



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Mehmet Can KARAGÖZ

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞ-
TİRME SUÇU (TCK m. 244)

Kamu Hukuku Ana Bilim Dalı
Yüksek Lisans Tezi

Antalya, 2019



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Mehmet Can KARAGÖZ

BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞ-
TİRME SUÇU (TCK m. 244)

Danışman

Dr. Öğretim Üyesi Mahmut KAPLAN

Kamu Hukuku Ana Bilim Dalı

Yüksek Lisans Tezi

Antalya, 2019

T.C.
Akdeniz Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğüne,

Mehmet Can KARAGÖZ'ün bu çalışması, jürimiz tarafından Kamu Hukuku Ana Bilim Dalı Tezli Yüksek Lisans Programı tezi olarak kabul edilmiştir.

Başkan : (İmza)

Üye (Danışmanı) : Dr. Mahmut Kaplan (İmza)

Üye : (İmza)

Tez Başlığı: Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)

Onay: Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

Tez Savunma Tarihi : 02/05/2019

Mezuniyet Tarihi : 20/06/2019

(İmza)
Prof. Dr. İhsan BULUT
Müdür

AKADEMİK BEYAN

Yüksek Lisans Tezi olarak sunduğum “BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU (TCK m. 244)” adlı bu çalışmanın, akademik kural ve etik değerlere uygun bir biçimde tarafımdan yazıldığını, yararlandığım bütün eserlerin kaynakçada gösterildiğini ve çalışma içerisinde bu eserlere atıf yapıldığını belirtir; bunu şerefimle doğrularım.

(imza)

Mehmet Can KARAGÖZ



T.C.

AKDENİZ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

TEZ ÇALIŞMASI ORJİNALLİK RAPORU



SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

ÖĞRENCİ BİLGİLERİ	
Adı-SOYADI	Mehmet Can KARAGÖZ
Öğrenci Numarası	
Enstitü Ana Bilim Dalı	Kamu Hukuku
Programı	Tezli Yüksek Lisans
Programın Türü	(x) Tezli Yüksek Lisans () Doktora
Danışmanının Unvanı, Adı-SOYADI	Dr. Öğretim Üyesi Mahmut KAPLAN
Tez Başlığı	Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiş-tirme Suçu (TCK m. 244)
Turnitin Ödev Numarası	

Yukarıda başlığı belirtilen tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam sayfalık kısmına ilişkin olarak, .../...../..... tarihinde tarafımdan Turnitin adlı intihal tespit programından Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nda belirlenen filtrelemeler uygulanarak alınmış olan ve ekte sunulan rapora göre, tezin/dönem projesinin benzerlik oranı;

alıntılar hariç %

alıntılar dahil % 'tür.

Danışman tarafından uygun olan seçenek işaretlenmelidir:

() Benzerlik oranları belirlenen limitleri aşmıyor ise;

Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylarım.

() Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise;

Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylar ve Uygulama Esasları'nda öngörülen yüzdelik sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.

Gerekçe:

Benzerlik taraması yukarıda verilen ölçütlerin ışığı altında tarafımca yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim.

...../...../.....

(imzası)

Dr. Öğretim Üyesi Mahmut

KAPLAN

İÇİNDEKİLER

KISALTMALAR.....	i
ÖZET.....	iii
SUMMARY.....	iv
ÖNSÖZ.....	v
GİRİŞ.....	2

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE İLİŞKİN TEMEL BİLGİLERİN TÜRK HUKUKUNDA VE TÜRK CEZA KANUNU SİSTEMATİĞİNDE DEĞERLENDİRİLMESİ

1.1 Bilişim, Bilişim Alanı ve Bilişim Sistemi Kavramları	3
1.1.1 Bilişim	3
1.1.2 Bilişim Alanı ve Bilişim Sistemi Kavramı	5
1.1.2.1 Yasa Koyucunun Tutumu	6
1.1.2.2 Bilişim Sistemi Hakkında Görüşler	8
1.1.3 Değerlendirme	9
1.1.3.1 Bilişim Yönünden.....	9
1.1.3.2 Bilişim Alanı ve Bilişim Sistemi Yönünden	11
1.2 Bilişim Sisteminin Unsurları	13
1.2.1 Duyuya Yönelen Aygıt.....	13
1.2.1.1 Donanım	14
1.2.1.2 Yazılım (Program ve Arayüz)	15
1.2.2 İç Bağlantı – Veri	17
1.2.2.1 Veri ve Bilgi Arasındaki İlişki.....	18
1.2.2.2 Bilişimsel Anlamda Veri	19
1.2.3 Dış Bağlantı – Ağ	20
1.2.3.1 Ağ Kavramı	20
1.2.3.2 Ağ Çeşitleri.....	21
1.2.3.2.1 Yerel Alan Ağları (LAN)	21
1.2.3.2.2 Kentsel Alan Ağları (MAN).....	21
1.2.3.2.3 Geniş Alan Ağları (WAN).....	22

1.2.3.2.4 İnternet	22
1.2.3.2.5 Ekstranet	23
1.2.3.2.6 Sanal Ağlar (VPN)	23
1.2.3.2.7 İnternet (Bilgisunar)	23
1.2.3.2.7.1 Tarihçe	23
1.2.3.2.7.2 Teknik Altyapı	25
1.3 Bilişim Sistemi Sayılan ve Sayılmayan Sistemler	26
1.3.1 Bilgisayar	29
1.3.1.1 Tarihçe	29
1.3.1.2 Donanımsal Özellikler	31
1.3.1.2.1 Anakart	31
1.3.1.2.2 İşlemciler	32
1.3.1.2.3 Bellekler	33
1.3.1.2.3.1 Fonksiyonlarına Göre Bellekler	33
1.3.1.2.3.2 Kullanım Amaçlarına Göre Bellekler	34
1.3.1.3 Yazılımsal Özellikler	35
1.3.1.3.1 BIOS, İşletim ve Uygulama Yazılımları	35
1.3.1.4 Çalışma Prensipleri	36
1.3.2 Cep Telefonu	36
1.3.3 ATM, Pos, Navigasyon ve Benzeri Cihazlar	39
1.3.4 Elektronik Ev Eşyaları	40
1.3.5 Robotik Çalışmalar, Yapay Zekâ, Otonom Ağır Sanayi ve Benzeri Cihazlar	40
1.3.6 Bulut Sistemler	42
1.4 Bilişim Sistemi Aktörleri	44
1.4.1 Mülkiyet ve Fikri Mülkiyet Yönünden	44
1.4.1.1 Geliştirici	44
1.4.1.2 Son Kullanıcı	45
1.4.1.3 Erken Erişim (Beta) Kullanıcılarının Durumu	45
1.4.2 Yetki ve Sorumluluk Yönünden	46
1.4.2.1 Genel Olarak	46
1.4.2.2 Türk Hukukunda Bilişim Ağları Üzerindeki Aktörler	46
1.4.2.2.1 İnternet Erişim Sağlayıcı	46
1.4.2.2.1.1 Erişim Sağlayıcıları Birliği	47
1.4.2.2.2 İnternet Yer Sağlayıcı	47
1.4.2.2.3 İnternet İçerik Sağlayıcı	49

1.4.2.2.4 Toplu Kullanım Sağlayıcılar	50
1.4.2.2.5 İnternet Servis Sağlayıcı Kavramı Sorunu.....	50
1.4.3 Amaç Yönünden	52
1.4.3.1 Kullanıcı	52
1.4.3.2 Bilişim Korsanı.....	53
1.4.3.2.1 Kavram ve Nitelendirme	53
1.4.3.2.1.1 Bilişim Korsanlarının Olumlu Yönlerine Dair Argümanlar	54
1.4.3.2.1.2 Bilişim Korsanlarının Olumsuz Yönlerine Dair Argümanlar	55
1.4.3.2.2 Sınıflandırma.....	56
1.4.3.2.3 Değerlendirme.....	57

İKİNCİ BÖLÜM

BİLİŞİM SUÇU KAVRAMI, TARİHSEL GELİŞİMİ, ÇEŞİTLERİ VE BİLİŞİM SUÇLARI İLE MÜCADELE KAPSAMINDA ALINAN ÖNLEMLER

2.1 Bilişim Suçu Kavramı ve Ortaya Çıkışı	60
2.1.1 Kavram	60
2.1.2 Tanım ve Kapsam.....	61
2.1.3 Tarihsel Gelişim	63
2.2 Bilişim Suçlarının Sınıflandırılması ve İşlenme Yöntemleri.....	65
2.2.1 Sınıflandırma	65
2.2.1.1 Bilişim Suçlarının Ayrı Bir Kategori Olmadığı Görüşü.....	65
2.2.1.2 Dört veya Daha Fazla Ayrımı Savunan Görüşler	65
2.2.1.3 Üçlü Ayrımı Savunan Görüşler	66
2.2.1.4 İkili Ayrımı Savunan Görüşler	66
2.2.1.5 Değerlendirme	67
2.2.2 Bilişim Suçlarının İşlenme Yöntemleri	68
2.2.2.1 Bilişim Suçlarının Ortak Aşamaları	68
2.2.2.1.1 Bilgi Toplama	68
2.2.2.1.2 Sisteme Sızma	69
2.2.2.1.3 Kalıcılığı Sağlama	70
2.2.2.1.4 İzleri Yok Etme	70
2.2.2.2 Bilişim Suçlarının İşlenmesinde Sık Görülen Yöntemler	71
2.2.2.2.1 Zararlı Yazılımlar (Malware)	71
2.2.2.2.1.1 Virüsler	72
2.2.2.2.1.2 Solucanlar (Worm).....	74

2.2.2.2.1.3 Truva Atları (Trojan Horse)	74
2.2.2.2.1.4 Mantık Bombaları (Logic Bombs)	75
2.2.2.2.1.5 Bukalemun	76
2.2.2.2.1.6 Salam Tekniği	76
2.2.2.2.1.7 Zararlı Reklam Yazılımları (Adware)	76
2.2.2.2.1.8 Fidyeye Yazılımı (Ransomware)	77
2.2.2.2.1.9 Arka Kapı (Gizli Kapı) Yazılımları	77
2.2.2.2.1.10 Tuş Kaydediciler (Keylogger)	77
2.2.2.2.1.11 İzleme ve Gizlenme (Sniffing ve Spoofing)	78
2.2.2.2.2 Hizmet Aksatma Saldırıları	79
2.2.2.2.2.1 DOS ve DDOS Saldırıları	79
2.2.2.2.2.2 İstenmeyen Posta (SPAM)	80
2.2.2.2.2.3 Tavşanlar	81
2.2.2.2.3 Sosyal Mühendislik	81
2.2.2.2.3.1 Oltalama (Phishing)	82
2.2.2.2.3.2 Sahte ve Geçici Postalar	83
2.2.2.2.4 Diğer Yöntemler	83
2.2.2.2.5 Hactivizmin Bilişim Suçu Olup Olmadığı Sorunu	85
2.3 Karşılaştırmalı Hukukta Bilişim Suçları ve Bu Suçlar ile Mücadele	86
2.3.1 Uluslararası Örgütler	86
2.3.1.1 Birleşmiş Milletler	86
2.3.1.2 OECD	88
2.3.1.3 Commonwealth	89
2.3.1.4 Karayip Topluluğu (CARICOM – Caribbean Community)	90
2.3.1.5 Sekizler Grubu (G8)	90
2.3.1.6 Amerikan Devletleri Örgütü (OAS – Organization of American States)	91
2.3.1.7 İnterpol	91
2.3.1.8 Avrupa Konseyi (COE)	91
2.3.1.8.1 Sanal Ortamda İşlenen Suçlar Sözleşmesi	93
2.3.1.8.1.1 Genel Olarak	93
2.3.1.8.1.2 Sözleşmenin Sistematiği	94
2.3.2 Ulusal Düzenlemeler	95
2.3.2.1 ABD	95
2.3.2.2 Almanya	96
2.3.2.3 Fransa	98
2.3.2.4 Japonya	100

2.3.2.5 İngiltere (Birleşik Krallık)	102
2.3.2.6 İtalya	104
2.4 Türk Hukuku'nda Bilişim Suçlarının Niteliği ve Bu Suçlarla Mücadelenin Gelişimi .	106
2.4.1 Tarihçe	106
2.4.2 Güncel Durum	107
2.4.3 Değerlendirme	108

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİN ENGELLENMESİ, BOZULMASI, VERİLERİN YOK EDİLMESİ VEYA DEĞİŞTİRİLMESİ SUÇU (TCK M. 244)

3.1 Genel Olarak.....	110
3.2 Korunan Hukuksal Değer	111
3.3 Suçun Maddi Unsurları.....	113
3.3.1 Konu	113
3.3.2 Mağdur.....	115
3.3.3 Fail	116
3.3.4 Eylem.....	117
3.3.4.1 Bilişim Sisteminin İşleyişini Engellemek veya Bozmak (TCK m. 244/1).....	118
3.3.4.1.1 İşleyişi Engellemek	119
3.3.4.1.2 İşleyişi Bozmak	121
3.3.4.2 Bilişim Sistemindeki Verileri Bozmak, Yok Etmek, Değiştirmek, Erişilmez Kılmak, Veri Yerleştirmek veya Verileri Başka Yere Göndermek (TCK m. 244/2) .	122
3.3.4.2.1 Verileri Bozmak	123
3.3.4.2.2 Verileri Yok Etmek	123
3.3.4.2.3 Verileri Değiştirmek.....	124
3.3.4.2.4 Verileri Erişilmez Kılmak	125
3.3.4.2.5 Veri Yerleştirmek.....	126
3.3.4.2.6 Verileri Başka Yere Göndermek	126
3.4 Suça Etki Eden Nedenler	127
3.4.1 Eylemin Bir Banka veya Kredi Kurumuna ya da Bir Kamu Kurum veya Kuruluşuna Ait Bilişim Sistemi Üzerinde İşlenmesi (m. 244/3)	127
3.4.2 Eylemin İşlenmesi Suretiyle Kişinin Kendisinin veya Başkasının Yararına Haksız Çıkar Sağlaması (m. 244/4)	129

3.4.2.1 TCK m. 244/4'ün Nitelikli Hal Olarak Kabul Edilip Edilemeyeceği Sorunu	129
3.4.2.2 TCK m. 244/4 Kapsamında Haksız Çıkarın Kapsamı ve Niteliği Sorunu	131
3.4.3 Suçun Terör Örgütü Faaliyeti Çerçevesinde İşlenmesi	133
3.5 Suçun Manevi Unsuru	133
3.6 Hukuka Aykırılık Unsuru	135
3.7 Suçun Özel Görünüş Biçimleri.....	138
3.7.1 Teşebbüs (Kalkışma)	138
3.7.2 İştirak	140
3.7.3 İçtima	140
3.8 Muhakeme	145
3.9 Yaptırım.....	145
SONUÇ	146
KAYNAKÇA.....	148
ÖZGEÇMİŞ	160

KISALTMALAR

ABD	: Amerika Birleşik Devletleri
ANSI	: American National Standards Institute
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CPU	: Central Processing Unit
dn.	: Dipnot
E.	: Esas
eTCK	: 765 sayılı eski Türk Ceza Kanunu
EIA	: Energy Information Administration
ETSI	: European Telecommunications Standards Institute
Fr.	: Fransızca
FrCK	: Fransız Ceza Kanunu
FSEK	: Fikir ve Sanat Eserleri Kanunu
GPU	: Graphics Processing Unit
HMK	: Hukuk Muhakemeleri Kanunu
IEEE	: Institute of Electrical and Electronics Engineers
ISO	: International Organization for Standardization
ISP	: Internet Service Provider
ITU	: International Telecommunications Union
İBK	: İçtihadı Birleştirme Kararı
İng.	: İngilizce
İOYYDHK	: İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun
İsp.	: İspanyolca
İt.	: İtalyanca
İtCK	: İtalyan Ceza Kanunu
JpCK	: Japon Ceza Kanunu
K.	: Karar
m.	: Madde
ODTÜ	: Orta Doğu Teknik Üniversitesi
PCI	: Payment Card Industry
RAM	: Random Access Memory

RG	: Resmî Gazete
RGS	: Resmî Gazete Sayısı
RGT	: Resmî Gazete Tarihi
ROM	: Read Only Memory
SOİSS	: Sanal Ortamda İşlenen Suçlar Sözleşmesi
T.	: Tarih
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: Türk Ceza Kanunu
TCKÖT	: Türk Ceza Kanunu Ön Tasarısı
TDK	: Türk Dil Kurumu
TIA	: Telecommunications Industry Association
TSE	: Türk Standartları Enstitüsü
UYAP	: Ulusal Yargı Ağı Projesi
vb.	: Ve Benzeri
yTCK	: 5237 sayılı yeni Türk Ceza Kanunu

Ö Z E T

Bilişim sistemleri son elli yıl içerisinde insanoğlunun yaşamını fark edilir biçimde değiştirmiştir. Günümüzde giderek artan bir hızla yaygınlaşmaya devam eden bu sistemler, suç içerikli eylemlerde de sıklıkla kullanılmakta, hatta bu eylemlerin hedefi haline gelmektedir. Bilişim suçları, saniyeler içinde gerçekleşebilmesi, uluslararası alanda etki göstermesi ve kanıtların elde edilmesindeki zorluk gibi birçok yönüyle geleneksel suç tiplerinden de farklılık göstermektedir. Bu nedenle bilişim sistemlerinin doğru özümsemiği bir ceza hukuku yaklaşımının geliştirilmesi gerekmektedir. TCK m. 244'te yer alan eylemler yalnızca bilişim sistemleri üzerinde işlenebilen ve görece yeni suç tiplerini oluşturmaktadır. Bu yüzden öncelikle m. 244'ün kapsamı net bir şekilde ortaya konulmalı ve benzeri suç tipleriyle olan ilişkisi belirlenmelidir. Ardından bilişim sistemlerinin yakın gelecekte beklenen değişim ve gelişimi göz önüne alınarak, bu suç tipinin kapsayıcı özelliğinin geliştirilmesi gerekmektedir. Bu çalışmada TCK m. 244, bilişim sistemlerine ilişkin önerilen bir model çerçevesinde incelenmeye çalışılmıştır.

Anahtar Kelimeler: Bilişim, bilgisayar, ceza hukuku, suç, internet.

S U M M A R Y



PREVENT OR CORRUPTION OF THE FUNCTIONING OF THE INFORMATION SYSTEM, SUPPRESSION OR CHANGE OF DATA CRIMES (TURKISH CRIMINAL CODE ARTICLE 244)

In the last fifty years, information systems have changed the life of human beings in a noticeable way. Nowadays, these systems, which continue to spread at an increasing pace, are frequently used and even become the target of these actions in criminal activities. Cyber crime differs from the traditional types of crime in many respects, such as the fact that it takes place in seconds, has an international impact and the evidence is difficult to obtain. For this reason, a new criminal law approach in which information systems are assimilated should be developed. The actions in Turkish Criminal Code article 244 constitute relatively new types of crime that can only be processed on information systems. Therefore, the scope of article 244 should be clearly identified and its relationship with similar types of crime should be determined. Considering the expected change and development of information systems in the near future, the inclusive feature of this type of crime needs to be developed. In this study, article 244 has been tried to be examined within the framework of a proposed model for information systems.

Key Words: Informatics, computer, criminal law, crime, internet.

ÖNSÖZ



GİRİŞ

Topluluk halinde yaşayan ve merakı nedeniyle sürekli gelişim içinde bulunan insanoğlu için bilişim, keşfedilmesi kesin ancak zaman gerektiren bir kavram olmuştur. Doğanın kendine özgü fiziksel ve kimyasal bağlantılarını ortaya çıkardıktan sonra, mekanik sistemlerle hayatlarını kolaylaştıran toplumlar, özellikle son yüzyıl içerisinde edindikleri yeni bilgilerle manyetik, elektronik vb. alanların çok daha hızlı ve verimli olabileceğini fark etmişlerdir. Atom parçacıklarının, elektromanyetizmanın insan algısına göre inanılmaz hızı ve kusursuz tepkimeleri, günlük yaşantıda kolaylık ve değişimleri de beraberinde getirmiştir.

Kalbi ortalama 1.2 hertz ile atan insanın, bugün 3 gigahertzi aşan hızlardaki (3 milyar hertz) aygıtları kendi kuralları ile kontrol edebilmesi, hukuk zemininde de düzenleme yapılmasını gerektiren bir alanın gerçekliğini ortaya koymuştur. Her yenilikte olduğu gibi, bilişim sistemlerinin de kötüye kullanılması, özellikle ceza hukukundaki karşılığı olan bilişim suçları konusunu günümüzde çalışılan en popüler alanlardan birisi haline getirmiştir.

İnsanoğlunun sürekli üzerine koyarak bugüne getirdiği bilişim sistemleri, bu paha biçilemez birikimin doğal sonucu olarak oldukça teknik bir yapıya sahiptir. Üstelik gelecek zamanlarda evrileceği yönü de kestirilemeyen bir olgudur. Bu nedenle klasik ceza hukuku sistematüğinde de kolaylıkla yerleştirilecek bir bölüme sahip olamamıştır. Halen mevzuatımızda bilişim ve bilişim sistemleri ile ilgili çelişkili tanımları ve ilerideki gelişmeleri kapsamaya çalışması nedeniyle isabetsiz genellemeleri sıklıkla görmekteyiz.

Buna karşın, bilişim suçlarının tanımlanması ve düzenlenmesindeki zorluğun temel etkeninin konunun teknik olmasından ileri geldiğini söylemek doğru olmayacaktır. Yoksa teknik eksiklikler, ilgili disiplinlerin ortak çalışması ise bugüne kadar çoktan aşılmış olurdu. Büyük çaplı bilişim suçları faileri, toplum gözünde suçlu yerine ileri zekalı sıfatı taşımakta, kendilerine saygıyla yaklaşılmaktadır. Büyük bilişim firmaları kendi sistemlerini en hızlı kıran hackerları bünyelerine katmakta ve ödöl vermektedir. Toplumdaki bilişim suçlarına yönelen algı da bilişim suçlarının düzenlenmesindeki temel sorunlardan birisini oluşturmaktadır.

Hukukun yorum metotları ile şekillenmesi, mühendisliğin ise yoruma yer bırakmayan, makineleri kontrol eden makine dilleri aracılığı ile genelleme ve formüller ile ifade edilmesi, iki zıt disiplinde ortak bir dil kullanılmasında yabancılik arz etmektedir.

Ülkemizde bilişim kavramı yoğunlukla bilgisayar üzerinden değerlendirildiğinden, günümüzde yaşanan teknolojik gelişmelerin çıkış noktası bilgisayar olan kısıtlı bir bakış açısıyla açıklanmaya çalışması da yaşanan zorluğun bir diğer nedeni olmaktadır.

Tüm bu zorluklara karşın, hukuk sistematüğinde bilişim alanının bugünü ve geleceğini kapsayan bir yapı oluşturulamayacağını söylemek de doğru olmayacaktır. Bilişim sistemleri, insan ürünü sistemler olarak elbette bir sınıra sahiptirler. Bu sınır da insan algısına hitap edecek olmalarıdır. İnsan algısının dışında olacak bir sistem, doğada karşılık bulsa bile hukuksal yönden bir anlam ifade etmeyecektir. Bu temel ilkedен yola çıkarak bilişim sistemleri ve suçlarının doğru şekilde değerlendirilebilmesi mümkündür.

Üç bölüm halinde incelenecek tezin birinci bölümünde bilişim, bilişim alanı ve bilişim sistemi kavramlarının sistematik bir şekilde tanımlanmasına, mevcut bilişim sistemlerinin örneklendirilmesine ve bunlar üzerinde bazı hak ve yetkilere sahip olan bilişim alanındaki aktörlerin açıklanarak, suçun unsurlarına netlik kazandırılmaya çalışılacaktır.

İkinci bölümde, bilişim suçları kavramı ile bilişim suçlarının tarihsel gelişimi ve buna paralel olarak bilişim suçlarıyla mücadelede yaklaşımlar ele alınarak, toplumdaki bilişim suçları algısı da incelenecektir.

Üçüncü bölümde TCK'nin 244. maddesinde düzenlenen bilişim sistemini bozma, engelleme, verilerin yok edilmesi veya değiştirilmesi suçunun unsurları, ilk iki bölümde ele alınacak açıklamalara uygun şekilde incelenecek, güncel sorunlar tartışılacak ve çözüm önerileri dile getirilecektir.

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE İLİŞKİN TEMEL BİLGİLERİN TÜRK HUKUKUNDA VE TÜRK CEZA KANUNU SİSTEMATİĞİNDE DEĞERLENDİRİLMESİ

1.1 Bilişim, Bilişim Alanı ve Bilişim Sistemi Kavramları

1.1.1 Bilişim

Bilişim de dahil olmak üzere bilişim terimleri denildiği zaman akla ilk gelen isim Prof. Dr. Aydın Köksal olmaktadır¹. Bilgisayar mühendisliği üzerine ülkemizdeki ilk doktora programını açan Köksal, aynı zamanda bugün sıklıkla kullandığımız 2500’ü aşkın² bilişim terimini de türeten kişidir. Bu nedenle bilişimle ilgili terimlerde öncelikle bilişim terimleri sözlüğündeki tanımlamalara yer verilecektir.

Bilişim sözcüğünü 1970 yılında türettiğini söyleyen Köksal, kelimenin yapısını şöyle açıklamıştır: “Bilişim sözcüğünü, Fr. informatique, İng. informatics, Alm. informatik, İt./İsp. infomatica olarak adlandırılan bilim ve meslek alanının Türkçe adı olarak, bilginin akışkan, devingen durumunu ve bu akışkanlığı sağlayan bilişim dizgelerini tanımlamak üzere, dönüş-lü/işteş çatıyı kullanarak bilmek eyleminden ad olarak türettim.”³

Görüleceği üzere information (bilgi) ile automatique (otomatik) kelimelerinin birleşiminden oluşan Fransız kökenli “informatique” kelimesinden farklı olarak Türkçe’de bilişim sözcüğü bilmek eyleminden türetilmiştir. Her ne kadar Türkçeye çevrildiği şekilde “enfor-masyon” sözcüğü bilişim ile eş anlamlı olarak kullanılmaktaysa⁴ da bilgi kökünden gelen⁵ ve dil yapısı daha uygun olan bilişim kelimesi isabetli olarak tercih edilmektedir. Biz de çalışmamızda bilişim sözcüğünü kullanmaya özen göstereceğiz.

Bilişim kavramının tanımı konusunda öğretilde belirgin bir ayrım olmadığı, genel olarak bilişim alanında yapılan işlemlerin sayılması yoluyla tanım yapıldığı görülmektedir. TDK, güncel sözlüğünde bilişimi “elektronik makine” ve “bilgi işlenmesi” unsurlarına vurgu yaparak tanımlamaktadır. Onlara göre bilişim, “İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi”dir⁶. TDK, bilişim terimleri

¹ Erdoğan, 2013: 5; Pallı, 2008: 34.

² Bunlara, bilgi işlem, donanım, yazılım, imleç, bellek vb. örnekler verilebilir. Köksal, 2010: 35.

³ Köksal, 2010: 44.

⁴ Peker, 2010: 10.

⁵ Dülger, 2015: 74.

⁶ http://tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5835cd984b7b85.49164390 (erişim tarihi: 25.02.2019).

sözlüğünde de aynı tanıma farklı kelimelerle yer verdiği gibi öğretide de aynı tanım üzerinden hareket edildiği görülmektedir⁷.

Bu tanıma biraz daha genişleten Dülger'e göre, "Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişimde kullandığı bilginin, özellikle bilgisayarlar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."⁸. Görüldüğü gibi Dülger, elektronik makine yerine bilgisayar terimini tercih etmiş ve bilişim alanındaki işlemlerin daha detaylı açıklamasına yer vermiştir. Gürler de benzer şekilde uzunca bir tanıma yer vermektedir⁹.

Tezcan/Erdem/Önok da bilgisayar vurgusu üzerinden bilişim tanımı yapmaktadır. Onlara göre bilişim, insanlar arası iletişimde kullanılan elektronik araçlarla ve özellikle de bilgisayar yardımıyla bilginin işlenmesi, saklanması ve aktarılmasıdır¹⁰.

Erdoğan, teknik bir konuda yeterli hakimiyetin bulunmaması nedeniyle yapılabilecek olası bir eksik tanımın, bilişim suçları yönünden kanunilik ilkesini zedeleyeceğini ileri sürerek bilişim tanımı yapmayı reddetmekte, veri işleme, veri saklama ve veri iletişiminin yapılması unsurlarına vurgu yapmakla yetinmektedir¹¹.

Artuk/Gökçen/Yenidünya, bilgisayar terimleri sözlüğüne daha yaklaşılarak "Bilişim, insanların, teknik, ekonomik, sosyal, kültürel, hukuksal veya benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılmasıdır." tanımını benimsemişlerdir¹².

