Özel, Cevat/Ahi, Gökhan M., *Bilişim Suçları'nda Usul Ve Sorumluluk Sistemi Üzerine Öneriler,* 2005, http://www.turkhukuksitesi.com, Erişim Tarihi: 15.01.2019.

130 Say, Kubilay, *Bilişim Suçlarından Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2006, s.60.

BugWare, Spoofing, Şifre Kırıcılar, Ağ Koklayıcıları, ScamPage, Salam Tekniği, Excel Macro virüsleri vb. yöntemler örnek olarak verilebilir. Aşağıda özetle izah edilen yöntemler, işlenen bilişim suçlarının tespit edilmiş genel yöntemleridir. Bu sebeple, ifade edilen yöntemlerle sınırlı kalınmamalı ve uygulayıcılar açısından örnek olarak değerlendirilmelidir.

A. Siber Ortam ve Siber Saldırılar

"Siber Uzay" terimi ilk kez, bilim kurgu romanı yazarı William Gibson tarafından 1980'li yılların başında kullanılmıştır. Bu terimin yerine günümüzde "siber ortam" terimi tercih edilmiştir. Buna göre, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan ortama "siber ortam" denilmektedir. Siber Güvenlik Olayı ise, bilişim sistemlerinin ya da bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi olayı olarak tanımlanmaktadır [131].

Günümüzde her türlü hizmet ve işlem siber ortamda gerçekleştirilmektedir. Siber ortam, insanlığın faydasına çok sayıda hizmeti sunmaktadır. Kamu ve özel kurum ve kuruluşlar, hizmet alanı olarak siber ortamdan yararlanmaktadır. Çok sayıda faaliyeti içinde barındıran siber ortam, kötü niyetli amaçlar içinde kullanılabilmektedir[132].

Siber ortam gerçekte bilişim sistemlerinde ayrı düşünülmemelidir. Siber ortam bilişim sistemlerini kapsayan bir üst başlık niteliğindedir. Bu ortamda gerçekleştirilen bilişim suçlarının yöntem ve araçları bilişim sistemleri/bilgisayarlarda kullanılanlarla birebir aynı niteliktedir.

Siber ortamdaki en önemli husus "siber güvenlik" kavramıdır. Siber güvenlik üç ayrı unsurdan oluşmaktadır. Bunlar; gizlilik, bütünlük ve erişilebilirliktir[133];

---

131 T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ocak 2013.

132 Kara, Mahzure, *Siber Saldırılar - Siber Savaşlar ve Etkileri, Yüksek Lisans Tezi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013, s.4.

133 Kara, s.4-5.

- Gizlilik, bilişim sistem ve verilerine sadece yetkili kişi ya da sistemlerce erişilebilmesini, bilişim sistemlerindeki verinin yetkisiz kişi ya da sistemlerce ifşa edilmemesini ifade etmektedir.

- Bütünlük, bilişim sistemleri ve bilginin yalnızca yetkili kişiler ya da sistemlerce değiştirilebilmesini ifade etmektedir.

- Erişilebilirlik ise, yetkili kişilerin ihtiyaç duyulan zaman ve kalitede bilişim sistemlerine ve bilgiye erişebilmesini ifade etmektedir.

Siber ortamı oluşturan bilişim teknolojileri, saldırılarda aracı olarak kullanılabilmektedir. Saldırılar, hackerlar vb. failler tarafından kişisel menfaat ya da başka saiklerle yapılabilmektedir. Bazı gruplar ise, saldırılarını siyasi hedef gözeterek propaganda yapmak ve dikkatleri üzerlerine çekmek için yapmaktadırlar. Devlet destekli saldırılar ise genellikle inkâr edilse de, hedef ülkenin siber ortamına müdahale etmek, ekonomik zarar vermek ve istihbarat bilgisi elde etmek amacıyla gerçekleştirilmektedir. Siber ortamda yaşanılan saldırılarla genellikle zarar verme amaçlanmıştır. Bu bağlamda bu suç türü ulusal bir güvenlik sorunu haline gelebilmektedir[134].

B. Bilgisayar/ Bilişim Sistemi Virüsleri

Bilgisayar virüsleri işletim sisteminin ve CPU ünitesinin kodlama mantığının verdiği imkanlar kullanılarak oluşturulan, kendi kendisini çoğaltabilen, kopyalarını farklı yöntemlerle başka sistemlere aktarabilen ve bu sistemleri de etkilemeye başlayan yazılımlardır. Bilgisayar virüsleri kolaylıkla kopyalanabilme ve yayılabilmektedir. Bu yayılma işlemine bilişim sektöründe "virüs bulaşması" denilmektedir. Sistemleri, özellikle veri depolama ünitelerini kullanılamaz hale getirebilen bilgisayar virüsleri, bulaştıkları bilişim sisteminde bulunan programları da çökerterek, sistem içinde muhtemel en fazla zararı verecek biçimde tasarlanmışlardır[135].

---

134 Kara, s.5.

135 Yenidünya/Değirmenci, s.85.

Bilgisayar virüsleri, en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedirler. Bilgisayar virüsleri ilk ortaya çıktıklarında başka kullanıcıların bilgisayarlarında sorun çıkarma, espri yapma gibi amaçlarla üretilmişlerdir. Ancak zaman içerisinde virüsler, başkalarının bilgisayarlarına girerek çeşitli suçlar için araç haline gelmişlerdir. Virüslerin bulaşması önce taşınabilir veri birimlerinin (disket) yaygınlaşması ile artış göstermiş, devamında da ağ teknolojileri ve internetle birlikte en üst seviyeye ulaşmıştır[136].

Virüsler, bulaştıkları bir bilişim sisteminde kendi kendini kopyalayarak çoğalmakta ve kullanıcıdan habersiz olarak programlanan koda göre kullanıcının izni olmadan zararlı ya da zararsız işlevlerini yerine getirmektedirler. Virüsler, bilgisayar ekranında rahatsız edici, çalışmaya kısa süre engel teşkil eden mesajlar şeklinde zararsız sayılabilecek türleri veya önemli dosyaların silinmesi ya da sistemi tamamen çalışmaz hale getirmesi gibi yıkıcı etkileri olabilmektedir. Virüsleri diğer kötü amaçlı yazılımlardan ayıran önemli özellik, bir e-posta'nın açılması, bir müzik, resim veya metin dosyasının çalıştırılması ile virüsün kendiliğinden yayılmaya başlamasıdır[137].

C. Sistem Güvenliğinin Kırılarak Veri İçeriğine Erişilmesi (Hacking)

Bilişim suçları incelendiğinde, özellikle internetin yaygınlaşmasından sonra, veri iletim ağları üzerinden bilişim sistemlerine girme vakalarında artış yaşanmıştır. Sözcük olarak "hack", kendisine ulaşım imkanı verilmeyen özelliklere, kullanıcının bir alet veya program aracılığıyla girmesine imkan tanınması olarak tanımlanmaktadır. "Hekleme" (hacking) kelimesi, sistemlerin doğasında bulunan açık kapıların kullanılarak sisteme sızılması olarak nitelendirilmiştir[138].

Bilişim sistemlerinin işleyişini merak eden ve sisteme müdahale eden kişilere "hacker" denilmektedir. Ancak zamanla bu kavramının yanında bir de "cracker" kavramı ortaya çıkmıştır. Crackerlar, kötü niyetli olarak kendisine ya da başkasına çıkar sağlamak maksadıyla sistem güvenlik duvarlarını aşmakta, sistem içindeki verileri bozmakta veya değiştirmektedirler. Hackerler ise, bilişim sistemi içerisine

---

136 Canbek/Sağıroğlu, s. 123; Kurt, s.70.

137 Özdilek, s.185.

138 Özdilek, s.166.

girerek her türlü bilgiye ulaşmalarına rağmen sisteme herhangi bir zarar vermeyebilmektedirler. Ancak günümüzde her iki kavramda iç içe geçmiş durumdadır[139].

Bilişim sistemlerine ait güvenlik özelliklerinin kırılarak içeri girilmesi fiilini; diğer suç türlerinden ayıran en önemli özellik, genellikle sisteme giriş esnasında yardımcı yazılımlar kullanılmadan fiilin bizzat bilişim suçunu işleyen kişi tarafından gerçekleştirilmesidir[140].

D. Truva Atı (Trojan)

Truva atı olgusu Yunan mitolojisinden gelmektedir. Buna göre; Yunanlılar ele geçiremedikleri Truva şehrine, barış simgesi olarak tahtadan yapılmış büyük bir at heykeli hediye etmiş, ancak atın içine gizlenen Yunan askerleri gece olunca heykelden çıkarak şehri ele geçirmişlerdir. Bu olgudan esinlenerek adlandırılan Truva atı yazılımları, görünüşte yararlı bir bilişim fonksiyonunu yerine getirmesi düşünülen fakat bunun yanında bilişim sistemine de zarar verebilecek gizli kodları içeren yazılımlar durumundadır. Genel olarak internet ortamında ücretsiz program sağlayan internet sitelerinden veya elektronik posta vasıtasıyla kullanıcılara ulaştırılmaktadırlar. Truva atları sisteme bulaştıktan sonra, kendisini sistem belleğine yüklemekte ve sistemdeki veya ağlardaki açıkları kullanarak, kendisini yerleştiren tarafın isteklerine göre faaliyete geçmektedirler. Truva atları virüsler gibi kendilerini kopyalayarak çoğalmamaktadır[137].

Truva Atı türü zararlı yazılımların boyutlarının çok küçük olması nedeniyle, tespit edilmeleri güç olmaktadır. Truva atları yerleştiği yerdeki birçok veriyi önceden programlanmış adres vb. yerlere gönderebilmektedir[141]. Bir programa yerleşen Truva Atı sayesinde fail, işletim sistemi açıklarından yararlanarak bütün sisteme hakim olabilmekte ve failin bütün komutları yerine getirilebilmektedir[142]. Bir başka ifadeyle

---

139 Gözüşirin, s.35-37.
140 Dülger, s.72.
141 Ergün, s.18.
142 Yenidünya/Değirmenci, s.79.

Truva Atları, hedefteki uzak bir bilgisayar sistemini kontrol etmek için tasarlanmıştır.

E. İstem Dışı Alınan Elektronik Postalar (Spam)

Spam sözcüğü ilk olarak, ABD kaynaklı Firma HormelFoodsCorporatio'un ürettiği gıdalarla ilgili kullandığı bir kısaltma olan "spicedporkand ham" sözcüklerinin baş harflerinden oluşmaktadır[143].

İstem Dışı Alınan Elektronik Postalar olan Spam, teknik olarak internet ortamında aynı mesajın çok fazla sayıdaki kopyasının, bu tür bir mesaj alma talebinde bulunmamış kişilere kendi istemleri dışında gönderilmesi olarak ifade edilmektedir. Spam, genellikle ürünün reklamları ya da sosyal içerikli bir mesajın dünya genelindeki kitlelere ulaştırılması amacıyla kullanılmaktadır. Bu tür mesajlar genellikle, veri tabanlarında çok sayıda e-posta adresi bulunduran kuruluşların, bu verileri bedel karşılığında satması sonucu artış göstermiştir. Spam mailleri sadece ticari içerikli olmamakta aynı zamanda politik bir görüşü veya kamuoyu oluşturma amaçlı çeşitli unsurları da içerebilmektedirler[144].

Bilişim suçları içerisinde değerlendirilen Spam maillerinin cezalandırılması hususunda "Tüketicinin Korunması", "Haksız Rekabet ve Medeni Kanun" hükümlerine göre değerlendirme yapılabilmekte. Bunun yanında, alınan maillerin içeriğinde hakaret ya da yasa dışı propaganda bulunması durumunda ilgili kanunlara göre ceza verilebilmektedir[145].

F. Ağ Solucanları

Ağ solucanları, herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve kendisi bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programlardır. Ağ solucanları genellikle bilgisayar virüsleriyle karıştırılmaktadır. Ancak ağ solucanları, bilgisayar virüsleri gibi sisteme zarar verme işlevi olmadan da sistem içinde dolaşabilmektedir. Ağ

---

143 Dülger, s.77.
144 Değirmenci, s.98.
145 Gözüşirin, s.40.

solucanları bilişim ağında ulaştıkları bir güvenlik duvarıyla karşılaştıklarında, tahmin edilmesi kolay şifre ve verileri kullanarak, güvenlik duvarlarını aşmaya çalışmaktadır. Güvenlik seviyesi düşük güvenlik duvarlarını kolaylıkla aşarak sisteme girmekte ve amaçlarına ulaşmaktadır[146]. Ağ üzerinden bir bilişim sistemine gelen ağ solucanları, amaca göre bir virüs gibi davranarak yazılıma zarar vermekte ya da sisteme bir Truva atı bırakmaktadır[147].

G. Casus Yazılımlar (Pishing)

Casus Yazılım Kullanmak olarak adlandırılan Phishing yöntemi, "PasswordHarvesting Fishing" sözcüklerinin kısaltmasından türetilmiştir. Phishing, kredi kartı bilgileri veya parola gibi gizli kalması gereken, başkaları tarafından bilindiğinde kişilerin zor durumda kalmasına neden olabilecek özel ve gizli bilgilere erişmek şeklinde gerçekleştirilir. Bu bilgileri elde etmek amacıyla, bu bilgileri güvenilir ve bilinen bir yerden geliyormuş gibi gösteren elektronik postalar veya web siteleri hazırlanmakta ve kullanıcıların bu bilgileri paylaşmaları istenmektedir. Kullanıcılar farkında olmadan özel bilgilerini bu zararlı yazılımlar vasıtasıyla art niyetli ve suç işleme kastı olan kişilere vermektedirler. Diğer zararlı yazılımlardan farklı olarak Phishing yazılımları bilişim sistemlerine kendi kendilerine bulaşmazlar. Kullanıcıların bir şekilde kandırılması ya da ikna edilmesi ve genellikle girilen bir internet sitesinden bulaşan casus yazılımlar sayesinde, faillerin art niyetli eylemlerini icra etmelerine sebebiyet vermektedir[148].

H. Zararlı Yazılımlar (Malware)

Malware sözcüğü "Malicious Software" kelimelerinin kısaltılmasıdır. Virüsler, trojanlar ve istenmeyen kötü niyetli yazılımlara verilen genel isimdir. Truva atı olarak bilinen virüs türleri de bu kategoriye girmektedir. Bir programın eklentisi olarak veya girilen virüslü bir web sitesinden de bilişim sistemlerine bulaşabilmektedirler.

---

146 Yaycı, s.35.

147 Değirmenci, s.87.

148 Ekizer, Hakan A., *Bilişim Suçları (Siber Suçlar)* https://www.ekizer.net/bilisimsuclari-sibersuclar , Erişim Tarihi: 07.05.2019.

Malware virüslerine Türkçe *zararlı/kötücül yazılım* denilmektedir. Bu virüsler, bulaştıkları bir bilgisayar ya da ağ sayesinde diğer bilgisayar ve ağlarda da zararlı sonuçlara yol açan istenmeyen yazılımlar olarak değerlendirilmektedir[149].

[149] Gözüşirin, s.33.

İKİNCİ BÖLÜM

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU

I. Suç Tipi Hakkında Genel Bilgiler

Bilişim suçları, Türk Ceza Kanunu ikinci kitabında "Topluma Karşı Suçlar" başlıklı üçüncü kısmın "Bilişim Alanında Suçlar" başlığını taşıyan onuncu bölümünde düzenlenmiştir. Bu kapsamda, 5237 sayılı Türk Ceza Kanunu'nun, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde yer alan düzenlemenin madde 244'ü; "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçlarını kapsamaktadır. Esasında yasa koyucunun bu suç kapsamında birden fazla suçu bir arada düzenlediği görülmektedir. Öyle ki, TCK m.244/1'e göre; bir bilişim sisteminin işleyişini engellemek veya bozmak eylemleri düzenlenirken, TCK m.244/2'de bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, var olan verileri başka bir yere göndermek eylemleri suç kapsamına alınmıştır. TCK m.244/4'te ise; birinci ve ikinci fıkralardaki eylemlerin işlenmesi suretiyle, başka bir suçun oluşmaması koşulu ile, kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması cezalandırılmıştır.[150] Buna göre ilgili madde;

> (1*) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*
>
> *(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.*
>
> *(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.*

---

[150] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, 4. Baskı, 2012, İzmir, s.872.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

şeklinde düzenlenmiştir.[151]

TCK'nın 244. maddesi, 765 sayılı Kanun döneminde hazırlanan 1997 ve 2003 tarihli Türk Ceza Kanunu Tasarıları (m.348, m.347)[152] esas alınarak düzenlenmiştir. Her iki tasarıda da bir bilişim sisteminin tahrip edilmesi, maddi unsuru oluşturan bir

---

[151] Maddenin gerekçesi şu şekildedir: Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir. Aracın fiziki varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir.

İkinci fıkrada, bu fillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi halinde, verilecek cezanın artırılması öngörülmüştür.

Üçüncü fıkrada ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.

[152] Tasarının 348. maddesi, " Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve yüzmilyon liradan beşyüzmilyon liraya kadar ağır para cezası verilir.

Bilişim sistemine hukuka aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve üçyüzmilyon liradan bir milyar liraya kadar ağır para cezası verilir.

Yukarıdaki fıkralarda belirtilen eylemlerle fail, başkasının zararına veya kendisinin veya başkasının yararına haksız bir menfaat sağlarsa iki yıldan beş yıla kadar hapis ve ikiyüzmilyon liradan birmilyar liraya kadar ağır para cezasına hükmedilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suçun cezası verilir"şeklinde düzenlenmiştir.

Tasarının 347.maddesi, " Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve üçmilyar liradan onbeşmilyar liraya kadar ağır para cezası verilir.

Bilişim sistemine hukuka aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve onmilyar liradan otuzmilyar liraya kadar ağır para cezası verilir.

Yukarıdaki fıkralarda belirtilen eylemlerle fail, başkasının zararına ve kendisinin veya başkasının yararına haksız bir çıkar sağlarsa iki yıldan altı yıla kadar hapis ve beşmilyar liradan yirmimilyar liraya kadar ağır para cezasına hükmedilir.

Bu suçlara teşebbüs halinde faillere tamamlanmış suçun cezası verilir." şeklinde düzenlenmiştir.

fiil olarak düzenlememiştir.[153]Tasarılarda yer alan 347. ve 348. maddelerin 2.fıkralarında ise, verilere müdahale teşkil eden fillere yer verilmiştir. Suçun oluşması için bilişim sistemine verileri sokmak veya sistemin içerdiği verileri yok etmek veya değiştirmek gerekmekteydi. 5237 sayılı TCK ise bu unsurlara ek olarak verilerin bozulmasını, erişilmez kılınmasını ve var olan verileri başka bir yere gönderilmesini aramıştır.[154]

Tasarılarda yer verilen para cezaları 5237 sayılı Kanuna alınmamış ve hapis cezaları da farklı olarak belirlenmiştir. Tasarılarda yer verilen, ancak 5237 sayılı TCK'ya alınmayan düzenleme ise her üç suça teşebbüsün tamamlanmış suç gibi cezalandırılacağına ilişin hükümdür.[155]

Ülkemizde mukayeseli hukuktan, uluslararası çalışmalardan ve Avrupa Topluluğu'nun bilişim suçları hakkındaki tavsiye kararlarından etkilenilerek, öncelikle 06.06.1991 tarih ve 3756 sayılı Kanun ile 765 sayılı Türk Ceza Kanununa "Bilişim Alanında Suçlar" başlığı altında 525. madde ilave edilmiş ve bu alandaki suçlar yaptırım altına alınmıştır. TCK m.244 kapsamında düzenlenen ve nitelikleri itibariyle farklılık arz eden bu suçların, bugünkü halinden farklılık arz etmiş olmasına rağmen, 765 s. TCK karşılığı 525/b maddesidir. 765 s. TCK'ya 1991 yılında 3756 s. Kanunla birlikte eklenen m. 525/b'nin birinci maddesi şöyledir:

" Başkasına zarar vermek veya kendisine veya başkasına zarar yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir."[156]

765 sayılı Türk Ceza Kanunu, 01.06/b-.2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile yürürlükten kalkmıştır. 5237 sayılı Türk Ceza

---

153 Akbulut, Berrin, Bilişim Alanında Suçlar, 2. Baskı, Ankara, Adalet Yayınevi, 2017, s. 174-175.

154 Akbulut, Bilişim Alanında Suçlar, s.175

155 Akbulut, Bilişim Alanında Suçlar,s.175

156 Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2012, s. 872

Kanunu'nun İkinci Kitap, Üçüncü Kısım, Onuncu Bölümünde yer alan "Bilişim Alanında Suçlar" başlığını taşıyan 243'üncü madde ile başlayıp 246'ıncı madde ile sona eren dört ayrı madde ile düzenlenmiştir[157].

5237 sayılı TCK'nın farklı bölümlerinde bilişim suçlarıyla işlenmesi olanaklı olan suç tipleri de bulunmaktadır. Bunlar, haberleşmenin gizliliğini ihlal suçu (m.132), haberleşmenin engellenmesi suçu (m.124), hakaret suçu (m.125), bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu (m.142/2"e"), bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu (m.158/1"f"), müstehcenlik suçu (m.226), kumar oynanması için yer ve imkan sağlama suçu (m.228), karşılıksız yararlanma suçu (m. 163)'dur.

Bunun dışında ülkemizde bilişim sistemlerine karşı suçlar yalnızca TCK'da düzenlenmemiş olup TCK'nın yanı sıra; 15.01.2004 tarihinde kabul edilen 5070 sayılı Elektronik İmza Kanunu'nda, 5846 sayılı Fikir ve Sanat Eserleri Hakkında Kanunu'nda ve 2499 sayılı Sermaye Piyasası Kanunu'nda bilişim suçlarına yer verilmiştir.

5237 sayılı Türk Ceza Kanunu'nun 244. maddesine bakıldığında Avrupa Konseyi Siber Suç Sözleşmesinin "verilere müdahale" başlıklı 4'üncü maddesi ile "sistemlere olan müdahale" başlıklı 5'inci maddesi ile benzer bir düzenleme yapıldığı görülmektedir. Maddenin 1. ve 2. fıkralarında bilişim sistemlerine veya verilere yönelik zarar verme eylemleri düzenlenmiştir. Bu maddenin birinci fıkrasında "bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması" eylemleri, ikinci fıkrasında ise "bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez, kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi" eylemleri suç tipi olarak düzenlenmiştir[158].