Ersoy, konuya bilgisayar terimleri sözlüklerini esas alarak yaklaşmış ve "Bilişim, bilginin elektronik olarak işlenip, yüksek hızlı veri, ses ve görüntü taşıyan iletişim hatları aracılığı ile taşınmasını ifade eder." tanımını benimsemiştir.

Akbulut, sözlükte yer alan bilişim tanımını benimsemekle birlikte, bilişimin belgeleme tekniğinin ayrı bir disiplin olarak kabul edilmesinin ardından ortaya çıkan, bilginin yönetilmesini ve işlenmesini sağlayan bir alan olarak tanımlamaktadır¹³.

⁷ Erdağ, 2010: 277; Yılmaz, 2011: 63.

⁸ Dülger, 2015: 75.

⁹ "İnsanlığın ortak mirası olarak binlerce yıl içinde ticari, teknik, ekonomik, hukuksal, vb. tüm alanlarda üretilmiş ve bilişimin ulaşabildiği her türlü verinin, elektronik araçlarla, özellikle bilgisayarlar aracılığıyla elektronik/sayısal bir hale dönüştürülerek, düzenli ve akılcı bir biçimde toplanması, işlenmesi, kaydedilmesi, sınıflandırılması, saklanması, bilgi haline dönüştürülmesi ve tüm bu işlemlerin sonuçlarının doğrudan sunulmasını, ya da ses, görüntü ve/veya veri taşıyabilen kablolu veya kablosuz iletişim hatları aracılığıyla aktarılmasını sağlayan bilim dalıdır." Gürler, 2015: 31.

¹⁰ Tezcan/Erdem/Önok, 2016: 943.

¹¹ Erdoğan, 2013: 8. Aynı yönde, Çakıcı, 2014: 309.

¹² Artuk/Gökçen/Yenidünya, 2010: 706. Aynı yönde, Ersoy, 1994: 151.

¹³ Akbulut, 2017: 13.

Son olarak Kurt’a göre, “Bilişim, her alandaki üretilmiş bilgileri içeren verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkihi ve iletilmesi ile ilgili bir bilim dalıdır.”¹⁴.

Üniversitelerimizin enformatik bölümlerine ait internet sayfalarında da bilişim tanımlarına rastlanmaktadır. Bu tanımların da yapılan işlemlerin tek tek sayılması yoluyla elde edildiği söylenebilecektir. Akdeniz Üniversitesi’nin internet sayfasında bilişim, “Bilginin toplanması, sınıflanması, depolanması, işlenmesi, iletimi ve kullanımı için gerekli sistemleri inceleyen, teknolojiyle ilgili uygulamalar ve araştırmalar yapılan bir bilim dalı” olarak tanımlanmıştır¹⁵. Benzeri bir tanım yapılan Afyon Kocatepe Üniversitesi’nin internet sayfasında ise ayrıca, bilişimin bilgisayar, haberleşme ve yönetim bilimlerinin birleşiminden oluşan bir bilim dalı olduğu ifade edilmektedir¹⁶.

Yabancı üniversitelerde, Türk öğretilindeki ortak noktaları benimseyen ancak işlemleri saymak yerine bilişimin kapsamına vurgu yapan bir bilişim tanımı görülmektedir. Edinburgh Üniversitesi, internet sayfasında, bilişimi doğal veya mühendislik ürünü sayısal sistemlerin yapısını, davranışlarını ve etkileşimlerini inceleyen bir bilim dalı olarak adlandırmaktadır¹⁷. Eğitim programlarında bilişimin kapsamındaki disiplinleri, doğal sistemlerle ilgilenen bilişsel bilim (cognitive science), sayısal mühendislik sistemlerle ilgilenen bilgisayar bilimi (computing science) ve doğal sistemleri öykünücü (emülatör) ile dizayn eden yapay zekâ (artificial intelligence) olarak belirlemiştir¹⁸.

1.1.2 Bilişim Alanı ve Bilişim Sistemi Kavramı

Bilişim kavramının tanımı kadar, bilişim sisteminin sınırlarının çizilmesi ve unsurlarının belirlenmesi de zorluk arz etmektedir. Bununla birlikte, nasıl ki bilişim sistemlerini anlamak için bilişim kavramının tanımına ihtiyaç duyulmaktaysa, bilişim alanındaki suçların doğru anlamlandırılabilmesi için de bilişim sistemlerini tanımlamak gerekliliği ortadadır. TCK sistematiğinde suçun “bilişim sistemi” üzerinde işlenebilmesi, suç konusunun tanımlanmasının önemini daha da arttırmaktadır. Bu konuda öncelikle yasa koyucunun bilişim sistemi hakkındaki düşüncelerini inceleyip, bunu öğreti ve içtihatlarıdaki açıklamalar ışığında değerlendirmek uygun bir metot olacaktır.

¹⁴ Kurt, 2005: 25.

¹⁵ <http://enformatik.akdeniz.edu.tr/enformatik-bolumu-hakkinda/> (erişim tarihi: 25.02.2019).

¹⁶ <http://enformatik.aku.edu.tr/bolum-hakkinda-2/enformatik-nedir/> (erişim tarihi: 25.02.2019).

¹⁷ <http://www.ed.ac.uk/informatics/about/what-is-informatics> (erişim tarihi: 25.02.2019).

¹⁸ Ülkemizde de benzeri disiplinler yaklaşım sergilenmektedir. Açıklamalar için, ODTÜ, <http://ii.metu.edu.tr/>, Ankara Üniversitesi http://enformatik.en.ankara.edu.tr/?page_id=46 (erişim tarihi: 25.02.2019).

1.1.2.1 Yasa Koyucunun Tutumu

eTCK’de bilişim suçlarına ilişkin bir bölüme veya bağımsız bir hükme yer verilmiştir. Bu nedenle bilişim alanına ilişkin ilk açıklamalara da ancak 1989 tarihli TCKÖT’de rastlanmaktadır¹⁹. Tasarının 342. maddesinin gerekçesinde bilişim alanı, “bilgileri toplayıp depo ettikten sonra bunları otomatik olarak işleme tabi tutma sistemlerinden oluşan alan” olarak tanımlanmıştır²⁰. 1989 tasarısı kanunlaşmasa da bazı maddeleri nakledilerek 3756 sayılı kanunun²¹ 20 – 24. maddeleri uyarınca on birinci bap başlığı “Bilişim Alanında Suçlar” altında 525 a, b, c ve d maddelerinde yer alan bilişim suçları TCK’ye girmiştir. Bu dönemde “bilişim alanı” terim olarak kullanılmış ancak “bilişim sistemi” yerine “bilgileri otomatik işleme tabi tutan sistem” kavramı kullanılmıştır.

Daha sonraki 1997 tarihli TCKÖT’ün 347. maddesinin gerekçesinde “verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma imkânı veren manyetik sistemlerin oluşturduğu alan” olarak tanımlanan bilişim alanı 2003 tarihli son tasarının²² 346. maddesinin gerekçesinde “verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemlerden oluşan alan” olarak ifade edilmiştir. Komisyon gerekçesinde ise bilişim alanı yerine bilişim sisteminin tanımının yapılması tercih edilerek “verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren manyetik sistemler” açıklaması getirilmiştir.

Bölüm başlığı olan “Bilişim Alanında Suçlar” ise gerek komisyonda gerekse TBMM Genel Kurulu’nda değişikliğe uğramıştır. Tasarıda “Bilişim Alanında Suçlar” olarak belirlenen bölüm başlığı, komisyon raporunda “Bilişim Sistemlerine Karşı Suçlar” olarak değiştirilmiş ancak genel kurulda önceki şekliyle “Bilişim Alanında Suçlar” olarak kabul edilmiştir. Meclis tutanakları incelendiğinde bu değişikliklerin sebebini Adana Milletvekili Tacidar Seyhan’ın parti grubu adına yaptığı konuşmasından öğrenmekteyiz:

“Bir kere, konunun başlığı "Bilişim Sistemlerine Karşı Suçlar"dır. Eğer, bir insan, girer, bankamatikte bir kişinin hesabına zarar verirse, o kişiye karşı, onun haklarına karşı da bir suç işlemiş olur, bankaya karşı, kuruma karşı da bir suç işlemiş olur; yani, buradaki suç, tek başına sisteme karşı işlenmemiştir, aynı zamanda kuruma karşı işlenmiştir, aynı zamanda kişilik hakları çiğnenmiştir. Bu nedenle, buradaki

¹⁹ Başbüyük, 2010: 155.

²⁰ Erdoğan, 2013: 9.

²¹ Kanun 06.06.1991 tarihinde kabul edilmiş, 14.06.1991 tarih ve 20901 sayılı RG’de yayımlanmıştır.

²² 12.05.2003 tarih ve 2092 sayılı yazı ile kanunlaşmak üzere TBMM’ye sunulmuştur. <http://www2.tbmm.gov.tr/d22/1/1-0593.pdf> (erişim tarihi: 25.02.2019).

başlığı "Bilişim Sistemlerine Karşı Suçlar" şeklinde değil de bu alanı kapsayacak genel bir değerlendirilmeye tabi tutmayı daha uygun gördük.”²³

Mevzuatımızda bilişim sisteminin başkaca tanımlarını da görmekteyiz. Ceza Muhakemesinde Ses ve Görüntü Bilişim Sistemlerinin Kullanılması Hakkında Yönetmelik’in²⁴ tanımlar ve başlıklar başlıklı 3. maddesinde bilişim sistemi, bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem olarak tanımlanmıştır. Ulusal Siber Güvenlik Stratejisi ve 2013 – 2014 Eylem Planında²⁵ ise “Bilişim sistemleri, bilgi ve iletişim teknolojileri vasıtasıyla sağlayan her türlü hizmetin, işlemin ve verinin sunumunda yer alan hizmetleri ifade eder.” denilerek donanım özelliklerinden ziyade yapılan işlemler üzerinden tanımlama yapılmıştır.

Tanımı yapılmamakla birlikte birçok kanunda da bilişim sistemine ibaresine yer verilmektedir²⁶. Hatta HMK m. 445/1’de UYAP’ın adalet hizmetlerinin elektronik ortamda yürütülmesi amacıyla oluşturulan bir bilişim sistemi olduğu ifade edilmiştir.

Mevzuatın bazı yerlerinde ise bilgisayar sistemi ifadesinin kullanıldığı görülmektedir²⁷. Türkiye’nin de taraf olduğu SOİSS’in 1. maddesinde “Bilgisayar sistemi²⁸ terimi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder.” denilmektedir. Ancak, yabancı kaynaklarda bilişim suçlarının da computer crime (bilgisayar suçları) olarak tanımlandığı ancak bilgisayar (computer) kavramının daha geniş anlamda kullanıldığı dikkate alınırsa²⁹, buradaki tanımın da aslında bilişim sistemine ait olduğunu düşünmek isabetli olacaktır. Nitekim bilgisayar ileride açıklanacağı üzere genel kullanıma sahip bir bilişim sistemine örnek verilebilir. Yoksa bilişim sistemlerinin bütünüyle bilgisayarlardan oluştuğunu iddia etmek gerçekçi olmayacaktır³⁰.

²³ Tutanak ve madde gerekçelerine ilişkin sorgu, ilgili kanun ve madde bilgileri girilerek <http://mevzuat.tbmm.gov.tr/mevzuat/faces/sorgu.jspx?> adresinden yapılabilmektedir. (erişim tarihi: 07.02.2017).

²⁴ Adalet Bakanlığı, 20.09.2011 ve 28060 sayılı resmî gazetede yayımlanmıştır.

²⁵ Bakanlar Kurulu Kararı, 20.06.2013 ve 28683 sayılı resmî gazetede yayımlanmıştır.

²⁶ Ceza Muhakemesi Kanunu, Çek Kanunu, İcra ve İflas Kanunu, Sağlık Hizmetleri Temel Kanunu, Türk Ceza Kanunu örnek verilebilir.

²⁷ Belediye Kanunu, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun örnek olarak gösterilebilir.

²⁸ İngilizce metninde de “computer system” olarak yer almaktadır.

²⁹ Eker, 2006: 104.

³⁰ “Bilişim bir bilim dalını, bilgisayar ise bir makineyi tanımlamaktadır. Bu nedenle iki farklı kavramı karşılayan bu iki sözcüğün içeriklerinin karşılaştırılması da mümkün değildir... Gerçekten de bilişim sistemi tek bir bilgisayardan çok daha fazla şeyi tanımlamakta ve birçok bilişim suçunun işleme aracı olarak, bilişim suçlarının incelenmesi açısından daha elverişli bir tanım olmaktadır.” Dülger, 2015: 74. Benzer yönde, Orta, 2015: 53.

1.1.2.2 Bilişim Sistemi Hakkında Görüşler

Öğretide, önceki tarihli eserlerde kanunda yer alan “bilgileri otomatik işleme tabi tutan sistem” kavramı üzerinden açıklama yapıldığı görülmektedir. Yazıcıoğlu bu deyimden kast edilenin bilgisayar olduğunu açıkça ifade etmektedir³¹. Yenidünya/Değirmenci, bu kavram ile akla ilk gelen aygıtın bilgisayar olduğunu, ancak sadece bilgisayarın değil verilerin manuel veya otomatik olarak işlendiği ve iletildiği her türlü aygıtın bu sistem içerisinde değerlendirilmesi gerektiğini söylemişlerdir³².

Kurt, bilişim sisteminin yazıcı, modem gibi tüm çevre birimleri dahil olmak üzere bilgisayardan beklenen tüm amaçları gerçekleştirmeye elverişli bir donanım ve yazılım bütünü olduğu görüşüne katılmaktadır³³.

Tezcan/Erdem/Önok’a göre bilişim sisteminden anlaşılması gereken, verileri saklama, toplama, işleme, değerlendirme, depolama ve aktarma olanağı veren sistemlerdir³⁴. Çakıcı da benzeri bir tanım yapmaktadır³⁵.

Karakehya’ya göre bilişim sistemleri bir veya birden fazla ünitelerden oluşan ve belirli bir sonuca ulaşmak için iş birliği sistemiyle çalışan ve güvenlik araçlarıyla da korunan bir bütün olarak anlaşılmalıdır³⁶. Genel veri işleme yeteneğine sahip olmayan makineler Karakehya’ya göre bilişim sistemi olarak sayılmamaktadır.

Orta’ya göre bilişim sistemi, verilerin belli bir düzen içinde bilgisayar oranında saklandığı ve tanımlanan bilgi gereksinmelerini karşılamak üzere dönemsel ya da talep üzerine raporlar üreten, gereken veriye kısa sürede erişim olanağı sağlayan belli bir donanım üzerinde işletilen yazılım ve veriler bütünüdür³⁷.

Daha sade tanım yapan Artuk/Gökçen/Yenidünya’ya göre bilişim sistemi, veri – işlem ve veri – iletişim unsurlarını taşıyan araçların bütünüdür³⁸. Erdağ da aynı görüşü savunmaktadır³⁹. Kızıltan ise bu unsurların sayısını üçe çıkartmış, verileri alma (girdi), işleme tabi tutma ve sonuçları çıktı olarak verme (çıkı) unsurlarına sahip sistemlerin bilişim sistemi olabileceğini söylemiştir⁴⁰.

³¹ Yazıcıoğlu, 1999: 653.

³² Yenidünya/Değirmenci, 2003: 45. Aynı yönde, Değirmenci, 2005: 199.

³³ Kurt, 2005: 141.

³⁴ Tezcan/Erdem/Önok, 2016: 945.

³⁵ Çakıcı, 2014: 309.

³⁶ Karakehya, 2009: 8.

³⁷ Orta, 2015: 53.

³⁸ Artuk/Gökçen/Yenidünya, 2010: 706.

³⁹ Erdağ, 2010: 277.

⁴⁰ Kızıltan, 2007: 5.

Gürler, öğretilerde yapılan tanımlarda verilerin iletilme ve aktarılma unsurları üzerinde durulmadığını iddia ederek uzunca bir tanımda bulunmuştur⁴¹. Ancak biraz önce değerlendirdiğimiz üzere bu unsurlara yer veren çok sayıda yazar olduğu da görülmektedir.

Taşkın ayrıca bir tanım yapmamış, TCK m. 243 gerekçesinde yer alan tanım üzerinden yola çıkarak bilişim sisteminin, verileri gönderip alabilmesi, otomatik işleme tabi tutabilmesi, manyetik olması ile belli bir amaç için özgülenmemesi, genel amaçlı kullanabilmesi ölçütlerine göre karar verileceğini söylemiştir⁴².

Erdoğan ise, bilişim hakkındaki düşüncelerine paralel biçimde, bilişim sisteminin de tanımının yapılmasının tipiklik uyarınca uygun olmadığını söyleyerek, veri saklama, işleme ve aktarma unsurlarına vurgu yapmıştır⁴³.

Bilişim sistemi hakkında açıklamalara yer veren Gazi Üniversitesi Bilişim Enstitüsü internet sayfasında bir tanım yapılmamakla birlikte, sistemin bir yaşam döngüsünün olduğu, her sistemin planlama, gereksinme çözümlemesi, tasarım, yapım, kullanım ve bakım aşamalarından geçtiği söylenmektedir⁴⁴.

Yargıtay da bilişim sistemi kavramının bilgisayardan daha geniş olduğunu vurgulamış, bilgisayarın verilerin depo edilmesi, saklanması, işlenmesi ve yeniden değerlendirilmesi faaliyetini gerçekleştirmesine karşın "bilişim sistemi" hem verilerin işlenmesi hem de verilerin aktarılmasını kapsadığını ifade etmiştir⁴⁵.

1.1.3 Değerlendirme

1.1.3.1 Bilişim Yönünden

Bilişimin gelişen teknolojilere de uyarlanabilecek genel-geçer bir tanımının yapılmasında güçlük yaşandığı bir gerçektir. Bu konuda Erdoğan'ın endişesine hak vermek ile birlikte, ileri sürdüğü görüşlere katılmamaktayız. Bilişim kavramında yapılacak bir tanımın eksikliği, esasen hukukçuların oldukça teknik olan bilişim alanındaki yetersizliklerine dayanmamaktadır.

⁴¹ “Verilere ulaşma, verileri toplama, otomatik işleme tabi tutma, depo etme, sınıflandırma, bilgiye dönüştürme ve sonuçlarının doğrudan sunulmasını ya da ses, görüntü veya veri taşıyabilen kablolu veya kablosuz iletişim hatları aracılığıyla iletebilme yeteneğine sahip bilişim cihazları ile varsa kurulu düzenin çalışmaya devam etmesini sağlayan elektronik veya manyetik sistem veya sistemler ile bu sistemlerin birbirine bağlanmasıyla oluşan ağların da dahil olduğu alandır.” Gürler, 2015: 33.

⁴² Taşkın, 2008: 10. Bazı yazarlar da aynı şekilde gerekçeye bağlı kalmışlardır. Yılmaz, 2011: 63.

⁴³ Erdoğan, 2013: 16.

⁴⁴ <http://be.gazi.edu.tr/posts/view/title/bilisim-sistemleri-98744> (erişim tarihi: 25.02.2019).

⁴⁵ Yargıtay CGK. 2007/6-136 E. 2007/150 K. 19.06.2007 T. (Eserdeki tüm yargı kararları Sinerji İçtihattan alınmış olup, bundan sonraki kararlar için ayrıca kaynak belirtilmeyecek, yalnızca istisna kaynaklar gösterilecektir.)

Sorun, ilk olarak, enerjiyi ve dolayısıyla bilgiyi taşıyan en küçük partiküllere ilişkin teorilerin sürekli olarak çürütülmesi⁴⁶ ve yeni bağlantıların açıklanmasından meydana gelmektedir. Diğer bir ifadeyle, fizik ve kimya bilimleri parçacıklarla ilgili henüz net sonuca ulaşabilmiş değildir. Dolayısı ile çok farklı materyallerden çok farklı bağlantılar aracılığı ile bugünkü anlayışımızı temelden değiştirecek bir sistemin kurulamayacağını kimse garanti edemeyecektir.

İkinci olarak ise gelişen üretim süreçleri bilişim alanında ve dolayısıyla tanımında değişemez bir durum olmayacağını ispatıdır. Daha önce bilgisayarlar röle ve vakum tüpleri ile hesaplama yaparken bugün onların yerini tamamıyla farklı çalışma prensibine sahip mikro işlemciler almıştır⁴⁷. İlk mikro işlemcide 2300 transistör bulunmasına karşın günümüzde bu sayının 5 milyarın üzerine çıkması da gelecekte çok farklı prensiplerin uygulanabileceği anlamına gelmektedir.

Özetle, teknik olarak bilişim alanını kapsayan bir tanım yapmak güçtür. Ancak teknik detayların gelişmesi hukukçuların kendi alanlarını kapsayıcı bir bilişim tanımı yapmasına engel olmamalıdır. Ayrıca eksik bir bilişim tanımının kanunilik ilkesini zedeleme ihtimali yanında, hiç tanımlanmayan bilişim kavramının da bu kez de suçun unsurlarından “tipikliğin” belirlenmesinde güçlükler yaşatacağı göz ardı edilmemelidir.

Bilişim hakkında yapılan tanımların uzadıkça daha az kapsayıcı hale geldiği de bir gerçektir. Veri üzerinde yapılan işlemlerin veya bilinen bilişim sistemlerinin sayılması yoluyla yapılacak tanımlar yukarıda ifade edildiği gibi yeni teknolojiler karşısında kanunilik ilkesi yönünden sıkıntı oluşturacaktır. Bu konuda inancımız, bilişimin var olmasında zorunlu ihtiyaç duyulan ortak yönlerini, tek tek sayma yöntemini tercih etmeden, en yalın haliyle ortaya koymak yönündedir.

Yapılan tüm tanımlar incelendiğinde “İnsanların teknik, ekonomik, toplumsal iletişiminde...özellikle bilgisayar gibi elektronik araçlarla... yüksek hızlı veri, ses ve görüntü taşıyan sistemler ile... verinin işlenmesi, depolanması, saklanması, iletilmesi... bilim dalı...” ifadelerine sıklıkla rastlandığı görülmektedir.

Bu ifadelerden bazıları tanımda tekrarlamalara neden olmaktadır. Örneğin “veri, ses, görüntü taşıyan” ifadesi bir tekrar içermektedir. Çünkü ses ve görüntü de aslında bir veridir ve diğer tüm bilgiler gibi kendilerine uygun bir formata çevrilmek suretiyle ve yine veri olarak taşınmaktadır. Benzer şekilde “verilerin kaydedilmesi ve saklanması”nın da teknik olarak birbirinden farkı bulunmamaktadır.

⁴⁶ Gelişimin kısa bir özeti için, Hawking, 2013: 87 – 91.

⁴⁷ http://www.chip.com.tr/haber/ilk-islemci-intel-4004-40-yasina-girdi_30334.html (erişim tarihi: 25.02.2019).

Bazı unsurlar da bilişim tanımında eksikliklere yol açmaktadır. Örneğin, elektronik ortamdan bahsedilmeden yalnızca bilginin iletilmesi ve depolanması yönünde bir tanım eksik kalacak, bu halde bilgiyi kitaplar aracılığı ile depolayan ve ziyaretçilerinin okumaları aracılığıyla bilgiyi ileten kütüphaneler de bilişim alanı içinde sayılacaktır.

Bununla birlikte bilişimin yalnızca elektronik ortamda hayat bulduğunu da söylemek gerekir. Manyetik ve optik alanlar da tıpkı elektronik alanlar gibi, ancak farklı çalışma prensipleri ile bilişime ev sahipliği yapabilmektedir ve gelecekte bu ortamlara yenilerinin de ekleneceği düşünülmelidir. Bazı tanımlarda yüksek hızlı olarak genellenen bu ortamlar bilişimin olmazsa olmaz unsuru olarak kendisini göstermektedir.

Aynı şekilde, bilişim ile bilgisayar kavramlarının farklı olduğu unutulmamalıdır. Bilişimin, bilgisayardan daha kapsamlı olduğu söylene de esasen bilgisayar bir bilişim sistemi örneğidir ve bilişim ile kıyaslanabilecek bir özellik taşımamaktadır.

Tüm bunlardan hareketle, en yalın genelleme açısından denilebilir ki, bilişim, beşerî yetiden üstün yöntemleri verinin her çeşit kontrolünde kullanan bir bilim dalıdır. Bu tanımda yer alan “beşerî yetiden üstün yöntemler” elektronik, manyetik veya optik gibi insanoğlunun bedensel ve ilkel araçların mekanik hızına göre belirgin bir üstünlük gösteren yöntemleri, “verinin her çeşit kontrolü” de verinin işlenmesi, boyut ve form değiştirmesi, depolanması, birleştirilmesi gibi işlemleri kapsamaktadır.

Bu tanımın temeline oturttuğumuz beşerî yetiden üstün yöntem kavramı, matematiksel ifadelerle de betimlenebilmektedir. Bilişim teknolojilerinde yaşanan ilerleme, matematiksel anlamda toplama değil, çarpma veya üstel biçimde ifade edilmektedir⁴⁸. Intel şirketinin eski başkanlarından Gordon Moore’un söylediği ve Moore yasası olarak bilinen tahmini bu üstel artışa örnektir: Moore’a göre entegre bir devrede inç başına düşen transistör sayısı her yıl ikiye katlanacaktır. İşte bilişim sistemlerinin ortak özelliklerinden bir tanesi çarpma veya üstel olarak ifade edilebilecek bir artışa elverişli olmasıdır. Bu sayede bilişim sistemleri başta normal sayılabilecek bir gelişme süreci gösterse de belli bir aşamadan sonra gücünü akıl almaz şekilde artırmaktadır.

1.1.3.2 Bilişim Alanı ve Bilişim Sistemi Yönünden

Öyle görülmektedir ki, bilişim alanı ve bilişim sistemi tanımları arasındaki ilişki mühendislik meselesinden çok hukuksal bir meseledir. Mühendislik alanında böyle bir ayrım ve açıklama yapılma ihtiyacı duyulmamıştır. Buna karşın ceza hukuku alanında kanunilik ilkesi

⁴⁸ Goodman: 2016: 58 – 59.

uyarınca gerek yasa koyucu ve gerek öğreti bilişim suçlarının konusu olan “bilişim sistemi”nin tanımının yapılması için haklı çabalar göstermektedir.

Yasa koyucunun “bilgileri otomatik işleme tabi tutan sistem” kavramından vazgeçerek bilişim alanı ve bilişim sistemine dayalı bir sistematik benimsemeye çalıştığı açıktır. Meclis komisyon ve genel kurulunda sürekli yapılan değişikliklerden sonra bölüm başlığı olarak “bilişim alanı” madde içeriği olarak da “bilişim sistemi” üzerinde karar kılınmıştır. Yine görüşmelerde her iki kavram hakkında da madde gerekçelerinde benzer tanımların yapıldığı görülmektedir. Bu nedenle nihai düzenlemede yasa koyucunun bilişim alanını daha geniş düşündüğü ve bu nedenle onu kısıtlayacak bir tanım yapmaktan kaçındığı düşünülebilir⁴⁹. O halde yasa koyucunun iradesine uygun olarak, bilişim alanını “bilişim sistemlerini içinde barındıran, en geniş anlamıyla bilişim olaylarının içerisinde gerçekleştiği alan” olarak tanımlamanın bir mahzuru yoktur.

Buna karşın yasa koyucu bilişim sistemini daha teknik bir kavram olarak değerlendirmiş ve suçun konusu haline getirerek madde gerekçesinde tanımlamada bulunmuştur. Bu tanım üzerinden öğretilde bilişim sisteminin unsurları üzerine birçok değerlendirme yapılmıştır. Bu değerlendirmelerin üçe ayrıldığını söyleyebiliriz. Bir grup yazarlar bilişim sistemini donanımsal, duyuya hitap eden yönleriyle tanımlamaya çalışırken, diğer grup yazılımsal, iç işleyişe özgü unsurlara yer vermiştir. Üçüncü grup yazarlar ise bu unsurların dengeli bir karışımına yer vermiştir.

Daha önceden, bilişim sistemlerinin bilgisayar ile neredeyse eş anlamlı olduğu, bilgisayarın bilişim sisteminin mutlak bir unsuru olduğu yönünde görüşler yaygınken, hızla gelişen teknoloji ile artık bilgisayarın bilişim sistemlerinin bir örneği olduğu ve bilişim sisteminin dar yorumlanmaması gerektiği⁵⁰, unsurları taşıyan her aygıtın bilişim sistemi olabileceği görüşü hâkim olmuştur. Otomatik işlem yapma özelliği de içeriğinin belirsiz olması nedeniyle geçen zaman içerisinde popülaritesini kaybetmiş görünmektedir.

Bugün geline nokta bilişim sisteminin unsurlarının belirlenmesi ve gelişecek teknoloji karşısında bu unsurların tazeliğinin korunması beklenmektedir. Biz de bu görüşe katılarak, unsurlarına göre yapılacak bir tanıma göre, bilişim sisteminin hem insanın herhangi bir duyusuyla hem de dışarıdan bir ağ vasıtası ile erişilebilen, içerisinde verinin her türlü işleme tabi tutulabildiği aygıt veya aygıtlar topluluğu olduğunu söyleyebiliriz.

⁴⁹ Yazıcıoğlu da bilgisayar alanında her 7 yılın bir asırlık gelişmeye eşit olduğunu vurgulamış, mukayeseli hukukta bir tanım yapılmaktan özellikle kaçınıldığını söylemiştir. Verdiği örnekler için, Yazıcıoğlu, 1999: 654. Benzer şekilde, Sarı, 2013: 77.

⁵⁰ “TCK m. 243 anlamında bilişim sistemi kavramı, dar anlamıyla ele alıp sadece bilgisayar ve internet gibi sistemlere indirgemen, bu sistemler de dahil olmak üzere bir bütün olarak ele alınmalıdır.” Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 920.

Bu tanımlar ışığında hangi aygıtların bilişim sistemi sayılıp sayılmadığına geçmeden önce, bilişim sistemi unsurlarını açıklamakta fayda olacaktır.

1.2 Bilişim Sisteminin Unsurları

Bilişim sisteminin tanımı kadar, genel geçer unsurların sistematik şekilde belirlenebilmesi de oldukça önemlidir. Öğretide bilişim sisteminin unsurları bakımından benzer açıklamalar görülse de tam bir görüş birliği bulunmamaktadır.

Kurt, bilişim sisteminin unsurlarını bilgisayar ve internet olarak ikiye ayırmıştır⁵¹. Donanım ve yazılımı bilgisayarın birer unsuru olarak görmüş, veri ve programı ile ilişkili olarak göstermiştir. Demircan ve Gürler de benzeri iki unsur olduğunu ifade etmekle birlikte veri kavramına unsurların içerisinde yer vermemişlerdir⁵².

Bize göre, her bilişim sistemi mutlaka insanın algılayabileceği bir aygıta sahip olmalı, kendi iç bağlantısında veri işlemlerini yapabilmeli ve çeşitli ağlar aracılığı ile dış bağlantı kurabilmelidir.

1.2.1 Duyuya Yönelen Aygıt

Aygıt, sözlük anlamıyla birçok parçadan yapılmış alet, birkaç aletin uygun şekilde birleştirilmesinden oluşan ve bazı deneylerin yapılmasına yarayan takım demektir⁵³. Gerçekten de bir bilişim sisteminde verinin saklanabilmesi, işlenebilmesi ve iletilebilmesi için birçok parçadan oluşan bir aygıtı ihtiyaç bulunmaktadır. Erem, şu sözlerle durumu özetlemektedir:

“ ‘Sibernetik’, ‘Enformatik’, ‘Bilgisayar’, ‘Kompüter’ hepsinin arkasında yer alan şudur: Makine.⁵⁴”

Bu aygıtın insan duyularından en az birine hitap etmesi gereklidir. Diğer bir ifadeyle, bilişim sisteminin insan tarafından algılanabilecek bir aygıtının bulunması gereklidir. Aygıtın tüm duyulara aynı anda hitap edebilmesi bir zorunluluk değildir. Bu anlamda hiçbir görselliğe ve ekrana sahip olmayan, yalnızca tuşlar vasıtasıyla kullanılan bir müzik çaların, aynı şekilde verileri saklayan ve herhangi bir ekrana sahip olmayan sunucuların (server) da diğer unsurları taşıdığı takdirde bilişim sistem aygıtı sayılmasına engel bulunmamaktadır.

Buna karşın, duyuya hitap etmeyen enerjilerden oluşan verilerin, ne kadar düzenli yapıya sahip olursa olsun bilişim sistemi olduğunu söylemek mümkün değildir. Örneğin, uzayda

⁵¹ Kurt, 2005: 27.

⁵² Demircan, 2016: 8; Gürler, 2015: 33.

⁵³ http://tdk.gov.tr/index.php?option=com_bts&view=bts (erişim tarihi: 25.02.2019).

⁵⁴ Erem, 1993: 179.

kaybolmadığı ve geri getirilebileceği iddia edilen ses dalgaları⁵⁵ yalnız başına bir anlam ifade etmemektedir.

Duyuya yönelen aygıtlar veri ile ilgili işlemleri yapabilmek için belli bir donanım ve yapacağı işe uygun olarak hazırlanmış yazılımlara sahip olmalıdır. Ancak, donanım ve yazılımın kalitesiz olması, işi beklenen şekilde gerçekleştiremiyor olması aygıtın bilişim sistemi sayılmadığı anlamına gelmeyecektir.

1.2.1.1 Donanım

Bilişim terimleri sözlüğüne göre donanım, bilgisayar izlenceleri, yordamlar, kurallar ve bunlara ilişkin belgelemeye karşıt anlamda, bilgi işlemede kullanılan fiziksel ögeler ya da fiziksel ögeler bütünüdür⁵⁶.

Öğretide, donanımın fiziksel (somut, maddi) ögelerden oluştuğuna dikkat çekilmektedir. Yenidünya/Değirmenci ve Kurt, bilgisayara ait maddi parça⁵⁷, Dülger ise somut unsur⁵⁸ ifadesini kullanmaktadır.

Fiziki öge kavramını daha ileri götüren Orta, donanımı, yazılımın zıt anlamı olarak kullanılan⁵⁹, somut olup elle tutulabilen⁶⁰ bir özellik vermektedir⁶¹. Kurt aynı şekilde “dokunulabilme” şartını ararken⁶², Demircan ise elle tutulabilme yerine gözle görülebilme kriterini esas alarak benzer bir tanım yapmaktadır⁶³.

Donanımı maddi özelliği dışında işlevi üzerinden de tanımlayan Kızıltan’a göre donanım unsurları, bilgisayara program ve verilerin girilmesini, işlem yapıldıktan sonra çeşitli bilgilerin alınmasını sağlayan fiziksel, elektriksel ve elektronik ekipman ve aygıtlardır⁶⁴. Gürler de benzeri işlevleri dile getirmiştir⁶⁵.

Donanımın sınırlı sayıda (numerus clausus) olmadığı öğretilde baskın görüş olarak ifade edilmekte ise de donanımı teknik açıdan bulunması gereken asgari unsurlar olarak gören ve kapsamını dar tutan bir görüş de mevcuttur⁶⁶.

Günümüzde donanımlar işlevine göre giriş (input) ve çıkış (output) donanımları, bulundukları yere göre ise iç (anakart, işlemci...) ve dış donanımlar (yazıcı, klavye...) olarak

⁵⁵ “Bilim insanları, Evren’in ortaya çıkmasını sağlayan Büyük Patlama’nın ‘ses kaydını’ elde etmeyi başardı.” <http://www.sabah.com.tr/dunya/2013/04/09/evrenin-760-bin-yasindaki-sesi> (erişim tarihi: 25.02.2019).

⁵⁶ http://tdk.gov.tr/index.php?option=com_bts&view=bts (erişim tarihi: 25.02.2019).

⁵⁷ Yenidünya/Değirmenci, 2003: 21; Kurt, 2005: 31.

⁵⁸ Dülger, 2015: 66.

⁵⁹ Yazar burada İngilizce donanım (hardware) ve yazılım (software) arasındaki zıtlıktan bahsetmiştir.

⁶⁰ Aynı yönde, Dijle, 2006: 8.

⁶¹ Orta, 2015: 32.

⁶² Kurt, 2005: 31.

⁶³ Demircan, 2016: 12. Aynı yönde, Alaca, 2008: 7.

⁶⁴ Kızıltan, 2007: 9.

⁶⁵ Gürler, 2015: 40.

⁶⁶ Gözüşirin, 2011: 12.

ayrılrsa da⁶⁷, bu ayrımlar konumuz bakımından özellik göstermediği için inceleme alanımız dışında kalmakta, yalnızca bilgi verilmekle yetinilmektedir.

Yapılan tanımlarda donanımın ortak özelliğinin fiziki ögeler olduğu görülmektedir. CPU, GPU, RAM, ROM, yan bellek gibi çeşitli bileşenler donanıma örnek olarak gösterilmektedir⁶⁸. Ancak bunlar esasen günümüz bilgisayar teknolojisinin bileşenleri olduğu için, ileride başka donanımların ortaya çıkabileceği veya mevcut olanlara ihtiyaç duyulmayabileceğini unutmamak gerekmektedir. Aksi halde bilişim sistemi anlamında donanımı günümüzdeki örnekleriyle kısıtlamış oluruz. Nitekim, mevzuatımızda donanım doğrudan tanımlanmamış, ancak telekomünikasyon gibi çeşitli elektronik altyapıları oluşturan unsurlar olarak geniş anlamıyla donanıma yer verilmiştir⁶⁹.

Genel olarak bilişim terimleri sözlüğünde yapılan tanıma ve fiziki öge kavramına katılmaktayız. Ancak, bunun öğretide “elle tutulabilme” “gözle görülebilme” şeklindeki bir duruma indirgenmesinin bilişim yaklaşımına uygun olmadığını da söyleyebiliriz. Bu konuda daha önce bahsettiğimiz gibi, “algılanabilen” “duyuların herhangi birine hitap eden” bir aygıtın parçası olması, donanımı açıklamak için daha uygun görünmektedir.

1.2.1.2 Yazılım (Program ve Arayüz)

Bilişim terimleri sözlüğüne göre yazılım, bir bilgi işlem dizisinin işleyişi ile ilgili bilgisayar izlencelerinin, yordamların, kuralların ve gerektiğinde belgelemenin tümüdür⁷⁰.

Mevzuatımızda donanımın aksine, yazılımın tanımına yer verildiği görülmektedir. 4691 sayılı Teknoloji Geliştirme Bölgeleri Kanunu’nun 3/1-l bendinde yazılım, bir bilgisayar, iletişim cihazı veya bilgi teknolojilerine dayalı bir diğer cihazın çalışmasını ve kendisine verilen verilerle ilgili gereken işlemleri yapmasını sağlayan komutlar dizisinin veya programların ve bunların kod listesini, işletim ve kullanım kılavuzlarını da içeren belgelerin, belli bir sistematik içinde, tasarlama ve geliştirme şeklinde ürün ve hizmetlerin tümü ile bu ürün ya da mal ve hizmetlerin lisanslama, kiralama ve tüm hakları ile devretme gibi teslim şekillerinin tümü anlamına gelmektedir.

Öğretide yazılımın tanımı ve niteliği konusunda önemli ayrımlar bulunmamaktadır. Orta, yazılımı, bir bilgisayarda donanıma hayat veren ve bilgi işlemede kullanılan programlar, yordamlar, programlama dilleri ve belgelerin tümü olarak tanımlamaktadır⁷¹.

⁶⁷ <https://www.youtube.com/watch?v=rME1yJ4xEeE> (erişim tarihi: 25.02.2019).

⁶⁸ Kızıltan, 2007: 9 – 10; Yayıcı, 2007: 6.

⁶⁹ Örneğin; 5809 sayılı Elektronik Haberleşme Kanunu’nda elektronik haberleşme alt yapısı, 6550 sayılı Araştırma Altyapılarının Desteklenmesine Dair Kanun’da araştırma altyapısı içinde yer verilmektedir.

⁷⁰ http://tdk.gov.tr/index.php?option=com_bts&view=bts (erişim tarihi: 25.02.2019).

⁷¹ Orta, 2015: 36.

Kurt, yazılımı bilgisayarın soyut bileşenini oluşturan, elektronik biçimde toplanabilen, kodlama olarak da adlandırılan, elektronik biçimde toplanabilen, depolanabilen, işlenebilen, bilgisayara işlerlik kazandıran komutlar bütünü olarak tanımlamaktadır⁷².

Gürler'e göre yazılım, bilişim sisteminin soyut bileşenlerini oluşturan, bilgisayarın ve tüm donanım unsurlarının çalışması ve temel işlevlerini yerine getirmesi için belirli bir mantık çerçevesinde yazılan, amaçlanan tüm fonksiyonların icra edilmesini sağlayan, dijital programlara (komutlara) verilen addır⁷³. Yayıncı da benzeri bir tanım yapmıştır⁷⁴.

Kanaatimizce, nasıl ki yabancı dil öğrenerek farklı milletten kişilerle iletişim kurabiliyorsak, programlama dilleri öğrenerek (C, C#, Java, Basic vb.) de makineler ile iletişim kurabilmekteyiz. Yazılım da işte bu aygıtlar ile yapılan başta talimat verme olmak üzere konuşma faaliyetleridir⁷⁵. Beşerî dillerden farkı ise makineler kendi dil kurallarını belirleyemediklerinden -en azından şimdilik- dil yapı ve kurallarını onlara bizim öğretmemiz gerekmektedir.

Yazılımlar, işlevine göre işletim (sistem) yazılımları ve uygulama yazılımları olarak ikiye ayrılmaktadır. İşletim yazılımları donanım parçalarının yönetilmesini sağlayıp, bilgisayar ve kullanıcı arasında köprü görevi görürken, uygulama yazılımları ise, belli bir işi görmek üzere, işletim sistemi üzerinde (içinde) ve ona uyumlu çalışan programlardır⁷⁶. Uygulamada, işletim sistemi tasarımcıları (windows, mac os...) uygulama yazılım araçlarını da ücretli veya ücretsiz olarak vermekte ve bağımsız programcıların kendi işletim sistemlerine uygun yazılımlar üretmesini teşvik etmektedir.

Yazılımlar, (bilgisayar) programlama ve programlar ile birlikte de ele alınmaktadır. Bazı yazarlar programa yazılım başlığı içinde yer verirken⁷⁷, bazıları ise ayrı başlık altında incelemeyi uygun görmüştür⁷⁸. Esasen, bilişim anlamında program, *her türlü yazılım ürünü* olarak tanımlanabilir. Nitekim, 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 1/B maddesinde bilgisayar programı, "bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir düzene konulmuş bilgisayar emir dizgesini ve bu dizgenin oluşum ve gelişimini sağlayacak hazırlık çalışmaları" olarak tanımlanmıştır. Bu yönüyle, bilgisayar programı, uygulama yazılımına benzer şekilde tanımlanmış ve bahsettiğimiz yazılım ürünü olma yaklaşımı

⁷² Kurt, 2005: 34. Aynı yönde, Kızıltan, 2007: 11; Demircan, 2016: 14.

⁷³ Gürler, 2015: 50.

⁷⁴ "Yazılım, bilgisayar donanımının iş yapabilmesi için belirli bir mantık çerçevesinde yazılmış komut topluluklarına, yani programlara denilmektedir." Yayıncı, 2007: 9.

⁷⁵ Dülger de yazılım dilini teknik alfabeye benzetmektedir. Dülger, 2015: 84.

⁷⁶ Kızıltan, 2007: 12; Yayıncı, 2007: 9; Gözüşirin, 2011: 14.

⁷⁷ Dülger, 2015: 66.

⁷⁸ Gözüşirin, 2011: 17.

da benimsenmiş görünmektedir. Bilgisayar programlarının FSEK kapsamında “dil ile ifade olunan eser” vasfında görüldüğünü de ifade etmek gerekmektedir⁷⁹.

Program tanımına katılmakla birlikte, yine FSEK’te yer alan arayüz tanımına katılmamaktayız. FSEK’e göre arayüz, bilgisayarın donanım ve yazılım unsurları arasında karşılıklı etkilenme ve bağlantıyı oluşturan program bölümleri anlamına gelmektedir. Halbuki donanım ve yazılım unsurları arasındaki etkileşim aşağıda inceleneceği gibi iç bağlantı yani veri yoluyla sağlanmaktadır. TDK, sözlüğünde daha isabetli olarak “bilgisayar yazılımlarının kullanıcı tarafından çalıştırılmasını sağlayan, çeşitli resimlerin, grafiklerin, yazıların yer aldığı ön sayfa” şeklinde bir tanım yapmaktadır. Bize göre de arayüz, (user interface – UI) elde edilen sonuçları kullanıcıya göstermek için oluşturulan programın görsel katmanı olarak tanımlanabilir. Örneğin bir yazı yazma uygulaması olan word programında paragraflar, yazı tipi ve puntosu gibi unsurlar komutlar aracılığıyla işlenirken, programın sanki sanal bir A4 kâğıdı üzerinde yazıyormuş izlenimi veren ve kullanıcı olarak bizlere ulaşan görseli ise arayüzü oluşturmaktadır.

1.2.2 İç Bağlantı – Veri

Bilişim sisteminin unsurlarından olan duyuya yönelen aygıt yukarıda bahsedilmişti. Ancak yalnız başına fiziki aygıtın varlığı bir sistemin bilişim sistemi olup olmadığı hakkında kesin bir bilgi vermemektedir. Bu aygıt aynı zamanda kendi iç bağlantısında veriler üzerinde işlem yapabilmelidir. Denilebilir ki, bilişim sistemlerini diğerlerinden ayıran en belirgin özellik veriler üzerinde işlem yapabilmesidir⁸⁰.

Bu noktada, veri kavramının bilişim sistemlerindeki yeri ve aynı zamanda TCK’de suçun konusu içinde sayılmasıyla daha da önem kazandığı⁸¹ görülmektedir.

Bu öneme karşın, yasal düzenlemelerde veriye yüklenen anlam konusunda tutarlılık bulunmamaktadır. Verinin tutarlı bir anlama sahip olması için de iki soruya yanıt bulunması gerekmektedir: Veri ile bilgi arasındaki fark nedir? Veri kavramı sadece bilişim alanında mı kullanılmaktadır? Elde edilecek yanıtlar, öncelikle verinin bilgiden ayrışmasını, ardından da verinin diğer anlamlarından arınmasını sağlayacaktır. Bu da verinin bilişim sistemi içerisindeki yerinin saptanması ve dolayısıyla suçun unsurlarının anlaşılabilmesi bakımından büyük katkı sağlayacağından bu konular sırasıyla incelenecektir.

⁷⁹ Öztan, 2008: 118.

⁸⁰ “Bilişim sistemlerinin temel özelliği, üzerinde yükseldiği yapıtaş veridir.” Yenidünya/Değirmenci, 2003: 47.

⁸¹ Erdoğan, 2013: 39.

1.2.2.1 Veri ve Bilgi Arasındaki İlişki

Veri ve bilgi arasındaki ilişkinin yoğunluğu, tanımları yapılırken birbirlerine yapılan atıflarla en baştan dikkat çekmektedir. Bilişim terimleri sözlüğüne göre veri, olgu, kavram veya komutların, iletişim yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi, bilgi ise bilgi işlemde kullanılan uzlaşımsal kurallardan yararlanarak kişinin veriye yönelttiği anlamdır⁸².

Öğretide de en sade tanımıyla, verinin, bilgilerin belirli bir formata dönüştürülmüş hali⁸³, işlenmemiş ham bilgi⁸⁴ olduğu söylenmektedir. Erdoğan da durumu ters haliyle ifade ederek bilgilerin elektronik ortamda görünebilmesi için veriye dönüştürülmesi gerektiğini söylemektedir⁸⁵.

Yasal düzenlemelerde veri kavramına sıkça yer verildiği görülmektedir. İÖYYDHK'ye göre veri, bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ifade etmektedir. Sanal Ortamda İşlenen Suçlar Sözleşmesinde ise “Bilgisayar verisi, bilgisayar sisteminin bir işlevini yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsili ifade eder.” denilmektedir. Bilgi kavramına aynı sıklıkta yer verilmemiş olsa da İÖYYDHK'nin 2. maddesinde tanımına yer verildiği, verilerin anlam kazanmış biçimi olarak ifade edildiği görülmektedir.

Görüüleceği üzere, veri ile bilgi arasında belirgin bir fark bulunmaktadır. Bu farkı Kurt, bilgi ve veri arasındaki durumu suyun katı, sıvı ve gaz hallerine benzetip özünde aynı ancak şekilde farklı kavramlar olduğunu söyleyerek açıklamaktadır⁸⁶. Dülger ise veri ve bilgi deyimlerinin birbirine benzetilme nedeninin İngilizce “data” ve “information” kelimelerinin eş anlamlı olarak “bilgi” şeklinde çevrilmesi olduğunu, bu nedenle “data-processing” kavramının karşılığının “bilgi-işlem” değil “veri-işlem” olması gerektiğini söylemektedir⁸⁷.

Buna karşın yasa koyucunun, hukuk öğretisi ve dilbilimciler tarafından tespit edilen bu ayrıma çok da özenle yaklaşmadığı ve bu nedenle bir karmaşanın meydana gelmiş olduğu söylenebilir. eTCK'de yer alan “bilgileri otomatik işleme tabi tutan sistem” deyimini işleme tabi tutulacak şeyin “bilgi” değil “veri” olması gerektiği, dolayısıyla bilginin yanlış anlamda kullanılması nedeni ile haklı olarak eleştirilmiştir⁸⁸.

⁸² http://www.tdk.gov.tr/index.php?option=com_bts (erişim tarihi: 25.02.2019).

⁸³ Yenidünya/Değirmenci, 2003: 48; Kurt, 2005: 37; Değirmenci, 2005: 200; Gürler, 2015: 32.

⁸⁴ Demircan, 2016: 20.

⁸⁵ Erdoğan, 2013: 39; Dülger, 2015: 85.

⁸⁶ Kurt, 2005: 38.

⁸⁷ Dülger, 2015: 84, dn. 104.

⁸⁸ Kurt, 2005: 38.

Özetle, bilgiyi insanın, veriyi ise makinenin anlamlandırabildiği söylenmelidir⁸⁹. Veri, makinelerin elektronik kütüphaneleridir ve yazılımlar ile makine dilinin doğal bir sonucudur.

1.2.2.2 Bilişimsel Anlamda Veri

Verinin, bilişim anlamı dışında kullanılan başkaca anlamları da mevcuttur. Bu farkların ortaya konulması esasen zorluk göstermese de bilgi ve veri arasındaki karmaşanın çözülmesine yardımcı olabileceği için incelenmesinde fayda vardır. Gerçekten de veri, diğer anlamlarıyla bilişim anlamında bir veriden çok bilgiye benzerlik göstermektedir.

TDK'nin güncel sözlüğünde verinin diğer anlamları hakkında bilgi verilmektedir. Buna göre veri, bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done demektir. Aynı zamanda elde edilen gözlem ve deneyin sonuçları da istatistiki veriyi göstermektedir⁹⁰.

Mevzuatımızda da verinin bu anlamıyla tanımlandığı yerler görülmektedir. Örneğin, 5429 sayılı Türkiye İstatistik Kanunu'nun 2. maddesinde veri, anket veya idari kayıtlar yoluyla elde edilen nicel ve/veya nitel istatistiksel bilgileri ifade edecek şekilde tanımlanmaktadır. 5070 sayılı Elektronik İmza Kanunu'nda elektronik veri, elektronik, optik veya benzeri yollarla üretilen, taşınan ve saklanan kayıtları, 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'da ise kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade etmektedir.

Bilişim sisteminin iç bağlantısını oluşturan veri ise bunlardan biraz farklıdır. Veri, genellikle 1 ve 0'lardan oluşan bir bit dizisidir⁹¹. Verinin bilgiye dönüşmesi için saklanma şekli ve veri yapısının da bilinmesi gerekmektedir. Örneğin, 0100 0010 0100 0001 0100 0010 0100 0001 şeklinde bir bit dizisi, ASCII veri yapısında "BABA" BDC veri yapısında "42414241" 32 bitlik tamsayı yapısında ise "1111573057" rakamı şeklinde anlaşılır⁹².

Bu bağlamda, bilişim anlamında verinin, istatistiksel veya "done" anlamındaki veriden farklı olduğu görülmektedir. Buna karşın verinin, diğer anlamlarından ayrılması için kullanılan "bilgisayar verisi" kavramı ise verinin içeriğini daralttığı için öğreti tarafından eleştirilmiş, yalnızca bilgisayarda bulunan soyut unsurların veri kabul edilmesinin başka makineler üzerinde suç sayılmaması sonucunu doğuracağı ifade edilmiştir. Nitekim TCK'nin 243. maddesinin gerekçesinde "Sistem içerisindeki bütün soyut unsurlar fıkra da geçen veri teriminin kapsamındadır." denilerek veri terimi oldukça geniş tutulmuştur.

⁸⁹ Kurt, 2005: 38.

⁹⁰ http://www.tdk.gov.tr/index.php?option=com_bts (erişim tarihi: 25.02.2019).

⁹¹ 1 ve 0 rakamları aslında devrede elektrik var veya yok durumunu göstermek için kullanılmaktadır. Nakov/Kolev, 2013: 145.

⁹² Çölkesen, 2006: 892.

Sonuç olarak öğretilerde bilgi ve veri arasında açıklanan bağlantıya uygun olarak, verinin, bilişim aygıtının iç işleyişini sağlayan, iletilebilen, kendi yapısı ve modeline sahip, anlamlandırılabilir değerler kümesi olduğu söylenebilecektir. İç işleyişin sağlanması verinin donanım ve yazılım ile uyumunu, anlamlandırılabilmesi de kendi yapısı sayesinde bilgiye dönüştürülebilmesi olarak ifade edilmelidir. Yine bulunduğu aygıtta elektronik, manyetik veya gelecekte çok daha farklı bir halde bulunabilecek olan verinin anlamını daraltmamak için yapısının bulunduğu yere göre değişkenlik gösterdiği bir değer kümesi olarak bahsedilmesinde fayda olacağı düşüncesindeyiz.

1.2.3 Dış Bağlantı – Ağ

Bir aygıtın bilişim sistemi sayılabilmesi için iç bağlantısında veri işleminin yanı sıra bir dış bağlantıya (aktarıma) da sahip olması gerekir. Öğretilerde bilişim sistemleri tanımında yapılan veri-iletişim özelliği işte bu dış bağlantı sayesinde sağlanabilmektedir.

Dış bağlantının varlığının tespitinde bilişim sisteminin edilgen bir rol üstlendiği düşünülmelidir. Yani, dış bağlantı unsuru “bir ağa erişebilen” değil, “bir ağ tarafından erişilebilen” şeklinde anlaşılmalıdır. Örneğin, modemi olmadığı için internet bağlantısı kuramayan bir bilgisayarın bilişim sistemi sayılmaması elbette mümkün değildir. Sonuçta bilgisayar aygıtı bir ağ tarafından erişilmeye uygun ve elverişli bir yapılanmaya sahiptir.

Bilişimle ilgili diğer kavramlarda olduğu gibi, ağ kavramı da yalnızca bilgisayar ağları olarak düşünülmemelidir. Bu doğrultuda öğretilerde “bilişim sistem ağları⁹³” gibi terimler de kullanıldığı görülmekte, biz ise yalın olarak ağ kavramını tercih etmekteyiz.

Bilişim sistemleri çeşitli şekiller altında sürekli olarak yenilik gösterdiği için, ağlar üzerinde de tüm bu farklılıkları standartlaştıracak ve optimize edecek çalışmalar yapılmaktadır. ISO, ITU, IEEE, ETSI, EIA, TIA, ANSI ve TSE gibi kurum ve kuruluşlar ağ standartları konusunda yaygın olarak faaliyet göstermektedir⁹⁴. Bu da ağ teknolojilerinin tıpkı gelişen bilişim aygıtları gibi gelecekte farklı şekillerde karşımıza çıkabileceğini göstermektedir.

1.2.3.1 Ağ Kavramı

Terim olarak ağ (network), bilişim terimleri sözlüğünde birçok nokta ile bunlar arasındaki bağlantılarla gösterilebilen bir dizgeye ilişkin yapı olarak tanımlanmıştır⁹⁵.

⁹³ Yenidünya/Değirmenci, 2003: 34; Erdoğan, 2013: 25.

⁹⁴ İnan, 2006: 61.

⁹⁵ http://www.tdk.gov.tr/index.php?option=com_bts&view=bts (erişim tarihi: 25.02.2019).

Öğretide Yenidünya/Değirmenci, birbirlerine kablolu veya kablosuz bağlanarak veri alışverişinde bulunabilen bilişim araçları ile bu imkânı sağlayan altyapının bilişim sistem ağını oluşturduğunu söylemektedir⁹⁶.

Gürler, bilgisayar ağlarını, en az iki veya ikiden fazla bilgisayarın sahip olduğu bilgileri paylaşmak veya kaynaklarını ortak kullanmak amacıyla bir iletim hattı üzerinden aralarında kurmuş olduğu bağlantı ile oluşan sistem olarak tanımlamaktadır⁹⁷.