Avrupa Siber Suçlar Sözleşmesi'nin 2 ila 10. maddeleri arasında düzenlenen suçlarda, Sözleşme'nin 4 ve 5. maddeleri bilişim suçları ile ilgilidir. Şöyle ki, Sözleşme'nin dördüncü maddesinde, kasten ve haksız olarak, bilgisayar verilerini

---

157 Gözüşirin, s.1-2.

158 Gözüşirin, s.54.

tahrip etme, silme, bozma, değiştirme veya erişilmez kılma suç olarak tanımlanmış; Sözleşme'nin 5. Maddesinde ise, bilgisayar verilerine yeni veriler girmek, bunları başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek ve erişilmez kılmak suretiyle, kasten ve haksız olarak, bir bilgisayar sisteminin işleyişini ciddi olarak engellemek suç olarak tanımlanmıştır[159].

Anlaşılacağı üzere sözleşmenin 5. maddesi 4. maddeden farklı olarak sisteme müdahale etme niteliği taşıyan eylemleri esas almaktadır. Buna göre sistemin işleyişinin ciddi olarak engellenmesini suç haline getirilmesi gerektiği belirtilmiştir. Sistemin işleyişinin engellenmesine ilişkin müdahaleler kapsamında, sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi esas alınmıştır. Bu açıdan fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında değerlendirilmemiştir.[160]

II. Korunan Hukuki Değer

244. maddede birden fazla suç tipi düzenlendiğinden suçla korunan hukuki değer hususunda ayrı ayrı belirleme yapılmalıdır. Bilişim sisteminin engellenmesi ve bozulması sistemin hem donanımına hem yazılımına zarar verici niteliktedir. Sistemin işleyişinin engellenmesi veya bozulması ifadeleriyle herhangi bir problem olmadan sistemin çalışmasındaki yarar korunmak istenmiştir. Dolayısıyla bu suç tipiyle birinci fıkrada bilişim sistemlerinin doğru ve işlevine uygun faaliyette bulunması korunmaktadır. Kanun koyucu bir bilgisayar sisteminin, gerek hukuka uygun veya hukuka aykırı olarak girilerek gerçekleştirilen kullanılmalarında gerekse herhangi bir kullanılmanın söz konusu olmadığı durumlarda, sistemde yer alan verilerin veya bunlardan oluşan bilgilerin veya veri işleme olayının herhangi bir hakka veya yetkiye dayanmayan tecavüzlere karşı korunması için bu maddeyi kabul etmiştir.[161]

---

159 Yılmaz, Sacit, "5237 Sayılı TCK'nın 244. maddesinde Düzenlenen Bilişim Alanındaki Suçlar". *Türkiye Barolar Birliği Dergisi* (92), 2011, s.66.

160 Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2012, s. 872

161 Akbulut, Bilişim Alanında Suçlar, s. 176

765 sayılı Türk Ceza Kanunun 525/b-1 maddesinde hem sisteme zarar vermeye yönelik fiillere hem soyut unsurlara yönelik hareketlere hem de sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlamaya yönelik davranışlara seçimlik olarak tek bir hükümde yer verilmişti.[162] Bu nedenle m.525/b-1 koruduğu hukuki değer konusunda değişik görüşler ileri sürülmüş ve bu konu tartışmalara yol açmıştır. Bazı yazarlar bu suç ile sisteme ve içeriğine karşı mala zarar verme fillerinin işlendiğini bu bakımdan bu maddeyle mülkiyet hakkının korunduğunu, klasik mala zarar verme suçunun özel bir şekli olduğunu, bu suçun sistem ve içeriğini esas alan mala zarar verme fillerini kapsadığını bu nedenle korunan hukuki değerin malvarlığı hakkı olduğunu ifade etmektedirler. [163]

Kanunun sistematiğinden anlaşıldığı üzere kanun koyucu bu suç tipiyle bilişim sistemindeki verilerin bireyin malvarlığı değerlerinden olmasından ziyade, bilişim sistemlerinin sağlıklı ve verimli şekilde işleyişini korumak istemektedir. Zira hüküm yalnızca verilerin malikinin yararlarını korumamaktadır. Malik olmasa bile veriler üzerinde tasarruf yetkisi varsa bu kişilerin yararları da korunmaktadır.

İkinci fıkrada ise, veriler üzerinde tasarruf yetkisi olan kişilerin verilerin bozulmadan, engel çıkartılmadan, verilere müdahale olmadan kullanmasındaki yararı korunmaktadır. Bilişim alanında suçlarla korunmak istenen bir diğer önemli hukuki yarar da bilişim sistemine karşı suçlar bakımından "*bilgisayarın dokunulmaz olması ve sistemin istendiği şekilde hizmet görmesi"dir*. TCK'nın gerekçesi incelendiğinde, sisteme ve veriye yönelik müdahalelerin, mala zarar verme suçuna göre özel bir düzenlemeye tabi tutulduğu görülmektedir. Sisteme ve veriye müdahale ile ilgili olarak madde gerekçesinde *"...sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir. Aracın fiziki varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir"* denmektedir. Bu ifade göz önüne alındığında sistem ve veriye

---

[162] Akbulut, Bilişim Alanında Suçlar, s.178.

[163] Dönmezer, Sulhi, Kişilere ve Mala Karşı Cürümler, 15. Baskı, İstanbul, 1998, s.528;Yazıcıoğlu,s.25;Koca, Mahmut, *"Hukukumuzda TCK'nın 244. maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu",* Bilişim Hukuku Konferansı (9-10 Ekim 2008), Yargıtay Başkanlığı Yayını, 2009,s.91.

müdahalenin genel olarak mala zarar verme suçu kapsamında değerlendirildiği ve TCK'nın 244/1-2. fıkralarında düzenlenen sistem ve veriye müdahalenin mala zarar vermenin özel bir şekli olarak kabul gördüğü görülmektedir[164]. Aynı yöndeki bir görüş de TCK m.244/1-2 bakımından mala zarar verme suçunun özel bir görünüş biçimini oluşturduğunu, bilişim sistemi ve onun içerdiği verilerin, mala zarar verme suçunun konusunu oluşturan mal kapsamı içerisinde ele alınamamasından kaynaklanan boşluğu doldurmak amacı güdülediğini, bu nedenle ilk iki fıkrada düzenlenen suçlar bakımından mala zarar verme suçunda olduğu gibi, mülkiyetin bu suçla korunduğunu belirtmektedir.[165]

Bilişim sisteminin engellenmesi ve bozulması internetin yaşamımızdaki önemi ve işlevi düşünüldüğünde haberleşme özgürlüğünü de kısıtladığı veya ortadan kaldırdığı söylenebilir[166].

Kanun koyucu, 244. madde ile bilişim sistemlerinin işleyişinin engellenmesini, bozulmasını, bir bilişim sistemindeki verilerin yok edilmesini, değiştirilmesini, erişilemez kılınmasını koruma altına almıştır.

Bu suçla korunan hukuksal değer, karma nitelikte olup; bilişim sistemi veya bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi ve değerlerine engel olmadan ulaşması ve bu değerleri kullanmasındaki çıkar suç ile koruma altına alınmaktadır[167].

Bu konudaki ileri sürülen bir yaklaşıma göre, suçla korunan hukuki yarar konusunda, 244'üncü maddenin 1. fıkrasında bilişim sistemi sahibinin mülkiyet hakkının, 2. fıkrada ise, zilyedin bilişim sistemi dokunulmazlığı, teknolojik gelişim

---

164 Ketizmen, Muammer, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara, 2008, s.118.

165 Tezcan D./ Erdem M./ Önok M., Teorik ve Pratik Ceza Özel Hukuku, 11. Baskı, Ankara, Seçkin Yayıncılık,2014, s.846; aynı görüşte bkz.: Akbulut, Bilişim Alanında Suçlar,s. 176

166 Artuk,M.Emin /Gökcen, A./Yenidünya,A.Caner, *Ceza Hukuku Genel Hükümler*, Ankara, 2015; aksi görüş için bkz :Akbulut, Bilişim Alanında Suçlar, s. 182

167 Dülger, s.231.

özgürlüğünü ve verinin içeriğine göre, mülkiyet hakkı, fikri mülkiyet hakkı, özel hayatın gizliliği ve ticari sırlar korunmaktadır[168].

Bu noktada ortaya çıkan sorun, bilişim sistemine karşı yapılmış fiziki bir saldırının bu madde kapsamında değerlendirilip değerlendirilmeyeceğidir. Dülger'e göre failin kastının yalnızca kişinin malvarlığına zarar vermek olduğu durumlarda, TCK m. 244 değil, mala zarar verme olan TCK m.151 uygulanacaktır[169]. Ancak, failin kastı, mala zarar verme yerine bir bilişim sisteminin donanım kısmına zarar vermek ise faile TCK 244 uygulanacaktır[170]. Bazı yazarlar ise; bu suçların mala zarar vermenin özel bir şekli olarak genel kabul gördüğünü, dolayısıyla bu suçun hukuki konusu ile klasik mala zarar verme suçunun hukuki konusunun paralellik gösterdiğini, bu bağlamda konu ele alındığında bu suçun "kişilere karşı suçlar" kısmının "malvarlığına karşı suçlar" bölümünde değil de "topluma karşı suçlar" kısmında düzenlenmesinin kanun yapma tekniği açısından önemli bir çarpıklık oluşturduğunu belirtmişlerdir.[171]

III. Suçun Unsurları

A. Maddi Unsurlar

1. Fail

Bu suçun faili herkes olabilmektedir. Kanunda bu suç tipine yönelik fail hususunda bir sınırlama getirilmemiştir. Türk Ceza Kanununun 244. maddesinde düzenlenen verilere veya sisteme müdahale niteliğindeki fiilleri gerçekleştiren ve fail olan kişinin tespiti için mülkiyet, kullanım veya tasarruf yetkisinin de göz önünde bulundurulması gerekir. Örneğin, TCK'nın 244. maddesinin 2. fıkrasındaki suçun faili, veriler üzerinde tasarruf yetkisine sahip olmayan kişidir. Sistemin işleyişinin

---

168 Kurt, s.162.

169 (1)Başkasının taşınır veya taşınmaz malını kısmen veya tamamen yıkan, tahrip eden, yok eden, bozan, kullanılamaz hale getiren veya kirleten kişi, mağdurun şikayeti üzerine, dört aydan üç yıla kadar hapis veya adlî para cezası ile cezalandırılır. (2) Haklı bir neden olmaksızın, sahipli hayvanı öldüren, işe yaramayacak hale getiren veya değerinin azalmasına neden olan kişi hakkında yukarıdaki fıkra hükmü uygulanır.

170 Günışığı, s.56.

171 Doğan, Ramazan. 5237 sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Ankara, 2014, s.109-110

engellenmesi veya bozulması fiili açısından ise suçun faili sistemin sahibi veya kullananın dışındaki kişi veya tasarruf yetkilisi dışında bir kişi olabilir. Dolayısıyla, TCK'nın 244. maddesinde yer alan suçların işlenip işlenmediğinin tespitinde malik veya kullananın veya tasarruf yetkilisinin kim olduğu tespit edilmelidir[172].Bu gibi durumlarda mülkiyet sahibinin kiracısının ya da kiracının mülkiyet sahibinin yetki alanına müdahalesi söz konusu olacaktır. Yargıtay da çeşitli kararlarında bu hususun araştırılması gerektiğine işaret etmektedir.[173]Örneğin; Yargıtay'ın bu konuda verdiği bir kadar da şu şekildedir:

"Sanığın savunması ve tüm dosya kapsamı dikkate alındığında, dosyada mevcut Türk Telekomünikasyon A.Ş.'nin 02.06.2006 gün ve 1537 sayılı yazısından hesaplara gelen paraların internette 85.97.140.0-85.97.143.255 IP aralığındaki 85.97.142.190 IP numarası kullanılarak aktarıldığının anlaşılması karşısında, bu numaranın kullanım bilgileri istenerek EFT'nin yapıldığı anda anılan numaranın bu şirket tarafından hangi kullanıcıya atandığının ilgili kurumdan araştırılıp tespit edildiğinde sanık ile irtibatı olup olmadığının saptanması gerektiğinin gözetilmemesi suretiyle eksik soruşturmaya dayanarak yazılı şekilde hüküm kurulması" gerekçesiyle hükmün bozulmasına karar vermiştir.[174]

Ancak çoğunlukla bilişim ağları vasıtasıyla bilişim sistemine girilerek verilere ulaşılması şeklinde işlendiği için bu konuda özel bir bilgiye sahip olan kişiler tarafından işlendiği görülmektedir. Bu şekilde, bilişim ağları vasıtasıyla işlenmesi suç tipi için aranmadığından bilişim ağlarını kullanmaksızın sistemi engelleyen, bozan, verileri yok eden veya değiştiren kimseler de bu suçun faili olabilir. Başkalarının haklarını ihlal etmediği sürece failin kendi sisteminin işleyişini engellemesi veya bozması veya verilerine müdahale etmesi suç niteliğinde değildir.

---

[172] Akbulut, Berrin, "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, Cilt 24, Sayı 2, 2016

[173] Doğan, s. 112

[174] Doğan, s. 113; Y.,11.CD, 28.01.2009 T, 2008/ 16570 Esas, 2009/101 Karar

Tüzel kişiler suçun faili olamaz. Bu suçun işlenmesi suretiyle bir tüzel kişinin yararına haksız menfaat sağlandığı takdirde tüzel kişi hakkında bunlara özgü güvenlik tedbiri uygulanır[175].

Bilişim suçlarının klasik suç tiplerinden ayıran en önemli faktörün suçun işlenmesinden sonra arkada iz bırakılmaması sebebiyle ortaya çıkan zorluk olduğu ifade edilmektedir. Bu durumda aslında suçların görünmezliğinden bahsedilebilir. Zira işlenen bir bilişim suçunun faillerini takip etmek ve yakalamak oldukça zor olmaktadır[176].

Bilişim suçlarının yapısı incelendiğinde, bu suçlar zaman ve mekân kavramlarını ortadan kaldırmaktadır. Dünya üzerinde herhangi bir yerden TCP/ IP protokolüne uygun olarak bağlanabilen biri, çok kısa bir süre içerisinde kendisinden çok uzakta yer alan başka bir bilgisayara erişerek bu suçu işleyebilir. Bu da, özellikle ceza muhakemesi hukuku açısından yeni sorunlar ortaya çıkarır, ulusal ve uluslararası alanda yeni düzenlemeler getirilmesini gerektirir. Bu yönüyle zaman faktörünün yeni bir boyutu var olup, milisaniye gibi çok kısa bir sürede bu suçlar işlenebilir[177]. Özellikle internet ortamının sınır ve mesafe tanımaması sebebiyle, faillerin tespiti çoğu zaman mümkün olmamakta, fail tespit edilse dahi devletler arasındaki farklı usul uygulamaları bulunması suçun kovuşturulmasını çoğunlukla olanaksız hale getirmektedir[178].

Bilişim suçu failleri, yaşıtlarına göre genellikle orta seviyenin üzerinde ve hatta ileri seviyede zekâya sahip özellikler taşıyabilmektedir.[179] Bu faillerin para elde etmekten çok kendi yeteneklerini ispatlama arzusundaki kişiler olduğu da

---

175 Koca, s.7.

176 Değirmenci, s. 75; Gözüşirin s.31.

177 Aydın, s.57-59.

178 Özel, Cevat/Ahi, M.Gökhan, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", *Güncel Hukuk*, S:6, 2005, s.21.

179 Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Ankara, 2005, s.46

belirtilmektedir[180]. Benzer şekilde bazı bilişim suçları faillerinin amacının marifetlerini sergilemek olduğuna değinilmektedir[181].

Bir kimsenin kendisine ait bulunan bir bilişim sistemi veya verilere zarar vermesi suç oluşturmayacağından, bir bilişim sisteminin ya da bir bilişim sistemi içerisinde yer alan verilerin kime ait olduğunun ortaya konulması büyük önem taşımaktadır. Zarara uğrayan bilişim sisteminin sahibi ile bilişim sistemi üzerinde saklanan verilerin sahibi daima aynı kişi olmayabilir. Bilişim sisteminin veya çeşitli veri depolama ünitelerinin malikinin, bunların bir kısmının veya tamamının kullanım hakkını devretmesi mümkündür. Bu durumda sistem sahibi saklanılan verilerin de sahibi değildir[182].

Bu problem sebebiyle, fail tespit edilirken bilişim sisteminin ve/veya bilişim sisteminde yer alan verilerin mülkiyet, kullanım ve tasarruf hakkının kime ait olduğu ve zararı kimin meydana getirdiği açıkça ortaya konulmalıdır[183].

Siber güvenlik kapsamında, bilişim sistemlerinin olası güvenlik açıklarının tespitini yapan yetkili kişilere faillik yüklenemeyecektir. Ancak, kendisine verilen bu yetkinin ve görevin sınırlarını aşan kişiler, örneğin sistemin bir kısmına girme yetkisi bulunan kişinin daha farklı bölümlere erişmesi gibi durumlarda fail olabilecektir. Bilişim sistemine sadece girme değil de sistemindeki verilerin engellenebilmesi ve değiştirilebilmesi gibi hususların ise daha özenli ve kontrollü yapılması gerekmektedir. Bu durumda sistem içindeki verinin geri getirilemeyecek şekilde yok edilmesi vb. durumlarda görevin planlanması ve yerine getirilmesinde ortaya çıkabilecek hususlara yönelik idari suçlar gündeme gelebilecektir.

2. Mağdur

Bu suçun mağduru açısından kanunda belirtilmiş bir özellik yoktur. Failin hareketi sonucu bilişim sistemi engellenen, bozulan ya da sistemdeki verileri yok

---

180 Yazıcıoğlu, s.25.

181 Kurt, s.58.

182 Gözüşirin, s.56; Dülger, Murat V., Bilişim Suçları ve İnternet İletişim Hukuku, 5. Baskı, 2014, s.409

183 Dülger, s.232.

edilen veya değiştirilen kişiler bu suçun mağdurudur. Bu bakımdan sistemin işleticisi, kullanıcısı ya da sahibi mağdur olabilir. Ancak tasarruf yetkisine sahip olmayan verilerin ilgili olduğu kişi ise suçun mağduru değildir. Suçtan zarar gören olabilir.[184] Bir tüzel kişinin bilişim sisteminin bozulması veya engellenmesi durumunda tüzel kişi mağdur kabul edilemediğinden, suçtan zarar gören olacaktır. Suçun mağduru ise tüzel kişiyi oluşturan gerçek kişiler olabilir. Kamu kurum ve kuruluşlarının bilişim sisteminin saldırıya uğramış olması durumunda mağdur toplumu oluşturan herkestir. Kısaca verilerin zararsızlık hakkı veya sistemin herhangi bir kesintiye uğramadan çalışmasındaki arızasızlık hakkı kime ait ise suçun mağduru da o kişidir.[185]

Bu bağlamda, kamu kuruluşları, bankalar ve güvenlik birimleri gibi gelişmiş bilişim altyapıları kullanan kurumlar, tüzel kişiliklerinden dolayı "mağdur" sıfatı taşıyamayacak, ancak bu suçtan "zarar gören" durumunda olacaklardır.

Veriler üzerinde tasarruf yetkisinin kime ait olduğu doktrinde tartışmalıdır. Veriler veya kanunda belirtilen diğer soyut unsurlar medeni hukuk anlamında bir şey olmadıkları için mülkiyetle ilgili kurallar ceza hukukuna kolayca uygulanamamakta, dolayısıyla da veriler üzerinde tasarruf yetkisine sahip kişi mülkiyet ilişkisiyle belirlenememektedir.[186] Mülkiyet ilişkisiyle belirlenemeyen verilerin yetkilisinin somut olayda tespit edilmesi her zaman kolay olmadığından, bu konuda değişik görüşler ileri sürülmüştür.[187]

Bazı yazarlar tasarruf yetkisinin bilişim sisteminin sahibine veya hukuka uygun zilyedine ait olduğunu, bir kişinin hem bilişim sisteminin maliki olabileceğini hem de veriler üzerinde tasarruf yetkisinin bulunabileceğini ya da bilişim sisteminin sahibi olmamakla birlikte veriler üzerinde tasarruf yetkisine sahip olabileceğini belirtmişlerdir.[188] Bazı yazarlar da verinin ilgilisi olmanın suçun mağduru olmak için

---

184 Akbulut, Bilişim Alanında Suçlar, s.185

185 Akbulut, s. 185

186 Akbulut, s 186

187 Ayrıntılı bilgi için bkz.: Akbulut, Bilişim Alanında Suçlar, s. 186

188 Akbulut, s. 187

yeterli olduğunu belirtmişlerdir.[189] Örneğin; internette yayınlanan bir sanal ekonomi 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.[190] Bilişim sisteminin maliki olmamakla birlikte veriler üzerinde tasarruf yetkisine sahip olan kişinin mağdur olabileceği konusunda örnek vermek gerekir ise; birinden kiraladığı bilgisayara verilerini kaydettiğinde, bilgisayarın sahibi olmamakla birlikte veriler üzerinde tasarruf yetkisine sahiptir. Bu verilere bir başkası tarafından zarar verildiğinde mağdur verileri kaydeden ve üzerinde tasarruf yetkisine sahip olan kişidir. Veri taşıyıcısının maliki başkası tarafından hukuka uygun olarak kaydedilen verilere zarar verirse 244. maddenin ikinci fıkrasında suçu işlemiş olur.[191]

765 sayılı TCK'nın 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, 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.[192]

3. Suçun Konusu

"Bilişim Sistemi" bu suçun konusudur. Bilişim sisteminin neyi ifade etiği mevzuatımızda Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelikte (m. 3/1-b) tanımlanmıştır. Buna göre, bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem, bilişim sistemini ifade etmektedir. TCK'nın 244. maddesinin 1.fıkrasında "*bilişim sisteminin işleyişi*" suçun konusunu oluşturmaktadır. Suçun oluşabilmesi için bir bilişim sistemi mevcut olmalıdır.