1.2.3.2 Ağ Çeşitleri

Ağlar farklı açılardan sınıflandırılmaktadır. Kullandıkları iletim ortamına göre kablolu (telli), optik⁹⁸ ve kablosuz (telsiz); topolojik yapılarına göre halka, örgü ve yıldız olarak ayrılmaktadır⁹⁹. Konumuzla ilgili olan ve mesafe (LAN, MAN, WAN) ile kullanıcılara (İnternet, İntranet, Ekstranet) göre yapılan ağ ayrımları ise daha detaylı incelenecektir.

Ağ çeşitlerine geçmeden önce, ethernet, gigabit ethernet, x.25, frame relay, ATM gibi terimlerin bir ağ çeşidi değil, aktarım ile ilgili servisler olduğunu hatırlatmak gerekmektedir¹⁰⁰.

1.2.3.2.1 Yerel Alan Ağları (LAN)

Sınırlı bir alanda etkili olan ve her türlü donanım mülkiyetinin ağına sahip olan kişiye ait olduğu ağlar yerel alan ağları (LAN – Local Area Network) olarak nitelendirilmektedir¹⁰¹. Yerel ağların coğrafi kapsamı konusunda net bir kıstas bulunmamakta, 500 metrelik¹⁰² veya 3 kilometrelik¹⁰³ bir mesafeyi kapsayabileceği kabul edilmektedir.

1.2.3.2.2 Kentsel Alan Ağları (MAN)

Bir şehre veya geniş bir yerleşkeye¹⁰⁴ yayılmış ağ olan kentsel alan ağları (MAN – Metropolitan Area Network), yerel ağlar arasında bağlantı kurarak geniş ağlar ve internet için bağlantı hizmetleri sağlamaktadır. Kablolu televizyon ağları ve birden fazla yerel ağdan oluşan ağlar, kentsel alan ağlarına örnek gösterilmektedir¹⁰⁵.

⁹⁶ Yenidünya/Değirmenci, 2003: 34.

⁹⁷ Gürler, 2015: 53.

⁹⁸ Optik ağlar hakkında ayrıntılı bilgi için, Polat, 2006: 620.

⁹⁹ Harmancı, 2006: 51.

¹⁰⁰ Bu servisler hakkında detaylı bilgi için, Tutkun, 2013: 82, 96, 114; İnan, 2006: 66.

¹⁰¹ İnan, 2006: 62.

¹⁰² Laudon/Laudon, 2014: 286.

¹⁰³ Manas, 2006: 192, şekil-2.

¹⁰⁴ Bazı yazarlar, yerleşke ağlarını yerel ağ ve kentsel ağ arasında değerlendirmektedir. Bu alana CAN (Campus Area Network) de denilmektedir. Laudon/Laudon, 2014: 286.

¹⁰⁵ İnan, 2006: 65.

1.2.3.2.3 Geniş Alan Ağları (WAN)

Geniş coğrafik bölgelere yayılmış olan geniş alan ağları (WAN – Wide Area Network) bir ülke için şehirler, kıtalar için ülkeler arası, gerekirse tüm Dünyada bağlantı yapılmasını gerektirmektedir¹⁰⁶. En yayılmış ve gelişmiş geniş alan ağlarından birisi de internettir¹⁰⁷.

1.2.3.2.4 İntranet

İntranet, aslında internet ağının protokol ve teknolojilerini kullanan, ancak bir kuruluşa özgü güvenlik duvarının ardında yer alan ve sadece yetkili kişilerin erişebildiği bir ağıdır. Genel olarak şirket içi veri aktarımlarında dışa kapalı olarak güvenli bir bağlantı amacıyla kurulur¹⁰⁸. İntranetin esas olarak kullanılma sebebi düşük maliyetle oluşturulan sistemle yüksek verimlilik sağlanabilmesidir¹⁰⁹.

İntranetler internete bağlı olmak zorunda değildir, bu da ağın internetle olan temel farkını oluşturmaktadır. İnternet üzerindeki bilgilere herkes ulaşabilirken intranet üzerinde kuruluşun çalışanları ve üyeleri üzerinde bir paylaşım yapılır. İnternet üzerinden intranete erişimin mümkün olmadığı söylenirse de¹¹⁰ bu durum, intranetin güvenlik duvarı (firewall) sayesinde kendisini yetkisiz kullanıcılardan koruduğu, internet üzerinden intranete kolaylıkla erişim sağlanabildiği şeklinde anlaşılmalıdır¹¹¹.

İntranet ile yerel ağ (LAN) da birbirinden ayrı kavramlardır. İntranet kullanıcılarının mutlaka aynı fiziki ortamdan ağa bağlanması şart değildir. Geniş alan ağları kullanılmak suretiyle kuruluşun başka bir şehirdeki bilgisayarından da intranet ağına erişim sağlanabilir. Diğer anlatımla, her yerel ağ aynı zamanda bir intranettir, ancak her intranet yerel ağ olmak zorunda değildir.

Günümüzde intranetin kapsamının genişlediği, kurumların kendi içlerinde oluşturduğu web sitesi ile portal olarak da bildiğimiz yapılarla eş anlamlı olarak kullanılmaya başlandığı görülmektedir¹¹². Yine, Microsoft'un SharePoint uygulamasının bir intranet örneği olduğu söylenebilir.

¹⁰⁶ İnan, 2006: 65.

¹⁰⁷ Laudon/Laudon, 2014: 287.

¹⁰⁸ Erdoğan, 2013: 27.

¹⁰⁹ İntranetin diğer avantajları için, Kartan, 2007: 37.

¹¹⁰ Kartan, 2007: 31.

¹¹¹ [\(http://bidb.itu.edu.tr/sevirdefteri/blog/2013/09/07/intranet-\(i%C3%A7-a%C4%9F\)-ve-extranet-\(d%C4%B1-C5%9F-a%C4%9F\)\)](http://bidb.itu.edu.tr/sevirdefteri/blog/2013/09/07/intranet-(i%C3%A7-a%C4%9F)-ve-extranet-(d%C4%B1-C5%9F-a%C4%9F)) (erişim tarihi: 25.02.2019).

¹¹² <https://www.umitegrioglu.com/intranet-portal-nedir-olmasi-gerekenler/> (erişim tarihi: 25.02.2019).

1.2.3.2.5 Ekstranet

Ekstranet de intranet gibi internet altyapısının kullanıldığı, buna karşın intranetten farklı olarak sadece kuruluş içinden değil, müşterilerin, bayilerin, alıcı ve satıcıların aynı ortamda olduğu bir ağı ifade etmektedir¹¹³. Ekstranetler özellikle e-ticaret ve e-devlet uygulamaları için kullanılmaktadır. Aynı kurumun farklı paydaşlara açık farklı ekstranetlerinin bulunması mümkündür¹¹⁴.

Aynı altyapıya sahip olması nedeniyle internet üzerinde işlenen suçların intranet ve ekstranet üzerinde de işlenmesi mümkündür.

1.2.3.2.6 Sanal Ağlar (VPN)

Günümüzde gittikçe bilinir hale gelen sanal özel ağlar (VPN – Virtual Private Network), başta internet olmak üzere bir geniş alan ağının içerisinde yapılandırılmış ağıdır. Bu ağlar daha düşük maliyetlerle aynı güvenlik, şifreleme ve ağ yönetimini sağladığı için klasik anlamda bir sunucuya göre gün geçtikte daha fazla tercih edilmektedir¹¹⁵.

1.2.3.2.7 İnternet (Bilgisunar)

İnternet, günümüzde en yaygın kullanılan geniş alan ağıdır. İnsanoğlunun gelişen ihtiyaçları sonucunda standartları oluşturulan bir teknik altyapı üzerinde gelişimini halen sürdürmektedir.

İnternetin yaygınlaşarak tüm insanlığa hitap etmesi, bilişim sistemleri üzerindeki aygıt bazlı ve yerel algının da değişmesine yol açmıştır. Bilişim sistemleri üzerindeki bu değişim de bilişim suçlarının evrilmesi ve çeşitlenmesinde önemli rol oynamıştır. Bu nedenle suçun unsurlarının anlaşılabilmesi için internetin gelişimi ve teknik özellikleri konusunda yüzeysel de olsa bilgi sahibi olmakta fayda vardır.

1.2.3.2.7.1 Tarihçe

Bilgisayarlar arasında uzaktan veri aktarımı için yapılan ilk denemeler 1968 yılında Kuzey Karolina Devlet Üniversitesi, Duke Üniversitesi ve Kuzey Karolina Araştırma Enstitüsü'nün bir araya gelmesi ile başlamıştır. Bu kurumlar, ilk uzak erişimli bilgisayar ağını kurmayı başarmışlar, bu ağa “Tringle Network” ismi vermişlerdir¹¹⁶.

Akademik çalışmalara karşın, internetin gelişmesindeki esas olayların askeri ve güvenlik amaçlı olduğu söylenebilir. Nitekim, Sovyetler Birliği'nin 1957 yılında Sputnik uzay ara-

¹¹³ Erdoğan, 2013: 27.

¹¹⁴ <https://www.turkcebilgi.com/ekstranet> (erişim tarihi: 25.02.2019).

¹¹⁵ Laudon/Laudon, 2014: 298.

¹¹⁶ Manas, 2006: 190.

cını göndermesi ile birlikte süregelen¹¹⁷ süper güç olma mücadelesi Amerikan DARPA¹¹⁸ kuruluşunun ARPAnet adıyla bugünkü internetin öncülü sayılan projeyi hayata geçirmesini sağlamıştır. Bu projenin temel amacı, olası bir nükleer saldırıda bilgi akışını devam ettirebilmek ve bunu tek bir merkez bilgisayara bağlı kalmadan gerçekleştirebilmektir¹¹⁹.

O güne kadar bilinen iki yöntemle iletişim organizasyonu sağlanıyordu. Merkezileştirilmiş (centralized) yöntemde bütün birimler tek bir merkezden yönetilirken, merkezi olmayan (decentralized) yöntemde, birden fazla merkez ve onlara bağlı birimler bulunuyordu. Ancak tüm bu sistemler dayanıksızdı, çünkü merkezin yok edilmesi durumunda diğer birimler de işlevsiz kalmaktaydı.

Bu soruna ilişkin internetin mantıksal çerçevesinin kurucusu olarak bilinen¹²⁰ Paul Baran 1964 yılında yayımlanan “On Distributed Communication” eserinde o dönem için devrim niteliğinde olan üçüncü bir yol ileri sürmüştür. Dağıtılmış (distributed) yöntemde, bilinen anlamda bir merkez olmaksızın, her birim birden fazla birime eşit seviyede bağlı bulunmaktadır. Dolayısı ile bir birim yok edildiği takdirde, iletişim yolu anında değiştirilerek veri akışı diğer birimler üzerinden devam ettirilebilmektedir. Baran, ayrıca “packet switching” gibi iletinin bütün olarak değil, bloklar halinde gönderileceği daha verimli bir sistemin de açıklamasını yapmıştır¹²¹. Bu da bilgisayarların sayıca az ve erişilemez olması, taşınabilir olmaması, veri tiplerinin farklı olması sonucunda oluşan birçok zorluk¹²² için önemli geliştirmeler sağlamıştır.

Meslektaşları tarafından başlangıçta uygulanma kabiliyetinin olmamasıyla eleştirilen¹²³ Baran’ın bu görüşleri ARPAnet yöneticilerinin dikkatini çekmiş ve uygulamasına geçilmiştir¹²⁴. 1969 yılında California’da bulunan 3 ve Utah’ta bulunan 1 merkez arasında yapılan iletişim başarıya ulaşmıştır¹²⁵. Kısa süre içerisinde oldukça büyüyen ağın yükü taşıyamayacağı anlaşıldığında ARPAnet ikiye bölünmüş, askeri amaçlar için yeni oluşturulan MİLNET ağı kullanılmaya başlanmıştır. Sonraki süreçte Amerikan NSF kuruluşu 13 üniversiteyi içine alacak bir ağ kurarak buna NSFnet adını vermiştir. Ticari kullanımların da yoğunlaşması

¹¹⁷ Kuruluş, misyon bölümünde durumu detaylı açıklamaktadır. <http://www.darpa.mil/about-us/about-darpa> (erişim tarihi: 25.02.2019).

¹¹⁸ Defense Advanced Research Projects Agency. Halen faaliyetlerini sürdürmekte olan kurum, yıllık 3 milyar dolara yakın bir bütçeyi yönetmektedir.

¹¹⁹ Dülger, 2015: 109.

¹²⁰ Manas, 2006: 190.

¹²¹ Detaylı bilgi için, Baran, 1964: 3.

¹²² <http://www.packet.cc/files/arpnet-computernet.html>

¹²³ <http://www.rand.org/about/history/baran.html> (erişim tarihi: 25.02.2019).

¹²⁴ <https://www.ibiblio.org/pioneers/baran.html> (erişim tarihi: 25.02.2019).

¹²⁵ Dülger, 2015: 110.

ile birlikte 1990'da ARPAnet, 1993'te NSF omurgası da kaldırılmış ve internet bugünlere kadar ulaşmıştır¹²⁶.

1.2.3.2.7.2 Teknik Altyapı

İnterneti bu denli popüler kılan özellik, herhangi bir kişi veya kurumun bütünüyle kontrolünde olmaması, özgür ve serbest dolaşım sağlanan bir alan oluşturularak, Dünya'nın her yerinde farklı türden aygıtlarla iletişim kurulabilmesidir. İnternetin teknik altyapısı başlı başına bir inceleme konusu olmakla birlikte, bilişim suçlarının analizi bakımından ihtiyaç duyulabilecek bazı temel bilgilerden bahsetmekte fayda vardır.

Farklı türden aygıtlar arasındaki iletişim için OSI referans modeli benimsenmektedir¹²⁷. Bu modelin en yaygın uygulamasını ARPAnet'in ilk protokolü olan NCP'nin (Network Control Program) yerine geçmek üzere Vinton G. Cerf ve Robert E. Kahn tarafından 1973 yılında hazırlanan¹²⁸ TCP/IP mimarisi oluşturmakta, bugün de geliştirilerek halen uygulanmaya devam etmektedir¹²⁹.

Benzerlerinde olduğu gibi TCP/IP mimarisinde de katmanlar kullanılmaktadır. OSI modelinde 7 katman olarak öngörülen yapı bu mimaride fiziksel, yönlendirme, ulaşım ve uygulama olarak toplam 4 katmana indirgenmiştir. Fiziksel katmanda verinin nasıl elektrik, ışık, radyo sinyali, vb. çevrileceği tanımlanır¹³⁰. Yönlendirme katmanında gelen veriye IP protokolü ile başlık bilgisi ek olarak eklenir, ulaşım katmanında TCP protokolü ile veriler uygun parçalara bölünür, bu parçalara sıra numarası verilir ve kaybolan parçalar tekrarlanır. Uygulama katmanındaki protokoller ise doğrudan uygulamalara hizmet verir¹³¹. (Örneğin, FTP – File Transfer Protocol ile dosya aktarımı, SMTP – Simple Mail Transfer Protocol ile posta gönderimi, HTTP – Hyper Text Transfer Protocol ile metin aktarımı.)

Son olarak internetin kullanıcılar arasında yaygınlaşmasının en önemli nedenlerinden birisi olan web (www – w3) üzerinde durmakta fayda vardır. İnternet üzerinde çalışan bir servis olan web 1989'da Tim Berners-Lee tarafından önerilmiştir¹³². Tarayıcılar (Explorer (edge) – firefox – chrome vb.) aracılığıyla erişilebilen web siteleri, metin, fotoğraf, video ve çeşitli multimedya öğeleri barındırabilmektedir. Web sitelerinde, bir hisse senedi fiyatının bildirilmesi gibi basit veya uçak bileti satın almak (ödeme – yer ayırma) gibi karmaşık hizmetler

¹²⁶ Manas, 2006: 191; Dülger, 2015: 111.

¹²⁷ “OSI referans modeli farklı mimarilerdeki iki sistemin iletişimini sağlamak üzere tasarlanmış 7 katmanlı bir yapıyı ve katmanların görevleri ile birbirleri arasındaki ilişkiyi ifade eder.” İnan, 2006: 61.

¹²⁸ Protokolün İngilizce metni için, “A Protocol for Packet Network Communication” <http://www-net.cs.umass.edu/653-04/documents/cerfkahn.pdf> (erişim tarihi: 25.02.2019).

¹²⁹ https://en.wikipedia.org/wiki/Internet_protocol_suite (erişim tarihi: 01.03.2016).

¹³⁰ https://tr.wikipedia.org/wiki/Fiziksel_katman (erişim tarihi: 01.03.2016).

¹³¹ Efe/Çölkesen, 2006: 56.

¹³² https://tr.wikipedia.org/wiki/World_Wide_Web (erişim tarihi: 01.03.2016).

verilebilir. Web üzerinde belgeler HTML (Hypertext Markup Language) denilen bir biçimlendirme dilinde yazılır, TCP ve IP protokolleri kullanılarak bu formatın web sunucusu ve istemci arasındaki aktarımı sağlanır¹³³. Web sitelerinin yoğun olarak kullanılmasına karşın internetin yalnızca web hizmetlerinden ibaret olmadığı da unutulmamalıdır.

1.3 Bilişim Sistemi Sayılan ve Sayılmayan Sistemler

Bilişim sisteminin sahip olması gereken 3 unsurdan (aygıt – iç bağlantı – dış bağlantı) ve bunların niteliğine ilişkin modelimizden yukarıda bahsedilmiştir. Ancak öğretide unsurların sayısı ve içeriği konusunda bir uzlaşma bulunmamaktadır. Dolayısıyla hangi sistemlerin bilişim sistemi sayılıp sayılmayacağı, hangi kriterlere göre değerlendirme yapılması gerektiği hususu günümüzde de tartışılmaya devam edilmektedir.

Buna ilişkin bir görüş, bilişim sisteminin temel öğelerinden birinin genel kullanım olduğunu ileri sürmektedir. Buna göre, elektronik veya manyetik sistemlerin aynı zamanda genel kullanıma hitap etmesi gerekmektedir¹³⁴. Bu görüşü savunanlar, genel kullanım dışında kısmen işlevi bulunan kumandalı TV, programlanabilir buzdolabı, şifreli yayın dekoderi gibi aygıtları bilişim sistemi içinde saymamaktadır¹³⁵. Belirsizliğin çözülebilmesi için yeni terimler ve ayırt edici özellikler belirlenmesi gerektiği de söylenmektedir¹³⁶.

Özellikle son yıllarda öne çıkan diğer görüş ise genel amaçlı kullanıma kriterine değinmeden veya açıkça eleştirerek, bilişim sisteminin bilgisayardan daha fazla bir anlam ifade ettiğini, bilişim sistemi için genişletici yorum metodunun kullanılması gerektiğini söylemektedir. Bu görüşe göre genel amaçlı kullanım kriteri belirsizdir ve suçun konusuz kalmasına neden olabilmektedir¹³⁷.

Yargıtay'ın da genel amaçlı kullanım kriterini benimsediği görülmektedir. CGK'nin bir kararında kısmi işlev gören aygıtların bilişim sistemi sayılmayacağı söylenmiştir:

“İster ‘bilişim sistemi’ isterse ‘bilgileri otomatik işleme tabi tutmuş’ sistem kavramı kullanılsın bununla ifade edilmek istenen genel amaçlı kullanıma müsait bilgisayarlardır.

Yoksa tek amaçlı çalışan bilgisayar destekli veya bilgisayar özelliklerinin bir kısmına haiz aletler ile atanmış bilgisayarlar bu yasanın kastettiği bilişim sistemi tabiri içinde değerlendirilemezler¹³⁸.”

¹³³ Dayar, 2006: 914.

¹³⁴ Taşkın, 2008: 10.

¹³⁵ Yazıcıoğlu, 1999: 657; Kurt, 2005: 141; Pallı, 2008: 36; Karakehya, 2009: 9. Taşkın, genel amaçlı kullanım kriterini kabul ederek, bilgisayar ve ATM'nin bilişim sistemi sayıldığını, cep telefonları, takograf cihazları ve dekoderlerin bilişim sistemi sayılmadığını söylemektedir. Taşkın, 2009: 334.

¹³⁶ Gürler, 2015: 39.

¹³⁷ Yenedünya/Değirmenci, 2003: 45; Erdağ, 2010: 279; Yılmaz, 2011: 63; Erdoğan, 2013: 13; Dülger, 2015: 76.

¹³⁸ Yargıtay, CGK, 2007/6-136 E. 2007/150 K. 19.06.2007 T.

Benzer şekilde, Yargıtay'ın başka bir kararında telsiz telefon ile başkasının kullandığı frekansa girerek konuşma yapılması eyleminin 765 sayılı TCK'nin 525. maddesindeki bilişim suçunu değil, 491. maddesindeki hırsızlık suçunu oluşturduğu söylenmiştir¹³⁹. Bu kararın gerekçesini ise 06.04.1990 tarih ve 2/3 sayılı İBK'ye dayandırılmıştır. Söz konusu İBK incelenildiğinde ise telefon hattından saplama yapmak eyleminin hırsızlık suçunu oluşturup oluşturmadığı tartışmasının yapıldığı görülmektedir. Yani telefon hattı ve verinin taşınabilir bir mal olup olmadığı tartışılmakta, bilişim sistemleri üzerine bağlayıcı bir içtihat oluşturulmamaktadır. Kaldı ki karar tarihinde 525. madde ve devamındaki bilişim suçları TCK'ye henüz girmediğinden İBK'nin iki suç tipi arasında bir değerlendirme yapması da olanaksızdır. CGK kararında bu konuya da değinmiş, sonradan yapılan bilişim suçlarına ilişkin düzenlemede, telsiz telefon konuşmalarının madde metninde olmadığını söyleyerek, hırsızlık hükümlerinin uygulanacağına hükmetmiştir. Dayanılan gerekçe itibari ile bilişim sistemi unsurları ile ilgili bir değerlendirme yapılmaksızın verilmiş olan karara katılmamız mümkün değildir.

Farklı bir konuyla ilgili ileri tarihli kararında Yargıtay daha detaylı inceleme yapmıştır. Manyetiğini değiştirmek suretiyle sahte kartlarla ankesörlü telefonları kandırarak ücretsiz konuşma yapılması eyleminin TCK 163. maddedeki otomatlardan karşılıksız yararlanma suçu değil, 244. maddedeki bilişim sistemindeki verilerin değiştirilerek çıkar sağlanması suçu olduğuna hükmedilmiştir¹⁴⁰. Gerçekten de gerek merkezi ARMS bilgisayar sistemi gerekse tele-

¹³⁹ Yargıtay, CGK, 1996/6-151 E. 1996/152 K. 25.06.1996 T.

¹⁴⁰ “Ankesörlü telefonlar, manyetik kart, kredi kartı ve smart kart ile çalışan hizmet telefonlarıdır.

Bu telefonlar katılan Kurum tarafından ücretsiz olarak meydanlar, hastaneler, terminaller, garlar, limanlar, metro istasyonları, askeri tesisler, Toplu konut alanları gibi halka açık yerlere tesis edilmekte, ARMS olarak adlandırılan merkezi bilgisayar sistemi ile yönetilmektedir. ARMS sisteminin, suçun işlendiği bölgede hizmet veren ve kendisine bağlı olan 200 adet D-3 manyetik kartlı ankesör makinesinin çalışma bilgilerini, (kullanılan kontör miktarı, manyetik karta ait barkot numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi vb.) bünyesinde bulundurduğu anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkot numaraları dahi bu sayede tespit edilebilmiştir.

Suç tarihinde kullanılan sistemin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura ihtiyaç vardır. Bunlardan birincisi, manyetik telefon kartı, diğeri ise kontör olarak adlandırılan kredidir. Bunlara sahip olunmadan, bir bilgi işlem biriminin parçası olan ve ARMS denilen sisteme bağlı bulunan ankesörlü makinelerden, Kurum'ca acil durumlarda kredisiz görüşme yapılabilmesine olanak sağlanmış bulunan sınırlı sayıdaki numara dışında görüşme yapılabilmesine olanak yoktur. Bu sistemde, manyetik kart üzerindeki barkodu okuyan makine, manyetik kart üzerinde kullanılmış kredi bilgileri bulunmadığı takdirde, okuduğu kartın kredi sınıflandırma özelliklerine göre 100, 60 veya 30kontör kredi yüklemesi yapmak suretiyle kullanıma hazır hale getirmektedir. Başka ifadeyle sistem, makineye takılan karttaki verilerin alınıp değerlendirilmesi suretiyle işlemektedir. Somut olayda sanığın, kredisiz bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasası'nın 525/B maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren 5237

fon terminalleri duyuya yönelen aygıt unsurunu, merkez bilgisayar sisteminde işlenen veriler iç bağlantı unsurunu, kartla aktif hale gelen ve kart bilgilerini merkeze gönderen kısım ise dış bağlantı unsurunu oluşturmakla, bu tür sistemlerin klasik mekanik sistem değil, bilişim sistemi olarak belirlenmiş olması isabetli olmuştur.

2000’li yılların başında verilmiş olan bir kararda banka ATM’lerinin de bilgileri otomatik işleme tabi tutan sistem olduğu yönünde karar verilmiş, ATM’lerin işlevleri ve merkeze bağlı olmasının bu kararda büyük önemi olmuştur¹⁴¹.

Yine son tarihli bir kararda, cep telefonunun bilişim sistemi sayıldığına ilişkin bozma kararı verildiği de görülmektedir¹⁴². Bu kararda özellikle cep telefonlarının kendi işletim sistemlerinin bulunduğu unsuruna dikkat çekilmektedir.

Tüm bu bilgiler ışığında düşüncemiz, bilişim sisteminin bilgisayar ve türevleri ile kısıtlı olmaksızın geniş olarak yorumlanması, bahsettiğimiz 3 kriter (aygıt – iç bağlantı – dış bağlantı) doğrultusunda her bir sistemin özelliğinin araştırılarak karar verilmesidir. Gelecekte yaşanacak teknolojik gelişmelere de bu sayede uygunluk sağlanabilmesi mümkün olacaktır.

Kriterler bakımından incelendiğinde, sıradan bir hesap makinesinin dahi bilişim sistemi sayılmasının önünde engel bulunmamaktadır. Nesnelerin internetine geçildiği günümüzde ev aletlerinin bile “zombi bilgisayarlar” dönüştürülerek ağ trafiğini çökertmek amacıyla eş zamanlı kullanıldıklarını biliyoruz¹⁴³. İlk bilgisayarın da modern bilgisayarın da ikilik tabandaki matematiksel işlemlerle çalıştığını düşündüğümüzde, hiç düşünemediğimiz aygıtların da bilişim suçları amacıyla bilişim sistemlerine dahil edilmesi mümkün olacağından, tek tek saymak suretiyle bilişim sistemleri sayılan veya sayılmayan aygıtların belirtilmesi doğru olmayacaktır.

Benzer şekilde, “genel amaçlı kullanma” kriterinin de içeriğinin belirsiz olması yönündeki eleştirilerine katılıyoruz. Genel amaçla kullanma sınırı nedir¹⁴⁴? Bugün Yargıtay tarafından bilişim sistemi olarak görünen ATM’ler banka veri tabanına bağlanma ve bankacılık işlemleri dışında hangi genel amaçlarla kullanılabilir? Günümüzde, metrenin milyarda biri ölçeğinde üretim yapılabilen tesisler ve kar maksimizasyonu amaçlı ekonomik sistem bir arada düşünüldüğünde, artık sadece belli amaçlar için tasarlanmış az hacim kaplayan birçok farklı aygıt görebilmekteyiz. Bilişim sistemlerinin geleceği de birçok işi tek başına yapabilen

sayılı Türk Ceza Yasası’nın 244.maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır.” Yargıtay, CGK, 2007/6-136 E. 2007/150 K. 19.06.2007 T.

¹⁴¹ Yargıtay, CGK, 2001/6-30 E. 2001/57 K. 10.04.2001 T.

¹⁴² “Cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmayacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması... bozulmasına...” Yargıtay, 8. CD. 2014/30037 E. 2015/14023 K. 18.03.2015 T.

¹⁴³ “Hackerlar DDoS saldırısı için buzdolabı kullanmış!” <http://shiftdelete.net/hackerlar-ddos-saldirisi-icin-buzdolabi-kullanmis-76351> (erişim tarihi: 25.02.2019).

¹⁴⁴ Aynı görüşte, Erdoğan, 2013: 12.

aygıtlardan ziyade kendi işini yapmakta uzmanlaşmış, hafif, bilgisayara göre daha hesaplı aygıtlar yönünde evrilecektir. Zira öğretide genel amaçlı kullanımı savunan Kurt, diğer yandan bilgisayarın tek bir işi yapmak üzere de dizayn edilebileceğini kabul etmektedir¹⁴⁵. Bu yönüyle bilgisayarların genel amaçlı olmak zorunda olmadığını kabul etmiş bulunmaktadır. Yargıtay’ın “genel amaçlı kullanım” yönünde verdiği kararlarda da bilgisayar tanımını oldukça geniş tuttuğu düşünüldüğünde aslında bir çelişki de oluşmayacaktır. Bu bakımdan her bir sistem için bahsettiğimiz 3 kriterin varlığını araştırmanın, genel amaçlı kullanım kriterine oranla daha verimli sonuçlar doğuracağı inancındayız.

Bu bakımdan sayma amacı gütmemekle birlikte, bilişim sistemi unsurlarına dair modelimizin örneklendirilmesi ve bilişim sistemlerinin çalışma prensiplerini anlamak bakımından bilgisayar başta olmak üzere bazı bilişim sistemleri incelenmelidir.

1.3.1 Bilgisayar

Bilgisayarlar, bilişim sistemlerinin en tipik örneklerini oluşturmaktadır. 19. yüzyılda delikli kartlar ile öncülleri ortaya çıkmaya başlamış olan bilgisayarların, 20. yüzyılda elektrik devrelerinin de kullanılmasıyla günümüzdeki tanıma uygun ilk örnekleri görülmeye başlanmıştır. Bilgi teknolojileri ve bilişim sistemleri uzun süreler boyunca bilgisayarlar aracılığı ile geliştiği için, yabancı terminolojide halen bilgisayar “computer” ifadesinin bilişim “informatics” teriminden fazla, kavramın da oldukça geniş anlamda kullanıldığı görülmektedir.

1.3.1.1 Tarihçe

Bilişim ve bilgisayar arasındaki bağlantı hakkında daha verimli bir tartışma yapabilmek için bilgisayarların tarihsel gelişimi ve teknik özellikleri hakkında yüzeysel de olsa bilgi sahibi olmanın faydası olacaktır.

İlk ve ilkel bilgisayarların tarihi milattan önce 3500 yıllarına kadar dayanır. Çin, Japonya ve Hindistan’da görülen elle hareket ettirilebilir hesap yapmaya yarayan abaküslerin, taşıdığı amaçlar bakımından bilgisayarların ilk örnekleri olduğu söylenebilir¹⁴⁶. Bu tarihlerden itibaren bilgisayarlar farklı teknik ve hacimlerde ancak benzer amaçlı olarak farklı yerlerde görülmüştür. 1801’de Fransa’da bir tekstil üreticisi olan Joseph Jacquard’ın işletmesinde bilgisayar kartının ön modelini dizayn ettiği, bu sayede dokuma aşamalarında tekrarlama yaptığı söylenmektedir. Hatta işçilerin kendi standartlarını tehdit eden bu makineyi sabote ettikleri ve olayın bilinen ilk bilgisayar suçu olarak söylenebileceği ifade edilmektedir¹⁴⁷.

¹⁴⁵ Kurt, 2005: 29.

¹⁴⁶ Erdoğan, 2013: 53.

¹⁴⁷ Akçam, 1999: 45.

Öğretide ise modern (elektronik) anlamda bilgisayarların gelişim süreci dört döneme ayrılmaktaysa da verilen tarihler bakımından kapsamları çok belirgin değildir. Buna karşın bilgisayarların gelişim sürecinde belirli patlama noktalarını esas alarak bir değerlendirme yapmak mümkündür.

Buna göre birinci dönem vakum tüplerinin kullanılmasından transistörlerin icadına kadar geçen kısa süre olmalıdır. Bu dönemde Amerikan ordusunda topçu atışlarının hesaplanması için ilk elektronik bilgisayar olan ENİAC (Electronic Numerical Integrator And Calculator) geliştirilmiştir¹⁴⁸. ENİAC'ta yer alan model, vakumlanmış tüplerde yer alan elektrotların ısıtılması suretiyle elektronların yayılması ve belirtilen gerilimin üzerindeyse tüpün diğer tarafına geçebilmesi şeklinde planlanmıştı. Bu üstün buluşa rağmen vakum tüpleri güvenilir değildi ve çok yer kaplıyordu. 18.000 tüp, tenis sahası büyüklüğünde bir yeri kaplıyor ve 30 ton ağırlığa erişiyordu. Ayrıca tüpler 1 saatte, 15 evin 1 günde kullandığı kadar elektrik harcıyordu. Bu nedenle bu teknolojinin üzerine düşülmedi ve alternatifleri düşünülmeye başlanarak transistörlerin icadının önü açıldı¹⁴⁹.

İkinci dönemde yarı iletken teknolojisi ile üretilen transistörler, bilgisayarların önünü açan temel etken oldu. Öyle ki, transistörün icadını, yakın çağı kapatıp bilişim çağını açan bir gelişme olarak, son yüzyılın en büyük icadı olarak da görülmektedir. Transistörler, en basit haliyle, vakum tüplerinin yaptığı işi, daha kararlı ve dayanıklı şekilde, çok daha küçük hacimlerde ve ısıtılma sorunu olmaksızın yapabilme imkânı vermişlerdir. Bu dönemde ilk transistörlü radyo da 18 Ekim 1954'te "Regency Tr 1" adıyla satışa sunulmuştur¹⁵⁰.

Ne var ki, transistörlerin icadından sonra devreler daha karmaşık hale gelmiş, devrelerin hacimce sıkıştırılması ve binlerce farklı boyuttaki parçaların lehimlenmesi sorunu baş göstermiştir¹⁵¹. İşte bu sorunun entegre devre (integrated circuit) buluşuyla çözümlenmesinin de üçüncü dönemi başlattığı söylenebilir. Jack Kilby (Texas Instruments) 1959'da germanyumdan yapılan devre patentini aldıktan sonra, günümüzde de halen işlemcilerini kullandığımız Intel firmasının kurucularından Robert Noyce 25 Nisan 1961'de silikondan yapılan entegre devre patentini almıştır¹⁵². Patentin alınmasının ardından 10 yıl geçtikten sonra Intel, tarihte ilk mikroişlemci olarak kabul edilen 4004 isimli işlemcisini 1971 yılında duyurmuştur. Bu noktada öğretide "transistörlerin yerini entegre devrelerin aldığı" yönündeki anlatım¹⁵³, tran-

¹⁴⁸ Dülger, 2015: 106.

¹⁴⁹ <https://ed.ted.com/lessons/how-transistors-work-gokul-j-krishnan> (erişim tarihi: 25.02.2019).

¹⁵⁰ <http://www.regencytr1.com/> (erişim tarihi: 25.02.2019).

¹⁵¹ <http://www.kimnezamanicatetti.com/entegre-devre/> (erişim tarihi: 25.02.2019).

¹⁵² Sonrasında taraflar arasında patent tartışmaları devam etmiş ve taraflar çapraz lisanslama (birbirlerinin lisanslarını bedelsiz kullanabilme) yolunu tercih etmişlerdir. <https://www.edn.com/electronics-blogs/edn-moments/4412805/Noyce-receives-1st-IC-patent--April-25--1961-> (erişim tarihi: 25.02.2019).

¹⁵³ Dülger, 2015: 107.

sistörlerden vazgeçilmesi değil, entegre devrelerde çok küçük hacimlerde bütünleşik bulunabilmesi şeklinde anlaşılmalıdır.

Günümüze kadar uzanan dördüncü ve son dönemin ise, bilgisayarın evlerimize girdiği, birçok uygulama yazılımlarının geliştirilerek bilgisayarların farklı amaçlarda hizmet verdiği, işletim sistemlerinin ve ara yüzlerin son kullanıcılara sunulduğu dönem olduğu söylenmekte ve 1981 yılında ilk kişisel bilgisayar olan “IBM PC”nin üretilmesinin bu dönemin başlamasında önemli bir dönüm noktası olduğu belirtilmektedir¹⁵⁴.

İşlemcilerin ikilik sayı sistemi yerine üçlük sayı sistemi kullanması¹⁵⁵, işlemci mimarilerinin 3 boyutlu çalışmaların geliştirilmesi ve özellikle kuantum bilgisayarlar gibi öneriler ise gelecek dönemin belirleyicileri olmaya adaydır. Tüm bu teknolojilerin arkasındaki değişmeyen tek amaç ise, elektronik akım yardımıyla matematik hesaplarının daha hızlı yapılabilmesidir. Baş döndürücü bu kadar teknolojiye rağmen, bilgisayar üzerinde gördüğümüz her işlem halen ve sadece bu aritmetik işlemlerden ibaret olacak kadar basittir.

1.3.1.2 Donanımsal Özellikler

Günümüzde bilgisayarlar insan hücre zarından dahi daha ince¹⁵⁶ ölçeklerdeki üretim teknolojileri ile muazzam bir performans ortaya koymakta, en zor hesaplamaları bile kısa zamanda gerçekleştirebilmektedir. Bu performansın en verimli şekilde elde edilebilmesi için bilgisayar bileşenleri de sürekli geliştirilmekte ve değiştirilmektedir. Bu noktada mevcut sistemler hakkında bileşenlerden biraz bahsedilmesi yerinde olacaktır.

1.3.1.2.1 Anakart

Anakart, bilgisayarın birincil ve en merkezi baskılı devre kartıdır. Bilgisayarın bütün organizasyon şeması anakart üzerinde bulunur¹⁵⁷. Temel olarak bütün bileşenler harici veya dahili olarak anakarta bağlandığı için bunlar arasındaki veri yolları ile işlemci ve bellek gibi çeşitli birimlerin ihtiyaç duyduğu enerjinin kontrolü anakart tarafından sağlanır. Bu yönüyle anakart, tüm sinir sisteminin de üzerinde bulunduğu insan iskeletine benzetilebilir.

Anakart üzerindeki tüm bileşenlerin iletişimi ise anakartın üzerindeki yongalar aracılığı ile sağlanmaktadır. Daha önceden kuzey köprüsü ve güney köprüsü olarak adlandırılan iki farklı yonga seti, gelişen teknoloji ile birleştirilmiş ve güney köprüsü kaldırılarak anakartın üzerinde PCH (Platform Controller Hub) tek bir yonga seti oluşturulmuştur. Hangi işleri iş-

¹⁵⁴ Dülger, 2015: 108.

¹⁵⁵ <http://www.bilim-teknoloji.com/uc-boyutlu-islemciler/> (erişim tarihi: 25.02.2019).

¹⁵⁶ İnsan zarının 12 nanometre olduğu bilinmektedir. Günümüzde gelişmiş işlemciler 10 nanometre ile üretilmekte olup, 7 nanometreye geçiş çalışmaları başlanmıştır.

¹⁵⁷ <https://tr.wikipedia.org/wiki/Anakart> (erişim tarihi: 06.03.2016).

lemcinin, hangi işleri bu yonga setinin yapacağı konusu tekniğe göre farklılık göstermektedir¹⁵⁸.

Son olarak, klavye ve fare gibi giriş aygıtları ile monitör ve yazıcı gibi çıkış aygıtlarının bağlanabilmesi için gerekli fiziki imkanların da anakartın üzerindeki portlardan sağlandığı belirtilmelidir.

1.3.1.2.2 İşlemciler

İşlemciler, üzerindeki transistörler aracılığıyla elektrik akımını kontrol eden ve bu sayede ikili sayı sistemindeki 0 ve 1'leri kullanarak veri işleme yeteneği kazanan donanımsal parçadır. Mühendislik bilimlerinde bilgisayarların genel olarak beş parçaya ayrıldığı, bunların giriş, çıkış, bellek, veri yolu ve kontrol birimi olduğu ve çoğu zaman son iki parçanın birleştirilerek işlemci adıyla anıldığı söylenmektedir¹⁵⁹.

Günümüzde, küçük ebatlardaki boyutu ve milyarlarca transistör barındırması nedeniyle mikro işlemci olarak da bahsedilen işlemciler, mantıksal birim (ALU – Arithmetic Logic Unit) ve yazmaçlardan oluşmaktadır. Mantıksal birim 4 işlemin ve karşılaştırma işlemlerinin yapıldığı bölümdür. İşlemcinin içinde bulunan 1 bitlik tam toplayıcı devresi, toplama işleminin yanı sıra sayının tersini alarak toplama yani çıkarma işlemini de yapabilmekte, bu sayede art arda toplama anlamına gelen çarpma ve art arda çıkarma anlamına gelen bölme işlemlerini de gerçekleştirebilmektedir¹⁶⁰. Yazmaçlar (saklayıcılar) ise bellek ile fonksiyonel birimler arasındaki veriyi düzenlemekte, mantıksal birime veri iletip cevapları saklamaktadır¹⁶¹.

Bir bilgisayarda bulunan CPU (Central Processing Unit – Merkezi İşlem Birimi) bir işlemi en hızlı şekilde yapmak üzere tasarlanan işlemcilerdir. Buna karşın birden fazla işlemi aynı anda yapabilmek için daha fazla çekirdeğe sahip GPU¹⁶² (Graphic Processing Unit – Grafik İşlem Birimi) adı verilen grafik işlemciler de bilgisayarlarda kullanılmaktadır. GPU'lar daha çok fizik hesapları ve grafik tabanlı hesaplamalar için kullanılmaktadırlar.

¹⁵⁸ Yonga setleri ve güncel anakart tasarımları hakkında detaylı bilgi için, <https://www.youtube.com/watch?v=IPX58C2lrEk> (erişim tarihi: 25.02.2019).

¹⁵⁹ Can, 2015: 4.

¹⁶⁰ Bahtiyar, 2007: 15.

¹⁶¹ https://tr.wikipedia.org/wiki/Yazma%C3%A7_%C3%B6be%C4%9Fi (erişim tarihi: 11.03.2016). Yazmaçlar hakkında detaylı bilgi ve çeşitleri için, <https://www.turkcebilgi.com/yazma%C3%A7> (erişim tarihi: 25.02.2019).

¹⁶² “GPU, grafik verilerinin işlenerek iki boyut formatında ekran üzerindeki piksellere ileten, kendine ait mikro işlemci ve belleği olan donanımdır.” Yazıcı, 2016: 16.

1.3.1.2.3 Bellekler

Bellekler, üzerinde veriyi geçici veya kalıcı olarak barındırabilen ve veri işlemcilerine kaynak sağlayan birimlerdir¹⁶³. Bilişim sistemleri sürekli daha iyi performans ve daha iyi üretim teknolojileri üzerine odaklandığından, verilerin belleklerden işlemcilere daha hızlı taşınabilmesi için sürekli olarak yeni teknolojiler geliştirilmektedir. Bu nedenle, bellekleri fonksiyonlarına ve kullanım amaçlarına göre incelemede fayda bulunmaktadır.

1.3.1.2.3.1 Fonksiyonlarına Göre Bellekler

Temel olarak bellekler veriyi kalıcı olarak saklayıp saklayamadıklarına göre uçucu (volatile) ve uçucu olmayan (non – volatile) bellekler olarak ikiye ayrılır.

Uçucu bellekler güç kesilmesi veya bilgisayarın yeniden başlatılması gibi durumlarda içindeki veriyi yitiren, kalıcı olarak saklama işlemi yapmayan belleklerdir. En çok bilinen örneği olan RAM (Random Access Memory – Rastgele Erişimli Bellek) üzerinde veri silme, yazma, okuma işlemlerinin ayrı ayrı yapılabildiği belleklerdir¹⁶⁴. Belli bir sıra takip edilmeksizin verilere erişilebildiği için bu ismi almıştır. Uçucu olan RAM'ler Dinamik (DRAM) ve Statik (SRAM)¹⁶⁵ olmak üzere ikiye ayrılırlar.

Uçucu olmayan, yani veriyi kalıcı olarak saklayabilen bellekler ise sahip oldukları teknolojiye göre ROM, PROM, EPROM, EEPROM, Flash Bellek olmak üzere farklı isimler almışlardır.

ROM (Read Only Memory – Sadece Okunur Bellek) daha sonradan değiştirilmemek üzere tasarlanmış, güç kaynağı kesilmesi ve bilgisayarı yeniden başlatma gibi durumlarda veri kaybına uğramayan belleklerdir¹⁶⁶. Üreticisi tarafından bir kez programlandıktan sonra yeniden değiştirilmesi mümkün değildir. Bu nedenle özellikle bilgisayarın başlangıç anında işletim sistemi devreye girmeden önce ihtiyaç duyduğu veriler bu belleklerde saklanmıştır¹⁶⁷.

ROM bellekler, fabrikada metal maskeleme aşamasında kalıcı olarak programlandığı için yeniden değiştirilmesi mümkün değildir. Bu nedenle değişik ihtiyaçları karşılayabilmek için sırasıyla PROM¹⁶⁸ (Programmable Read Only Memory), EPROM¹⁶⁹ (Erasable Program-

¹⁶³ Bu nedenle birçok yerde veri taşıyıcısı ismine de rastlanmaktadır. Türk Ticaret Kanunu'nda veri taşıyıcıları hakkında detaylı bilgi için, Dülger, 2014b: 135.

¹⁶⁴ Kurt, 2005: 33.

¹⁶⁵ SRAM'ler içindeki verileri yenileme ihtiyacı duymadığından daha hızlı çalışır. Buna karşın tek yongaya daha çok hafıza yerleştirilebilen, daha az maliyetli ve daha az güç tüketen DRAM'ler günümüzde daha çok kullanılmaktadır. http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/Bellek%20Birimleri.pdf (erişim tarihi: 25.02.2019). Çalışma prensiplerine ilişkin detaylı bilgi için, Toker/Zeki, 2006: 121.

¹⁶⁶ <http://bidb.itu.edu.tr/sevirdefteri/blog/2013/09/06/bellek-turleri> (erişim tarihi: 25.02.2019). Yenidünya/Değirmenci, 2003: 23.

¹⁶⁷ Dülger, 2015: 67.

¹⁶⁸ PROM da aynı ROM gibi bir kez programlanabilmesine karşın, bu işlemin fabrika dışında, dağıtıcının istediği herhangi başka bir yerde yapılması imkânını sağlar.

mable Read Only Memory) ve EEPROM'lar¹⁷⁰ (Electronically Erasable Programmable Read Only Memory) üretilmiştir. Flash Bellekler ise RAM ile sabit sürücü (hard disk) özelliklerini birleştirmesiyle günümüzde yoğun olarak kullanılmaktadır. Yine FRAM'ler (Ferroelectric RAM) esasında bir RAM türü olmasına karşın üretildiği ferro elektrik malzeme sayesinde verileri kalıcı olarak saklayabilmektedir¹⁷¹.

Kısa bir zaman aralığında bellek teknolojisinin gelişim süreci göz önüne alındığında, gelecekte elimizdeki bilgilerin hızlıca eskiyeceğini, uçucu ve uçucu olmayan bellek ayrımının dahi kalmayacağı düşünülebilir.

1.3.1.2.3.2 Kullanım Amaçlarına Göre Bellekler

İşlevlerinin dışında veri saklama kapasitesi de belleklerin kullanım alanlarını belirleyen önemli bir etkidir. Ucuz maliyetle büyük kapasitedeki verileri saklayabilen bellekler bilgisayarın ana belleğini oluştururken, daha hızlı veri aktarabilmesine karşın maliyeti nedeniyle az boyuttaki verileri barındırabilen bellekler ise sistem performansını artırma amaçları için kullanılmaktadır.

Günümüzde, büyük depolama ihtiyaçları nedeniyle bu ihtiyacı karşılayabilen iki tür ana depolama belleği bulunmaktadır. Bunlardan biri olan HDD (Hard Disk Drive) manyetik bir plaka ile onlar üzerinde okuma ve yazma işlemi yapan kafalardan oluşur¹⁷². Çalışma prensibi gereği HDD'nin maksimum hızı kendi okuma kafalarının mekanik hareketi ile kısıtlanmış durumdadır. Bu nedenle mekanik değil elektronik yöntemlerle çalışan SSD (Solid State Drive – Katı Hal Sürücüsü) daha yüksek hız ve performans gösterir. Bu yönüyle düşünüldüğünde ana depolama amacıyla kullanılan belleklerin farklı çeşitlerinin olduğu ve gelecekte daha farklı şekilde görüleceği söylenebilir.

Ana depolama bellekleri ne kadar hızlı çalışırsa çalışsın, yine de işlemcinin hızına yetişemez. Kalabalık halde bulunan verilerin arasından ihtiyaç olanının seçilmesi vakit kaybına neden olmaktadır. Bu nedenle bazı verilerin ana depolamadan ayrılarak daha kolay ulaşılabilir bir yerde tutulması gerekmektedir. Bu nedenle bilgisayarlarda ana depolama ile işlemci

¹⁶⁹ EPROM, üzerinde yer alan küçük saydam pencereden verilecek kuvvetli morötesi ışınlarla verileri silme ve dolayısıyla tekrar tekrar programlama imkanını vermektedir.

¹⁷⁰ EPROM'lara morötesi ışık verilebilmesi için genellikle sistemden sökülüp yeniden monte edilmesi gerektiğinden, silme işleminin elektronik olarak ve çok daha hızlı gerçekleştirilebildiği EEPROM'lar üretilmiştir. Bu yönüyle yazılıp silinme bakımından EEPROM'ların salt okunur olmadıkları, RAM işlevini gördüğü söylenebilse de, veri yazılması için önce tüm verilerin silinmesi gerektiği, yani rastgele (random) okuma yapmaması yönünden RAM'lerden ayrılmaktadır.

¹⁷¹ Toker/Zeki, 2006: 118.

¹⁷² Taş, 2013: 25.

arasında bazı ara bellekler bulunur. RAM'ler ve önbellekler¹⁷³ bunlara örnek olarak verilebilir.

1.3.1.3 Yazılımsal Özellikler

Donanımın tek başına varlığı ona bilişim sistemi olma özelliği vermez. Onu yönlendirecek ve komut verecek programların da bulunması zorunludur. Bu sayede verilerin nasıl işleneceği ve ortaya çıkan verinin bilgiye nasıl dönüştürüleceği de belirlenmiş olacaktır. İşte donanımı anlamlı bir şekilde harekete geçiren her türlü komut dizisine *yazılım* denmektedir. Bugün öğretilen tartışılan ve “bilgileri otomatik olarak işleme tabi tutma” deyiminin de yazılımdan kaynaklandığını düşünmekteyiz. Bu, yazılımların otomatik olarak üretilmesinden değil, bir kez üretildikten sonra donanımı belli bir sistematik içerisinde otomatik olarak kullanmasından ileri gelmektedir.

1.3.1.3.1 BIOS, İşletim ve Uygulama Yazılımları

Yazılımlar basit mantıksal devrelere ilişkin komutlardan, çok daha karmaşık sistemlere kadar değişkenlik gösterir. Bu da yazılımların amaçlarına göre ayrılabilceğini göstermektedir.

BIOS (Basic Input Output System) bilgisayarın temel yazılımıdır. Kalıcı bir yazılım olup, ROM bellekte saklanır¹⁷⁴. Açılışta donanımları kontrol etmek, voltaj ve frekans düzeylerini ayarlamak, kullanılmayan donanımı doğrudan kapatmak, işletim sisteminin başlayacağı belleği belirlemek gibi zorunlu işlevleri görür¹⁷⁵. İçerdiği verileri kalıcı ve salt okunur olarak sakladığı için tarih, saat gibi bilgisayar kapalı olduğunda da değişmesi gereken bilgileri ayrı bir bellekte saklar ve enerji ihtiyacını bios pili denilen çok düşük güç tüketimli pilden karşılar. Bu nedenle BIOS üzerinde yapılacak bir manipülasyonun işletim sistemi düzeyinde çözülmesi mümkün olmayacaktır.

İşletim yazılımları bilişim sistemlerinin çalışmasını ve temel fonksiyonlarını yerine getirmesini sağlar¹⁷⁶. Bu yazılımların adeta kurallarını kendi koydukları bir dünya oluşturduğu söylenebilir, yapabileceklerinin sınırlarını yine kendisi çizmektedir. Genel olarak işletim sistemi firmaları ile donanım firmaları sürekli iletişim halinde oldukları için, yazılım-donanım iş birliği sağlanarak makine diline yakın ve sisteme az yük getirerek yüksek performans sağlanmış olur.

¹⁷³ Önbellekler genellikle Static RAM'lerden oluşan ve işlemciye yakın bulunan küçük bellek birimleridir. <http://teknolojiProjeleri.com/teknik/onbellek-cache-nedir> (erişim tarihi: 25.02.2019).

¹⁷⁴ <http://www.elektrikport.com/teknik-kutuphane/bios-nedir-bios-ayarlari-nasil-yapilir/15085#ad-image-0> (erişim tarihi: 25.02.2019).

¹⁷⁵ <https://tr.wikipedia.kim/wiki/BIOS> (erişim tarihi: 30.01.2016).

¹⁷⁶ Kurt, 2005: 35.

İşletim sistemleri oldukça kompleks yapılar olduğundan¹⁷⁷, tüm güvenlik önlemlerine karşın içlerinde çok sayıda açık tespit edilmektedir. Açıkların giderilmesi için çıkarılan yamaların yanı sıra yeni teknolojileri dahil eden kod blokları düşünüldüğünde, sistemin yaşam döngüsü ve açıkların neden tümüyle giderilemediği daha net ortaya konulmaktadır.

Uygulama yazılımları ise işletim sistemleri içerisinde çalışan ve belli bir amacı gerçekleştirmeye yönelik¹⁷⁸ geliştirilmiş yazılımlardır. Bu yazılımların bir bölümü işletim sistemi ile birlikte sunulsa da büyük çoğunluğu bağımsız (üçüncü parti) geliştiriciler tarafından üretilmektedir. Üstelik işletim sistemi sahibi firmalar, daha çok geliştiricinin kendi platformlarına program tasarlamasını, bu sayede pazar payını arttırmayı istemektedir. Birçok hükümet de bilişim devrimi olarak adlandırdığı günümüzde öğrencilik çağından itibaren vatandaşlarını kodlama öğretmeye teşvik etmektedir. Bu nedenle faydalı yazılımların yanı sıra birçok zararlı yazılım da hızla yayılmaktadır.

1.3.1.4 Çalışma Prensipleri

Yukarıda ana hatlarıyla bahsedilen donanım – yazılım iş birliği, küçük farklılıklarla birlikte tüm bilişim sistemlerine hayat vermektedir. Bu bağlamda bilgisayarın çalışma prensiplerine de kısaca değinmekte fayda olacaktır.

Güç kaynağından beslenen bilgisayarda ilk olarak BIOS devreye girmekte ve donanımları her defasında test etmekte, yeni bir donanım fark ederse onu işlevsel hale getirmektedir. Her bilgisayarda BIOS ayarlarına giriş için bir tuş atanmış durumdadır. Bu tuşa açılma esnasında basılmadığı ve sorunlu donanım bulunmadığı sürece işletim sistemi yüklü bulunduğu bellek üzerinden otomatik olarak çalışmaya başlamaktadır.

İşletim sisteminin öngördüğü servisler ile birlikte, başlangıç esnasında doğrudan çalışma komutu verilen diğer programlar da otomatik olarak açılırlar. Diğer programlar ise ancak kullanıcının açılma komutunu vermesiyle devreye girerler, bundan önce sistem üzerinde bir etkileri olmamaktadır. Bu bakımdan zararlı yazılımların büyük çoğunluğu sistemin açılışında devreye girmek üzere tasarlanmıştır, bu sayede başka programları da başlatabilir ve zararlı işlemleri yerine getirebilirler.

1.3.2 Cep Telefonu

Telefon, sözlük anlamıyla “konuşmaları ileten veya yansıtan düzenek”, “birbirinden uzakta bulunan kişilerin konuşmasını sağlayan aygıt” demektir. Cep telefonu ise “kişinin ya-

¹⁷⁷ İstatistiklere göre Microsoft’un 2007 yılında sunduğu Windows 7, 40 milyon satıra yakın koddan oluşmaktadır. <https://informationisbeautiful.net/visualizations/million-lines-of-code/> (erişim tarihi: 25.02.2019).

¹⁷⁸ Dölger, 2015: 68.

nında taşıyabildiği, kablosuz telefon, mobil telefon” olarak tanımlanmaktadır¹⁷⁹. Bu tanımlar gelinen süreçte cep telefonlarının fonksiyonlarını¹⁸⁰ ve kullanım alanlarını ne yazık ki kapsamamaktadır.

Halk arasında akıllı telefon (smartphone) olarak adlandırılan telefonlar, aslında bilgisayarlarla aynı aileden gelmektedir. Yukarıda bahsedildiği üzere masaüstü veya dizüstü bilgisayarlar bir anakart üzerinde bulunan birden fazla çip ile çalışmaktadır. Ancak aynı çözümün cep telefonlarına uygulanması mümkün değildir. Çünkü bilgisayar donanımının aynı şekliyle cep telefonuna sığdırılması mümkün değildir. Kaldı ki sığdırılsa bile bu kez işlemciler bilgisayardaki gibi soğutulamayacağından ısınmak suretiyle bozulacak, bozulmasa bile harcadığı enerji yüzünden telefonlar sürekli şarj edilmek zorunda kalacaktır.