---

189 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s.434

190 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s.434

191 Akbulut, Bilişim Alanında Suçlar, s.187

192 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s.433

Maddenin 2. fıkrasındaki suçun konusu ise "*bilişim sistemindeki veriler*"dir. Veri; bilgilerin formatlaştırılmış halidir. Daha kapsamlı tanımıyla veri, bilişim sistemlerinin üzerinde işlem yapabildiği ve bu işlemlere dayalı sonuçlar çıkarabildiği, saklayabildiği, yeniden okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği bilgilerin sayısal kodlara dönüştürülmüş şeklidir.

Veri, harf, rakam, grafik veya tespiti mümkün başka işaretlerden ibaret olan ve sistemin kendisine göre çalıştığı bilgidir. Sistem içindeki bütün unsurların veri niteliğinde kabul edildiği belirtilmektedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2/1-k hükmünde veri, *"bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"* şeklinde tanımlanmıştır. Alman CK ise 202a maddesinin ikinci fıkrası gereği, sadece elektronik veya manyetik ya da doğrudan algılanamayan herhangi bir surette saklanabilen veya iletilebilen verileri bilişim suçları kapsamında veri kabul etmektedir. Burada değerlendirmemiz gereken bir diğer husus '*verinin bulunduğu yer*'e ilişkindir. Bir görüşe göre, suçun konusunu oluşturan veri mutlaka bilişim sisteminin içinde yer alan bir veri olmalıdır. Disket, CD, flash bellek gibi veri taşıma ve saklama cihazlarında yer alan veriler bu suçun konusunu oluşturmaz. Bunlar ve bunlara benzeyen diğer cihazlar içerisindeki verilerin bozulması veya zarara uğratılması halinde mala zarar verme suçu (m.151) oluşabilir. Diğer bir görüşe göre ise, TCK'nın 244. maddesinin 2. fıkrasında yer alan seçimlik unsurlardan birinin gerçekleşmesi şartıyla sorunun içtima kapsamında değerlendirilmelidir. Örneğin verilere zarar vermek amacıyla cihazlara zarar verilmesi halinde TCK m. 151 ile 244 arasında fikri içtima ilişkisi söz konusu olacaktır. Çünkü bilişim sistemi içinde yer alan donanım kavramı içine ana kart, ekran, yazıcı, ses sistemi, disk, disket, modem kartı, manyetik bant gibi maddi bünyeye sahip parçalar da girmektedir. Dolayısıyla sistemde yer alan veri kavramıyla bilgisayarın hafızasında kayıtlı bulunan veriler anlaşıldığı gibi, anakart üzerindeki

veri yollarına takılmak suretiyle kullanılan birimlerdeki veriler de kabul edilmelidir[193].

İçinde hiçbir veri bulunmayan bilişim sistemlerinin bu suça konu olup olamayacağı hususu doktrinde tartışmalıdır. Dülger'e göre; içinde hiçbir veri bulunmayan bir bilişim sistemi ya da veri taşıma aracı bu suçun konusunu oluşturamaz.[194] Çünkü maddenin düzenleme amacı klasik anlamda bilişim sisteminin somut yapısı olan donanım unsuruna verilen zararları cezalandırmak değil, bilişim sisteminin soyut unsurları olan verilerde ve bilişim sisteminin işleyişinde meydana getirilen zararları cezalandırmaktır.[195]

4. Fiil ve Netice

5237 sayılı TCK'nın 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. Maddenin üçüncü fıkrasında, birinci ve ikinci fıkrada düzenlenen fiillerin banka veya kredi kurumuna ya da bir kamu kurum/kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali ağırlaştırıcı sebep olarak düzenlenmiştir. Maddenin son fıkrasında, birinci ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde cezalandırılması kabul edilmiştir[196].

5237 sayılı TCK'nın 244. maddesinin birinci fıkrasındaki "bilişim sisteminin işleyişinin engellenmesi veya bozulması" fiilleri ayrı bir suç, ikinci fıkrasındaki "bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez

---

193 Akbulut, s.92.

194 Doğan, s. 114; Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 412

195 Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s. 412

196 Ketizmen, s.113.

kılınması, sisteme verilerin yerleştirilmesi ve verilerin başka bir yere gönderilmesi" fiilleri de ayrı bir suç tipi olarak öngörülmüştür[197].

Maddede düzenlenen suçlar neticeli suçlardır. Örneğin sistemin işleyişinin engellenmesi veya bozulması suçun netice unsurunu oluşturmaktadır. Dolayısıyla bu suçlar neticeli suçlar niteliğindedir[198]. Her iki fıkrada da netice birden fazla hareketle meydana gelebildiğinden, bu suçun seçimlik hareketli bir suç olduğu söylenebilir. Yani hareketlerden herhangi birinin gerçekleşmesi durumunda, suç gerçekleşmiş olmaktadır[199].

Maddede geçen hareketlerin işleniş şeklinin suçun oluşumunda bir önemi yoktur. Bundan dolayı suçun serbest hareketli bir suç olduğu da söylenebilir[200]. Bu fiil, direkt sisteme fiziki etki yoluyla gerçekleştirilebileceği gibi bilişim ağları vasıtasıyla uzaktan etki edilmek suretiyle de gerçekleştirilebilir[201]. Ancak doktrinde bazı yazarlar bu suçun konusunun sistemin soyut unsurları olduğunu, sistemin fiziki unsurlarına zarar vermenin bu suçu değil, mala zarar verme suçunu oluşturduğunu ifade etmekte, yalnızca soyut unsurlara zarar vermenin 244. maddedeki suçu oluşturacağını belirtmektedirler. Örneğin, bu yaklaşımdaki doktrin görüşüne göre, sistemin donanım unsurlarına yönelik saldırılar mala zarar verme suçu olarak değerlendirilmeli, bu suçtan hüküm kurulmalıdır[202]. Yazarların bu ayrıma gitmesinin sebebi, bilişim suçu kapsamındaki zarar vermelerin konusunu oluşturan malvarlığı ile klasik mala zarar vermenin konusunu oluşturan malvarlığı değerlerinin farklılık göstermesidir[203].

Bu suç genellikle icrai hareketle işlenebilecek bir suç tipidir. Ancak, örneğin, teknik destek sorumlusunun, kasıtlı olarak bir virüs saldırısını önlemek için gerekli yazılımları sisteme yüklememesi ya da sistemi dışarıdan saldırıya karşı savunmasız

---

197 Gözüşirin, s.55.

198 Akbulut, Bilişim Alanında Suçlar, s. 190; Sırf hareket suçu olduğuna ilişkin bkz.: Özbek/Kanbur/Doğan/ Bacaksız/ Tepe, s. 881.

199 Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler*, Ankara, 2008, s.175.

200 Bağlı hareketli suç olduğuna ilişkin bkz.: Özbek/Kanbur/Doğan/ Bacaksız/ Tepe, s. 881.

201 Kızıltan, s.78.

202 Özgenç, s.122.

203 Yılmaz, s.8.

bırakması halinde olduğu gibi bazı istisnai durumlarda suç icrai bir hareket gerçekleştirmeksizin failin ihmali hareketleriyle gerçekleşebilir[204].

Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunun oluşumu için failin eylemleri neticesinde bir zararın meydana gelmesi gerekir. Nitekim kanunun lafzi yorumuna bakıldığında, "engelleyen, kılan, bozan, yerleştiren, gönderen, erişilmez kılan, değiştiren, yok eden" gibi ibarelerin yapılan eylemlerin zarar verici nitelikte olduğunu göstermektedir. Bu suç tipi birden fazla ve farklı hareketle gerçekleştirilebildiğinden meydana gelen neticeler de birbirinden farklı olabilecektir. Suçun oluşumu için hareket ya da hareketlerin tamamlanması ve sonucunda zararın meydana gelmesi önemlidir[205].

Diğer bir görüşe göre, bu hareketler bilişim sistemleri açısından zarar verici özelliğe sahip olduğundan, suçun gerçekleşmesi açısından bir zararın oluşması aranmaktadır. Her ne kadar zararın ortaya çıkması madde metninde belirtilmese de, bu suç neticesinde bilişim sisteminde veya verilerde bir zarar meydana geleceği muhakkaktır[206].

TCK m.244'ün 4. fıkrası, tali norm niteliğinde düzenlenmiştir. Bu nitelikte olduğu maddede "başka bir suç oluşturmaması" ibaresiyle ortaya konulmuştur. Asli norm- tali norm ilişkisi, normların içtima şekillerinden biridir. Bu içtima şeklinde, asli norm gerçekleştiğinde tali norm geriye çekilir ve uygulanmaz.[207] Diğer bir ifadeyle bahse konu suçla failin, kanunla düzenlenmiş ayrı bir özel normu ihlal etmesi durumunda, bu özel suç tipinin hükümleri uygulanacaktır. Bu durumda fail ayrıca, TCK m.244/4'deki genel norm hükümlerinden sorumlu tutulamayacaktır. Örneğin, bir kamu kurumu veya banka çalışanının, bilişim suçu işleyerek hesabına para aktarması veya bu sistemler üzerinden haksız menfaat temin etmesi durumunda, faile "zimmet/irtikap" suçu hükümlerinin yüklenmesi gerekmektedir.

---

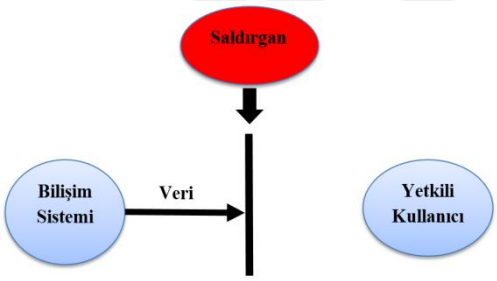
204 Dülger, s.239.
205 Gözüşirin, s.62.
206 Dülger, s.239.
207 Akbulut, Bilişim Alanında Suçlar, s. 221

Suçun maddi unsurunun izahı bakımından bu maddede bahsedilen hareketlerin her birinin ayrı ayrı açıklanmasında fayda vardır:

a. Bilişim sisteminin işleyişinin engellenmesi veya bozulması

Türk Ceza Kanununun 244. maddesinin birinci fıkrasında *bilişim sisteminin engellenmesi veya bozulması*ndan bahsedilmektedir. Sistemin işleyişinin engellenmesi veya bozulması suçun netice unsurunu oluşturmaktadır. Dolayısıyla bu suç neticeli bir suçtur. Bu neticeleri gerçekleştirmeye elverişli her türlü hareketle bu suç işlenebilir. Önemli arz eden nokta, bilişim sisteminin işleyişinin engellenmesi sonucunu doğuran bir hareketin yapılmış olmasıdır. Bu belirleme sebebiyle suç serbest hareketli bir suçtur.[208] Doktrinde bu suçun bağlı hareketli sırf hareket suçu olduğunu ifade eden yazarlar da vardır[209].

Şekil-2. Bilişim sisteminin engellenmesi veya bozulması



Kaynak: Ekizer, 2019.

Engelleme ve bozmadan ne anlaşılması gerektiği noktasında bir açıklama yapmamız gerekirse; **engelleme**, sistemin gereği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenmesidir. Bunun sonucunda da sistemin hızı yavaşlamakta, daha önceden çalıştırdığı dosyaları açamamakta, sistem performansında azalma meydana gelmektedir. Örneğin, işleyen sisteme yöneltilecek yoğun elektromanyetik dalgalarla sistem işleyişinin etkilenmesi ya da işletim sisteminin devre dışı bırakılması bu

---

208 Akbulut, Bilişim Alanında Suçlar, s. 190

209 Özbek/Kanbur/Doğan/ Bacaksız/ Tepe, s. 881

anlamda engelleme sayılır.[210]Verilerin bozulması, yok edilmesi, erişilmez kılınması, verilerin değiştirilmesi, sisteme veri yerleştirilmesi, sistemdeki verilerin iletilmesi suretiyle de sistemin işlemesine engel olunabilir. Burada önemli olan bilişim sisteminin işleyişini engellenmesi sonucunu doğuran bir hareketin yapılmış olmasıdır. Sistem işliyor ancak yavaş işliyorsa sistemin işlemesi engellenmemiştir.[211]Yargıtay sistemin işleyişinin engellenmesini, bilişim sisteminin verimli çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi olarak nitelendirmektedir.[212] Bu engelleme daimi ya da geçici olabilir. Bu açıdan arada bir fark bulunmamaktadır. Engelleme, "sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılmasıdır"[213]. Bilişim sisteminin işleyişinin engellenmesinin sürekli veya geçici olmasının bir önemi yoktur[214].Örneğin, bir bilişim sistemine bir yazılım yerleştirilmek suretiyle o bilişim sisteminin işleyişine müdahale ediliyorsa, burada yapılması gereken değerlendirme müdahalenin etkisidir. Eğer sisteme yüklenen yazılım(örneğin bir virüs programı);

- bilişim sisteminin işleyişini *geçici* olarak kesintiye uğratmışsa *"engelleme",*

- bilişim sisteminin işleyişini o an itibariyle *kalıcı* olarak sonlandırmışsa *"bozma"* eylemi gerçekleşmiş olur.[215]

Bilişim tesisinin veya veri işlem taşıyıcısının yetkili kişinin tasarruf alanından uzaklaştırılması (gizlemek veya çalmak gibi), şifrenin değiştirilmesi veya şifre

---

210 Yılmaz, s.9.

211 Akbulut, Bilişim Alanında Suçlar, s. 191

212 11. CD, 13.03.2013 gün, 2011/2816 E., 2013/ 4065 K., Akbulut, Bilişim Alanında Suçlar, s. 190; doktrinde de aynı şekilde belirleme yapan yazarlar bulunmaktadır. Bkz.: Mahmutoğlu, Bilişim Alanındaki Suçlar, s.866.

213 Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* Ankara, 2009, s.187.

214 Malkoç, İsmail, *Açıklamalı-İçtihatlı Yeni Türk Ceza Kanunu*, Ankara, 2007, s.1679.; Dönmezer, s.528; Yazıcıoğlu, Bilgisayar Suçları, s.263, Akbulut'a göre, bilişim sisteminin işleyişinin geçici olarak engellenmesi durumunda da madde 244/1'deki suç oluşacaktır. Ancak sistemin işleyişinin her tür engellenmesinin cezalandırılmaması gerekmektedir. Kanunda herhangi bir sınırlandırma bulunmamakla birlikte, sistemin işlemesini önemsiz ölçüde engelleyen veya birtakım değişikliklerle meydana getirilen durumun ortadan kalkmasına neden olan hallerin 244. Maddenin cezalandırılması kapsamı dışında tutulması gerekir. Haksızlık içeriğinin azlığı nedeniyle ceza verilmemesi yoluna gidilmesi gerekir(Akbulut, Bilişim Alanında Suçlar, s. 193).

215 Özbek/Kanbur/ Doğan/ Bacaksız/ Tepe, 2012, s.878

ilavesiyle sistemin kullanılmasına engel konulması, programın bozulması, sistemin kilitlenmesi hareketleri de sistemin işlemesine engel olmak niteliği taşımaktadır.[216]

Bozma ise *"sistemin veri işleme faaliyeti yapamayacak hale getirilmesidir"*. Sistemin olağan ve normal koşullarda yerine getirmiş olduğu işlevini yapamaz hale getirilmesi bu kapsamda bozmadır. Sistemin fiziki unsurlarına zarar vererek veya yalnız soyut unsurlarına yapılacak müdahaleyle bilişim sisteminin işlemesinin bozulmasına sebep olunabilir. Örneğin sistemin parçalarının değiştirilmesi, bazı verilerin silinmesi veya hatalı program teslimi veya virüs göndermek suretiyle bilişim sisteminin işleyişinin bozulması söz konusu olabilir. Bozma, bilişim sisteminin genel olarak işleyişine yönelik olabileceği gibi, bu işleyişe katkısı veya etkisi olan herhangi bir unsurun tahrip edilmesiyle de olabilir[217].

Yargıtay'a göre bilişim sisteminin işleyişinin bozulması, "bilişim sistemine dâhil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi veya fiziki olarak dahi zarar verilmesi" olarak anlaşılmalıdır.[218]

Bozmak sözcüğü "bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek, bir yerin bir şeyin düzenine zarar vermek, dokunmak, karıştırmak; kötü duruma getirmek" şeklinde anlamlandırılmaktadır[219].

Bilişim sisteminin normal yapması gerekeni yapamayacak hale getirilmesi sağlanıyorsa sistemin işleyişi bozulmuştur. Sistemin kendisinden isteneni tamamen veya kısmen yerine getiremeyecek olması bozulma açısından önemsizdir. Sistemin işleyişinin bozulması durumunda sistemin işleyişinin engellenmesi de söz konusu

---

216 Akbulut, Bilişim Alanında Suçlar, s. 191

217 Karagülmez, Ali, "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", *Çağın Polisi Dergisi*, Sayı:46, 2005, s.42-56; Akbulut, Bilişim Alanında Suçlar, s. 194

218 11.CD, 13.03.2013 gün, 2011/2816 E- 2013/4065 K, Akbulut, Bilişim Alanında Suçlar, s. 194

219 TDK (Türk Dil Kurumu), *Büyük Türkçe Sözlük*, https://www.tdk.gov.tr , Erişim Tarihi: 14.05.2019.

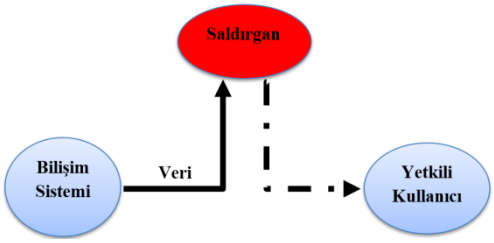
olabilmektedir.[220]Ancak bilişim sisteminin işleyişini engellenmesi halinde her zaman sistemin bozulması söz konusu olmayacaktır, bu sebeple kanun koyucu ayrı ayrı belirleme yapmıştır.[221]

b. Bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, sisteme veri yerleştirilmesi veya mevcut verilerin başka yere gönderilmesi

Bilişim sistemindeki verileri *bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek ve var olan verileri başka bir yere göndermek* fiilleri, TCK m.244/2'de yaptırım altına alınmıştır.[222] Maddede bahsi geçen bu seçimlik hareketlerden birinin gerçekleşmesiyle suç tamamlanmış olacaktır.

Kanun koyucu 2.fıkrada verilerin kullanılmasına müdahale niteliği taşıyan belirlemelere yer verdiği gibi bu nitelikte olmayan hareketlere de yer vermiştir. Verilerin bozulması, yok edilmesi, erişilmez kılınması, değiştirilmesi, verilerin istenen amaç doğrultusunda kullanılmasına engel olma niteliği taşırken, sisteme veri yerleştirilmesi veya verilerin başka yere gönderilmesi bu nitelikte değildir.[223]

Şekil-3. Bilişim sisteminde verilerin bozulması veya değiştirilmesi



Kaynak: Ekizer, 2019.

---

220 Akbulut, Bilişim Alanında Suçlar, s. 195

221 Kurt, s.164; Akbulut, Bilişim Alanında Suçlar, s. 195; Doğan, s. 119

222 Akbulut'a göre; bu suçun, birinci fıkradan sonra düzenlenmesi yerine ilk fıkrada düzenlenmesinin daha doğru olacaktır. Zira sistemin engellenmesi veya bozulması fiilleri 1. fıkrada belirtilen fiillerle de gerçekleştirilebilmektedir. TCK'nın 1. ve 2. fıkrasının yer değiştirmesi düzenleme şekli itibariyle daha yerinde bir düzenleme niteliği taşıyacaktır (Akbulut, Bilişim Alanında Suçlar, s. 195)

223 Akbulut, s. 195

Verilerin bozulması, verilerin kullanılabilirliğine zarar verilmesidir. Bu hareket verileri barındıran depolama aracının fiziksel olarak çalışamaz hale getirilmesi seklinde gerçekleştirilebileceği gibi, verileri oluşturan sayısal kodların bozulması ile de gerçekleştirilebilir[224].

Verilerin bozulmasının sonucu olarak, veriler artık usulüne uygun olarak kullanılamayacak hale getirilmektedir. Bozmak, verilerden elde edilmek istenen faydanın elde edilememesine yol açmaktır. Bilişim sistemlerine sızan ve virüs olarak adlandırılan programlar vasıtasıyla sistemde yer alan verilerin tahrip edilmesi bozmaya örnektir. Sistemin fiziki varlığına yapılacak müdahaleler sonucunda içindeki verilerin zarar görmesi halinde de verilerin bozulmasından söz edilebilir[225]. Ancak fiziki müdahalelerde amaç verilerin bozulmasına yönelik olmalıdır.[226]

Verilerin bozulması fiili, verilerin kendisinden beklenen işi yapamayacak duruma getirilmesi, verilerin işlevini yitirecek biçimde şeklinin değiştirilmesi suretiyle gerçekleşebilmektedir. Bilişim sistemlerine fiziksel olarak zarar verilmesi dışında zarar verme eylemlerinin hepsi verilere zarar verilmesi seklinde gerçekleştirilmektedir[227].

Verilerin bozulması ile yok edilmesi kavramları aynı anlamı taşımamaktadır. Verilerin bozulmasında veri sahibinin mülkiyet hakkı son bulmamaktadır. Dolayısıyla bozulmuş da olsa ortada bir veri bulunmaktadır. Oysa verilerin yok edilmesinde veri yok olduğundan mülkiyet hakkı da ortadan kaldırılmaktadır. Bu bağlamda veri malikinin veriye tekrar ulaşması olanağı artık bulunmamaktadır.[228]

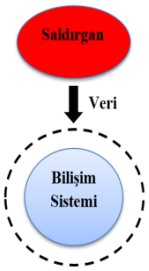
244. maddenin birinci fıkrasında yer alan bilişim sisteminin işleyişinin bozma suçu ile ikinci fıkrasında yer alan verileri bozma suçu arasında fark kast unsurundadır. Bilişim sisteminin işleyişinin bozulması amacıyla verilere zarar verilmesi durumunda failin amacı verileri bozmak değildir. Ancak maddenin 2.