Bu nedenle tüm sistemin tek bir çip üzerinde yer alması için çalışmalar yapılmıştır. İşlemci, grafik işlemci ve bellek gibi tüm gereksinimlerin tek bir çip üzerine toplandığı bu sistemlere SoC (System on Chip) denilmektedir¹⁸¹. Bu sistemlerdeki güç tasarrufu ve ısınma sorunları ile ilgili olarak ise işlemci mimarilerinden kısaca bahsedilmelidir.

Bilişim aygıtları komutlarına göre CISC (Complex Instruction Set Computer) ve RISC (Reduced Instruction Set Computer) olarak ayrılmaktadır. CISC modelinde, yüksek performans elde edilmesine karşın karmaşık olması, yenilenen her model ve her yeni nesilde işlemcilerin giderek daha da karmaşık olmasına ve birçok komutun kullanılmamasına neden olmaktadır. RISC modelinde ise komutlar tek bir format ve saat döngüsüne indirgenmektedir¹⁸². Diğer model kadar yüksek performans vermemesine karşın, daha küçük hacimlerde ve daha az enerjiyle çalışması bakımından öne çıkmaktadır. İşte günümüzde kullanılan akıllı telefonlar çoğunlukla RISC modelini uygulayan bir mimari olan ARM¹⁸³ (Acorn RISC Machine) ile çalışmaktadır. Bu sayede henüz bir masaüstü veya dizüstü bilgisayar kadar güçlü performans veremese de yakın bir performansı çok küçük hacimlerde ve az enerji tüketimiyle başarabilmektedir. Özetle RISC çözümleri, az enerji tüketmesi sayesinde akıllı telefonlardaki ısınma ve batarya ömrü sorunlarını aşabilmektedir. Bu bakımdan akıllı telefonların, bilgisayarların farklı bir versiyonu olduğu ve bilişim sistemi sayıldığında tartışma bulunmamaktadır.

¹⁷⁹ http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c39dd02e5db73.43360491 (erişim tarihi: 25.02.2019).

¹⁸⁰ GSM teknolojisi hakkında detaylı bilgi için, Ukşal, 2015: 11.

¹⁸¹ <https://www.chip.com.tr/haber/system-on-chip-hakkinda-bilmeniz-gerekenler-40217.html> (erişim tarihi: 25.02.2019).

¹⁸² Teknik detaylar hakkında daha fazla bilgi için, Jamil, 1995: 13; Şentürk, 2009: 1 – 2.

¹⁸³ “ARM işlemciler taşınabilir cihazlardan (PDA, cep telefonu, medya oynatıcılar, avuç içi oyun üniteleri ve hesap makineleri) bilgisayar parçalarına kadar (disk sürücüler, masaüstü) tüketici elektroniğinin her alanında yoğun olarak kullanılmaktadır.” Türk, 2011: 4. 1983 yılında üzerinde çalışılmaya başlanan ARM mimarisi, İngiliz bir şirket tarafından tasarlanmakta ve üreticilere lisanslanmakta olup, işlemciler şirket tarafından doğrudan üretilmemektedir. CISC tarafında ise Intel x86 ve x64 mimarilerine sahip işlemcileri üretmekte ve lisanslamaktadır.

Yargıtay da bir kararında yerel mahkemenin cep telefonlarının bilişim sistemine girme suçunun konusunu oluşturmuyacağından bahisle verilen kararı bozmuş, böylece akıllı telefonların bilişim sistemi olduklarını kabul etmiştir¹⁸⁴. Buna ilişkin cep telefonlarının da kendi işletim sistemleri olduğu gerekçe gösterilmiş olsa da söz konusu gerekçeyi yetersiz bulmaktayız. İşletim sistemlerinin yanı sıra bilişim sistemlerine dair diğer unsurların varlığının da araştırılması gerekmektedir.

Akıllı telefon sayılmayan cep telefonlarının ve ankesörlü telefonların bilişim sistemi sayılıp sayılmayacağı ise ayrıca değerlendirilmelidir. Bu aygıtlar, akıllı telefon benzeri donanım unsurlarına sahip olmamakla birlikte telefon ağının bir parçasıdır. Analog telefon ağlarının 1980'li yıllarda sayısal telefon ağına dönüştürülmesi¹⁸⁵ de bu aygıtların bir bilişim sistemine dahil olduğunu göstermektedir. Nitekim sayısal iletişimde sinyaller ikili sayılarla (0 ve 1) kodlanarak uygun gerilimle aktarılır. Sayısal işaretler şifrelenebilir ve kodlanabildiğinden

¹⁸⁴ Buna karşın, kararda yazılı işletim sistemi tanımına katılmamaktayız. "Bilgisayarın çalışmasını düzenleyen tüm programlara işletim sistemi denilmekte olup işletim sistemlerinin sadece bilgisayarlarda değil cep telefonlarında, tablet PC'lerde de kullanılması mümkündür. İşletim sistemleri Windows 8, Android, Linux gibi isimler almaktadır.

Bir bilgisayarın işleyişi ve özellikle de verimliliği, işletim sistemi ile ilgilidir. İşletim sisteminin ana görevi, bilgisayarın çalışması için gerekli komutları vermek ve işlevleri sağlamaktır. Donanım ile yazılım arasındaki bağlantıyı sağlayan işletim sistemi çalışmadığı takdirde bilgisayarın kullanılması, program yüklenmesi olanaksızdır. En çok kullanılan ve en çok bilinen işletim sistemleri aşağıda örneklendirilmiştir.

(Unix - Unix Çeşitleri) (System V, BSD, Solaris, AIX.) (Linux - Linux Dağıtımları) (Pardus, Ubuntu, Fedora, Debian.) (Windows - Windows Sürümleri Windows 7, Windows 8, Windows Server 2012) (MacOS - MacOS/iOS Sürümleri OS X, IOS) (Android)

Windows: Microsoft şirketinin geliştirdiği Windows (pencereler) kullanıcıya grafiklerle ve görsel iletilerle yaklaşarak, yazılımları çalıştırmak, komut vermek gibi klavyeden yazma zorunluluğunu ortadan kaldırarak, dünyada en çok kullanılan işletim sistemidir. En çok kullanılan sürümü Windows 7 olup özellikle tablet PC'ler için Windows 8 geliştirilmiştir.

Apple iOS: iOS eski adıyla (iPhone OS) Apple'ın orjinal olarak iPhone için geliştirdiği ancak daha sonra iPod Touch ve iPad'de kullanılan mobil işletim sistemidir.

Android: Cep telefonlarında ve tabletlerde en çok kullanılan mobil işletim sistemi olan Android'in en yaygın sürümleri 2.3 Gingerbread, 4.0 Ice Cream Sandwich, 4.1 Jelly Bean'dır.

Somut olayda; katılanın cep telefonundan çekilmediği halde sanığın; "Sen H.'i değil, parayı seviyorsun ... kızım seninle görüşmez, bırak kızımın peşini, dolanma peşinde, seni uyarıyorum, H.'in seninle işi olmaz, bir daha bir araya gelmeniz ben hayattayken imkansız" şeklindeki mesajı oluşturduğu ve telefonuna geldiği iddiasıyla boşanma dava dosyasında delil olarak ibraz ettiğinden bahisle açılan davada, sanık suçlamayı kabul etmemiş, bilirkişi raporunda ise iletişim detaylarında suça konu mesajlaşmaya dair kayıt bulunmadığı, ancak cep telefonlarına özel yazılımlar yüklenerek veya internet vasıtasıyla mesaj oluşturulabileceği belirtilerek mesaj çekilen ve mesaj alan cep telefonlarının incelenip, iletişim kayıtlarıyla karşılaştırılması gerektiğinin bildirilmesi karşısında, cep telefonlarında mobil işletim sistemleri bulunduğu ve program yüklenebilmesinin mümkün olduğu gözetilerek, taraflara ait cep telefonları alınıp uzman bilirkişi tarafından incelenip, iletişim kayıtları ile karşılaştırılmak suretiyle program yükleme veya internetten gönderme şeklinde suça konu mesaj gönderilip gönderilmediğinin araştırılması, sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken, cep telefonlarının bilişim sistemine girme ve orada kalma suçunun konusunu oluşturmuyacağından bahisle, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması, yasaya aykırı, katılanın temyiz itirazları bu itibarla yerinde görülmesi olduğundan hükmün bu sebepten dolayı 5320 sayılı Yasanın 8/1. Maddesi uyarınca uygulanması gereken 1412 sayılı CMUK'nın 321. maddesi gereğince bozulmasına 18.03.2015 gününde oybirliği ile, karar verildi." Yargıtay, 8. CD. 2014/30037 E. 2015/14023 K. 18.03.2015 T.

¹⁸⁵ Can/Akın, 2006: 74.

aynı kanalda birden fazla güvenilir haberleşme sağlanabilir¹⁸⁶. Tüm bu nedenlerle cep telefonlarının bilişim sistem aygıtı olarak görülmesi gerekmektedir. Yargıtay da bir kararında ankesörlü telefonları yanıltarak manyetik kartlarla kredi yüklenmesi olayını TCK m. 244/4 kapsamında bilişim sistemlerini bozmak veya verileri değiştirmek suretiyle haksız zarar etme suçu olarak değerlendirmekte¹⁸⁷ ankesörlü telefon ve merkezi sistemini isabetli olarak bilişim sistemi kabul etmektedir.

1.3.3 ATM, Pos, Navigasyon ve Benzeri Cihazlar

ATM (Automated Teller Machine – Otomatik Vezne – Bankamatik), müşterilerin bir banka görevlisi olmaksızın temel işlemleri yapmasını sağlayan bir elektronik bankacılık aygıtıdır¹⁸⁸. Yapısı itibariyle içinde bilgisayar bulunan, para çekme ve yatırma, banka veya kredi kartı girişi gibi aparatlara sahip bir aygıt olduğu söylenebilir. Kendi içinde veri işlem yapan ve dış bağlantı aracılığıyla merkez veritabanı ile bağlantı kuran ATM'lerin bilişim sistemi sayıldığında kuşku bulunmamaktadır. Son yıllara kadar büyük çoğunluğu Windows XP işletim sistemiyle çalışan¹⁸⁹ ATM'ler, ilgili sisteme desteğin kesilmesinden sonra Windows 10 işletim sistemine geçirilmekte, buna ilişkin çalışmalar ATM Industry Association (ATMIA) tara-

¹⁸⁶ <http://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/say%C4%B1sal-ve-analog-ileti%C5%9Fim-ve-internet-eri%C5%9Fim-teknolojileri> (erişim tarihi: 25.02.2019).

¹⁸⁷ “Ankesörlü telefonlar, manyetik kart, kredi kartı ve smart kart ile çalışan hizmet telefonlarıdır. Bu telefonlar katılan Kurum tarafından ücretsiz olarak meydanlar, hastaneler, terminaller, garlar, limanlar, metro istasyonları, askeri tesisler, Toplu konut alanları gibi halka açık yerlere tesis edilmekte, ARMS olarak adlandırılan merkezi bilgisayar sistemi ile yönetilmektedir. ARMS sisteminin, suçun işlendiği bölgede hizmet veren ve kendisine bağlı olan 200 adet D-3 manyetik kartlı ankesör makinesinin çalışma bilgilerini, (kullanılan kontör miktarı, manyetik karta ait barkot numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi v.s) bünyesinde tokatladığı anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkot numaraları dahi bu sayede tespit edilebilmiştir. Suç tarihinde kullanılan sistemin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura ihtiyaç vardır. Bunlardan birincisi, manyetik telefon kartı, diğeri ise kontör olarak adlandırılan kredidir. Bunlara sahip olunmadan, bir bilgi işlem biriminin parçası olan ve ARMS denilen sisteme bağlı bulunan ankesörlü makinelerden, Kurum'ca acil durumlarda kredisiz görüşme yapılabilmesine olanak sağlanmış bulunan sınırlı sayıdaki numara dışında görüşme yapılabilmesine olanak yoktur. Bu sistemde, manyetik kart üzerindeki barkodu okuyan makine, manyetik kart üzerinde kullanılmış kredi bilgileri bulunmadığı takdirde, okuduğu kartın kredi sınıflandırma özelliklerine göre 100, 60 veya 30 kontör kredi yüklemesi yapmak suretiyle kullanıma hazır hale getirmekte, kullanım süresince yaptığı hesaplamaların sonucuna göre kalan kredi miktarını saptayıp manyetik karta işlemektedir. Başka ifadeyle sistem, makineye takılan karttaki verilerin alınıp değerlendirilmesi suretiyle işlemektedir.

Somut olayda sanığın, kredisiz bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasası'nın 525/B maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren 5237 sayılı Türk Ceza Yasası'nın 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır. Uygulamada hangi Yasanın daha lehe sonuç verdiği hususu da Yerel Mahkemece değerlendirilip saptanmalıdır.” Yargıtay CGK. 2007/6-136 E. 2007/150 K. 19.06.2007 T.

¹⁸⁸ <https://www.investopedia.com/terms/a/atm.asp> (erişim tarihi: 25.02.2019).

¹⁸⁹ Yakın zamana kadar bankamatiklerin % 95'inin Windows XP işletim sistemiyle çalıştığı söylenmektedir. <https://www.webtekno.com/yazilim/bankamatiklere-yakinda-windows-10-isletim-sistemi-gelecek-h8015.html> (erişim tarihi: 25.02.2019).

findan sürdürülmektedir¹⁹⁰. Hatta ATM'ler bilişim suçlarına ilişkin önemli bir alan oluşturmaktadır. Örneğin, ATM'lerde bulunan kulaklık girişinden, az da olsa veri aktarımı gerçekleştirilmesi nedeniyle sistemlere izinsiz yazılımlar yüklendiği ve sistem açıklarından faydalandığı ileri sürülmektedir¹⁹¹.

Yargıtay eski tarihli bir kararında ATM'nin bilişim sistemi sayıldığını ve başkasına ait kart ve şifre ile para çekilmesi eyleminin bilgileri otomatik işleme tabi tutmuş olan sistemi kullanarak hukuka aykırı yarar sağlama suçunu oluşturduğu söylemektedir¹⁹².

Pos, hologram ve navigasyon gibi belli bir amaç için özgülenmiş diğer elektronik aygıtların da bilişim sisteminin unsurlarını taşıması halinde bilişim sistemi sayılması gerektiğini düşünmekteyiz¹⁹³. Aksi düşüncede genel amaçlı kullanım kriterinin benimsenmesi halinde bu aygıtlar bilişim sistemi sayılmayacak ve çelişkili bir durum oluşacaktır.

1.3.4 Elektronik Ev Eşyaları

Akıllı ev kavramı 1990'lı yılların başından itibaren literatüre girmeye başlamıştır. "Home Networking" adı verilen teknoloji ile internete bağlı olan evde tüm aygıtların birlikte çalıştırılması ve onları internete bağlayacak bir ağ geçidi bulunması planlanmaktadır. Bu sayede örneğin çamaşır makinelerine güncel yıkama programları kendiliğinden indirilebilecektir. Akıllı ev aygıtları altı alt başlıkta incelenmektedir. Bunlar akıllı ev ağ bağlantısı, akıllı ev otomasyonu, akıllı ev aletleri, akıllı evde eğlence teknolojisi, akıllı ev tıbbi teknolojileri ve akıllı ev mobil teknolojisidir¹⁹⁴. Bunların bazıları günümüzde kullanılabilir durumdayken, bazıları ile ilgili çalışmalar ise halen devam etmektedir. Bu tür akıllı ev teknolojileri de gerekli unsurları taşıdığından bilişim sistemi sayılmaktadır.

1.3.5 Robotik Çalışmalar, Yapay Zekâ, Otonom Ağır Sanayi ve Benzeri Cihazlar

Bilişim teknolojileri yalnızca bilgisayar ve akıllı telefonlar gibi yaygın aygıtların gelişimiyle değil, teknolojinin sınırlarını zorlayan sistemlerle de yakından ilgilenmektedir. Robotik ve tıbbi çalışmalar ile otonom ağır sanayi bu sistemlere örnek verilebilir. Hatta yapay zekâ barındıran her sistemin doğrudan bilişim sistemi sayıldığını söylemek yanlış olmayacaktır. Bu kavramları detaylarına inmeden açıklamakta fayda vardır.

İlk kez 1956 yılında Dartmouth Üniversitesi'nin bir yaz konferansında kullanılan yapay zekâ kavramı, günümüzde birbirinden çok farklı becerilere sahip aygıtlar olarak karşılık

¹⁹⁰ <https://www.atmia.com/news/is-your-atm-prepared-for-the-windows-10-migration/5760/> (erişim tarihi: 25.02.2019).

¹⁹¹ <https://prezi.com/zr2bjeshzcot/atmlerin-isletim-sistemleri/> (erişim tarihi: 25.02.2019).

¹⁹² Yargıtay CGK. 2001/6-30 E. 2001/57 K. 10.04.2001 T.

¹⁹³ Benzer yönde, Apaydın, 2015: 17.

¹⁹⁴ Can/Akın, 2006: 75 – 76.

bulmaktadır. Buna karşın yapay zekâ tanımı bazen sadece daha başarılı bir reklam kampanyasının malzemesi olmakta, aslında ortada bilinen anlamda bir yapay zekadan söz edilememektedir. Bu nedenlerle yapay zekâ kavramını üçe ayırmak mümkündür.

İlk grupta görünüşte yapay zekaya sahip aygıtlar bulunmaktadır. Öyle ki bu aygıtlar oldukça çok sayıda ihtimale karşı hazırlıklı bulunsa da, bunlar aslında kendisine önceden öğretilmiş ve kodlanmış halde bulunmaktadır. Örneğin bir satranç yazılımı binlerce, belki milyonlarca hamleyi hesap edebilmesine karşın, bunu kendisi öğrenmemiş, bir algoritma aracılığıyla öğretilmiştir. Yani yazılımın öğretilenin dışındaki bir hamlede bulunması mümkün olmamaktadır.

İkinci gruptaki dar kapsamda yapay zekaya sahip cihazlar ise “makine öğrenimi” ilişkisiyle çalışmaktadır. Buna göre aygıtlar aktif bir şekilde öğrenebildiğinden, aynı olayın tekrarlanması halinde yeni öğrendiği ve daha isabetli sonucu uygulaması mümkün olmaktadır. Buna örnek olarak Google’ın AlphaGo ürünü verilebilir. Kentilyonlarca hamle bulunan go oyununa ilişkin bu yazılıma hamleler tek tek kodlanmamış, bunun yerine yazılımda kendi hatalarından ders çıkaracak bir algoritma kullanılmıştır. Bunun sonucunda kendi kendine milyonlarca maç yapan yazılım oyunu daha doğru oynamayı öğrenmiş ve 2016 yılında oyunun büyük ustasını yenmeyi başarmıştır¹⁹⁵.

Üçüncü gruptaki geniş kapsamda yapay zekaya sahip cihazlar ise aslında ikinci grupta olan cihazlarla aynı kategoridedir. Onlardan farkı ise yalnızca tek bir konuda değil, her konuda öğrenebilme yeteneğine sahip olmalarıdır. Henüz insan beynine rakip eşdeğer bir örneği görülememiş olsa da, Terminatör vb. bilimkurgu filmlerinde sıklıkla karşımıza çıkmaktadır.

Robotlar ise verilen görevleri ya doğrudan insan gözetimi altında önceden tanımlanmış bir programa göre ya da yapay zekâ tekniklerini kullanarak genel ilkeler çerçevesinde yapan mekanik bir aygıttır¹⁹⁶. Bilişim suçları bakımından tartışılması gereken konu ise hangi robotların bilişim sistemi içerisinde sayılıp sayılmayacağıdır. Çünkü farklı ülkelerin farklı standartlarına göre en basitinden en karmaşığın birçok aygıt robot olarak kabul edilebilmektedir¹⁹⁷. Gerçekten de robot denilince akla yalnızca insan veya hayvanlara benzeyen akıllı aygıtlar gelmemelidir. Sanayilerde kullanılan ve kol biçimindeki aygıtlar, muayene ve yıkım amaçlı

¹⁹⁵ Ekşioğlu, 2018: 19 – 20.

¹⁹⁶ Akın, 2006: 671.

¹⁹⁷ Örneğin, Japon Sanayi Robotları Birliği’nin robot sınıflandırmasına göre 6 sınıf robot vardır. Bunlar (1.) Bir işletmen tarafından elle hareket ettirilen çok serbestlik dereceli bir aygıt (2.) Bir görevin ardışık adımlarını önceden belirlenmiş değişmeyen bir yöntemle göre yapan ve değiştirilmesi zor olan bir aygıt (3.) Sınıf 2’ye benzeyen ancak değiştirilmesi kolay olan aygıtlar (4.) İnsan işletmenin robotu yönlendirmesiyle görevi elle yapan robot adımları sonradan yapmak üzere kaydeder. Sonrasında aynı hareketleri kaydedilmiş bilgiye göre tekrarlar (5.) İşletmen robota görevi elle öğretmek yerine bir hareket programı verir (6.) Çevresini anlamak için gerekli olanaklara ve bir görevi görevin yapılacağı çevredeki koşullardaki değişikliklere karşın başarıyla tamamlayabilme becerisine sahip olan bir robot. Akın, 2006: 671.

farklı biçimlerdeki aygıtlar da teknik anlamda birer robottur. Bu noktada bilişim bilimini tanımlarken kullandığımız “beşerî yetiden üstün yöntem” kıstasını kullanmak gerektiğini düşünmekteyiz. Buna göre mühendislik anlamında robot olarak sayılan ancak yalnızca bazı mekanik hareketlerden ibaret olan (beşerî yetiden yalnızca kaba kuvvet anlamında önde olan) aygıtlar bilişim suçlarının konusu kabul edilmemelidir. Bununla birlikte veri işleyen veya yapay zekâ aracılığıyla öğrenme becerisine sahip aygıtlar bilişim sistemi olarak kabul edilmelidir. Günümüzde yapay zekâ sayesinde kendiliğinden merdiven inip çıkabilen, tekme atıldık-tan sonra ayağa kalkabilen veya engellerin üzerinden atlayabilen insansı robotlar¹⁹⁸ ile çeşitli gezegenlerde keşif yapan ve numune toplayan robotlar¹⁹⁹ bilişim sistemlerinin bugünkü üst sınırlarını oluşturmaktadır.

1.3.6 Bulut Sistemler

Bulut sistemler son yıllarda sıklıkla karşımıza çıkmaya başlayan bir kavram olup, ne olduğu açıklanmadan önce sanallaştırma kavramı incelenmelidir. Bilindiği gibi bilgisayarlar açık bulunduğu zaman boyunca her zaman tam kapasite ile çalışmazlar. Oyun oynarken, internet sitelerinde haber okurken veya ofis işlerini bilgisayar üzerinde yaparken, bilişim sistemlerinin yalnızca belli bir bölümü kullanılır. İşte sanallaştırma kavramı da kaynakların verimli kullanılması amacıyla ortaya çıkmıştır. Bir işletim sisteminin bir yazılım kullanılarak sanal ortamda iki veya daha fazla bilgisayarmış gibi mantıksal olarak parçalara ayrılmasına sanallaştırma denilmektedir²⁰⁰. Masaüstü sanallaştırması, ağ sanallaştırması, donanım sanallaştırması ve depolama sanallaştırması olarak dört ana başlıkta incelenmektedir²⁰¹. Tüm bu kategorilerin ortak amacı, aygıtların veya ağ genişliğinin parçalara bölünerek en verimli şekilde kullanılabilmesinin sağlanmasıdır.

Bulut bilişim de sanallaştırmanın kullanıldığı, ancak sanallaştırmadan daha geniş bir kavramdır. Bulut bilişim, kullanıcının taleplerine göre arttırılabilen veya azaltılabilen oranda, bir ağ üzerinden bilişim kaynaklarının sağlanması hizmeti şeklinde tanımlanmaktadır. Bir sistemin bulut özelliğini taşıması için genel olarak 5 kriter aranmaktadır. Bunlar geniş ağ erişimi, kesintisiz ve beklemeksizin kullanıcıya hizmet verme, esneklik (bulut sistemin ilgili bölümünde taleplerin artması halinde diğer bölümlerden o bölüme kaynak aktarılması), kulla-

¹⁹⁸ <https://www.bostondynamics.com> (erişim tarihi: 25.02.2019).

¹⁹⁹ Mars'ta görev yapan Curiosity isimli robot hakkında, https://www.nasa.gov/mission_pages/msl/index.html (erişim tarihi: 25.02.2019).

²⁰⁰ Bozkurt Yüksel, 2016: 22.

²⁰¹ <https://azure.microsoft.com/tr-tr/overview/what-is-virtualization/> (erişim tarihi: 25.02.2019).

nıcıların istedikleri zaman hizmet modelini değiştirebilmesi ve hizmetin ölçülerek kullanıldığı kadar ödeme imkanının sağlanmasıdır²⁰².

Bulut sistemler coğrafi olarak değişik yerlere dağıtılan bilgisayarların işlemci güçleri, ağ kapasiteleri ve depolama kapasiteleri ile büyük bir sistem haline geldiğinden birçok avantaj barındırmaktadır. Kaynaklar anlık olarak aktarılabildiğinden, sistem verimli kullanılmakta, bu da maliyetleri düşürmektedir²⁰³. Yine verilerin farklı yerlerde yedeklenmesi daha kolay sağlanabildiğinden veri kaybının meydana gelmesi zorlaştırılmaktadır. Uygulamalar bulut ortamında yer aldığından (kişisel bilgisayara herhangi bir uygulama kurulumu gerektirmediğinden) güncelleme ve versiyon uyumsuzlukları da yaşanmamaktadır. Buna karşın, sistemin ağ bağlantısı olmadan erişilememesi ve dağıtılmış vaziyette olduğundan bilişim korsanlarına karşı daha açık hedef haline gelmesi dezavantajları olarak sayılmaktadır²⁰⁴. Microsoft Azure, Google Drive Apple iCloud gibi çözümler ve UYAP sistemi bulut sistemlere örnek olarak gösterilmektedir.

Tüm bu açıklamalar karşılığında bulut sistemlerin bilişim sistemi sayıldığına şüphe yoktur. Hatta bulut sistemin tanımı, bilişim sistemi unsurlarını kendi bünyesinde harmanlamaktadır. Burada tartışılması gereken husus ise bulut bilişimin bilişim sistemi olarak sınırlarıdır. Örneğin bir bulut sisteme yapılan saldırıda kaç sistem olduğu varsayılmalı ve kaç mağdurdan söz edilmelidir? Bu durumu yakın zamanda gerçekleşen bir örnekle açıklayabiliriz. 2014 yılında Apple iCloud platformuna gerçekleşen saldırıda birçok ünlünün fotoğrafları ele geçirilmişti. Yapılan açıklamada ise “Find my iPhone” uygulamasında yaşanan bir açıktan kaynaklı olarak kaba kuvvet (brute force) saldırısı gerçekleştirildiği, yani seri olarak parolaların denenerek doğru parolanın bulunduğu söylenmiştir²⁰⁵. Burada her ne kadar bulut uygulamadaki açıktan faydalanılsa da, sonuçta her bir kullanıcının bulut sisteme erişmek için bir aygıt (iPhone) kullandığı göz ardı edilmemelidir. Bulut sistemler görünürde tek bir sistem olmakla birlikte, gerçekte kullanıcı sayısı kadar farklı erişim aygıtı ve bilişim sistemi bulunmaktadır. Bu nedenle saldırı yapılan her bir kişi suçun ayrı ayrı mağdurdur ve farklı eylemler gerçekleştiğinden zincirleme suç koşullarının oluşmadığı da gözetilmelidir.

²⁰² Bozkurt Yüksel, 2016: 22 – 23.

²⁰³ Sosyal medya sitelerinin gelişiminin ardından maliyetlerin düşürülmesi, e-ticaretin gelişimine katkıda bulunması ve istihdama olan etkisi nedeniyle bulut sistemler birçok devletin bilgi iletişim politikalarında öncelikli hale gelmiştir. Henkoğlu/Külcü, 2013: 63.

²⁰⁴ Bozkurt Yüksel, 2016: 38.

²⁰⁵ <https://www.webtekno.com/sosyal-medya/icloud-nasil-hacklendi-h2966.html> (erişim tarihi: 13.01.2019).

1.4 Bilişim Sistemi Aktörleri

Yapabildiği muazzam işlere karşın, bilişim sistemleri geliştirilirken yüksek miktarda yatırımlara ihtiyaç duymaktadır. Ayrıca birçok işlevi yerine getirebilen bu sistemler, genellikle kullanıcıların o anki isteklerine göre çalışacak şekilde tasarlanmaktadır. Tüm bu durumlar da bilişim sistemleri üzerinde farklı yönlerden aktörlerin yer aldığını göstermektedir.