---

224 Çekiç, s.124.
225 Artuk/Gökcen/Yenidünya, s.134; Doğan, s. 119.
226 Doğan, s. 119
227 Gözüşirin, s.57-58.
228 Doğan, s.120

fıkrasında yer alan verileri bozma fiilinde fail, bilişim sistemine zarar vermek istememektedir[229].

Şekil-4. Bilişim sisteminde verilerin yok edilmesi, erişilmez kılınması veya sisteme veri yerleştirilmesi



Kaynak: Ekizer, 2019.

Verilerin yok edilmesi, bilişim sisteminde depolanmış verilerin tamamen ve telafisi olmayacak şekilde tanınmaz hale getirilmesidir. Kanun koyucu burada yok etme ile somut anlamda yok etmeyi değil; bilişim alanında yer alan ve verileri "sil" komutu ile erişilmez kılmayı kastetmektedir. Nitekim doktrindeki bir görüşe göre de, verilerin yok edilmesi ile bozulmasından farklı olarak, tamamıyla ortadan kaldırmanın kastedildiğini belirtmiştir. Zira bozma fiilinde tamir edilebilecek bir durum söz konusuyken, silmede böyle bir durum mümkün değildir[230].

Bilişim alanında "sil" komutu verildiğinde, veri tamamen yok olmamakta, yalnızca dosyalama sistemine göre, o veriye ulaşmayı sağlayan anahtar kodları değişerek veriye normal yoldan ulaşımın engellenmesi söz konusudur. Bu gibi durumlarda verilerin zaman alıcı uğraşlar sonrasında geri getirilmesi mümkündür ve veriler "geri dönüşüm kutusuna" gönderilmektedir. Bu tip durumlarda dahi verilere ulaşmanın engellenmesinin söz konusu olduğu ve verilerin yok edilmiş sayılacağı belirtilmektedir. "Yok edilen" bilgilerin birtakım yardımcı aletler aracılığıyla geri getirilebilmesi durumunda suçun oluşup oluşmayacağı tartışmalıdır. Bazı yazarlar geri getirilme imkânı varsa, telafisi mümkün olmayacak şekilde tanınamaz yapmanın

---

229 Dülger, s.236.; Taşkın, s. 46, Doğan, s. 120

230 Kurt, s.168., Doğan, s. 120

gerçekleşmediğini kabul etmektedir. Dolayısıyla bu görüşteki yazarlara göre geri getirme imkânı varsa verilerin yok edilmesi değil, başka seçimlik unsurlar kapsamına, örneğin şartları taşıyorsa verilerin erişilmez kılınmasına girmesi söz konusudur. Örneğin, kopyası bulunan verilerin silinmesi durumunda, verilerin yok edilmesi gerçekleşmemektedir. Aksi görüşteki yazarlar ise, verilerin ortadan kaldırılmasının, ortadan kaldırılan verilere bazı araç veya programlarla ulaşabilme imkânının varlığının suçun oluşmasını engellemeyeceğini kabul etmektedirler[231].

Avrupa Siber Suç Sözleşmesinin "verilere müdahale" başlıklı 4. maddesinde, verilere zarar verme ile her ne kadar "silme" eylemine yer verilmediği belirtilse de, silmenin "yok etme" ya da "erişilmez kılma" kapsamında değerlendirilebileceği görüşü ileri sürülmektedir[232]. Ancak verileri yok etmek ile erişilmez kılmak kavramları aynı şeyi ifade etmemektedir. Verilerin erişilmez kılınmasında veri sistemde yer almasına rağmen hak sahibinin veri üzerinde istediği faaliyetleri yapamaması veya içeriğine ulaşamaması durumu söz konusudur. Örneğin; veriye şifre konulması halinde hak sahibi verisini kullanamamaktadır. Buna karşılık yok etmede hak sahibi veriyi tamamen kaybetmektedir.[233]

Verilerin üzerinde bulunduğu depolama ünitelerine yönelik fiziki müdahaleler nedeniyle de veriler yok olabilir. Bu hallerde de madde de geçen fiil gerçekleşmiş olacaktır[234].

Verilerin değiştirilmesi, kaydedilmiş verilerin başka bir bilgi içeriği almasını ifade etmektedir. Veriler üzerinde yapılan bir tür manipülasyondur. Verilerin başka biçimlere sokulması, yeni içerik kazandırılması veya niteliklerinin değiştirilmesi bu eyleme örnek teşkil eder[235]. Verilerin değiştirilmesinde amaç, veriyi yok etmek veya

---

231 Dülger, s.236.; Doğan'a göre ise, verinin bulunduğu yerden geri dönüşüm kutusuna atılması halinde veri artık yok edilmiş sayılmalıdır ve veriye tekrar ulaşabilme imkanının varlığı suçun oluşmasını etkilemez (bkz.: Doğan, s. 121).; aksi görüşteki Akbulut'a göre de, geri getirme imkanı varsa verilerin yok edilmesi söz konusu olmayacaktır (bkz.: Akbulut, Bilişim Alanında Suçlar,s. 197).;

232 Karagülmez, s.189.

233 Doğan, s. 122

234 Dülger, s.237; Doğan, s.122

235 Mahmutoğlu, s.856

erişilmez kılmak olmayıp, orijinal veri yerine yanlış bilgilere erişilmesini sağlamaktır. Virüs ve Truva atı gibi kötü amaçlı kodların sisteme sokulması ve bu nedenle verilerin farklı bir hale gelmesi de verilerin değiştirilmesi kavramı içinde değerlendirilmelidir.[236]

Verilerin değiştirilmesi durumunda verilerin orijinal halinden başka bir hale dönüştürülmesi söz konusudur. Suçun oluşumu açısından failin saikinin önemi bulunmamaktadır[237].Değiştirmenin orijinal verilerde yapılması gerekir. Kopya edilmiş verilerde yapılan değişikliklerde m.244/2 uygulanmaz.[238]

Bir bilişim sisteminde bulunan dosyaların ya da resimlerin bir başkasıyla değiştirilmesi de bu suç tipine girmektedir. Verilerin değiştirilmesinde amaç veriyi yok etmek veya erişilmez kılmak demek değildir. Veriye ulaşıldığında yanlış bilgilere erişilmesini sağlanmaktadır. Bu nedenle veri değiştirildiğinde sistem işleyişine devam etmektedir. Örneğin içerik değiştirmeksizin başka bir program dili koduna çevirme veya şifrenin ve şifresiz yazının değişimi de verilerin değiştirilmesi kapsamındadır.[239]

Verilerin tamamen veya kısmen değiştirilmesi suçun oluşumu açısından bir farklılık göstermemektedir. Hiçbir sonuç meydana gelmese de verilerin değiştirilmesi dahi kendi başına suç teşkil etmektedir. Örneğin, nüfus müdürlüğünün bilişim sistemine girerek nüfus bilgilerini değiştiren kişinin veya üniversitenin bilişim sistemine girerek notlarını değiştiren bir öğrencinin fiili verilerin değiştirilmesi suçunu oluşturacaktır.[240]

Verilerin değiştirilmesi sonucu bilişim ortamında cinayetlerin işlendiği konusunda dünyada çarpıcı örnekler mevcuttur. İngiltere Liverpool Hastanesinin

---

236 Doğan, s. 122-123

237 Kurt, s.82.

238 Akbulut, Bilişim Alanında Suçlar, s. 198; Yargıtay 8. CD. 24.06.2013 gün, 2012/32866 E.-2013/18872 K. "Katılana ait Hotmail adresinin şifresini tespit ederek bu adrese giren ve yeni şifre oluşturarak e-mail adresini uzun bir süre kullanan ve oradaki özel fotoğrafları alan suça sürüklenen çocuğun eyleminin TCK'nın 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK'nın 244/1. maddesinden hüküm kurulması" (Karar Uyap Yargıtay Bilişim Sisteminden alınmıştır.16.07.2019)

239 Akbulut, s. 198

240 Doğan, s. 123

bilgisayarına giren bir şahıs, doktor reçetelerinde değişiklikler yapmış ve yanlış ilaçları alan hastalardan bazıları ölmüştür. Yine 15 yaşındaki bir bilgisayar kullanıcısı genç, ABD'nin California eyaletindeki bir hastanenin sistemine girerek orada yatan bir hastanın hastalığının seyrine dair bilgileri ve reçeteleri sırf eğlence olsun diye değiştirmiş, hasta büyük bir alerjik reaksiyon sonucu şoka girmiş ve ölüm tehlikesi atlatmıştır.[241] Bu durumda fiil adam öldürme suçunu oluşturacağı için fail adam öldürmek suçu nedeniyle cezalandırılacaktır.[242]

Failin eylemi sonucunda verilerin değiştirilip değiştirilmediği hususunun kuşkuya yer vermeyecek şekilde ortaya çıkarılması gerekmektedir. Nitekim Yargıtay bu konuda *" Oluşa ve dosya kapsamına göre; suça sürüklenen çocuğun mağdur katılanın facebook şifresini ele geçirerek, facebook sayfasına hakaret içeren yazılar yazdığı ve mağdur katılan vekilinin temyiz dilekçesi ekinde yer alan dilekçe suretinden mağdurun facebook adresine ulaşamadığı ve bu değiştirilen bilgileri silemediği anlaşıldığından, teknik bilirkişi marifeti ile rapor aldırılarak suça sürüklenen çocuğun, mağdurun facebook sayfasına ne kadar süre ile girdiği buradaki bilgileri değiştirip değiştirmediği, mağdurun suç tarihinden sonra facebook sayfasına girip girmediği tespit edildikten sonra suça sürüklenen çocuğun hukuki durumunun tayin ve takdiri gerekirken eksik araştırma ile yazılı şekilde hüküm kurulması, yasaya aykırı…"*olduğunu belirtmiştir.[243]

Verilerin erişilmez kılınması, "verilerin saklandığı bilgisayara ya da veri taşıyıcısına erişimi olan bir kişi için verilerin ulaşılabilirliğini önleyen ya da sona erdiren herhangi bir fiil; mağdurun istediği an bilişim sistemindeki verilere ulaşmasının engellenmesi; verilerin malikinin ya da ilgilisinin istediği zaman ve istediği verilere ulaşmasının engellenmesi" olarak tanımlanmıştır.[244]

Verilerin erişilmez kılınması fiilinde, veriler bozulmamakta ve yok edilmemektedir, sadece verilere erişmek için gerekli olan işlem bağı koparılmaktadır.

---

241 Avşar/ Öngören, Bilişim Hukuku, s. 126

242 Doğan, s. 123

243 Doğan, s.123; 8. C.D., 29.01.2014 gün , 2013/9454 E. ve 2014/1795 K.

244 Doğan, s. 124

Örneğin bir kimsenin bilgisayarındaki word sayfasına şifre koymak veya mevcut şifreyi değiştirmek bu fiil kapsamındadır.[245]

Yargıtay bu konuda *"mağdura ait Facebook ve MNS hesaplarına giren ve hesap şifrelerini değiştirmek suretiyle mağdurun hesaplara erişimini engelleyen sanığın, eylemine uyan TCK'nın 244/2, 43. madde ve fıkraları uyarınca mahkumiyetine karar verilmesi gerektiği gözetilmeden sanığın suç kastı bulunmadığından bahisle yasal ve yeterli olmayan gerekçe ile beraatine hükmolunması, yasaya aykırı"* demiştir.[246]

Yine Yargıtay'ın vermiş olduğu bir karar da şu şekildedir: *"Sanığın şikayetçiye ait elektronik posta adresinin şifresini değiştirdiğini ancak bunu şikayetçinin isteği üzerine yaptığını ve adresi şikayetçiye geri verdiğini beyan eden savunmalarının aksine şikayetçinin beyanlarıyla da uyumlu şekilde dosya içerisinde mevcut şikayetçinin bilgilerinin aktarıldığı elektronik posta adresi olan ...@ hotmail.com adresinin suç tarihinden sonra da sanık tarafından kullanıldığının anlaşılması karşısında, sanığa atılı TCK'nın 244/2. maddesinde düzenlenen suçun oluştuğu ve sanığın mahkumiyetine kadar verilmesi gerektiği gözetilmeden, dosya içeriğiyle uyuşmayan soyut gerekçelerle sanığın beraatine karar verilmesi, yasaya aykırıdır."*[247]

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 suçun oluşumu açısından bir önemi yoktur; verilere ulaşılmasının engellenmesi suçun oluşumu için yeterlidir. Bu suçun işlenebilmesi için bir yöntem öngörülmemiştir. Fail, verileri fiziksel olarak başka yere naklederek verilere erişimi kılmayı engelleyebileceği gibi, şifreleme gibi yöntemlerle verilere erişimi engelleyebilir. Verilere erişimin engellenmesinde herhangi bir süre belirtilmediğinden suçun uzun süreli ya da kısa süreli işlenmesi

---

[245] Doğan, s.124

[246] Doğan, s. 124; 8. C.D., 21.04.2014 gün, 2013/13127 E., 2014/10178 K.

[247] Doğan, s.125; 8. C.D., 08.01.2014 gün, 2012/2731 E., 2014/ 8912 K.

arasında bir fark yoktur[248]. Ancak bu konuda farklı görüşler bulunmaktadır. Bazı yazarlar verilerin erişilmez kılınmasının sürekli olması gerektiğini belirtirlerken, bazı yazarlar geçici bir süre verilerin kullanılmasının engellenmesinin bu fiil açısından yeterli olduğunu ifade etmektedirler.[249]

Veri yerleştirmek, bir bilişim sistemine, sahibinin ya da ilgilisinin izni olmaksızın, çeşitli verilerin eklenmesi, yüklenmesi ya da kaydedilmesi seklinde gerçekleşmektedir. Bu eylemin meydana gelmesi bakımından; veri yüklenen bilişim sistemine failin hukuka aykırı ya da hukuka uygun bir şekilde girmiş olmasının bir önemi yoktur[250]. Bir başka tanıma göre veri yerleştirme hareketi, sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkânını ortadan kaldırmadan bazı ek verileri sisteme ilave etmektir. Bu durumda verilerin güvenilirliği zarar görmektedir[251].

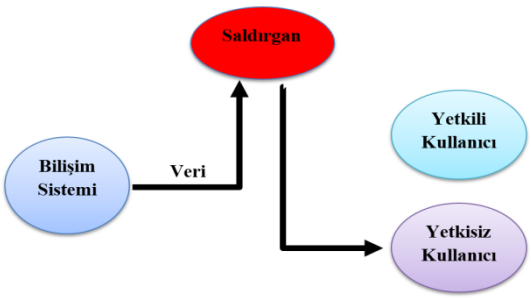
Veri yerleştirmek eylemi, bir bilgisayarın başına oturarak veri taşıma araçlarından birisi ile ya da internet, intranet gibi ağlarla yapılabileceği gibi, disket, CD, flash bellek gibi veri taşıma araçlarıyla verinin sisteme aktarılması şeklinde de yapılabilir.

Veri yüklenen sisteme fail hukuka uygun olarak girmiş olsa dahi veri yerleştirme suçu gerçekleşmiş olabilir. Örneğin bedeli ödenerek bir sisteme giren failin eğer o sisteme veri yerleştirme yetkisi yoksa suç gerçekleşmiş sayılacak ve fail cezalandırılacaktır. Bu nedenle, sisteme girmenin faile veri yükleme hakkı verip vermediği failin cezalandırılması bakımından önem taşımaktadır.[252]

Şekil-5. Bilişim sitemindeki mevcut verilerin başka yere gönderilmesi

---

248 Gözüşirin, s.60-61.
249 Akbulut, Bilişim Alanında Suçlar, s. 200
250 Dülger, s.237.
251 Mahmutoğlu, s.859.
252 Taşkın, s. 48; Doğan, s.125



Kaynak: Ekizer, 2019.

Var olan verileri başka yere göndermek ise, bir sistemdeki verilerin başka bir sisteme gönderilmesidir. Bir bilişim sisteminde yer alan verilerin, bir başka bilişim sistemine ya da veri depolama aracına sahibinin ya da ilgilinin rızası olmaksızın gönderilmesi, aktarılması, taşınması ya da kopyalanması bu suçu oluşturmaktadır. Veriler bir başka yere gönderilirken, kaynak veriler silinirse işlem "taşıma", olduğu gibi korunursa işlem "kopyalama" olarak adlandırılır[253].

Gerçekte bu suç veri transferi olarak tanımlanmakla birlikte, verilerin transferi sonucunda herhangi bir sonuç olmasa dahi, bu fiil nedeniyle failin cezalandırılması öngörülmektedir[254].

Bir bilişim sisteminde yer alan verilerin başka bir yere gönderilmesi suçunda, gönderme eylemi bir bilişim ağı aracılığıyla yapılabileceği gibi, verilerin bulunduğu bilgisayara bir veri taşıma aracının bağlanması ve verilerin bu aracın üzerine kaydedilmesi yoluyla da yapılabilir[255].

Verilerin nereye kopyalandığının herhangi bir önemi bulunmamaktadır. Fiil ticari verilerin, askeri verilerin veya kamuya ait gizli verilerin bir başka sisteme gönderilmesi gibi failin işine yarayabilecek veriler hakkında gerçekleşebileceği gibi, failin işine yaramayan verilerin transferi veya gönderilmesi şeklinde de gerçekleştirilebilir[256].

---

253 Çekiç, s.127.
254 Kurt, s.170.
255 Dülger, s.238.
256 Kurt, s.170.

Bu hareketin oluşması açısından verilerin kopyasının gönderilmesi mi gerektiği, yoksa verilerin orijinalinin mi gönderilmesi gerektiği madde metninde herhangi bir ayırıcı belirleme olmadığı için anlaşılamamaktadır. Ancak orijinalinin gönderilmesi durumunda fıkrada geçen hareketlerin kapsamına giren bir durum oluşacaktır.[257]

Verilerin kullanılmasına müdahale niteliği taşıyan hareketler çoğunlukla icrai bir hareketle gerçekleştirilir. Ancak ihmali hareketle de suçun işlenmesi mümkündür. Eğer fail, belirli bir icrai davranışta bulunma hukuki yükümlüğü altında olmasına rağmen verilerin kullanılmasına engel olucu hareketleri önlemiyorsa 2. fıkradaki suçu gerçekleştirmiş olacaktır. [258] Örneğin bir kuruluşta, bilişim sisteminden sorumlu olan kişinin sistemin güvenliğini sağlamaya yarayan antivirüs yazılımlarını sisteme yüklememesi nedeniyle fail bu suçu işlerse, failin eylemi ihmali hareketle gerçekleşmiş olacaktır.[259]

Kanun koyucu suç sayılan eylemleri ayrıntılı olarak düzenlemiştir. Ancak bu durumda da kavramların ayrımının ve sınıflandırılmasının yapılması kolay olmamaktadır. [260] Zira seçimlik hareketli bir suç olarak düzenlenen maddede; eylemlerin bir kaçının aynı anda gerçekleşmesi mümkündür. Aynı fıkrada düzenlenen eylemlerin biri ya da birkaçının gerçekleşmesi durumunda tek suç işlenmiş olacaktır. Maddede düzenlenen tüm bu eylemlerin cezası aynı olduğundan eylemin seçimlik hareketlerden hangisinin kapsamında kaldığı konusunda yapılacak bir hata verilecek ceza açısından bir değişiklik meydana getirmeyecektir. Seçimlik hareketlerden birden fazlasının yapılması halinde temel ceza belirlenirken alt sınırdan uzaklaşılarak ceza tayini vermek gerekecektir.[261] Buna karşılık gerçekleştirilen fiil, hem 1. fıkranın hem de 2. fıkranın düzenlemesinde yer alan kavramların kapsamına giriyorsa sorun içtima kapsamında çözümlenmelidir.[262]

---

257 Akbulut, Bilişim Alanında Suçlar, s. 203

258 Akbulut, Bilişim Alanında Suçlar, s. 201; Doğan, s. 128;Taşkın, s. 50

259 Taşkın, s. 50

260 Akbulut, Bilişim Alanında Suçlar, s. 201

261 Doğan, s. 128

262 Akbulut, Bilişim Alanında Suçlar, s.202

B. Manevi Unsur

765 sayılı Türk Ceza Kanununda (m. 525/b-1'de) zarar vermek veya yarar sağlamak maksadıyla hareket edilmesi gerekmekteyken 5237 sayılı TCK'nın 244. maddesinin 1. ve 2. fıkralarında düzenlenen suçlar, kasten işlenebilmektedir. Suçların oluşması için olası kast dahi yeterlidir. Kast için suçun kanuni tanımında yer alan unsurların bilinmesi gerekir. Suç işleme kastının varlığı için failin, bir bilişim sistemine izinsiz olarak girmeye hakkının olmadığını, bilişim sistemine izinsiz olarak girerken hukuka aykırı şekilde hareket ettiğini bilmesi ve sonuçlarını istemesi gereklidir. Fail, bilişim sistemine girmek için mağdurun rızasını almış olsa bile, sistem içerisinde rızayı aşacak şekilde işlemler yapması halinde, yine suç işleme kastından bahsedilecektir. Bir diğer ifadeyle kastın varlığı için, failin sistemdeki verileri değiştirdiğini, yok ettiğini, bozduğunu, erişilmez kıldığını, sistemin işleyişini engellediğini, sistemin işleyişini bozduğunu bilmelidir. Failin muhtemel bilmesi de tipikliğin oluşması için yeterlidir. Hata halinde kastı ortadan kaldıran tipiklik hatası söz konusudur ve madde 30 hükmü uygulanır. Suçların taksirli şekline ilişkin bir düzenleme olmadığından taksir halinde cezalandırılmaları söz konusu değildir[263].

Maddenin dördüncü fıkrasında düzenlenen suç esasında ilk iki fıkraya atıf yapılarak hazırlanmıştır. Bu fıkra ile 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 yararına haksız çıkar sağlaması, bu sayılan fiiller başka bir suç oluşturmadığı takdirde cezalandırılmaktadır. Bu suçun oluşabilmesi için yukarıda verilenler doğrultusunda, failde yalnızca kastın bulunması yeterli olmayıp "kendisine ya da başkasına haksız bir çıkar sağlama" maksadının bulunması gerekmektedir. Failin amacı burada sisteme ya da verilere zarar vermek değil hukuka aykırı yarar sağlamaktır. Yani diğer fıkralardan farklı olarak bu fıkra için özel kast aranmaktadır[264].

---

263 Yılmaz, s.9.

264 Gözüşirin, s.65-66.

Bu hususta, "haksız bir çıkar" ifadesi ile sadece maddi yarar anlaşılmaması gerektiği değerlendirilmektedir. Mesela bir öğrencinin; öğretmenine ait bilişim sistemine girerek kendisinin veya bir arkadaşının notlarını değiştirmesinin, ya da düzeltmesinin de haksız bir çıkar oluşturacağı örneğini verilmektedir[265].

TCK m.224 'ün 1. ve 2. fıkralarında belirtilen suçların nitelikli hali 3. fıkrada ifade edilmiştir. Bu fıkrada açıklanan suç türünün, bilişim sistemlerine yönelik işlenen "soyut tehlike suçu" olduğu değerlendirilmektedir.

C. Hukuka Aykırılık Unsuru

Hukuka aykırılık unsuru, işlenen fiile hukuk düzeni tarafından müsaade edilmemesi, fiilin hukuk düzeni ile çatışma halinde bulunması anlamına gelmektedir. Bir fiilin hukuka aykırı olması, onun bütün hukuk sistemine aykırı olması sonucunu doğurur[266].

Hukuka uygunluk nedenlerinden ilgilinin rızasının gerçekleşmesi mümkündür. Yetkili kişi verilerin yok edilmesine, değiştirilmesine veya diğer fiillere rıza göstermişse suç oluşmaz. Ancak bu rızanın fiili hukuka uygun hale getirmesi bakımından belli şartları taşıması gerekir. Bu şartlar, kişinin üzerinde mutlak surette tasarrufta bulunabilecek bir hakkının mevcut olması; rıza gösterenin rızasının kapsamını, önem ve sonuçlarını algılayabilecek durumda olması ve rıza beyanının mutlaka suçtan önce veya en geç icra hareketlerinin yapılması sırasında verilmiş olmasıdır[267].

Her zaman bilişim sistemin malikinin rızası hukuka uygunluk sebebi sayılmayabilir. Mağdurun doğru tespit edilmesi ve rızanın o kişiden alınması gerekmektedir. Çünkü üzerinde işlem yapılan bilişim sistemiyle, bu sistemin içerdiği verilerin maliki her zaman aynı kişi olmayabilir. Verilerin veya bilişim sistemin

---

265 Kurt, s.175.

266 Demirbaş, Timur, *Ceza Hukuku Genel Hükümler*, 2014, s.256.

267 Hafızoğulları, Zeki/Özen, Muharrem, *Türk Ceza Hukuku Genel Hükümler*, Ankara, 2010, s.276.

maliki veya ilgilisi tarafından verilen rıza her somut olayda ayrıca tespit edilmeli ve değerlendirilmelidir[268].

Görevin ifası kapsamında gerçekleştirilen fiiller de 244. madde çerçevesinde fiili hukuka uygun hale getirir.

IV. Suçun Nitelikli Hali

Ceza Kanunumuzun 244. maddesinin 3. fıkrasında, 244. maddenin birinci ve ikinci fıkrasında yer alan fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum/kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde cezanın yarı oranında arttırılacağı düzenlenerek nitelikli hale yer verilmiştir.[269] Bu fıkrayla birlikte maddenin 765 sayılı TCK'daki karşılığı olan 525. maddedeki önemli bir eksiklik giderilmiştir. Nitekim bir kişisel bilgisayarın işleyişinin engellenmesinden doğacak zarar ile bir bankanın bilgisayarının işleyişinin engellenmesinden doğacak zarar arasında ciddi derecede fark vardır. Bu nedenle bankanın sistemine verilen zarar sonucunda fail için daha ağır bir ceza öngörülmesi hakkaniyetle bağdaşmaktadır[270].

Kanun koyucu ortaya çıkan ciddi zararları bu konuda bir ayrım yaparak cezalandırma yoluna gitmiştir.[271] Kanun koyucu nitelikli halin uygulanmasını banka veya kredi kurumu ya da kamu kurum/kuruluşlarıyla sınırlandırmıştır. Fıkrada geçen kamu kurumları veya kuruluşları ibaresi merkezi idare, yerel yönetimler ve hizmet yönünden yerinden yönetim kuruluşları da dahil olmak üzere tüm idari kuruluşların karşılığı olarak kullanılmaktadır[272].

---

268 Gözüşirin, s.67.

269 Yargıtay 8.CD.,29.04.2014 gün, 2013/9376- 2014/10958. "Sanığın, katılana ait eczane şifresiyle SGK'nın bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçete bilgilerini silme şeklindeki eylemi nedeniyle hükmolunan cezanın SGK'nın kamu kurumu olması nedeniyle TCK'nın 244/3. maddesi gereğince arttırılması gerektiğinin gözetilmemesi karşı temyiz bulunmadığından bozma nedeni yapılmamıştır."(Karar Uyap Yargıtay Bilişim Sisteminden alınmıştır. 20.07.2019)

270 Dülger, s.189.

271 Çekiç, s.131.

272 Akbulut, *Bilişim Alanında Suçlar*, s.149.

İdare Hukukunda kamu kurumları ile kamu idareleri arasında yapılan ayrımın anayasal ve yasal dayanağı olmadığı için Ceza Kanunu vb. kanunlarda kullanılan kamu müesseseleri kavramının çoğu zaman tüm idari kuruluşları ifade edecek şekilde kullanıldığı kabul görmektedir[273].

Nitelikli halin uygulanmasını sağlayan banka kavramı, mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını ifade etmektedir. Bu kanuna göre, mevduat bankası; kendi nam ve hesabına mevduat kabul etmek ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini; katılım bankası, özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini; kalkınma ve yatırım bankası ise, mevduat veya katılım fonu kabul etme dışında; kredi kullandırmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini ifade etmektedir[274].

V. Suçun Netice Sebebiyle Ağırlaşmış Hali

Bu suç kapsamındaki fiillerin neticesi sebebiyle suçun ağırlaşmış halinin uygulanabilmesi için, bilişim sistemine girilmesi veya orada kalınması nedeniyle, sistemin içerdiği verilerin yok edilmesi veya değiştirilmesi gerekmektedir. Diğer bir ifadeyle TCK'nun m.244'ün 1. fıkrasında belirtilen hareket ile gerçekleşen netice arasında nedensellik bağının bulunması gerekmektedir. Dolayısıyla, ortaya çıkan neticenin de objektif isnat özelliği taşıması gerekmektedir. Bu yaklaşıma göre, "verilerin yok edilmesi", verilerin varlığının sonlandırılması anlamına gelmektedir. "verilerin değiştirilmesi" ise kaydedilmiş verilerin arzu edilenden başka bir içerik taşımasını ifade etmektedir. Yok olan ya da değiştirilen verinin bedelinin de (maddi ve manevi karşılığı) faydalanılan sistem ile olması önemsizdir. Sonuçta, bilişim

---

[273] Günday, Metin, *İdare Hukuku,* 9. Baskı, Ankara, 2004, s.464.

[274] Bankacılık Kanunu, 2019, https://www.tbb.org.tr/Content/Upload/Dokuman/613/5411_Mart13.pdf Erişim Tarihi: 13.05.2019.

sistemine sadece girilmesi ile girilmesi sonucu veriler üzerinde değişiklik meydana gelmesi farklı suçlar olarak değerlendirilmekte ve bir nevi TCK m.244 ile "*bilişim sistemine girme"* suçunun ağırlaşmış hali düzenlenmiştir[275].

Bilişim suçları kapsamındaki faillerin, verilerin yok olması ya da değişmesi bakımından "taksirinin" olması gerekmektedir. Madde gerekçesinde, failin verileri yok etmek ya da değiştirmek amacıyla eylemde bulunması gerektiği ifade edilmektedir. Bu durumda eğer kasıtlı olarak verileri yok etmiş ya da değiştirmişse m. 244/2 uygulanmalıdır. Doktrindeki bazı yazarlar, TCK m.244 ile TCK 243/3[276] arasında uygulama karışıklığı çıkabileceğini, dolayısıyla m. 244 ile m. 243'ün aynı maddede toplanmasına ihtiyaç olduğunu ileri sürmektedirler[277].

VI. Suçun Özel Görünüş Şekilleri

A. Teşebbüs

Failin işlemeyi amaçladığı bir suçun elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle sonuca ulaşamaması hali teşebbüs olarak adlandırılmaktadır. Türk Ceza Kanununun 244. maddesinin 1. ve 2. fıkralarında düzenlenen suçlara teşebbüs mümkündür. Fail sistemi engellemeye veya bozmaya yönelik herhangi bir eylemi gerçekleştirmesine rağmen, elinde olmayan nedenlerle netice gerçekleşmemişse, suç teşebbüs aşamasında kalmış demektir. Örneğin, failin sisteme yerleştirdiği bir virüs programının harekete geçer geçmez sistem sahibi tarafından fark edilmesi üzerine, verilerde bir zarar oluşturmadan virüsün yok edilmesi durumunda, fiil teşebbüs aşamasında kalmıştır[278].

Söz konusu suçun seçimlik hareketli olması sebebiyle maddede sayılan hareketlerin bir kısmının tamamlanmış, bir kısmının ise teşebbüs aşamasında kalması halinde, dikkat edilmesi gereken, seçimlik hareketli suçlarda, birden fazla hareket aynı anda gerçekleşse de olayda tek bir suçun oluştuğunun kabul edileceği kuralıdır.

---

[275] Akbulut, Berrin,s.149.

[276] TCK 243; "*Bilişim sistemine girme*" suçunu, maddenin 3. fıkrası ise, *bilişim sistemine girme suçunun netice sebebiyle ağırlaşmış halini"* kapsamaktadır.

[277] Özbek,Veli Ö./Doğan,Koray/Bacaksız, Pınar/Tepe, İlker, *Türk Ceza Kanunu Özel Hükümler,* 10. Baskı, Ankara, 2004, s.938.

[278] Akbulut, s12.

Bu kural uyarınca, seçimlik hareketlerden bir tanesi dahi teşebbüs aşamasında kalmış diğeri tamamlanmışsa, ortada yine tek bir suçun var olduğu kabul edilir. Bunların dışında veri yerleştirmek için sistemin içine giren fail, gönüllü olarak bu fiilden vazgeçmiş ise, TCK 244/2'ye teşebbüsten değil, TCK 243'ten sorumlu tutulacaktır. Gönüllü vazgeçme halinde failin gönüllü olarak vazgeçtiği ana kadar yapmış olduğu eylemler başka bir suçu oluşturduğu takdirde fail bu suçtan cezalandırılır (TCK md.36) hükmü gereği fail, bilişim sistemine girme suçundan dolayı cezalandırılacaktır[279].

Yargıtay kararlarında da bilişim suçlarına teşebbüs konusuyla ilgili değerlendirmeler yapılmıştır: "*Bilişim sistemindeki verileri değiştirmek suretiyle haksız menfaat elde edilmesi suçunun sanık tarafından EFT'nin şikayetçi şirketin hesabından sahte olarak açtırmış olduğu hesaba intikali anında tamamlandığı gözetilmeyerek eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini aleyhe temyiz olmadığından bozma sebebi sayılmamıştır."(Y.11.CD.25.06.2007, 2007/2168-4372 E-K).* Bunun yanında,*"Sanıkların, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdıkları hesaba bilişim sistemi aracılığıyla göndererek yine sahte kimliklerle çekmek istemesinden ibaret eylemlerinin paranın açılan hesaplara transferiyle suçun tamamlanacağı gözetilmeden paranın çekilmemesi nedeniyle teşebbüs aşamasında kaldığından bahisle eksik ceza tayini isabetsizliği karşı temyiz olmadığından bozma nedeni yapılmamıştır."*[280].

B. İştirak

Türk Ceza Kanununun 244. maddesinde öngörülen hareketlerle suçun oluşması bakımından faille ilgili özel bir belirleme yapılmamıştır. Dolayısıyla iştirak açısından TCK'nın 37 vd. (38, 39 ve 40.) maddeleri uygulanarak genel hükümler çerçevesinde

---

279 Mahmutoğlu, s.865.

280 Yılmaz, s.9-10.

değerlendirilmelidir. Bu suç tipi bakımından tüm iştirak şekillerinin gerçekleşmesinin mümkün olduğu söylenebilir[281].

C. İçtima

5237 sayılı TCK'da, gerçek içtima (kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır) kuralı benimsenmiş; bu kuralın istisnaları ise, Kanun'un birinci kitabında bileşik suç (m. 42), zincirleme suç (m. 43) ve fikri içtima (m. 44) olarak gösterilmiştir.

244. maddede tanımlanan suçlar bileşik suç tanımına girmemektedir. Bunun sebebi bileşik suçların, birden fazla hukuki konusu olan suçlar olmasıdır. Bu suçların işlenmesiyle birden çok hukuki değerin ihlal ediliyor olması, haklı olarak kanun koyucuyu bileşik suçların, bu suçların unsurunu ya da ağırlaştırıcı nedeni oluşturan suçlara oranla daha ağır bir cezaya tabi tutulmasına yönlendirmektedir. Çünkü bileşik suçta failin sebep olduğu kötülük, bileşenleri oluşturan suçlara göre çok daha fazladır. Bundan başka, bileşik suçta kanunun suç saydığı bir fiil, kimi zaman başka bir suçun nitelikli ve ağırlaştırıcı sebebi olabilmektedir. Bu halde, temel suç bir değişikliğe uğramamakta, sadece suçun cezası artırılmaktadır. Böylece bir suçun ağırlaştırıcı nedeni olan diğer bir suç, artık kendi kimliğini yitirmekte ve her suçta ağırlaştırıcı sebeplerin tabi olduğu kurallara tabi olmaktadır. Söz konusu maddede ise böyle bir düzenleme bulunmamaktadır[282].

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarının zincirleme suç şeklinde işlenmesi mümkündür. Failin, bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçunu birden çok kez işlemesi halinde, 43. maddede düzenlenmiş olan zincirleme suç meydana gelecektir. Ancak zincirleme suç kapsamına alabilmemiz için failin bu eylemleri, aynı suçu işleme kararı kapsamında değişik zamanlarda icra etmesi gerekir. Bu durumda faile bu suçların her birinden dolayı ayrı ayrı değil, bir ceza verilmekte fakat cezanın oranı arttırılmaktadır. Örneğin; aynı suçu işleme kararı kapsamında

---

[281] Y.11.CD.12.05.2009, 2009/3700-6207 E-K; Mahmut, Koca/İlhan, Üzülmez, *Türk Ceza Hukuku Genel Hükümler,* Ankara, 2009, s.250.

[282] Yılmaz, s.10.

bilişim sisteminin çalışmasının engellenmesi veya hukuka aykırı olarak veri yerleştirilmesi halinde zincirleme suç meydana gelir.[283] Burada dikkat edilmesi gereken nokta zincirleme suçun oluşabilmesi için, mağdurun aynı olması gerekliliğidir.

Bahsi geçen maddede 1. ve 2. fıkralar bir arada gerçekleşmiş olabilir. Bu durumda sorun fikri içtima (TCK m. 44) kapsamında çözümlenmelidir. Tek fiille farklı suçlar ortaya çıkmıştır. Bu konuda öğretide bazı yazarlar verilerin yok edilmesi, değiştirilmesi, bozulması, erişilmez kılınması veya sisteme verilerin ilave edilmesi sistemin işleyişinin engellenmesi sonucunu doğurmuşsa 244. maddenin 2. fıkrasının değil, 1. fıkrasındaki suçun oluşacağını belirtmektedir. Bu yazarlara göre 2. fıkradaki suçun oluşması için verilere müdahale niteliği taşıyan hareketin bilişim sisteminin işleyişini engelleme boyutuna ulaşmaması gerekmektedir[284].

Bir diğer husus, bu maddede yer alan suçun işlenmesi için hukuka aykırı olarak bilişim sistemine girmek ve sistemde kalmak gerektiğinden bahisle TCK m.243'ün TCK m.244'e nazaran geçit suç olarak kabul edilmesi ve failin sadece TCK m.244'e göre cezalandırılması gerektiğini ifade eden görüşün yanında TCK m.244'ün, TCK m.243'ün öngördüğü biçimde sisteme girmeden gerçekleştirilmiş olabileceğini, bu sebeple de TCK m.243'te yer alan eylemlerin TCK m.244'ün bir unsuru veya nitelikli hali olmadığı gerekçesiyle burada gerçek içtima hükümlerinin uygulanması gerektiğini ileri süren görüşün mevcut olmasıdır[285].

Gerçekten bilişim sistemine girmeden verilerin bozulması söz konusu olabilir. Bu durumda zaten TCK m.243'ten bahsedemeyiz. Ancak bilişim sistemine girerek veri bozma, yok etme halleri varsa yine görünüşte içtima söz konusu olup gerçek içtimayı kabul eden ikinci görüş isabetsizdir. Zira TCK m.244'ün oluşması halinde bu suç tipinin gerçekleştirilebilmesi için TCK m.243'ün gerçekleştirilmiş olması

---

283 Yargıtay 8. CD., 08.01.2014 gün, 2012/33044 E-2014/236 K, "… Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK'nın 43. Maddesi gereğince arttırılması gerektiğinin gözetilmemesi."

284 Akbulut,s.14.

285 Meran, Necati, *Yeni Türk Ceza Kanununda Sahtecilik, Malvarlığı, Bilişim Suçları ile Ekonomi ve Ticari Alanda Suçlar,* 2. Baskı, Ankara, 2008, s.118.

gerekir. Bu halde m.244, m.243 açısından tüketen norm niteliğindedir. Tüketen-tüketilen norm ilişkisi gereği TCK m.244'ün uygulanması kabul edilmelidir.[286]Bu hususta bir görüşe göre; failin kastının ilk başta yalnızca hukuka aykırı olarak bir bilişim sistemine girmek olduğu, ancak sistem içerisindeyken fikir değiştirerek sistem içerisinde yer alan veriler üzerinde oynama yapması durumunda, gerçek içtima kurallarının uygulanmaması gerektiği ifade edilmektedir[287].

Tüketen-tüketilen norm ilişkisi (geçitli suç), bir normun, diğer bazı normlar tarafından korunan hukuki değerlerin tümünü ortak bir şekilde koruduğu durumlarda ortaya çıkar. Bu şekilde bir normun diğer bir normu bünyesine alması halinde, bünyeye alınmış norm varlığını kaybetmiştir ve uygulanma imkanı yoktur. TCK'nın 244. maddesinin birinci fıkrasında bilişim sistemine karşı düzenlenen fiillerin, sistemdeki veriler aracılığıyla gerçekleştirilmesi halinde, her iki fıkradaki suçlar da ihlal edilmiş olacaksa da, ikinci fıkradaki suç, birinci fıkradaki suç tarafından yutulur ve sadece birinci fıkradaki suçtan cezalandırmaya gidilir. Bu durumda her iki fıkrayı ihlal eden hareketler bağımsız eylem olarak kabul edilmemektedir[288].

Ceza Kanunumuzun 244. maddesinin 1. ve 2. fıkrasındaki suçların, 4. fıkradaki bilişim sistemleri aracılığıyla hukuka aykırı çıkar sağlamak suçu arasındaki ilişki ise fiil tekliği ilişkisidir. Birden fazla fiil ve birden fazla suç bulunmayıp tek fiil ve tek suç bulunmaktadır. Çünkü 1. ve 2. fıkrada yer verilen fiiller 4. fıkradaki suçun unsuru niteliğindedir. Dolayısıyla verilere müdahale ederek veya sistemin işleyişini bozarak ya da engelleyerek çıkar sağlayan kişi 4. fıkra hükmüne göre cezalandırılacaktır.[289]

Verilere zarar verme suçu ile 151. maddedeki mala zarar verme suçu arasındaki ilişki bakımından doktrinde farklı görüşler mevcuttur. Bir görüşe göre burada, TCK m.44 uyarınca farklı neviden fikri içtima kuralının uygulama alanı bulacağı ve failin ağır olan suçtan cezalandırılacağı kabul edilmektedir. Diğer bir görüş ise; maddede

---

[286] Mahmutoğlu, s.880.

[287] Karagülmez, s.191.

[288] Yılmaz, s.11.

[289] Akbulut, Berrin, *Türk Ceza Hukukunda Bilişim Suçları*, Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2000, s.130.

bahsi geçen bilişim sistemi kavramının, TCK m.151'de yer alan klasik mal kapsamında olmadığını, bu nedenle de TCK m. 151 ile 244'ün farklı hukuksal değeri koruduğunu ileri sürmüştür[290].

Aynı hukuki değeri koruyan farklı iki norm olduklarını söyleyen görüşe göre, buradaki sorun özel normun genel norma önceliği prensibi gereği bilişim sistemini özel olarak koruyan bir norm olan TCK m.244'ün uygulanması ile çözülecektir. 244. madde mala zarar verme suçuna göre bazı ek özelliklere sahip olan özel norm niteliğinde olması sebebiyle uygulama alanı bulur. Örneğin fail bilişim sistemine zarar vermek suretiyle verileri de yok etmişse veya verileri bozmuşsa içtima ilişkisinin ortaya konulması gerekir. Çünkü bu durumda fail, hem mala zarar verme suçunu hem de 244. maddeyi ihlal etmiştir. Eğer fail, kendine ait bilişim sistemine zarar vermek suretiyle, sistemde bulunan başkasına ait verilere zarar vermişse, şöyle bir değerlendirme yapabiliriz: Kişinin kendi malına zarar vermesi mala zarar verme suçunu oluşturmadığından yalnızca m. 244/2'yi ihlal etmiştir. Türk Ceza Kanununun 244. maddesinde ifade edilen bilişim sisteminin işleyişinin engellenmesiyle haberleşmenin engellenmesi (TCK m. 124) de gerçekleştirilmiş olabilir. Tek fiille farklı suçların gerçekleştirilmesi söz konusu olduğundan fikri içtima kuralları uygulanmalıdır[291].

TCK m. 244/2'de düzenlenen, bilişim sistemindeki verilerin başka bir yere gönderilmesi aynı zamanda TCK m. 136'daki kişisel verilerin hukuka aykırı olarak başkasına vermek, yaymak veya ele geçirmek suçunu gündeme getirebilir. Böyle bir durumda iki suç arasında TCK m. 44 gereği farklı neviden fikri içtima kurallarının uygulanması gerekmektedir[210].