Bilişim sistemi aktörleri, bilişim suçlarında mağdur ve suçtan zarar görenin belirlenmesi ile bu suçlarda fikri içtima konusunda özellik gösterdiğinden detaylı şekilde incelenecektir.

1.4.1 Mülkiyet ve Fikri Mülkiyet Yönünden

Bilişim sistemlerinin ve özellikle verilen mülkiyetinin her bir somut olay için tespit edilmesi zorluk göstermiş ve öğretilerde tartışmalara neden olmuştur. Mülkiyet konusunda ileri sürülen bazı kriterler bulunmaktadır. Bunlar, verileri hukuka uygun olarak iktisap eden kişinin tasarruf yetkisine sahip olması, verilerin kendisi hakkında bir şeyler söylediği kişinin yetkiye sahip olması, veri taşıyıcısına (USB bellek, CD vb.) sahip olan kişinin veri üzerinde yetkiye sahip olması, verileri üreten fikri hak sahibinin aynı zamanda tasarruf yetkisine de sahip olması, verilerin yüklenmesini veya nakledilmesini sağlayan kişinin tasarruf yetkisine sahip olmasıdır. Bu kriterlerin tamamı eleştirilmiş, hiçbirinin tek başına yeterli olmadığı ifade edilmiştir²⁰⁶. Bununla birlikte her bir somut olay için bu kriterlerin bir veya birkaçının birlikte kullanılmasında fayda bulunduğu da bir gerçektir.

1.4.1.1 Geliştirici

Geliştiriciler, bilişim sistemi unsurlarını vücuda getirenler olarak kabul edilebilir. Ürünleri ticari veya gönüllülük esaslarına göre son kullanıcıların hizmetine sunarlar.

Hızla gelişen bilişim sektöründe, geliştiriciler de uzmanlık alanlarına ayrılmak durumunda kalmıştır. Bunların içerisinde en kolay fark edilenleri donanım üreticileridir. Milyar dolarlar ile ölçülen yatırım ve üst düzey teknoloji gereksinimleri nedeniyle ancak az sayıda firma bu performans rekabeti içerisine girebilmektedir. Yazılım geliştiricileri arasında ise durum tam tersidir. Günümüzde büyük işletim sistemi geliştiricileri, kendi sistemleri için uygulama üretecek sayısız geliştirici bulma peşindedir. “Üçüncü parti yazılım geliştiricileri” olarak anılan bu geliştiriciler, aslen bir ara tabaka oluşturmakta ve mevcut sistem ile son kullanıcı

²⁰⁶ Akbulut, 2017: 186.

arasındaki köprüyü kurmaktadır²⁰⁷. Yazılım geliştiricileri de kendi aralarında arayüz ve grafik çalışmalarına yoğunlaşan tasarımcılar, pratik kodlama üzerine yoğunlaşan programlayıcılar (kodlayıcı) ve yazılım hatalarını test ederek bulma üzerine uzmanlaşmış test mühendisleri olarak ayrılmaktadır.

1.4.1.2 Son Kullanıcı

Son kullanıcılar, bilişim sistemleri üzerinde bir fonksiyon değişikliği gerçekleştirmeyen, sistemden mevcut özellikleri dahilinde faydalanan kişilerdir. Genellikle geliştiriciler ile aralarında bir lisans vb. sözleşme bulunur. Geliştiricilerin de vücuda getirdikleri bilişim sistemleri üzerinde aynı zamanda son kullanıcı sıfatı taşıması mümkündür.

Mevzuatta son kullanıcı terimine de yer verildiği görülmektedir. Elektronik Haberleşme Kanunu'nun 3. maddesinde son kullanıcı, “elektronik haberleşme hizmeti ve/veya elektronik haberleşme şebekesi sağlamayan gerçek veya tüzel kişileri” tanımlamaktadır. Yine VIII Beş Yıllık Kalkınma Planı Hazırlık Çalışmalarına Ait Genelge’de “son kullanıcı olan tüketici yararı” deyimine yer verildiği görülmektedir.

Son kullanıcı kavramı, tüketici kavramı ile benzerlik gösterse de bazı farklar barındırmaktadır. Tüketici, ticari veya mesleki olmayan amaçlarla kullanımı ifade etmekte, son kullanıcı ise daha kapsayıcı bir kavram olup amaç fark etmeksizin kullanımı ifade etmektedir²⁰⁸.

1.4.1.3 Erken Erişim (Beta) Kullanıcılarının Durumu

Erken erişim kullanıcıları, henüz tamamlanmamış bir donanım veya yazılımın geliştirme sürecine dahil olan kişileri tanımlamak amacıyla kullanılmaktadır. Bu kullanıcılar donanım ve yazılıma diğer kişiden daha önce erişme ve deneyimleme şansı elde etmekteyken, geliştiriciler ise erken erişim kullanıcılarının geri dönüşleri ve kullanım sırasında elde ettikleri diğer verilerle geliştirme sürecini tamamlamaktadır. Bazı durumlarda ise erken erişim kullanıcıları vermiş oldukları ücretle ürünün hem tamamlanmadan önceki hem de tamamlandıktan sonraki kullanım haklarını elde etmektedir. İki tarafın da faydasına olan bu yöntem günümüzde gittikçe artan bir oranda uygulanmaya devam etmektedir.

Erken erişim kullanıcıları her ne kadar geliştirme sürecine dahil olarak sistem işlevini yönlendirme şansına sahip olsa da, sistemin tamamlanmış bölümü üzerinde son kullanıcı olarak kabul edilmelidir. Bununla birlikte sistemin tamamlanmaması nedeniyle geliştiricinin ih-

²⁰⁷ 2017 yılı itibarı ile Google Play Store’da yer alan uygulama sayısının 2 milyon 800 bin adedi geçtiği söylenmektedir. <http://teknolojituru.com/2017/07/05/uygulama-magazalarinda-kac-milyon-uygulama-var/> (erişim tarihi: 16.02.2018).

²⁰⁸ Nitekim Elektronik Haberleşme Kanunu’nda ayrı ayrı tanımlanan son kullanıcı ve tüketici kavramları arasındaki farktan da bu sonuç çıkarılabilmektedir.

mali veya icrai davranışla veri üzerinde TCK m. 244/2’de yer alan eylemleri gerçekleştirmesi halinde suçun unsurları oluşmayacaktır.

1.4.2 Yetki ve Sorumluluk Yönünden

1.4.2.1 Genel Olarak

İnternet erişimi, kullanıcıların gözünde bir bilgisayar ve modemden ibaret olsa da, gerçekte çok daha karmaşık bir yapıya sahiptir. Çok sayıda kullanıcının farklı isteklerinin oluşturduğu internet trafiğini ayarlayabilmek için güçlü bir altyapıya ihtiyaç vardır. İşte, kullanıcıları internet ortamına dahil eden bu kurumlar internet erişim sağlayıcıları olarak anılmaktadır.

1.4.2.2 Türk Hukukunda Bilişim Ağları Üzerindeki Aktörler

1.4.2.2.1 İnternet Erişim Sağlayıcı

5651 sayılı İÖYYDK’nin 2/1-e bendinde erişim sağlayıcılar “Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek ve tüzel kişi” olarak tanımlanmıştır. Bu tanımdan da anlaşıldığı üzere erişim sağlayıcılar içerikten değil, içeriğe ulaşabilmek için aracı olmaktan sorumludur²⁰⁹. Bu durum yine aynı kanunun 6/2 fıkrasında “Erişim sağlayıcı, kendisi aracılığıyla erişilen bilgilerin içeriklerinin hukuka aykırı olup olmadıklarını ve sorumluluğu gerektirip gerektirmediğini kontrol etmekle yükümlü değildir.” denilerek açıkça vurgulanmıştır. Bununla birlikte özel hukuktaki sorumluluk bakımından içerik ile ilgili hukuksal bir sorun olduğunu bilen ve teknik açıdan mümkün, kendisinden beklenebilecek bir davranışı gerçekleştirmeyen erişim sağlayıcıların da sorumlu olacağı kabul edilmektedir²¹⁰.

Erişim sağlayıcılar, çevirmeli hatlar, kablolu veya kablosuz geniş bant bağlantıları gibi hizmetlerle kullanıcıların internete erişimini sağlar. Genel olarak da bu hizmet kullanıcı ile erişim sağlayıcı arasında bir abonelik sözleşmesiyle ücret karşılığı olarak verilmektedir²¹¹. Erişim sağlayıcıların aynı zamanda verecekleri başka hizmetler aracılığı ile yer veya içerik sağlayıcıları olmalarında da bir engel bulunmamaktadır.

Türkiye Cumhuriyeti sınırları içerisinde erişim sağlayıcı olabilmek için BTK’den faaliyet izin belgesi alınması gerekmektedir²¹². 5651 sayılı kanunda her ne kadar gerçek ve tüzel kişilerin erişim sağlayıcı olabileceği belirtilmiş olsa da, ilgili yönetmelikte²¹³ sadece sermaye

²⁰⁹ Sınar, 2001: 42.

²¹⁰ Öztan, 2008: 631.

²¹¹ Doğu, 2016: 17.

²¹² Bu gereklilik ilk kez 2001 yılında yayımlanan Telekomünikasyon Hizmetleri Yönetmeliği’nde düzenlenmiş olup, öncesinde bir lisans veya ruhsat süreci söz konusu değildir. Avşar/Öngören, 2010: 118.

²¹³ Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesi-ne İlişkin Usul ve Esaslar Hakkında Yönetmelik, 24.20.2007, RGS: 26680.

şirketlerinin başvurusu düzenlenmiş, gerçek kişilere ilişkin bir düzenlemeye yer verilmemiştir. Bu bakımdan mevcut durumda sadece yönetmelikte yer alan şartları taşıyan sermaye şirketlerinin erişim sağlayıcı olabileceği görülmektedir. Güncel olarak faaliyette bulunan internet erişim sağlayıcılar BTK'nin sitesinde listelenmektedir²¹⁴.

1.4.2.2.1 Erişim Sağlayıcıları Birliği

5651 sayılı kanuna 2014 yılında eklenen 6/A maddesi uyarınca Erişim Sağlayıcıları Birliği kurulmuştur. Birlik, 5809 sayılı EHK kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmecilerin katılmasıyla oluşur ve koordinasyonu sağlama amacı güder.

Erişim sağlayıcıları birliği 5651 sayılı kanunun 8. maddesi dışında kalan erişimin engellenmesi kararlarını yerine getirir. Birliğe yapılan tebligatlar tüm üye erişim sağlayıcılarına yapılmış sayılır. Birliğe üye olmayan erişim sağlayıcıları faaliyette bulunamaz. (5651 SK m. 6A/5,6,7,10)

Erişim Sağlayıcıları Birliği'nin kurulmasına ilişkin yasa değişikliği hakkında iptal istemiyle Anayasa Mahkemesi'ne başvurulmuş, mahkeme ESB'nin kurulmasına ilişkin düzenlemenin anayasaya aykırı olmadığına karar vermiştir²¹⁵. Anayasa Mahkemesi, kararında ayrıca ESB'nin vakıf, dernek veya kamu kurumu niteliğindeki meslek kuruluşları kapsamında değerlendirilemeyeceği, idari teşkilat yapısı içinde yer almayan, kanunla kurulmuş kendine özgü bir kurum olduğunu söylemiştir. ESB'nin internet sitesinde ise birliğin özel hukuk tüzel kişiliğine sahip olduğu ifade edilmiştir²¹⁶.

1.4.2.2.2 İnternet Yer Sağlayıcı

5651 sayılı İÖYYDK'nin 2/1-m bendinde yer sağlayıcı “Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişiler...”dir. Yer sağlayıcıların da yurarda erişim sağlayıcılarda bahsedildiği gibi BTK'den faaliyet izin belgesi alması gereklidir. Erişim sağlayıcılardan farklı olarak gerçek kişilerin de yer sağlayıcı belgesi alabileceği faali-

²¹⁴ <http://yetkilendirme.btk.gov.tr/> (erişim tarihi: 11.04.2019). Toplamda 273 erişim sağlayıcının faaliyetine devam ettiği görülmektedir.

²¹⁵ Anayasa Mahkemesi, 2014/87 E. 2015/112 K. 08.12.2015 T. RGT: 28.01.2016, RGS: 29607. Verilen karşı oyun gerekçesinde ESB'ye yapılan tebligatın tüm üyelere yapılmış sayılacağına ilişkin düzenlemenin hukuk güvenliği ve adil yargılama ilkelerine uygun olmadığı söylenmiştir. Günümüzde e-tebligat uygulamasının gide-rek yaygınlaşması ve tüm erişim sağlayıcılara tebligat yapmanın kolay hale gelmesi de bu karşı oyun geçerliliğini arttırmaktadır.

²¹⁶ <https://www.esb.org.tr/biz-kimiz> (erişim tarihi: 28.07.2018).

yet yönetmeliğinde gösterilmektedir. Güncel yer sağlayıcıları listesi de BTK'nin internet sayfasında yayınlanmaktadır²¹⁷.

Yer sağlayıcıları bir kütüphane gibi düşünmek mümkündür. Bir kütüphanenin kitapları (içeriği) depolayacak bir yere ve kullanıcıların kolay ve hızlı şekilde aradığı kitaba ulaşabileceği sisteme ihtiyacı vardır. Dolayısıyla yer sağlayıcılar sadece kendi birkaç kitabını saklayan küçük ölçekli bir kütüphane olabileceği gibi, belli bir depolama ücreti karşılığı herkesin erişime sunduğu kitaplarını barındıran devasa bir yapı da olabilir.

Yer sağlayıcılar içerikleri fiziksel yapılar içinde barındırdıklarından, içeriğe erişebilmek için sistemin de sürekli açık bulundurulması gerekmektedir²¹⁸. Aksi halde sağlıklı bir internet erişimine sahip olunsu bile içeriğe erişmek mümkün olmayacaktır. Günümüzde profesyonel yer sağlayıcılar, kendilerinden hizmet alan kullanıcılara gerçek zamanlı olarak %99'un üzerinde sunucularını açık bulundurmayı taahhüt etmektedirler.

İçeriğe ulaşılabilen fiziksel sunucuları barındıran yer sağlayıcılara, sahip oldukları yetkiler dolayısıyla bazı sorumluluklar da yüklenmiştir. Yer sağlayıcılar 5651 sayılı kanunda ve uygulama yönetmeliğinde yer alan hükümler çerçevesinde BTK başkanlığı, adli makamlar veya hakları ihlal edilen kişiler tarafından hukuka aykırı içeriklerden haberdar edildiği takdirde teknik olarak engelleme imkânı bulunduğu ölçüde içeriği yayından kaldırmakla yükümlüdür. Ayrıca, trafik bilgilerini altı ay²¹⁹ saklamakla, bu bilgilerin doğruluğunu ve bütünlüğünü zaman damgaları ile birlikte saklamak ve gizliliğini temin etmekle de yükümlü tutulmuşlardır.

Yer sağlayıcıların özel hukuktaki sorumluluğu dar tutulmaktadır. Erişilebilir kılınan içeriğin hukuka aykırı olduğundan haberi olmayan yer sağlayıcının sorumluluğunun söz konusu olmadığı, ancak haberdar olması halinde derhal harekete geçerek bilginin silinmesi veya erişimine engel olunması gerektiği ifade edilmektedir²²⁰.

6518 sayılı kanunun 88. maddesiyle 5651 sayılı kanunun 5. maddesine eklenen 5 fıkra uyarınca yer sağlayıcılar BTK başkanlığının talep ettiği bilgileri teslim etmekle ve belirtilen tedbirleri yer almakla yükümlü tutulmuşlardır. Ancak bu düzenleme Anayasa Mahkemesi tarafından iptal edilmiş²²¹, daha sonra 671 sayılı Olağanüstü Hal Kapsamında Bazı Kurum ve

²¹⁷ <https://www.btk.gov.tr/ticari-amacli-hizmet-verenler-yer-saglayici-listesi> (erişim tarihi: 28.07.2018). Kendi bünyesinde hizmet veren 299 ve ticari amaçlı hizmet veren 1198 yer sağlayıcı olduğu görülmektedir.

²¹⁸ Gül, 2016: 26.

²¹⁹ 30.11.2017 tarihinde Resmî Gazetede yayımlanan uygulama yönetmeliği uyarınca yer sağlayıcılara trafik bilgilerini 6 ay saklama yükümlülüğü verilmiş ise de 19.02.2014 tarihinde 5651 sayılı kanunda yapılan değişiklik ile, trafik bilgilerinin 1 yıldan az ve 2 yıldan fazla olmamak üzere yönetmelikle belirlenecek bir süre kadar saklamakla yükümlü olduğu belirtilmiştir. Normlar hiyerarşisinin daha üst basamağında yer alan (lex superior) ve sonraki tarihli düzenleme (lex posterior) niteliği taşıyan kanun hükmü karşısında yönetmelik hükmünün uygulama alanı kalmamaktadır. Bu bakımdan yönetmelikte gerekli düzenlemelerin yapılması gerekmektedir.

²²⁰ Öztan, 2008: 631.

²²¹ Anayasa Mahkemesi, 2014/87 E. 2015/112 K. 08.12.2015 T. RGT: 28.01.2016, RGS: 29607.

Kuruluşlara İlişkin Düzenleme Yapılması Hakkında Kanun Hükmünde Kararname ile bilgileri talep etme yetkisi başkan yerine kuruma verilmiştir.

Son olarak, belli donanımı sağlayabilen herkesin kolaylıkla bir sunucuya (server) sahip olduğu düşünüldüğünde, BTK'ye bildirilmemiş çok sayıda yer sağlayıcının da internet ortamında aktör olarak varlığının göz ardı edilmemesi gerektiği söylenmelidir.

1.4.2.2.3 İnternet İçerik Sağlayıcı

5651 sayılı kanunun 2/1-f bendine göre içerik sağlayıcı, internet ortamı üzerinden kullanıcılarına sunulan her türlü bilgi veya veriyi üreten, değiştiren veya sağlayan gerçek ve tüzel kişidir. Servis ve yer sağlayıcıların aksine, içerik sağlayıcıların bir izin belgesi bulunması şart olmamakla birlikte, esasen bir teknik bilgi ve özel bir donanıma sahip olmaları dahi gerekli değildir. Bu bakımdan içerik sağlayıcılar kitap yazarları olarak düşünülebilir, kitapların hangi ebatta ve hangi malzeme ile basılacağı veya hangi kütüphanede depolanacağı konusunda bir tercihte bulunabilir (yer sağlayıcı seçebilir) ancak kitabının içeriği dışında (basımı ve dağıtımı gibi) bir sorumluluk üstlenmez.

Kanun, içerik bakımından bir kısıtlamada bulunmamış ve “her türlü bilgi veya veri” den bahsetmiştir. Bu kapsamda kendi web sitesi içeriğini hazırlayan kişilerden, bir forumda makale paylaşımdan, sosyal medya sitelerinde paylaşım yapanlardan, haber ve forum içeriklerine yapılan yorum yapan kişilerin tamamı içerik sağlayıcısı statüsündedir²²².

İçerik sağlayıcıların özel hukuk yönünden geniş sorumluluklara sahip olduğu kabul edilmektedir. İçerik sağlayıcı kendisine mal ettiği, kendisine veya başkasına ait içeriği kaydettiği veya hizmete hazır tuttuğundan sınırsız sorumlu olduğu, gerekli kontrol ve özeni göstermek durumunda ve eser hakkında bağlantılı hak sahiplerinin de maddi ve manevi haklarına saygı göstermek zorunda olduğu belirtilmektedir²²³.

İçerik sağlayıcı bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak sunuş biçiminden içeriği benimsediği ve içeriğe ulaşılmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur. (5651 SK m. 4/2) Bununla birlikte çoğu zaman aynı içeriğin farklı web sitelerinde herhangi bir bağlantı veya alıntı ibaresi olmaksızın yer aldığı görülmektedir. Öyle ki, kopyala – yapıştır yöntemiyle alınan bu içeriklerde yazım hataları dahi aynı olabilmektedir. Bu durumda fikri mülkiyete ilişkin hakları ayrı tutarak, 5651 sayılı kanunun kapsamı geniş tuttuğu gözetilerek her bir kişinin içerik sağlayıcı olduğunun kabulü uygun olacaktır. Nitekim burada kişilerin amacı başkasına bağlantı sağlamak değil, o içeriği kullanıcıların hizmetine sunmaktır.

²²² Doğu, 2016: 18; Gül, 2016: 26.

²²³ Öztan, 2008: 630.

1.4.2.2.4 Toplu Kullanım Sağlayıcılar

5651 sayılı kanunun 2/1-i bendine göre kişilere belli bir yerde ve belli bir süre internet kullanım olanağı sağlayan kişiler toplu kullanım sağlayıcılardır. Toplu kullanım sağlayıcıları, personellerine interneti kullandıran üniversiteler ve şirketler gibi kuruluşlar olabileceği gibi, ticari amaçla faaliyet gösteren internet kafeler de olabilir²²⁴. Bu ayırım ticari amaçla internet toplu kullanım sağlayıcıları tanımlayan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelikte de görülmektedir²²⁵.

Toplu kullanım sağlayıcılar erişim ve yer sağlayıcılar gibi teknik bir işleve sahip değildir. Kendi aboneliklerini diğer kullanıcıların hizmetine açmaktadırlar²²⁶. Gelişen süreçte de ücretsiz toplu kullanım sağlayan kurumların artacağı²²⁷, buna karşın internet altyapısının gelişmesi ve bireysel kullanımın ucuzlaşması nedeniyle ticari amaçlı toplu kullanım sağlayıcıların azalacağı öngörülmektedir.

Toplu kullanım sağlayıcıların İOYYDHK'nin 7. maddesi uyarınca hukuki ve cezai sorumluluklarının bulunmadığı, yalnızca internet ortamında suç sayılan yayınlara kullanıcıların erişimlerini engellemekle yükümlü oldukları, aksi halde uygulanabilecek yaptırımın ise para cezası olduğu ifade edilmektedir²²⁸.

1.4.2.2.5 İnternet Servis Sağlayıcı Kavramı Sorunu

İnternet aktörleri tanımlanırken üzerinde durulması gereken kavramlardan birisi de İnternet Servis Sağlayıcıdır (İSS – Internet Service Provider – ISP). 5651 sayılı kanunda sadece erişim, yer, içerik ve toplu kullanım sağlayıcılardan bahsedilmiş, internet servis sağlayıcısına yer verilmemiştir. Bu nedenle servis sağlayıcısının ayrı bir kavram mı olduğu, yoksa mevzuatta düzenlenen kavramlardan biri veya birkaçını kapsayıp kapsamadığı yönünde bir belirsizlik oluşmuştur.

Bu belirsizlik, öğretilerde de farklı görüşleri beraberinde getirmiştir. Gerek 5651 sayılı kanundan önceki gerekse sonraki dönemde yazılan bazı eserlerde internet servis sağlayıcı ile erişim sağlayıcısının ayrı ayrı tanımlandığı ve farklılıklarının olduğu söylenmektedir. Bu görü-

²²⁴ Erdoğan, 2013: 389.

²²⁵ Yönetmeliğin 3/1-l bendine göre ticari amaçlı toplu kullanım sağlayıcılar, internet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlar da bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan gerçek ve tüzel kişilerdir.

²²⁶ Doğu, 2016: 19.

²²⁷ Belediyeler başta olmak üzere birçok kurum ücretsiz wifi noktaları oluşturma yarışına girmişlerdir. <https://isttelkom.istanbul/hizmetlerimiz/ibb-wifi-hizmetleri/> (erişim tarihi: 01.08.2018), <http://www.ankara.bel.tr/haberler/buyuksehirde-uccretsiz-wi-fi-hizmeti/#.W2IKObihmUk> (erişim tarihi: 01.08.2018). İnternet kafeler ise artık oyun platformlarına dönüşmektedir. <https://www.haberturk.com/ekonomi/teknoloji/haber/762100-internet-kafeler-azaliyor> (erişim tarihi: 01.08.2018).

²²⁸ Öztan, 2008: 632.

ş e göre erişim sağlayıcılar, servis sağlayıcılardan farklı olarak başkalarına ait bilgileri kendi sunucularında depolayarak erişilebilir kılma yönünde bir hizmet vermezler²²⁹. Görüldüğü üzere bu görüş, internet servis sağlayıcılarını, erişim ve yer sağlayıcıların bir birleşimi olarak tanımlamaktadır. Hatta bazı eserlerde erişim, yer ve toplu kullanım sağlayıcı ayrımına girmeksizin kapsayıcı bir terim olarak yalnızca internet servis sağlayıcı ifadesinden bahsedildiği de görülmektedir²³⁰.

Diğer bir görüş ise internet servis sağlayıcının mevzuattaki karşılığının erişim sağlayıcı olduğunu, aralarında bir farkın olmadığını söylemektedir²³¹. Buna karşın servis sağlayıcının yaptığı işler arasında internet erişiminin sağlanmasının yanı sıra sunuculuk²³² (hosting) veya toplu kullanım hizmetlerinin verildiğinden de bahsedilmektedir.

Mevzuatta da internet servis sağlayıcı kavramının tanımlandığı bir metin olmamasına karşın birçok yerde kavramın kullanıldığı görülmektedir. Bunların en belirginini 5651 sayılı kanunda yer almaktadır. Kanunun 6/A maddesi Erişim Sağlayıcıları Birliği'nin "5809 sayılı Elektronik Haberleşme Kanunu kapsamında yetkilendirilen tüm internet servis sağlayıcıları ile internet erişim hizmeti veren diğer işletmelerin..." katılmasıyla oluştuğunu belirtmektedir. Bu yönüyle internet servis sağlayıcıların tüm erişim hizmeti veren işletmeleri kapsamadığı sonucu çıkmaktadır.

Ülkemizin de tarafı olduğu Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin "tanımlar" başlıklı 1. maddesinde kavramın hizmet sağlayıcı olarak erişim, yer ve toplu kullanım sağlayıcılarını kapsayacak şekilde düzenlendiği görülmektedir²³³. Sözleşmenin İngilizce metninde "service provider" olarak yer alan terim, nedense servis sağlayıcı olarak değil hizmet sağlayıcı olarak çevrilmiş ve kavram karmaşasına bir çözüm getirilememiştir.

Sonuç olarak, internet servis sağlayıcının tarafı olduğumuz uluslararası sözleşme ve mevzuatta yer alan hükümlere göre erişim, yer ve toplu kullanım sağlayıcılarının bir veya birden fazlasının yetkilerini bünyesinde barındırabilen kapsayıcı bir kavram olduğunu söylemek mümkündür. Bununla birlikte iç hukukumuzda detaylı şekilde yapılan ayırım karşısında internet servis sağlayıcı teriminin pratikte bir önemi kalmamıştır. Mevzuatın da erişim, yer, içerik ve toplu kullanım sağlayıcıları çerçevesinde inşa edilmesi faydalı olacaktır.

²²⁹ Sınar, 2001: 41-42; Gürler, 2015: 62.

²³⁰ Akçam, 1999: 80.

²³¹ Dülger, 2015: 870; Turan, 2016: 136.

²³² Dülger, 2015: 442.

²³³ "Hizmet sağlayıcı terimi:

i. Hizmetlerini kullananlara bir bilgisayar sistemi aracılığıyla iletişim kurma olanağı sağlayan her türlü kamu veya özel sektör tüzel kişisini, ve
ii. Böylesi iletişim hizmeti veya bu hizmetlerin kullanıcıları adına bilgisayar verilerini işleyen veya depolayan diğer her türlü tüzel kişiyi ifade eder."

1.4.3 Amaç Yönünden

Bilişim aktörlerinin her biri bilişim sistemleri üzerinde oldukça farklı amaçlar güder. Sadece zorunlu gördüğü işleri yapan kişilerden, bilişim sisteminin derinliklerini keşfetmek ve bilinmeyene ulaşmak isteyene kadar geniş bir yelpazeden bahsetmek mümkündür. Bu nedenle bilişim suçları bakımından da değerlendirmeye uygun en sade haliyle, bilişim aktörleri amaçları yönünden kullanıcılar ve bilişim korsanları olarak ikili bir sınıflandırmaya tabi tutulabilir.

1.4.3.1 Kullanıcı

Kelime anlamıyla kullanmak, bir şeyden belli bir amaçla yararlanmak demektir²³⁴. Kullanıcıları da tam olarak bu ifadeyle, bilişim sistemlerinden, onlara özgülenen amaçlar doğrultusunda ve kısıtlamaları dahilinde yararlanan kişi olarak tanımlayabiliriz. İşlerini yürütmek için ofis programlarını kullanan masa başı çalışanları veya çizim programı kullanan tasarımcılar klasik bir bilişim sistemi kullanıcısıdır. Bu bakımdan bir kullanıcıyı bilişim korsanından ayıran temel özellik, sistemin öngörülen sınırlarını aşmamasıdır. Bu yönüyle de denilebilir ki, kullanıcıların büyük çoğunluğu “bilişim sistemi gibi düşünemeyen” kişilerden oluşmaktadır.