VII. Suça Yönelik Yaptırım

Kanun koyucu bilişim suçlarını 1991 yılında 3756 sayılı Kanun'la yaptırıma bağlarken, mala zarar verme suçunda kabul ettiği esası, sabotaj ve verilere müdahale

---

290 Mahmutoğlu, s.890.

291 Özbek, s.922.

teşkil eden fiillerin aynı fıkrada aynı suç kapsamında düzenlediği 525/b-1 açısında da benimsemiş ve cezasını hem hürriyeti bağlayıcı ceza hem de para cezası olarak öngörmüştür.[292]

Türk Ceza Kanununun 244. maddesinde, bir bilişim sisteminin işleyişini engelleyen veya bozan kişinin, bir yıldan beş yıla kadar hapis cezası ile cezalandırılması öngörülmüştür (f. 1). Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin ise, altı aydan üç yıla kadar hapis cezası ile cezalandırılması hüküm altına alınmıştır (f. 2). Maddenin 3. fıkrasında ise sistemi engelleme, bozma, verileri yok etme veya değiştirme fiillerinin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek cezanın yarı oranında artırılacağı hüküm altına alınmıştır.

Türk Ceza Kanununun 244. maddesinin 1. ve 2. fıkrasında yer alan suçlar resen takip edilen suçlardandır. CMK m. 237'ye göre, resen takip edilen bu suçların davasına, suçtan zarar gören kişilerin katılması mümkündür. Mağdur, suçtan zarar gören gerçek veya tüzel kişiler kamu davasına katılabilirler.

VIII. Suçu Soruşturma ve Kovuşturma

A. TCK'da Yer Alan Hususlar

Türk Ceza Kanunun 244. maddesinin 1. ve 2. fıkrasında yer alan suçlar resen takip edilen suçlardandır. Resen takip edilen bu suçların davasına, suçtan zarar gören kişilerin katılması mümkündür. Mağdur, suçtan zarar gören gerçek veya tüzel kişiler kamu davasına katılabilirler (CMK m.237).[293]

Bilişim suçlarının bazı hallerde şikayet üzerine kovuşturulması mümkün olabilir. Örneğin, yabancı bir ülkede bilişim suçlarından birini işleyen Türk vatandaşı

---

[292] Akbulut, Bilişim Alanında Suçlar, s. 212-213

[293] Akbulut, Bilişim Alanında Suçlar, s.215

failin daha sonra Türkiye'ye gelmesi durumunda, suçun takibi şikayet üzerine yapılacaktır. Bu halde vatandaş iade edilmeyeceğinden, Türkiye'de yargılanması gerekmektedir. Türk Ceza Kanununun 11. maddesine göre, Bir Türk vatandaşı, 13. maddede yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı bir yıldan az olmayan hapis cezasını gerektiren bir suçu yabancı ülkede işlediği ve kendisi Türkiye'de bulunduğu takdirde Türk kanunlarına göre cezalandırılır. Bu halde soruşturma ve kovuşturma yapılması şikayete bağlı değildir. Ancak TCK m. 11/2' de yer aldığı üzere suçun cezası, bir yıldan az hapis cezasını gerektirdiğinde resen soruşturma ve kovuşturma yapılamamakta ve suçtan zarar görenin veya yabancı hükümetin şikayeti gerekmektedir. Bu durumda şikayet, vatandaşın Türkiye'ye girdiği tarihten itibaren altı ay içinde yapılmalıdır.

244. maddenin 2. fıkrasındaki suçun cezası da altı aydan başladığından, alt sınır bir yıldan az olduğundan resen soruşturma ve kovuşturma yapılamayacak, suçtan zarar görenin veya yabancı hükümetin şikayeti aranacaktır. Dolayısıyla yabancı ülkede suç işleyip Türkiye'ye gelen Türk vatandaşı fail hakkında şikayet gerçekleşirse soruşturma ve kovuşturma yapılıp cezalandırılması söz konusu olacaktır. Yabancı ülkede işlenen suç, bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ise, bu suçun cezasının alt sınırı bir yıldan başladığından resen takip yapılacaktır[294].

Görevli mahkeme, Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 11. ve 12. maddeleri gereğince asliye ceza mahkemesidir. Ancak TCK'nın 244/2.maddesinde düzenlenen bilişim sistemindeki verileri değiştirme ve erişilmez kılma suçunun yanında, ayrıca TCK'nın 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunun da işlenmesi halinde 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 12.maddesi uyarınca ağır ceza mahkemeleri yetkilidir. Bu gibi durumlarda dava asliye ceza mahkemesine açılmış ise mahkemenin görevsizlik kararı vererek dosyayı görevli ağır ceza mahkemesine göndermesi

---

[294] Akbulut, Bilişim Alanında Suçlar, s.215

gerekir.[295]Yetkili mahkeme CMK m. 12 gereğince suçun işlendiği yer mahkemesidir. Suçun işlendiği yer ise TCK m. 8'e göre belirlenecektir. Bu maddeye göre hareketin kısmen veya tamamen işlendiği veya neticenin gerçekleştiği yer suçun işlendiği yerdir. Hareketin gerçekleştirildiği yer, kişinin bedenen bulunduğu yeri ifade etmektedir. Ancak hareket yeri, beden olarak bulunulan yer dışında hareketin aynı anda ortaya çıktığı yer veya hareketin kısımlara bölündüğü yeri de kapsamaktadır. Bilişim suçlarında kişinin beden olarak bulunduğu yer ile hareketin açığa çıktığı yerler çoğunlukla farklı yerlerdir. Bu nedenle her iki yer de hareket yeridir[296].

Adli Bilişim sürecinde yürütülen işlemlerle ilgili olarak uyulması gereken esaslar sırasıyla Ceza Muhakemesi Kanunu'nun 134'üncü maddesinde, Adli ve Önleme Aramaları Yönetmeliği'nin 17'nci maddesinde ve Suç Eşyası Yönetmeliği'nin 9'uncu maddelerinde yer almaktadır[297].

Bilişim suçlarının soruşturma aşamasında delillerin incelenmesinde, delillerin mutlaka kopyalarının üzerinde çalışılması gerektiğinden elde edilen delillerin güvenilir bir yöntemle imajlarının alınması gerekmektedir. Alınan imaj sayesinde, eldeki verilerin o şahsa ait olduğu belirlenmiş olmakla birlikte elde edilen deliller

---

[295] Doğan, s.141; Yargıtay 8.CD., 18.12.2013 gün, 2013/735 E.-2013/29491 K., "Oluşa ve dosya kapsamına göre; şikayetçiler….. isimli kişilere ait msn adreslerini kırarak ilgili adreslerdeki kişilerin arkadaşlarından onlarmış gibi yazışarak kendine yarar sağlamak amacı ile kontör talep edip şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK'nın 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturup oluşturmayacağına ilişkin delilleri takdir ve tartışmanın 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunun 12.maddesi uyarınca ağır ceza mahkemesinin görevinde bulunduğu gözetilerek görevsizlik kararı verilmesi gerekirken, yargılamaya devamla yazılı şekilde hüküm kurulması"(Karar Yargıtay Uyap Sistemi üzerinden alınmıştır. 02.08.2019);

Yargıtay 8.C.D. 24.12.2012 gün 2012/21826 e- 2012/39370 k. " oluşa ve dosya kapsamına göre, mağdure F.Ç'nin işvereni olan Av. A.A'nın facebook şifresini bir şekilde ele geçiren sanığın, bu adresten mağdure ile A.A gibi yazışarak 700 TL'lik kontör kartı aldırıp şifrelerinin kendisine gönderilmesini temin ederek kullandığı telefon hattına yüklemesi şeklinde gerçekleşen eylemin, TCK'nın 158/1-f maddesinde yazılı bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu oluşturabileceği ve bu suça bakma ve delilleri takdir etmenin ağır ceza mahkemesine ait olmasına karşın, görevsizlik kararı verilmeyerek yargılamaya devamla yazılı şekilde hüküm kurulması"

[296] Özbek, Veli Ö., İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları, *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, C. 4, S. 1, 2002, s.126-127; Akbulut, Bilişim Alanında Suçlar, s. 216.

[297] Aydoğan, s.18-25.

üzerinde oynama yapılmadığı da ispatlanmış olacaktır. Sayısal delillerin inkar edilmemesini sağlamak, delillendirme işlemindeki sayısal delilin sahibi, onu ele geçiren şahıslar, delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların sonradan inkar edilememesi anlamına gelmektedir. Bu konuda özellikle delile ilk ulaşma anında, olay yerindeki kolluk görevlilerine iş düşer. Zira CMK'nın 169'uncu maddesinde, "….her soruşturma işlemi tutanağa bağlanır…" hükmü ile tanzim edilecek tutanakta, yine CMK'nın 134'üncü maddesinin 3'üncü bendi doğrultusunda "… bütün verilerin yedeklemesi yapılır" denilen veriler, olay yerinde bulunanlar tarafından yazılı hale getirilerek ilgili kişilere imzalatılmalıdır. Böylelikle delillerin inkar edilmemesi büyük ölçüde sağlanmış olur[298].

B. **CMK'da Yer Alan Hususlar**

Ceza Muhakemesi Kanunu'nda (CMK) Adli bilişim ile ilgili hükümler 4.Bölüm olan Arama ve El Koyma Bölümü'ndeki "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlığı altında 134'üncü maddede, düzenlenmiştir. Buna göre;

1. CMK 134'üncü Maddesinin 1. Bendi

CMK'nın 134'üncü maddesinin birinci bendine göre;

> "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkanının 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 haline getirilmesine hakim tarafından karar verilir."

Ancak bu maddede kopyası çıkarılan verinin nasıl ve ne kadar bir süre ile koruma altına alınacağı belirtilmemiştir. Dolayısıyla bu hali ile "Elektronik Delil Muhafaza Etme" aşamasını içermemektedir. Ayrıca bu maddede cep telefonu, cep

---

[298] Gözüşirin, s.92.

bilgisayarı, dijital fotoğraf makinesi, dijital kamera vb. gibi taşınabilir cihazlara yönelik bir hüküm de bulunmamaktadır. Adli bilişimin ana konusu elektronik delillerdir ve elektronik delil kaynağını sadece bilgisayar ile sınırlandırmak mevzuya dar bir pencereden bakmak demektir. Teknolojinin gelişimi ile günümüzde hemen herkesin kullanmış olduğu bu cihazlarda adli bilişim uzmanlarınca elde edilebilecek çok önemli bilgiler bulunabilmektedir.

> Bu tür cihazlara el konulması ile ilgili olarak CMK'nın 116. maddesinde "*Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, iş yeri veya ona ait diğer yerler aranabilir*" hükmü ile 123. Maddesinde;
>
> *(1) İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan mal varlığı değerleri muhafaza altına alınır,*
>
> *(2) Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyaya elkonulabilir*" hükümleri yer almaktadır.

CMK'da 116 ve 123. maddeler bulunmasına rağmen 134. maddeye yer verilmesinin, 134. maddeyi daha özel bir hüküm haline getirdiği düşünülmektedir. Bu nedenle nasıl bilgisayar ve bilgisayar programları ile bilgisayar kütüklerine yönelik işlemler genel arama maddelerinden ayrı tutulup CMK'nın 134. maddesine göre işleme tabi tutuluyorsa, aynı şekilde teknik açıdan aynı kapsamda değerlendirilmesi gereken cep telefonu, cep bilgisayarı ve elektronik veri barındıran diğer cihazlara yönelik arama işlemleri de genel arama hükümlerinden çıkarılmalı ve CMK'nın 134. maddesinde belirtilmelidir. Bunların yanında CMK'nın 1. bendinde yer alan "başka surette delil elde etme imkanının bulunmaması halinde" ön koşulu, olay mahallinde el konulan bilgisayar ve içerisinde elektronik veri barındırabilen diğer cihazlara yönelik arama işleminin gecikmesine neden olabilecektir. Karagülmez bu sorunun CMK'nın 116. maddesinde belirtilen "suç delillerinin elde

edilebileceği hususunda makul şüphe varsa" koşulunun CMK'nın 134. maddesine eklenmesi ile giderilebileceğini belirtmektedir[299].

2. CMK 134'üncü Maddesinin 2. Bendi

CMK'nın 134'üncü maddesinin ikinci bendine göre, "Delil Toplama" aşamasında, bilgisayar ve çıkarılabilir donanımlara el konulabileceği belirtilmektedir. Ancak bu durum "bilgisayarda bulunan şifrenin çözülememesi" koşuluna bağlanmıştır.

> *"Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir."*

Yukarıda ifade edilen bilgisayara el koymanın "şifrenin çözülememesi" şartı ile belirlenmesi kanunun bu maddesinin hazırlanışında teknik bilgilerin yetersiz olduğu sonucunun çıkarılmasına yol açabilir. Çünkü yedekleme işlemi için bilgisayarın açılması gerekli değildir. Oysa burada delil olabilecek verilerin kopyalanması için, kullanıcının bilgisayarda oturum açarken başkalarının girmesini engellemek amacıyla oluşturduğu parola nedeniyle bilgisayar oturumuna girilememenin kastedildiği anlaşılmaktadır. Ayrıca bahsedilen kopyalama işleminin parola koruması olmayan bir bilgisayar oturumuna girilerek bilgisayarda delil olabilecek ve olayla ilgili olduğu düşünülen resim, doküman vb. verilerin başka bir depolama ünitesine aktarılması olduğu tahmin düşünülmektedir. Adli bilişimde yukarıda bahsedilen kopyalama işlemi kabul edilemez. Delil bütünlüğü açısından elektronik delilin yalnızca bazı dosyalarının veya verilerinin kopyalanması değil, delilin tamamı ile birebir kopyasının alınması gerekmektedir. Birebir kopyalama yapmamanın iki türlü sakıncası vardır:

---

[299] Karagülmez, s.267.

1. Kopyalanan verilerin gerçekten orijinal delilden alındığı ispat edilemez.

2. Orijinal delilin içerisinde bulunan silinmiş veriler elde edilemez.

Birebir yedek alma işleminde bilgisayar hard diski yedekleme ünitesine direkt olarak bağlanabildiği için bilgisayarı açmak gerekmez ve dolayısı ile bilgisayarı açma, oturum başlatma ile ilgili şifre çözme işlemine gerek yoktur. Bilgisayarlara el koyma şartı bilgisayarlarda bulunan verilere erişim için gerekli şifrelerin çözülememesine bağlanmalıdır. Ayrıca bilgisayarlara el koyma şartı yedekleme işleminin uzun sürecek olmasından dolayı da yapılabilir. Bilgisayar ve çıkarılabilir depolama ünite sayısının fazla olması dolayısıyla yedekleme yapılacak verilerin büyüklüğü nedeni ile delil toplama işlemi çok uzun sürebilir. Böyle durumlarda delillerin olay mahalli yerine kolluk kuvvetlerinin laboratuvarlarında yedeklenmesi daha uygun ve güvenilir sonuçlar verecektir.

3. CMK 134'üncü Maddesinin 3. Bendi

Adli bilişimde "Delil Toplama" aşamasında orijinal verilerin birebir kopyası (imaj) alınmaktadır. CMK'nın 134'üncü maddesinin üçüncü bendine göre bilgisayardaki verilerin yedeklenebileceği belirtilmektedir.

> "*Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.*"

Ancak bu maddede bilgisayar haricindeki CD, DVD, disket, çıkarılabilir hafıza birimleri (USB memory, SD Card vb.) gibi veri depolama ünitelerinin yedeklenebileceği belirtilmemektedir. Bu hali ile maddenin yetersiz kaldığı açıktır. Çünkü günümüzde kişiler bilgisayarlarındaki işletim sisteminin çökmesi veya çalışamaz hale gelmesi ihtimaline binaen önemli bilgilerini CD, DVD harici hard disk vb. gibi harici veri depolama birimlerinde saklamaktadırlar. Ayrıca taşınabilir hafıza ünitelerinde önemli bilgilerin bulunabileceği göz ardı edilmemelidir.

4. CMK 134'üncü Maddesinin 4. Bendi

CMK'nın 134'üncü maddesinin dördüncü bendine göre;

> "*İstemesi halinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır*."

Hükümden anlaşılacağı üzere elektronik ortamda çıkarılan kopyaların şüpheli veya vekili tarafından talep edilmedikçe şüpheliye veya vekiline verilmesi gibi bir zorunluluk bulunmamaktadır.

5. CMK 134'üncü Maddesinin 5. Bendi

CMK'nın 134. maddesinin beşinci bendinde, "Delil Toplama" aşamasında, bilgisayar ve çıkarılabilir donanımlara el konulmadan (bilgisayar ve çıkarılabilir donanımlarının kolluk kuvvetleri laboratuvarlarına götürülmeden) verilerin yedeğinin alınmasının olay mahallinde de yapılabileceği düzenlenmektedir.

> "*Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır*."

Ancak bu maddede kopyası alınan verilerin kağıda yazdırılması kısmının uygulanabilirliği pek mümkün değildir. Çünkü bir bilgisayardan kopyası alınan verilerin tümünün kağıda yazdırılması tonlarca evrak yığını manasına gelmektedir ki bunların çoğu gereksiz bilgi olarak karşımıza çıkmaktadır.

IX. Bilişim Suçlarının Önlenmesine Yönelik Tedbirler

Bilişim suçlarının önlenmesine yönelik tedbirleri açıklamadan önce öncelikle burada karşılaşılan en büyük sorunlardan birisi, bu suçların uluslararası yargı boyutunun bulunmamasından dolayı öncelikle hangi ülkenin hukukunun uygulanacağıdır. Geleneksel ceza yargılamasında hukukunda, suçun işlendiği yer mahkemesine yargılama yetkisi verilmiştir. Fakat bu kural bilişim suçları bakımından yetki sorununu çözmekten uzaktır. Bilişim suçlarında suçun işlendiği yer önemli bir sorun teşkil etmektedir. Özellikle failin yabancı ülkede oturması durumunda veya kimliğinin belirlenemediği durumlarda ciddi hukuki sorunlar ortaya

çıkmaktadır. Taşkın buradaki en etkili çözüm önerisini şu şekilde belirtmiştir: Hava korsanlığı ve terör eylemlerinde olduğu gibi, bu suçun insanlığa karşı işlendiğinin kabul edilmesi ve failin yakalandığı yer mahkemesinin suçun soruşturulmasında ve kovuşturulmasında yetkili olduğunun benimsenmesidir. Diğer bir görüş ise bilişim suçlarında, hangi ülkenin kendisini yetkili sayıyorsa onun derhal müdahale etmesini ve yargı yetkisinin geçerli olması gerektiğini savunmaktadır. Diğer bir temel sorundan bahsedecek olursak, ceza yasalarımızın yetersizliğidir. Bilişim suçlarının dinamik yapısı da bu yetersizliği perçinlemektedir. Fakat 765 sayılı TCK ile bu konuda ki pek çok yetersizlik ortadan kaldırılsa da yine de önemli eksiklikler bulunmaktadır.[300]

A. Bireylerin Alması Gereken Tedbirler

Bireyler alacakları önlemler ile göreceği zararları ortadan kaldırabileceği için önemli görevler düşmektedir. Bireysel kullanıcılarla şirketler, sistemlerinin güvenliğini artırıcı yazılımlar kullanarak görecekleri zararı azaltmalıdır. Bilişim suçlarının çoğu, özellikle şirketlerin ticari saygınlıklarını zedeleyeceği düşüncesi ile soruşturmaya yetkili kurumlara bildirilmemektedir. Bu da önemli bir sorun teşkil etmektedir. Bundan dolayı, bireylerin uğradıkları mağduriyetleri yetkili birimlere rahatlıkla iletmelerini sağlamak, halkın öz denetimine başvurmak bilişim suçlarıyla mücadelede önem taşımaktadır.[301]

Her birey öncelikle kullandığı bilişim sisteminin güvenliğini sağlamak zorundadır. Bu sayede sistemde bulunan verilerin ve sistemin kendisinin gizliliği ve bütünlüğü her türlü tehlikelere karşı korunmaktadır. Bilişim sistemlerinin güvenliği aşağıda gösterilen başlıklar altında gerçekleştirilmektedir[302].

- İdari ve kurumsal güvenlik,
- Personel güvenliği,
- Fiziksel güvenlik,

---

300 Taşkın, s.175-177.
301 Taşkın,s.177-178.
302 Dülger, s.156.

- İletişim ve elektronik güvenliği,
- Donanım güvenliği,
- Yazılım güvenliği,
- İşlem güvenliği,

Bu hususta farklı ayrımlar da yapılabilmektedir. Örneğin, fiziksel güvenlik, ağ bazında güvenlik, bilgisayar bazında güvenlik, iletişim bazında güvenlik ve politika bazında güvenlik biçiminde gruplandırma yapılabilmektedir[303].

Bu güvenlik önlemleri sayesinde, bilişim sistemleri için öngörülen güvenlik sağlanmakta ve hem sistemde bulunan verilere yetkisiz kullanıcıların erişimleri önlenmekte hem de sistemin kesintisiz biçimde çalışması sağlanmaktadır.

Uygulamada yaygın olarak başvurulan ve etkili önlemlerden birisi bilişim sistemlerinde "firewall" adlı güvenlik duvarı yazılımlarının kullanılmasıdır. Bilişim sistemlerine antivirüs programlarının yüklenmesiyle de bu yazılımlar devamlı güncellenmekte ve yeni virüslerin bilişim sistemlerine girmesinin önüne geçilmekte, ayrıca daha önce giren kötü amaçlı yazılımlar da temizlenebilmektedir. Fakat kullanıcılar tarafından alınan bu önlemlere rağmen bilişim alanında tam anlamıyla güvenlik sağlanmayabilmektedir. Bilişim sistemlerinin güvenliği için geliştirilen sistemlerin zamanla bir açığı bulunmakta ve bu açık nokta bulunarak sisteme giriş mümkün olmaktadır. Bu nedenle bilişim sistemlerinde olabildiğince iyi ve güncel güvenlik önlemi alınmaya çalışılmalıdır.

Bilişim suçuna müdahale suçun ilk tespit edildiği anda başlamaktadır. En kritik nokta da bu aşamadır. Eğer suçu ilk fark eden kişinin bu konuyla ilgili yeterli bilgisi yoksa çok önemli bilgi ve deliller istem dışı yok edebilmektedir. Bu sebeple ilgili kişilere mutlaka eğitim verilmeli, olağan dışı herhangi bir olayın fark edilmesi

---

[303] Uzunay, Yusuf, "Dijital Saldırılar, Emniyet Güçleri Açısından Önemi ve Korunma Yolları", *Polis Bilimleri Dergisi*, C.5 S.2 Ankara, 2003, s.12.

durumunda bilişim suçları konusunda eğitilmiş bir uzmana ulaşmaları sağlanmalıdır[304].

Bir bilişim suçunun meydana geldiği tespit edildiğinde, olay mahallinde bulunan bilgisayar, cep telefonu vb. cihazlar açık durumda ise kesinlikle kapatılmamalıdır. Çünkü kapatma esnasında geçici bilgiler silinmekte ve bu bilgilere tekrar ulaşılamamaktadır[305].

Bahse konu bilişim cihazlarının inceleme neticesinde laboratuvara götürülmesi düşünülürse, dizüstü bilgisayar, cep telefonu, cep bilgisayarı veya tablet bilgisayarlarının şarj seviyelerinin yeterli olup olmadığı kontrol edilmelidir. Masaüstü bilgisayarları için taşıma öncesinde çalışan programlar ve açık olan uygulama pencerelerindeki bilgiler not edilmeli, hard disk imajı alınmalı ve bu şekilde kapatılarak taşınmalıdır. Aynı şekilde olay mahallinde bulunan bilgisayar veya cep telefonu gibi cihazlar eğer kapalı durumdaysalar kesinlikle açılmamalıdır. Aksi halde verilerin değişmesine neden olunabilir. Cep telefonları faraday poşetlerinde taşınmalı, taşıma esnasında cep telefonlarına gelebilecek aramalar ya da kısa mesajlar engellenmeli ve telefonun hizmet aldığı son konum bilgisinin değişmemesi sağlanmalıdır. Aksi halde telefona gelebilecek arama ya da kısa mesajlarla, kişilerin son arama listesi ve mesaj kutusu içeriği değişecek ve hatta silinen mesajlar üzerine veri yazıldığı için tekrar elde edilemeyebilecektir. Bunun yanında, kişinin son hizmet aldığı konum bilgisi de taşıma esnasında değişerek delilin orijinalliği bozulacaktır[306].

İnternet üzerinden veya ağ bağlantısına kapalı bir sistem üzerinde veri alış-verişinin yapıldığı durumlarda güçlü veri tabanı sistemleri kullanılmalıdır. Günümüzde bu amaçla hazırlanmış çok sayıda yazılım bulunmaktadır. Ancak bu yazılımların güvenilir ve Lisanslı Yazılımlar olmasına çok dikkat edilmelidir[307].

---

304 Uzunay Yusuf/Koçak, Mustafa, Bilişim Suçları Kapsamında Dijital Deliller, *AB'05 Akademik Bilişim Konferansı*, Gaziantep, Şubat 2005, s.3.

305 Özdilek, Ali O., *Bilişim Suçları ve Hukuku,* İstanbul,2006, s.204.

306 Aydoğan, s.14.

307 Dilber, s.70.

Bilişim sistemlerine yönelik bireysel önlemler aşağıda yer alan şekilde özetlenebilir[308];

- Büyük öneme sahip bilgiler hiçbir dış bağlantısı olmayan bilgisayarlarda saklanmalıdır.
- Çok önemli veriler; server, kişisel bilgisayar donanımları ve iletişimin tamamının koruma altına alınması suretiyle gerçek koruma sağlanabilmektedir. Bu bağlamda güvenlik hem fiziksel, hem de elektronik güvenliği kapsamalıdır.
- Herhangi bir sisteme gelen e-posta ve mesajları kontrol eden "güvenlik duvarları" mutlaka kullanılmalıdır.
- Kolay tahmin edilebilir şifre veya parolalar kullanılmamalıdır.
- Sistem sürekli izlenmeli ve herhangi bir kuşku duyulduğunda ağ sistemi yenilenmelidir.
- Şifre ve parolalar düzenli olarak değiştirilmelidir.
- İçeriği bilinmeyen şüphe uyandıran internet sitelerine girilmemelidir.
- Bilinmeyen bir adresten gelen e-postalar açılmamalıdır.

B. Kurum ve Kuruluşların Alması Gereken Tedbirler

Kurum içerisindeki bilgilerin farklı mekanlarda, farklı biçimlerde ve dağınık olarak bulunduğu göz önünde bulundurulmalıdır. Uygun tedbirlerin alınmadığı durumlarda, çoğu zaman çalışanlar kurum içerisindeki dağınık bilgilerden haberdar olmayabilmektedir. Bu nedenle bilgi tasnif edilmelidir.

Bilgi işlem merkezlerinde yetkilendirilmiş ve güvenilir personel çalıştırılmalıdır.

Bilişim suçlarının aydınlatılmasında önemli bir yeri bulunan Adli bilişim laboratuvarının yapısı ve fonksiyonları uluslararası örneklerine göre teşkil edilmelidir.

---

[308] Alkan, Necati, "Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler", *Çağın Polisi Dergisi*, S.35, 2003, s.305.

Lisanslı adli bilişim programlarının temin edilmesi ve bu kapsamdaki eğitimlerle, uzmanların adli bilişim programlarına hakim olması sağlanmalıdır.

Adli bilişim sistemlerinde elektronik/dijital delillere uygun prosedürler belirlenmelidir. Delil inceleme ve raporlamasına yönelik, detaylı talimat ve formlar hazırlanmalı ve tutarlılık sağlanmalıdır[309].

Bilgi güvenliği ve adli bilişim eğitimi verilebilecek birim oluşturulmalıdır. Bilgi güvenliği konusunda kamu ve özel kurumaların dikkati çekilmeli, bilişim suçlarında tepki mekanizmalarının yetenekleri dolayısıyla bilgi güvenlik düzeyleri arttırılmalıdır.

Mevcut "hacker" faaliyetlerine yönelik arşiv çalışması yapılmalı ve tüm yönleri, birbirleriyle ilişkileri ve organizasyonları tespit edilmelidir. Böylece karakteristikleri, teknikleri ve hedefleriyle ilgili geniş bir veri tabanı oluşturulması sağlanmalıdır.

Bilişim suçlarının önlemesi amacıyla internet ortamı rastgele taranmalıdır.

Bilişim suçları ile etkin mücadeleye engel olan, şüpheli ve zaman kaybı yaratan bilgi kaynakları tespit edilmelidir.

Zaman ve bilgi kaybının önlenmesi için farklı bölgelerde Adli Bilişim Laboratuvarları tesis edilmeli ve uygulamaları için Ulusal Standartlar tespit edilmelidir.

Dijital delil arama süreçlerine yönelik detaylı yasal yöntemler tespit edilmelidir. Bu sayede ülke içindeki ve uluslararası davalarda tazminat ödenmesine neden olacak yanlışlıklar önlenebilecektir.

Dijital delillerin şifrelenmiş olabilme hususu göz önünde bulundurularak, bilgisayar sistemleriyle şifre kırma teknikleri üzerine araştırmalar yapılmalıdır.

Bilişim sistemlerine yönelik veri madenciliği ve yapay zeka uygulamalarına ağırlık verilmelidir.

---

[309] Çiçek, s.18-19.

Eğitici ve öğreticilerinin bilişim suçları konusunda daha bilinçli olması sağlanmalı, gelecek nesillerini yetiştirecek eğitim kurumlarının müfredatında yer alan bilgisayar dersi içeriğine bilişim suçu ve bilgi güvenliği konuları eklenmelidir.

Hukuk fakültelerinde konu ile ilgili çalışmalara ağırlık verilmelidir. Bilişim suçları konusunda gelecekte karar verici personel olacak kişilere, teknik bilgi eğitimi de verilmelidir.

Bilişim teknolojilerinde işlenilen bilgiler doğrultusunda tüm kullanıcıların ortak sorumluluk yüklenmesi sağlanmalıdır. Üstlenilen sorumluluk sebebiyle herkes karar vermek durumunda olduğundan "ast" kavramı ortadan kalkmakta ve herkes yönetici olmaktadır[310].

Kolluk kuvvetlerinin suçu öğrenme yöntemlerinde önceliği kendisine yapılan ihbarlar almaktadır. Yapılacak olan ihbarların içeriğinin sağlam olarak tespiti, soruşturmaya yön verecek önemli bir etkendir. Bu kapsamda, bilişim suçlarına ilişkin yapılan ihbarlar 155 Polis İmdat veya 156 Jandarma İmdat telefon hattından ya da karakollara veya savcılıklara yapılan yazılı bildirimden oluşmaktadır. Kolluk içerisinde ayrı bir birim oluşturması ve bu birimin, kendisine yapılan ihbarları değerlendirerek, gerek duyulması halinde bilişim ekiplerine ya da adli makamlara haber vermesi daha verimli sonuçlar doğurabilecektir. Bilişim konusunda bilgili, olay yeri incelemesi hakkında deneyimli, soruşturma usulleri konusunda eğitimli personelden oluşan ve 24 saat esasına göre hizmet yürütecek kolluk kuvveti bilişim ekiplerinin oluşturulması önem arz etmektedir[311].

Bir bilişim suçunda olay ne kadar karmaşık olursa olsun, her soruşturmada kabul edilen temel kural; "Her Temas Bir İz Bırakır" mantığıdır. Bir suçlu arkasında işlediği suçla ilgili delil, iz ve emareleri veya teknolojinin gelişimine paralel olarak bunlara eklenecek yeni emareleri bırakmaması hemen hemen imkansızdır. Ancak kolluk kuvvetleri suç işlenirken kullanıldığı değerlendirilen bilişim sistemlerine nasıl müdahale etmesi gerektiğini, muhtemel delilleri nasıl toplanacağını, topladığı

---

310 Hüsnü, Erkan, *Bilgi Toplumu ve Ekonomik Gelişme,* Ankara, Türkiye İş Bankası Kültür Yayınları, 1998, s.88.

311 Gözüşirin, s.105-106.

delilleri nasıl taşıması gerektiğini iyi bilmelidir. Aksi durumda suçun ispatı için kullanılması muhtemel deliller farkında olunmadan karartılabilmekte ya da eksik araştırma yapılması suretiyle çözümü çok zor olaylarla mücadele etmek zorunda kalınmaktadır[312].

Kişiler ve kurumlar tarafından alınan bu önlemlere rağmen bilişim alanında tam güvenlik sağlanamamaktadır. Bilişim sistemlerinin güvenliği için geliştirilen bütün sistemlerde bir açık bulunmaktadır ve bu açık noktadan sisteme girilmesi mümkün olmaktadır. Bundan dolayı bilişim alanında kesin güvenlik değil, "en iyi güvenlik" sağlanmaya çalışılmaktadır. Bilişim suçlarının önlenmesi için bireysel ve kurumsal olarak kullanıcıların, kendi sistemlerine uygun olarak hem verileri hem de sistemin devamlılığını korumaya yönelik iyi bir güvenlik engeli oluşturmak ve kullanmak konusunda bilinçlendirilmeleri gerekmektedir.[313]

C. Devletlerin Alması Gereken Tedbirler

Bilgi güvenliği konularında iyi bir kurumsal mekanizma ve acil durum yönetimi tesis edilmelidir. Bu hususta bir sorun yaşandığında, sorunu çözüp bilgiyi kullanılabilir halde tutacak uygulanabilir planlar hazırlanmalıdır.

Bilişim suçlarının tespit edilmesini desteklemek için, ağ yönetimi, ağ analizi ve ağ paketi incelenmesi konularında çalışılmalar yapılmalı ve suç aktiviteleri kayıt altına alınmalıdır.

Veri güvenliği amacıyla Ulusal veri savunma sistemleri oluşturulmalıdır.

Akademik, askeri ve endüstriyel uzmanlık birikimleri bir araya getirilmelidir. Birimler arasında iyi bir koordinasyon sağlanmalı, ağ teknolojilerindeki yeni teknoloji ve donanımların tespiti amacıyla ulusal adli bilişim teknolojilerinin geliştirilmesi çalışılmalarına hız verilmelidir.

Adli bilişim laboratuvarlarının kurulumu, yukarıdaki birimler ile koordinasyon sağlandığı takdirde ihtiyaçları en iyi şekilde karşılayacak yapıya sahip olacaktır.

---

[312] Ortabağ, H., "Kolluğun Adli Bilişim Delillerine Müdahale Yöntemleri", *Jandarma Dergisi*, Sayı:117, 2007, s.15.

[313] Dülger, Bilişim Suçları ve İnternet İletişim Hukuku, s.762-763.

Bilişim Suçları ve Adli Bilişim alanında bilirkişi olarak görev alacak ve laboratuvarlarda çalışacak personelin de akreditasyonu önemli bir husus olmaktadır[314].

Devlete düşen en temel görevlerden biri bilişim güvenliği sağlayacak önlemleri almak ve bilişim suçlarıyla mücadele edecek olan personel yetiştirmektir. Kolluk güçlerinin, yargıç, savcı ve savunmaların bilişim suçları hakkında özel eğitimden geçmeleri gerekmektedir. Bilişim suçlarının gelişken yapısı nedeniyle eğitim süreci içerisinde başka bilişim suçları ortaya çıkabileceğinden ve bundan dolayı personelin eğitimi de çağın gerisinde kalmaması için eğitimlerin sürekli ve düzenli bir eğitim olması gerekmektedir. Ayrıca adliyelere özel " Bilişim Savcılıkları" ile "Bilişim Mahkemeleri"nin kurulması bu suçlarla ilgili uzmanlaşmaya gidileceğinden önemli bir adım olacaktır. Ayrıca bilişim suçlarında başka yaptırımlar da öngörülmelidir, yalnızca hapis cezası yerine, başka seçenekli yaptırımların uygulanabilmesi için yasal düzenlemeler yapılmalıdır.[315]

E-devlet uygulamalarında veri ve bilgi güvenliği için gerekli önlemler alınmalıdır. Saldırıya maruz kalabilecek sistemler, önleyici üniteler, suçu takip edecek birimler, teknik destek birimleri ve bu konuda ARGE faaliyetlerini yürütecek birimlerin nitelikleri ve sorumlulukları belirlenmelidir. Koordinasyonu sağlayacak bir üst birim oluşturmalıdır. Koordinasyon faaliyeti uluslararası boyutta da yürütülmelidir. Sonuçta bilişim suçları teknolojiyi kullanan bütün ülkelerin ortak problemi haline gelmiştir. Bilişim suçları ile etkin bir mücadele, teknolojik gelişmeler çerçevesinde küreselleşen dünyada işbirliği ile mümkün olabilecektir[316].

Siber tehditler ve bilişim suçlarıyla mücadelede delillendirme, klasik soruşturmalardaki adli tıp bilimine benzemekte, ancak kendine has teknik bir altyapısı olan adli bilişim alanı ile adli soruşturma sürecinde bazı farklılıklar arz

---

[314] Çiçek, s.18-30.

[315] Taşkın,178-181.; "5237 Sayılı TCK'da öngörülen "denetimli serbestlik" uygulaması böyle yaptırımların hukuk sistemimize kazandırılması bakımından da yol gösterici ve güzel örnektir." (Bkz.: Taşkın, s.182).

[316] Özdemir, M., *Bilişim Suçları ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler Ve Çözüm Önerileri,* http://www.caginpolisi.com.tr/bilisim-suclari-ve-mucadelede-tasra-teskilatinda-karsilasilan-problemler-ve-cozum-onerileri/, Erişim Tarihi: 14.05.2019.

etmektedir. Bu bağlamda, bu tür delillerin toplanması, muhafazası, değerlendirilmesi ve bilirkişi tarafından incelemesi gibi faaliyetlerin, uzman kişiler tarafından yerine getirilmesi gerekmektedir[317].

Baroların bilişim suçları ile müdahale sürecine katılması ile hukuksal manada tarafsızlığın sağlanması desteklenecektir. Baroların sürece katılması, bilişim ekiplerinin olay yerinde bir suça ilişkin delil elde etme amacıyla, şüphelinin bulunduğu yere gidilmesini haber verilmesi şeklinde olacaktır. Müştekinin talep etmesi durumunda kolluğun bulunduğu yere barodan görevli gidebilmelidir. Kolluk tarafından, bir bilişim suçuyla ilgili şüphelinin bilgisayarı veya bilişim sisteminde arama yapılması esnasında barodan görevli bulundurulması hukuki bir durum olacaktır. Baro görevlisi burada hukuki anlamda kolluğun yaptığı çalışmanın yerindeliğini denetleyecek veya izleyecektir. Yapılan işlemin ardından hazırlanacak olan tutanağa baro görevlisinin imzasını atması, soruşturmada şeffaflığı arttıracaktır[318].

Bilişim suçları konusundaki problemler; hukuki, uygulama ve teknik boyutlar arasındaki koordinasyon eksikliğinden kaynaklanmaktadır. Suçla, günümüzde ve gelecekte daha etkin mücadele edebilmek için daha iyi teşkilatlanma ve teknik altyapı gereklidir. Özellikle soruşturma ve kovuşturma safhasında, yapılacak teknik incelemelerdeki sürenin azaltılması, bireylerin ve kurumların kişisel, mülki ve ticari haklarını koruyacaktır. Bilişim suçlarında, teknik inceleme yapan Adli Bilişim laboratuvarlarının ve kolluk kuvvetlerince yürütülen soruşturmaların aynı kamu çatısı altında bulunması bir açıdan tarafsızlık sorununa neden olmaktadır. Bu sebeple Adli Bilişim laboratuvarlarının bağımsız bir kurum ya da kuruluş bünyesinde yer alması uygun olacaktır[234].

---

317 Atıcı, Bünyamin/Gümüş, Çetin, "Sanal Ortamda Gerçek Tehditler: Siber Terör", *Polis Dergisi*, Sayı: 37, 2003, s.57-66.

318 Gözüşirin, s.109.

SONUÇ

Bilişim teknolojilerindeki bu hızlı gelişmeler suçluların da ilgisini çekmekte, normal yollarla işlenemeyecek suçlar bilişim teknolojileri sayesinde kolaylıkla işlenebilmektedir. Bilişim teknolojileri ne kadar gelişirse, kötüye kullanmak isteyenlerin de bu teknolojiyi bir suç aracı olarak kullanma arzuları o kadar artmaktadır. Bilişim sistemleri vasıtasıyla işlenen suçlar hırsızlık, dolandırıcılık vb. gibi klasik suç tipleri ile benzerlik gösterse de, işleniş yöntemleri, suçun boyutları ve suçun mağduru gibi açılardan klasik suçlardan ayrılmaktadır.

Bilişim teknolojileri alanında yaşanan gelişmeler hayatın her alanında büyük değişimler meydana getirmiştir. Bu gelişmeler insanlığa fayda ve kolaylık sağlamanın yanında uğraşılması güç bazı sorunları da beraberinde getirmiştir. Örneğin; bir kişinin bankacılık işlemlerini yapmak üzere banka şubesine giderken fiziksel saldırıya uğraması neticesinde parasını çaldırması gibi ihtimal söz konusudur. Ancak bu ihtimal, banka veya birey tarafından gerekli önlemlerin alınmadığı durumlarda, bilişim sisteminin önemli bir aracı durumundaki internet bankacılığı kullanımı neticesinde, banka hesaplarında yer alan paranın başka bir hesaba transferi veya kredi kartı bilgilerinin ele geçirilerek kredi kartlarının suç kastıyla kullanılması gibi birçok elektronik dolandırıcılığa maruz kalma ihtimali olarak ortaya çıkmaktadır. Bilişim suçları kapsamındaki elektronik deliller ise yapıları itibariyle kolaylıkla bozulabilmekte ve değiştirilebilmektedirler. Bu hassas yapılarından dolayı adli bilişim olarak adlandırılan ve özetle bilgisayar inceleme ve analiz yöntemleriyle bilgisayar ve diğer cihazlarından elektronik delil elde ederek, yargıya intikal ettirilmesi süreci olarak tanımlanan özel işlemler titizlikle yapılmalıdır. Bu titiz çalışma, kolluk kuvvetleri bünyesinde oluşturulan adli bilişim uzmanlarınca yürütülmektedir[319].

Bilişim sistemleri kapsamında işlenen suçlarla ilgili ülkemizde ilk uygulamalar, Fransız hukuk istemi temel alınarak, 1991 yılında 765 sayılı TCK'da yapılan eklemelerle yaptırım altına alınmıştır. 2005 yılında yürürlüğe giren 5237

---

[319] Aydoğan, s1.

sayılı yeni TCK ile bilişim alanındaki suçlar, teknoloji ve suçun işlenme kapsamında yaşanan gelişmeler doğrultusunda yeniden düzenlenmiştir. Bu bağlamda madde 243, madde 244 ve madde 245 olmak üzere bilişim alanındaki suçlar başlığı altında üç ayrı grupta ve toplamda sekiz ayrı suç yaptırıma bağlanmıştır. TCK'nun 244. maddesinde düzenlenen "sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları" siber suç sözleşmesinin gereğini yerine getirmek ve bu suçların ihlal ettiği hukuki değerleri korumak adına yapılan düzenlemelerdir.

Sonuç olarak bilişim alanında işlenen suçlar, gün geçtikçe önemini artırmaktadır. Hayatın her alanında karşılaşılan bilişim suçları sadece maddi çıkar sağlama amacıyla işlenmemekte, birçok farklı kişi ve grup tarafından terör, propaganda vb. amaçlarla da işlenmektedir. Günümüz toplum hayatı, her bireyin küçük ama gereken bütün işlevleri yerine getirebilen bilişim sistemlerini yanında taşımasına zorlamaktadır. Bu teknolojik araçlar sayesinde de bireyin, bilişim suçuna maddi kayıplara veya manevi zararlara uğrayarak mağdur şeklinde taraf olma olasılığı oldukça artmaktadır.

Toplumun bireylerinin ve kurumların korunması amacıyla yasa koyucu tarafından suçun önlenmesine yönelik bazı düzenlemeler yapılmaktadır. Ancak, alınan tüm önlem ve düzenlemelere karşın bilişim suçlarının işlenme oranları her geçen gün daha da artmaktadır. Bilişim suçları kapsamında yapılan ceza hukuku alanındaki düzenlemeler tek başına bu suçların önlenmesi için yeterli olamamaktadır. Özellikle gelişen teknolojiyle birlikte bilişim alanında yeni suç işleme yöntemlerinin ortaya çıkması, yapılan hukuki düzenlemelerin eksik veya yetersiz kalmasına neden olmaktadır. Dolaysıyla da ceza kanunlarında, gelişen suç tiplerine yönelik güncel düzenlemeler yapılmalıdır.

Bilişim suçlarının ortaya çıkan bireysel ve toplumsal ciddi sonuçlarına karşı yürütülecek mücadele çok yönlü gerçekleştirilmelidir. Bu mücadelenin en önemli boyutunun, bilişim sistemini kullanan kişi, kurum ve devletlerin konu ile ilgili almaları gereken önlemlerini iyi tespit etmelerinin, bunları sık sık gözden geçirmelerinin ve güncel tutmalarının gerektiği değerlendirilmektedir.

KAYNAKLAR

Akbulut, Berrin, *Türk Ceza Hukukunda Bilişim Suçları*, Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2000.

Akbulut, Berrin, "Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme". *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 2016, Cilt 24, Sayı 2.

Akbulut, Berrin, *Bilişim Alanında Suçlar* Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Ankara,2017.

Akbulut, Berrin, Ceza Hukuku Genel Hükümler, 5. Baskı, Ankara, 2018.

Akdoğdu, Pınar ve Şahin, Mehmet, *Bilişim Teknolojilerindeki Gelişmenin Turizm Sektörüne Etkisi ve Kullanım Alanları*, 2004, https://www.Bilgiyonetimi.org ,Erişim Tarihi: 07.01.2019.

Akıncı, Hatice/ Alıç, Emre ve Er, Cüneyd, *Türk Ceza Kanunu ve Bilişim Suçları,* Atamer, Yeşim (Ed.), İnternet ve Hukuk, Bilgi Üniversitesi Yayınları, İstanbul, 2004, No: 51

Aksoy, İpekçioğlu P., "Gözaltında Alınan İfadenin Önemi ve Delil Değeri", *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, Ankara, 2008, Sayı: 3, Cilt: 57

Albayrak, Ruşen A., *Bilişim Sistemleri Gelişmişlik Düzeyi ve Yönetim Önceliklerinin Bilişim Sistemleri Üst Düzey Yöneticisinin Rollerine Etkisi: Finans, Sanayi Ve Kamu Sektörlerinde Bir İnceleme*, Doktora Tezi, İstanbul Teknik Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul,2007.

Alkan, Necati , "Terör Örgütlerinin İnternet Ortamında Yürüttüğü Faaliyetler". *Çağın Polisi Dergisi*, 2003, S.35.

Altunok, Ebru ve Vural, Fatih A., "Bilişim Suçları", *Denetişim Dergisi*,2011.

Arbak, Yasemin, "Örgütlerde Bilgisayar Destekli Bilgi Sistemlerinin İncelenmesine Yönelik Kurumsal Bir Yaklaşım", *Verimlilik Dergisi*,1995,

Artuk, M.Emin/Gökcen, A/Yenidünya A. Caner, *Ceza Hukuku Genel Hükümler,* Ankara,2015.

ASCII totextconverter, http://www.unit-conversion.info/texttolls/ascii/, Erişim Tarihi: 10.05.2019.

Atamer, Yeşim, *İnternet ve Hukuk,* İstanbul, Bilgi Üniversitesi Yayınları, 2004, No: 51.

Atıcı, Bünyamin ve Gümüş, Çetin, "Sanal Ortamda Gerçek Tehditler: Siber Terör", *Polis Dergisi*, 2003, Sayı:37.

Avşar, Zakir/ Öngören, Gürsel, Bilişim Hukuku, İstanbul, Türkiye Bankalar Birliği, 2010, Yayın No:270, https://www.tbb.org.tr/Content/Upload/Dokuman/801/BILIŞIM_HUKUKU.pdf, Erişim Tarihi: 24-08-2019.

Ay, Mustafa, *Bilişim Teknolojilerinin Muhasebe Denetiminde Kullanılması ve Türkiye'de Faaliyet Gösteren Bağımsız Denetim Firmalarında Bilişim Teknolojilerinin Kullanım Düzeyi Üzerine Bir Araştırma,* Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2007.

Aydın, Emin D. , *Bilişim Suçları ve Hukukuna Giriş,* Ankara,1992.

Aydoğan, Hakan, *Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri,* Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2009.

Bankacılık Kanunu, https://www.tbb.org.tr/ Content/Upload/Dokuman/613/5411_Mart13.pdf, Erişim Tarihi: 13.05.2019.

Barca, Mehmet, Yeni Ekonomide Bilgi Yönetiminin Stratejik Önemi, *I. Ulusal Bilgi, Ekonomi ve Yönetim Kongresi*, Kocaeli Üniversitesi İİBF, Hereke-Kocaeli, 2002.

Barutçugil, İsmet, *Bilgi Yönetimi*, İstanbul, Kariyer Yayınları: 24,2002, Yönetim Dizisi: 7.

Bayer, Metin ve Kaygısız, Mustafa, *Olay Yeri İnceleme*, Emniyet Genel Müdürlüğü, Ankara,2002.

Bayraktar, R., *Veritabanı ve Akılcı Düşünce Üzerine*, 2002, http://www.bilgiyonetimi.org/cm/pages/mkl_gos.php?nt=127, Erişim Tarihi: 17.01.2019.

BT Hukuku (İ.Ü. Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi)., 2009, http://bthukuku.bilgi.edu.tr/pages/top_05.asp?id=0&r=4%2F9%2F2008+8%3A57%3A24+AM&lid=tr, Erişim Tarihi: 20.12.2018.

Bülbül, Hasan, *Rekabet Üstünlüğü Sağlamada Ürün ve Süreç Yeniliği: Bilişim Teknolojileri Uygulaması*, Basılmamış Doktora Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2003.

Cambazoğlu, Türker, Yararlı Bilgi Yönetiminde İnsan Faktörü, *Türkiye Bilişim Vakfı Eğitim Seminerleri,* 2000.

Canbek, Gürol ve Sağıroğlu, Şeref, "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Başkaya, Şenol (Ed.), *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 2007, Cilt: 22, No:1, Ankara.

Çekiç, Burak, *İnternet Aracılığı İle İşlenen Suçlar*, Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul,2006.

Ceyhun, Yurdakul ve Çağlayan, Ufuk M., *Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta,* Türkiye iş Bankası Kültür Yayınları, Ankara,1997.

Çiçek, İlker, *Ülkemizde Adli Bilişim Laboratuvarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları,* Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul,2008.

Davenport, Thomas H. ve Prusak, Laurence, *İş Dünyasında Bilgi Yönetimi,* 1.Basım, Çeviren: Günhan Günay Rota Yayınları,2001.

Demirbaş, Timur, *Ceza Hukuku Genel Hükümler,* 2014.

Demirkol, Zafer, *İnternet Teknolojileri,* İstanbul, 2001.

Dervişoğlu, Gökçe H., *Stratejik Bilgi Yönetimi,* Dışbank Kitapları Bilgi Yönetim Dizisi, 2004.

Dilber, Caner, *Bilişim Teknolojilerinin Bilgi Yönetimi Üzerine Etkisi: İstanbul'da Bilişim Sektörü Üzerine Bir Uygulama*, Yüksek Lisans Tezi, Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü, Kütahya,2008.

Doğan, Ramazan, 5237 sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Ankara, 2014.

Dokurer, Semih, *Bilişim Suçları ve Adli Bilişim*, 2019, https://docplayer.biz.tr/8768747-Semih-dokurer-semih-dokurer-kpl-gov-tr.html, Erişim Tarihi: 14.05.2019.

Dönmezer, Sulhi, Kişilere ve Mala Karşı Cürümler, 15. Baskı, İstanbul, 1998.

Dülger, Murat V. , *Bilişim Suçları,* Ankara, 2004

Dülger, Murat V.,Bilişim Suçları ve İnternet İletişim Hukuku, 5. Baskı, Ankara, 2014.

Ege, İlhan ve Sezer, Sevgi, *Bilgi Teknolojileri Kullanımı İle Akademik Verimlilik İlişkisi: Erciyes Üniversitesi Örneği*,2004, https://www.ilhanege.com, Erişim tarihi: 20.12.2018.

Ekizer, Hakan A., *Adli Bilişim Sertifikasyonları*, 2019,https://www.ekizer.net/adli-bilişim-sertifikasyonları/ Erişim Tarihi: 14.05.2019.

Ekizer, Hakan A., *Adli Bilişim (ComputerForensics-Bilgisayar Kriminalistiği),2019,* https://www.ekizer.net/adli-bilisim-computer-forensics/, Erişim Tarihi: 20.05.2019.

Ekizer, Hakan A., *Bilişim Suçları (Siber Suçlar), 2019,* https://www.ekizer.net/bilisimsuclari-sibersuclar, Erişim Tarihi: 07.05.2019.

Erdağ, İhsan A., "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* 2010, C. XIV, S: 2.

Erdi, Ali ve Durduran, Savaş, Türkiye Coğrafi Bilgi Sistemi Çalışmalarında Kurumsal Politikalar ve Bir Öneri, *3.Coğrafi Bilgi Sistemleri Bilişim Günleri Bildirileri*, Fatih Üniversitesi, İstanbul, 2003.

Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* Ankara, 2008.

Eryılmaz, Bedri M., *Yedekler İstenirse Veriliyor,* https://www.internethaber.com/news_detail.php?id=155128, Erişim Tarihi: 21.11.2018.

Evcimen, I.V. ve Evcimen, T.T., Bir Yüksek Öğretim Kurumunun Sıfır Noktasından Kavramsal Tasarımı: Özyeğin Üniversitesi Akademik Tasarımı ve Geliştirme Süreci, *2008 Oxford Business &Economics Conference (OBEC),* St. Hugh'sCollege, Oxford, İngiltere, ISBN: 978-0-9742114-7-3.

Hüsnü, Erkan, *Bilgi Toplumu ve Ekonomik Gelişme,* Ankara, Türkiye İş Bankası Kültür Yayınları,1998.

Gazi Üniversitesi, *Bilgisayar Nedir?*,http://w3.gazi.edu.tr/~akaraci/bilgkull.HTM, Erişim Tarihi: 13.12.2018.

Gözüşirin, Mesih, *5237 Sayılı Türk Ceza Kanununda Bilişim Suçları Ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi*, Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara, 2011.

Güleş, Hasan K./Özata, Musa, *Sağlık Bilişim Sistemleri,* Ankara, 2005.

Gümüş, Çetin, *Bilişim Suçları ile Mücadelede Polisin Eğitimi*, Yayımlanmamış Doktora Tezi, Fırat Üniversitesi Sosyal Bilimler Enstitüsü, Elazığ,2008.

Günday, Metin, *İdare Hukuku,* 9. Baskı, Ankara, 2004.

Hafızoğulları, Zeki /Özen, Muharrem, *Türk Ceza Hukuku Genel Hükümler*, Ankara, 2010.

Helvacıoğlu, Deniz A., *Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi*, Atamer, Yeşim (Ed.), İnternet ve Hukuk, *İstanbul, Bilgi Üniversitesi Yayınları*, 2004, No: 51.

Henkoğlu, Türkay, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, 2. Baskı, İstanbul, 2014.

Kara, Mahzure, *Siber Saldırılar - Siber Savaşlar ve Etkileri, Yüksek Lisans Tezi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2013.

Karabağ, Solmaz F., "Bilgi Yönetiminde Donanım ve Yazılım Teknolojileri", *Çukurova Üniversitesi Sosyal Bilimler Dergisi*, 2005, Cilt:14 Sayı:1.

Karadal, Himmet, Savaş, Orhan ve Kazan, Halim, *Bilişim Teknolojilerinin Yönetim Sürecine Etkileri: Aksaray'da Bir Araştırma*, 2008, Bilgi Teknolojileri Kongresi, Bildiri Özetleri.

Karahoca, Adem/Karahoca, Dilek, *İşletmeciler, Mühendisler ve Yöneticiler İçin Yönetim Bilişim Sistemleri ve Uygulamaları,* İstanbul, 1998.

Karagül, Aziz, *Bilgi Yönetim Sürecinde Kurumsal Kaynak Planlaması Uygulamalarının Muhasebe Bilgi Sistemine Etkisi*, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü,2006.

Karagülmez, Ali, "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", *Çağın Polisi Dergisi*, 2005, Sayı:46.

Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* Ankara, 2009.

Kaya, Bensghir T., *Bilgi Teknolojileri ve Örgütsel Değişim*, Ankara, 1996.

Kaygusuz, Mustafa, *Adli Bilimler,* Ankara, 2005.

Keser Berber L., *Adli Bilişim,* Ankara, 2004.

Keskin, İbrahim, "Bilişim Suçları", *Adalet Dergisi*, 2007, Y: 99, S: 29.

Ketizmen, Muammer, *Türk Ceza Hukukunda Bilişim Suçları,* Ankara, 2008.

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.

Koca, Mahmut, *Ceza Muhakemesi Hukukunda Delilleri*, Özbek Özer V. (Ed.), *Ceza Hukuku Dergisi*, Ankara, 2006.

Koca, Mahmut, Hukukumuzda TCK'nın 244. Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, Bilişim Hukuku Konferansı (9-10 Ekim 2010) Yargıtay, 91.

Kunter, Nurullah/Yenisey, Feridun/Nuhoğlu, Ayşe, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku,* 16'ncı Baskı, İstanbul, 2008.

Kurt, Levent, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* Ankara, 2005.

Mahmut, Koca/ İlhan, Üzülmez, *Türk Ceza Hukuku Genel Hükümler,* Ankara, 2009.

Mahmutoğlu, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", İÜHFM, 2013, C.LXXI, S.1, S.857-889. (Bilişim Alanındaki Suçlar)

Malkoç, İsmail, *Açıklamalı-İçtihatlı Yeni Türk Ceza Kanunu*, Ankara, 2007.

Meran, Necati, *Yeni Türk Ceza Kanununda Sahtecilik, Malvarlığı, Bilişim Suçları ile Ekonomi ve Ticari Alanda Suçlar,* 2. Baskı, Ankara, 2008.

Nakilcioğlu, İsmail H., Eğitimde e-Dönüşüm: Bilişim Toplumu İçin Eğitimcilerin Eğitimi. *Ulusal Bilişim Kurultayı,* Ankara, TBD 21,2004.

Ortabağ, H., "Kolluğun Adli Bilişim delillerine müdahale yöntemleri", *Jandarma Dergisi*, 2007,Sayı: 117.

Öğüt, Adem, *Bilgi Çağında Yönetim,* 2. Baskı, Ankara,2003.

Özdemir, Mehmet, *Bilişim Suçları ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler ve Çözüm Önerileri*, 2019, http://www.caginpolisi.com.tr/bilisim-suclari-ve-mucadelede-tasra-teskilatinda-karsilasilan-problemler-ve-cozum-onerileri/, Erişim Tarihi: 14.05.2019.

Özbek, Onur, *Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri*, https://www.umut.org.tr/userfiles/files/Document/document_ONUR%20OZBEK.doc , Erişim Tarihi: 14.05.2019.

Özbek, Veli Özer, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 2002, C. 4, S. 1, s. 126-127.

Özbek, Veli Özer/ Kanbur, Nihat/ Doğan, Koray/ Bacaksız, Pınar/ Tepe, İlker, *Türk Ceza Kanunu Özel Hükümler , 4*. Baskı, Ankara, 2012.

Özbek,Veli Özer/ Doğan, Koray/ Bacaksız, Pınar/ Tepe, İlker, *Türk Ceza Kanunu Özel Hükümler,* 10. Baskı, Ankara, 2016.

Özdilek, Ali O., *İnternet ve Hukuk,* Ankara, 2002.

Özdilek, Ali O., *Bilişim Suçları ve Hukuku,* İstanbul, 2006.

Özel, Cevat, *Bilişim Suçlarının Türk Ceza Kanunu ve Tasarıdaki Hükümler Yönünden Mukayeseli Değerlendirilmesi-Öneriler*, Tevetoğlu, Mete (derl.), Bilişim Hukuku, *İstanbul, Kadir Has Üniversitesi Yayınları,* 2004, s.85-91.

Özel, Cevat, *Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı*, Atamer, Yeşim (Ed.), *İnternet ve Hukuk,* İstanbul, Bilgi Üniversitesi Yayınları No: 51, 2004, s.341-363.

Özel, Cevat ve Ahi, M.Gökhan, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", *Güncel Hukuk*, 2005, S, 6, s. 21, http://www.turkhukuksitesi.com, E.T:15.01.2019.

Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler,* 2008.

Özgüler, Canbey V., Yeni Ekonomi Anlayışı Kapsamında Gelişmiş ve Gelişmekte olan Ülkeler: Türkiye Örneği, *Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Yayınları,* Eskişehir, 2003.

Özkaya, Elif, "Bilgi Teknolojisinin Yarattığı Parazitler", Gürdilek, Raşit (Ed.), *NTV Bilim Dergisi*, Sayı:1, İstanbul, 2009, s.60-64.

Özmen, Ş., *Ağ Ekonomisinde Yeni Ticaret Yolu E-ticaret*, 1. Baskı, İstanbul, Bilgi Üniversitesi Yayınları Yayın no:32, İstanbul, 2003.

Öztürk, Bahri/Erdem, M.Ruhan, *Uygulamalı Ceza Muhakemesi Hukuku,* 9'uncu Baskı, Ankara, 2006.

Öztürk, Mustafa İ., *Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri*, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara,2007.

Pallı, Hayati, *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, Yayımlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri,2008.

Parlar, Ali, Hatipoğlu, Muzaffer ve Yüksel Güngör E., *Ceza Muhakemesi Hukukunda Deliller, Çapraz Sorgu ve İspat,* Ankara, 2008.

Peker, Bekir, *Bilişim Suçları Ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu*, Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Konya,2010.

Sarıhan, Tan D., *Herkes İçin İnternet ,*2.Baskı, 1995.

Say, Kubilay, *Bilişim Suçlarından Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2006.

Saylı, M., Akdeniz D., Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar, Bursa, 2001.

Schjolberg, Stein, *The Legal Framework - Unauthorızed Access ToComputer. Systems*, Aktaran: Demircan Tunç. *Bilişim Alanında Suçlar*, Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi Sosyal Bilimleri Enstitüsü, Konya,2007.

Sevim, Şerafettin ve Öncel, Mesut, İşletmelerde Bilişim Teknolojilerinin Kullanım Düzeyinin Belirlenmesine Yönelik Bir Saha Çalışması, *İNET. TR*. 02 Konferansı, 2002.

Sınar, Hasan, *İnternet ve Ceza Hukuku,* İstanbul,2001.

Süzer, H.D, "Yükselen 4 Teknoloji", *Digital Dergisi,* No.11, 2004, s.28-31.

Şahin, Cumhur, *Ceza Muhakemesi Kanunu Gazi Şerhi*, Ankara, 2005.

Şafak, Ali ve Bıçak, Vahit, *Ceza Muhakemesi Hukuku ve Polis,* 6'ncı Baskı, Ankara, 2005.

Şener, Selçuk, *Karar Destek ve Üstyönetim Bilişim Sistemleri ve Türkiye'de Bilişim Sektöründe Bir Analiz*, Yüksek Lisans Tezi, Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2006.

Şenocak, Cengiz, *Maddi Suç Delilleri ve Ateşli Silahlar,* Ankara,1995.

Tanşu, Okan, *Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler*, Atamer, Yeşim (Ed.), İnternet ve Hukuk, İstanbul, Bilgi Üniversitesi Yayınları No: 51, 2004, s.139-157.

Taşkın, Şaban Cankat, Bilişim Suçları, Bursa, 2008.

Tezcan D./ Erdem M./Önok M., Teorik ve Pratik Ceza Özel Hukuku, 11. Baskı, Seçkin Yayıncılık, Ankara 2014

Topaloğlu, Mustafa, *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması,* İstanbul,1997.

Topaloğlu, Mustafa, *Bilişim Hukuku,* Adana, 2005.

TDK (Türk Dil Kurumu), *Büyük Türkçe Sözlük*, https://sozluk.gov.tr, Erişim Tarihi: 14.05.2019.

Uzunay, Yusuf, "Dijital Saldırılar, Emniyet Güçleri Açısından Önemi ve Korunma Yolları", *Polis Bilimleri Dergisi*, C.5 S.2, Ankara 200

Uzunay Yusuf, Dijital Delil Araştırma Süreci, 2.*Polis Bilişim Sempozyumu*, Ankara 2005.

Uzunay Yusuf ve Koçak, Mustafa, Bilişim Suçları Kapsamında Dijital Deliller, *AB'05 Akademik Bilişim Konferansı*, Gaziantep, 2005.

Yalçıner, Filiz ve Şahin, Fikret, *Açıklamalı Bilgisayar Terimleri Sözlüğü*, İstanbul, 1993.

Yaycı, Esra, *Bilişim Suçları*, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2007.

Yazıcıoğlu, Yılmaz, *Bilgisayar Suçları: Kriminolojik, Sosyolojik Ve Hukuki Boyutları ile*, İstanbul,1997.

Yenidünya, A. Caner, ve Değirmenci, Olgun, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,* İstanbul,2003.

Yenidünya, A. Caner, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu", *Legal Fikri ve Sınai Haklar Dergisi*, İstanbul, 2005, s.758.

Yenisey, Feridun, *Ceza Muhakemesi Hukukunda Delil*. Özbek, Özer V. (Ed.), *Ceza Hukuku Dergisi*, Ankara, 2007, Yıl:2, Sayı:4, s.11-54.

Yılmaz, Sacit, "5237 Sayılı TCK'nın 244. maddesinde Düzenlenen Bilişim Alanındaki Suçlar", *Türkiye Barolar Birliği Dergisi* (92), 2011.