Tanım olarak basit görünse de farklı cinsiyette, yaşta ve milletteki milyonlarca kişinin bir o kadar farklı tercihini değerlendirmek kolay değildir. Kullanıcı deneyimleri günümüzde büyük ticari şirketlerin önemli harcamalar yaptığı konuların başında gelmiştir. Hatta birçok yazılım daha özelleştirilebilir ve başarılı ürünler sunmak için kullanıcı istatistiklerini firmalarıyla paylaşabilmek için izin istemektedir.

Normal şartlarda kullanıcılar yeni başlayandan uzmana kadar giden bir düzlem üzerinde derecelendirilmektedir. Bilişim sistemlerinde ise daha isabetli olacak şekilde kullanıcılar hedef odaklı ve uygulama odaklı olarak ayrılmaktadırlar. Hedef odaklı kullanıcılar, yalnızca ulaşmak istedikleri amacı umursayan kişilerdir. Örneğin kelime işleme programında düzenleyebildiği metnin PDF imajına dönüştürüldüğü zaman neden düzenlenemediğiyle ilgilenmezler, onların amacı sadece “harf yazmaktır”. Bilgisayardaki dosya ve klasör gibi kavramları günlük hayattakine paralel şekilde düşünerek eşleştirmeye çalışıp, kendi zihinlerinde karışıklığa yol açarlar. Uygulama odaklı kullanıcılar ise bilişim sistemine özgü kavramları anlayan, ancak ihtiyaç duydukları kadar öğrenen kişilerdir. Karşılarına çıkan her yeni sorun ve ihtiyaçta yeni bir yazılım ile çözüm bulma arayışına girer. Yaratıcılıkları kullandıkları yazılımın be-

²³⁴ http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5b68a731da6348.17455142 (erişim tarihi: 07.08.2018).

cerisi kadardır. Programcılar genellikle bu kategoride bulunurlar. Kendilerini kullandıkları yazılımlarla sınırlamayı kabul etmeleri yönüyle bilişim korsanlarından ayrılmaktadırlar²³⁵.

1.4.3.2 Bilişim Korsanı

Bilişim korsanları, kullanıcı sınırlarını aşarak “bilişim sistemi gibi düşünebilen” kişilerdir. Sadece gördükleriyle değil, bilişim sisteminin tam olarak ne yaptığını bilmek isterler. Bilişim korsanlarına karşı etik ve hukuksal yönden “insanlığın ilerlemesini sağlayanlar”dan “siber teröristler”e kadar çok farklı yaklaşımlar bulunması nedeniyle konu detaylı olarak incelenecektir.

1.4.3.2.1 Kavram ve Nitelendirme

Günlük hayatta sıkça kullanılan hacker kavramı, TDK sözlüğüne bilgisayar korsanı olarak girmiş ve “Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işlemler yapmak için kullanan kimse” şeklinde tanımlanmıştır²³⁶.

Dilimizde bilgisayar sistemi yerine isabetli olarak bilişim sistemi deyiminin kullanıldığından yukarıda bahsedilmiştir. Benzer şekilde bilgisayar korsanı yerine kavram bütünlüğünü sağlamak ve anlam genişliğini kapsamak açısından bu eserde “bilişim korsanı” deyimini kullanılacak, Türk Bilişim Derneği’nin bilişim terimleri karşılıklar sözlüğünde hacker yerine önerilen “çökertici” deyimini ise şimdilik tercih edilmeyecektir²³⁷.

TDK’nin bilişim korsanına getirmiş olduğu tanım bütünüyle yeterli ve doğru olmasa da, halihazırda “hacker” kelimesinin de neyi ifade ettiği tartışılmaya devam etmektedir. En genel tanımıyla hacker, herhangi bir şeyi kullanım amacı dışında kullanma yeteneği olan kişilere verilen isimdir. Bu bağlamda bilişim alanı dışında da hacker olmak mümkündür. Buna örnek olarak, pişirilip yenilmesi amacı taşıyan pirinci, bir anda tuz boşalması ve nemlenmesin diye tuzluğun içine koyan kişinin de hacker olarak kabul görmesi verilmektedir²³⁸. Öğretimde ise Yenidünya/Değirmenci hacker kavramını sisteme müdahale eden, onu kesintiye uğratan kişi olarak tanımlamıştır²³⁹. Bununla birlikte, bilişim korsanlığı noktasında yalnızca hacker deyiminin tercih edilmediğini, farklı yöntemleri uygulayanlara hacker, phreaker²⁴⁰, cracker gibi farklı adlandırmalar yapıldığına da dikkat çekmek gerekir. Bu kelimelerin tamamı Türk-

²³⁵ <https://stuartsierra.com/2006/07/12/the-three-types-of-computer-user> (erişim tarihi: 07.08.2018).

²³⁶ http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5b63661a167a09.59216281 (erişim tarihi: 02.08.2018).

²³⁷ <http://eski.tbd.org.tr/index.php?sayfa=sozluk&mi1&tipi=entr&harf=H> (erişim tarihi: 02.08.2018).

²³⁸ Çıtak, 2018: 1.

²³⁹ Yenidünya/Değirmenci, 2003: 58.

²⁴⁰ Genellikle telefon sistemlerini kilitleyen bilgisayar korsanlarına verilen isimdir.

çeye çevrilmemiş olmakla birlikte hepsinin birer bilişim korsanı olduğunu ifade etmek gerekir. Bilişim korsanlarının isimlerini aldığı bu yöntemlere ise ileride değinilecektir.

1.4.3.2.1.1 Bilişim Korsanlarının Olumlu Yönlerine Dair Argümanlar

Bilişim korsanlarının olmazsa olmaz bir önem derecesinde övüldüğü veya yerden yere vurulduğu bir nitelendirmeye karşılaştıklarını kolaylıkla görebiliriz. Bilişim korsanlarını faydalarından bahsedilirken onların bir sanat – zanaat yaptığı²⁴¹, modern dünyanın Robin Hood’u olarak kabul edildiği söylenmektedir²⁴². Bilişim korsanlarının yaptığı çalışmaları teknolojik gelişmelerde önemli bir pay olarak görülüp ve büyük bilişim şirketleri sahiplerinin de hacker deneyimleri olduğunu belirtilmektedir. Hatta hackerların karakterlerinden bahsedilerek, genellikle zeki, meraklı ve entelektüel birikime sahip kişiler olarak tanımlanırlar²⁴³. Onlar, yeni şeyler öğrenme konusunda önüne geçilemez bir isteğe sahiptirler ve korkunç şekilde ayrıntıya önem vermektedirler²⁴⁴. Tüm bunların bir sonucu olarak gerek medyanın yüzeysel haberlerinde gerekse oluşturulan politik algılarda bilişim korsanlarının kapüşonlu olarak gezen karanlık tipler olarak tanıtılmasını rahatsız edici bulunmaktadır²⁴⁵.

Bilişim korsanlarını da günümüze kadar gelen süreçte üç farklı kuşağa ayıran yazarlar, her kuşağın kendine özgü etik değerleri olduğunu, bunların ortak noktası olarak ise bilginin zorunlu olarak özgür olması gerektiği, sistemlere veya bilgisayarlara erişimin kısıtlanamayacağı gibi ilkelerin yer aldığını söylemektedir. Hatta ikinci kuşak bilişim korsanları, sistemlere zarar vermemeyi kendilerine ilke edinmelerine karşın, işlemcilerin boştaki durmasını kaynak verimsizliği olarak yorumlamaktadır²⁴⁶.

Bilişim korsanlarının sahip oldukları ilerleme ve gelişme merakının bilişim alanında da oldukça faydalı buluşları sağladığı ifade edilmektedir. Bu yaklaşımın ticari amaçla ve özellikle lisans ücreti ile kullanmak üzere geliştirilen yazılımlara karşı, açık kaynak kodu²⁴⁷ hare-

²⁴¹ Saka, 2013: 36.

²⁴² Karagülmez, 2014: 88.

²⁴³ Yılmaz, 2016: 25.

²⁴⁴ Dilek, 2007: 49. “(Hackerlar) deşifre ediyorlar. Nasıl yapıldığını, nasıl çalıştığını merak ediyorlar. Daha iyisini yapıyorlar. Başka türlü yapmanın yollarını arıyorlar. Tekniğin bilgisini paylaşıyorlar. Tüketim kültürüne, popüler olana direnmiyorlar. Bilginin tekellerde kalmaması için çalışıyorlar. Bunları yaparken de çoğunlukla kahraman ya da kurtarıcı olmak, mesajlar vermek gibi dertleri de yok. Sadece girdabın dışında durmaya çalışıyorlar. Zorunda oldukları için değil, keyif ve haz aldıkları için, sadece yapabildikleri için çalışıyorlar.” Keleş, 2013: 8.

²⁴⁵ Çıtak, 2018: 2.

²⁴⁶ Akdeniz, 2013: 11 – 13.

²⁴⁷ Açık kaynak kodlu yazılımlar (open source software), ilgilenen herkesin yazılım kodlarına erişebildiği ve hayal ettiği değişimi gerçekleştirebildiği yazılım projeleridir. Gönüllülük esasına dayanan bu projeler birçok aklın ortak akıl olarak birleşebilmesiyle, yeni özellikleri geliştirmede ve güvenlik açıklarını kapatmakta daha esnek yönetim şemasına sahiptir.

ketini başlattığı, günümüzde birçok ücretsiz yazılımın bu şekilde kullanıcıların hizmetine sunulduğu söylenmektedir²⁴⁸.

2006 yılında yapılan bir araştırma hackerların toplum gözündeki merak edilen hatta imrenilen algısını da ortaya koymaktadır. Çoğunluğu bilişim alanında belli oranda deneyime sahip kişiler arasından yapılan ankete göre katılımcıların %42,2'si teknik imkân ve bilgiye sahip olmaları halinde hackerlik yapabileceklerini söylemektedirler²⁴⁹

Son olarak, bilişim dünyasında oldukça tanınmış olan hacker The Mentor'un manifestosunun bir bölümü aktarılabilir. Kendilerinin okulda diğer çocuklardan daha akıllı olduğunu, daha kolay kavradığını, bilgisayarların işlem gücünün bu nedenle cezbedici olduğunu, sırf bu yüzden kendilerinin tehdit veya ukala olduğunu düşündüklerini ve dışlandıklarını söyleyen Mentor, şu ünlü sözlerle tamamlar:

“Artık burası bizim dünyamız. Elektron ve devre anahtarlarının güzelliği. Zaten var olan, aç-gözlü vurguncularca işletilmese sudan ucuz olacak bir hizmeti parasız olarak kullanıyoruz ve bize suçlu diyorsunuz. Keşfediyoruz... ve bize suçlu diyorsunuz. Bilginin peşinden gidiyoruz... ve bize suçlu diyorsunuz. Deri rengi olmadan, milliyet olmadan, dinsel tarafdırlık olmadan var oluyoruz... ve bize suçlu diyorsunuz. Atom bombaları yapıyorsunuz, savaşlar çıkarıyorsunuz, öldürüyorsunuz, hile yapıyorsunuz ve bize yalan söyleyerek bizim kendi iyiliğimiz için olduğuna inandırmaya çalışıyorsunuz, yine biz suçlu oluyoruz. Evet suçluyum, suçum merak. Suçum insanları nasıl görüldüğüne değil, ne söylediği ve ne düşündüğüne göre değerlendirmek. Suçum sizden daha akıllı olmak, bunun için beni asla affetmeyeceksiniz²⁵⁰.”

1.4.3.2.1.2 Bilişim Korsanlarının Olumsuz Yönlerine Dair Argümanlar

Bilişim korsanlığını zararlı eylemler olarak gösteren argümanlar ise, onlara haksız derecede sempati ile bakıldığını, günümüzde bilişim korsanlarının teknolojik ilerleme merakını bir yana bırakarak sadece ticari ve zarar verici amaçlı eylemlerde bulunduklarını²⁵¹, şirketlerin milyarlarca dolar zarar ettiğini söylemektedir²⁵².

Bilişim korsanlarının olumsuz yönlerinin özellikle son yıllarda öne çıktığı da ileri sürülmektedir. Bu görüşe göre yirmi beş yıl gibi kısa bir süre içerisinde bilişim tehditlerinin doğası da değişmiştir. Bilişim korsanları ilk zamanlarda daha çok bir gülücük almak için bu eylemlerde bulunurken, günümüzde tüm bu eylemler para ve güç odaklı bir hal almıştır. Sadece bilişim suçları üzerine kurulu organize suç örgütlerinden siber terörizme kadar verilebi-

²⁴⁸ Akdeniz, 2013: 14.

²⁴⁹ Dijle, 2006: 49.

²⁵⁰ (Çeviri: Işık Barış Fidaner) Keleş, 2013: 94.

²⁵¹ Yenedünya/Değirmenci, 2003: 60.

²⁵² Yılmaz, 2016: 26.

lecek örnekler, artık bilişim korsanlığının farklı ve tehlikeli bir konumda olduğunu göstermektedir²⁵³.

Yine, bilişim korsanı denildiğinde akla gelen on beş yaşlarında, annesinin evinde bir odada yaşayan, çevresi cips paketleriyle dolu klavyeyi kucağında taşıyan bir insan modeli devrinin geride kaldığı söylenmektedir. Artık bizzat devletlerin veya büyük şirketlerin birbiri arasındaki rekabete dayalı eylemlerde bulundukları, bilişim suçlarının yalnızca gençlerin bir tür öğrenme aracı olmadığı da göz ardı edilmemelidir²⁵⁴. Ayrıca çocukların içinde bulunduğu eylemlerin de her zaman çok masum olduğu söylenemez. Örneğin, Polonya'nın Lodz kentinde yaşayan 14 yaşındaki bir çocuk, raylar üzerindeki makasları kontrol edebilen bir kızılötesi verici geliştirerek tek bir dokunuşla iki tramvayın çarpışmasına ve dört vagonun raydan çıkmasına neden olmuştur. "Biraz eğlence" amacıyla meydana gelen bu ciddi kazada ise şans eseri can kaybı yaşanmamıştır²⁵⁵.

1.4.3.2.2 Sınıflandırma

Bilişim korsanları yaptığı eylemlerin zarar verip vermemesi yönüyle çeşitli ayrımlara tabi tutulmuştur. Bunların arasında en sık kullanılanı, beyaz şapkalı, siyah şapkalı ve gri şapkalı bilişim korsanları ayrımıdır.

Renklerden de tahmin edilebileceği üzere siyah şapkalı bilişim korsanları yalnızca çıkarları doğrultusunda karar vererek, bilişim sistemlerinin gelişmesini ve açıklarını kapatmayı hedeflememektedir. Çıkarları gerektirdiği ölçüde bir bilişim sistemine zarar verme noktasında tereddüt yaşamamaktadırlar. Yaptıkları eylemler bilişim alanının dışına taşarak mağdurların gerçek hayatlarında da önemli etkiler oluşturabilmektedir. Yaptıkları işler genellikle yasadışı olduğundan kendilerini gizlemekte ve toplumda bir şöhret sahibi olma amacı gütmektedirler.

Beyaz şapkalı bilişim korsanları ise siyah şapkalıların tam tersidir. Siyah şapkalı bilişim korsanlarının bildikleri tüm yöntemleri bilir ve hatta uygularlar. Ancak bunu sistem sahibinin bilgisi dahilinde yaparlar, sistemdeki güvenlik açıklarını tespit ederek siyah şapkalı bilişim korsanlarının olası saldırılarını engellemeye çalışırlar.

Gri şapkalı bilişim korsanları ise asıl işleri güvenlik olmayan, sistem sahibinin bilgisi olmaksızın sistemdeki güvenlik açıklarını araştıran kişilerdir. Bir açık bulduklarında ise durumu sistem sahibine bildirirler. Gri şapkalı korsanlar genellikle açık buldukları zaman sahip oldukları şöhret ile manevi tatmin duyarlar ve başarılı olanları genellikle istihdam edilmek

²⁵³ Goodman, 2016: 24, 27.

²⁵⁴ Goodman, 2016: 42.

²⁵⁵ <https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html> (erişim tarihi: 11.02.2019).

amacıyla davet edilmektedir²⁵⁶. Bazı eserlerde gri şapkalı bilişim korsanlarının, beyaz şapkalılardan daha az bilgiye sahip ve her an siyah şapkaya geçebilecek olan bilişim korsanları olduğu ifade edilmektedir²⁵⁷.

Bilişim korsanları arasındaki bu ayrım, aynı zaman etik bilişim korsanlığı (ethic hacking) kavramının ortaya çıkmasını sağlamıştır. Etik bilişim korsanları, yapılan ayrım gözetilmeksizin, yapmış olduğu işlerde belli ahlak kurallarını gözetten bilişim korsanlarıdır²⁵⁸. Elbette “belli ahlak kuralları”nın çerçevesini objektif şekilde çizmenin zor olduğu da göz önünde bulundurulmalıdır²⁵⁹. Buna karşın günümüzde bir kişinin etik bilişim korsanı olduğunu belgeliyebilmesi mümkündür. EC- Council tarafından verilen sertifikasyon programı ve sonrasında uygulanacak bir sınav ile sertifikalı etik bilişim korsanı olmak mümkündür²⁶⁰.

Öğretide yapılan başka bir ayırmada ise hacker ve cracker arasındaki farklılıklardan bahsedildiği görülmektedir. Buna göre hackerlar sisteme giren ve bilgileri elde edebilen kişiler olsa da sisteme veya dosyalara bir zarar vermezler. Ancak crackerlar girmiş oldukları sistemi bozma, dosyaları değiştirme veya şifreleme amacı güderler ve yıkıcı bir etkiye sahiptirler²⁶¹.

Yine, yapılan başka bir ayırmada “siber suçlular” kavramına yer verilmiş ve bunların idealistler, açgözlülükle hareket eden profesyonel suçlular ve siber teröristler olarak üçe ayrıldığı söylenmiştir. Buna göre idealistler genellikle 12-19 yaş arası gençlerden oluşur ve toplum hiyerarşisinde yukarı tırmanma amacı güderler. Profesyonel suçlular kendilerine nakit sağlandığı sürece herhangi bir siber suç işlemekten çekinmezler. Siber teröristler ise sadece para değil, aynı zamanda savundukları görüşün de reklamını yaparlar²⁶².

1.4.3.2.3 Değerlendirme

TDK'nin kullandığı bilgisayar korsanı veya daha geniş anlamıyla bilişim korsanı ifadesi kabul edileceği üzere olumsuz bir çağrışıma sahiptir. Alternatif olarak önerilen çökertici deyimini ise yine aynı olumsuz anlamdadır. Halbuki bilişim korsanı kavramı olumlu ve olumsuz örnekleri içinde barındıran karma bir yapıdadır. Bu nedenle öncelikle yenilikçi ve yıkıcı bilişim korsanlarının tamamını kapsayacak bir tanım üzerinde uzlaşılarak, olumlu ve olumsuz çalışma yapanları ayrı şekilde sınıflandırmak faydalı olacaktır.

²⁵⁶ Bu konu hakkında, Çıtak, 2018: 4.

²⁵⁷ Yılmaz, 2016: 25.

²⁵⁸ Etik bilişim korsanlığı konusunda iç hukukumuzda henüz yasal bir düzenleme bulunmamaktadır. Karagülmez, 2014: 97 – 98.

²⁵⁹ Çıtak, 2018: 5.

²⁶⁰ <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/> (erişim tarihi: 03.08.2018).

²⁶¹ Yılmaz, 2016: 24; Dilek, 2007: 48 – 50.

²⁶² Turhan, 2006: 59 – 60.

Bilişim korsanlarının bütünüyle faydalı veya zararlı bir faaliyet olduğunu söylemek de doğru olmayacaktır. Örneğin bir oyunun dosyalarına erişip değiştirmek suretiyle oyuna hiçbir zarar vermeden farklı modlar üretmek de esasen bir bilişim korsanlığı örneğidir²⁶³. Benzer şekilde kullanmış olduğu yazılımda aradığı özelliği bulamayan bir kişinin, yazılım dosyaları üzerinde oynayarak, kendi amacına uygun şekilde çalışmasını sağlaması da bilişim korsanlığı faaliyetidir.

Bilişim korsanı bu yönüyle çilingire benzetilebilir. Bir çilingir, kapıları ve kasaları açma marifetini hiç kullanmayabilir, yalnızca meslek olarak gerektiği kadar kullanabilir, hırsızlık yapmak amacıyla kullanabilir veya belki de üçüncü bir iyiniyetli kişinin yararına bir tefecilik çetesinin elindeki senetleri aşırmaq için de kullanabilir. Bilişim korsanı da aynı bu şekilde meziyetlerini nasıl kullanacağına kendisi karar verir. Suçu oluşturan unsur bu meziyeti edinmesi değil hangi şekilde kullandığıdır. İşte bu nedenle bilişim korsanı kavramının da bu yönleri düşünülerek salt olumsuz anlam taşıması gerekmektedir.

Önceleri bilişim sistemlerine zarar verip vermemeleri yönünden hacker ve cracker olarak yapılan ayırım, günümüzde yerini isabetli olarak siyah, gri ve beyaz şapkalı bilişim korsanı ayırımına bırakmıştır. Çünkü her “hacker”ın, sisteme girip kullanıcı kredi kartı bilgilerini elde etme örneğinde olduğu gibi zararlı eylemlerde bulunmadığını iddia etmek doğru olmayacaktır. Aynı şekilde her cracker sistemde yıkıcı bir etki yapmamaktadır. Örneğin, lisanslı bir yazılımı herhangi bir bedel ödmeden kullanılabilir hale getiren bir kişi, sistemin bütünlüğüne bir zarar vermemekte, aksine son kullanıcının lehine bir sistem çalışması sağlamaktadır. Bu nedenle hacker ve cracker gibi kavramlar bilişim korsanlarının amaçlarını değil yöntemlerini belirleyen nitelermelerdir ve siyah, gri ve beyaz şapkalı bilişim korsanları ile karıştırılmamalıdır. Bilişim korsanlarının izledikleri yöntemler ise eserin ikinci bölümünde açıklanmaktadır.

Gri şapkalı bilişim korsanlarının tehlike arz ettiğini ileri süren görüşe katılmamız da mümkün değildir. Gri şapkalı bilişim korsanları arasında çalışmalarına henüz başlamış ve kendisini geliştirmeye çalışanlar olduğu kadar, büyük kurumlarda çalışarak kendisini ona kuruma bağlamak ve kısıtlamak istemeyen oldukça yetenekli bilişim korsanları da vardır. Siyah şapkalı bilişim korsanlığına geçiş ise gri şapkalılar kadar beyaz şapkalılar arasında görülmesi de mümkündür ki bu “etik bilişim korsanlığı” meselesidir.

²⁶³ Hatta bu modlar öyle seviyelere gelmiştir ki, Half – Life adlı oyunun bir grup taraftarı, oyunu gönüllü olarak yeni bir oyun motorunda güncel teknolojilere uygun şekilde yeniden tasarlamıştır. Büyük beğeni alan bu çalışma Black Mesa olarak oyundan farklı bir ad ile piyasaya sunulmuş ve üstelik oyunun gerçek sahipleri tarafından da desteklenmiştir.

Bilişim korsanları ve karakterleri hakkında öznel değerlendirmeler bir kenara bırakılırsa, bir bilişim korsanının en basit haliyle “bilişim sisteminin işlemesi gerektiği şekilde işlememesine neden olan kişi” olduğu söylenebilir. Diğer bir ifadeyle bilişim korsanı, bilişim sisteminin ulaşmak istediği amacı ile teknik detayları (kodlar vb.) arasındaki farklılıkları kendi lehine kullanan kişidir. Bilişim korsanlarının hangi eylemlerinin ceza gerektirip gerektirmeyeceği ise tamamıyla suç politikası ile ilgili bir konu olmaktadır. Bu noktada yasa koyucunun, bilişim sistemlerinin gelişmesi noktasındaki girişimcilik ile yıkıcı bilişim faaliyetleri arasındaki dengeyi iyi gözetmesi gerekmektedir.



İKİNCİ BÖLÜM

BİLİŞİM SUÇU KAVRAMI, TARİHSEL GELİŞİMİ, ÇEŞİTLERİ VE BİLİŞİM SUÇ- LARI İLE MÜCADELE KAPSAMINDA ALINAN ÖNLEMLER

2.1 Bilişim Suçu Kavramı ve Ortaya Çıkışı

2.1.1 Kavram

Önceki bölümde de bahsedildiği gibi, suçta kanunilik ilkesi ve tipiklik unsurunun doğru şekilde belirlenmesi bakımından, bilişim suçları konusunda gerek kullanılacak isim ve gerekse yapılacak tanımın hem tereddüde yer vermeyecek şekilde kapsayıcı biçimde düzenlenmesi, hem de istenilen amacı aşacak şekilde geniş tutulmaması gerekmektedir. Bu durum da diğer kavramlar gibi bilişim suçlarının isimlendirilmesi konusunda da henüz tam bir uzlaşma sağlanamamasına neden olmaktadır.

Bilişim suçlarının teknik bir içeriğe sahip olması, çoğunlukla bu suç tiplerini belirlemez kılmıştır. Hemen hemen pek çok eserde bilişim suçlarının tespit edilmesinin zorluğundan bahsedilmektedir²⁶⁴. Halbuki bilişim suçlarına dair emareler, söylendiği anda kısa süre içeriğinde uzay boşluğuna karışan hakaret içerikli ses dalgalarının tespitinden daha zor olmamalıdır.

Bilişim suçlarına verilen adlandırmaların bir bölümü, kaynağını döneminin popüler bilişim sistemlerinden almış ve gelişen teknolojiler uyarınca da değişmiştir. Nitekim, bilişim suçlarının ilk ortaya çıktığı yıllarda “bilgisayar suçu”, günümüzde ise “internet suçları” deyiiminin arttığını görebiliriz. Yine yakın zamanlarda, siber suç (cyber crime), teknoloji veya ileri teknoloji suçu (techno – high tech crime), bilişim teknolojileri suçu (IT crimes), elektronik suç (e-crime) gibi isimlendirmeler de görülmektedir²⁶⁵.

Öğretide genel kabul gördüğü üzere, bilgisayar suçları kavramı, bilişim suçlarının bildiğimiz anlamdaki ilk örneklerinin Amerika Birleşik Devletleri’nde görülmesi nedeniyle, onların terminolojisine uygun olarak türetilip kabul görmüştür. Halbuki bilişim suçları terimine göre çok daha dar bir kapsamı ifade etmektedir²⁶⁶. Aynı şekilde internet suçları kavramı da bilişim sistem ağlarının sadece internetten oluşmadığı gözetildiğinde, örneğin, intranet ve ekstranet gibi ağlar üzerinde işlenen suçları tanımlamakta yetersiz kalmaktadır²⁶⁷.

²⁶⁴ Bu duruma ilişkin kısa bir değerlendirme için, Önok, 2013: 1232.

²⁶⁵ Erdoğan, 2013: 44; Karagülmez, 2014: 53; Bıçkın, 2006: 147.

²⁶⁶ Gül, 2016: 25; Taşkın, 2008: 12.

²⁶⁷ Dülger, 2015: 79; Erdoğan, 2013: 45; Gürler, 2015: 74; Orta, 2015: 77.

Günümüzde bilişim alanında işlenen suçlar ile ilgili olarak iki kavramın ön plana çıktığını, bunların da “bilişim suçu” ile “siber suç” olduğu görülmektedir. Siber suç daha çok bilişim korsanları veya kolluk kuvvetleri²⁶⁸ gibi uygulamacılar arasında popüler olarak görülen bir deyim olmakla birlikte, tarafı olduğumuz Sanal Ortamda İşlenen Suçlar Sözleşmesi’nde de siber suç (cybercrime) ifadesi yer almaktadır. Buna karşın öğretilerde genel olarak bilişim suçu deyiminin kullanıldığı ve bilişim suçlarının siber suçları da içine alan bir üst kavram olduğu ifade edilmektedir. Bu görüş, siber suçların yalnızca bilişim sistem ağları aracılığıyla gerçekleştirilen eylemleri kapsadığını söylemektedir²⁶⁹.

Özellikle Amerikan hukukunda görüldüğü şekliyle bilişim suçları, bilgisayar bağlantılı suç²⁷⁰ (computer related crime), bilgisayarla işlenen suç (computer assisted crime) ve bilgisayara karşı işlenen suçlar (crimes against computer) şeklinde ayrılmaktadır. Bu ayrım aslında bilişim suçlarının özünü anlatmaktan çok, suçların sistematik şekilde sınıflandırılması amacını taşıdığından bu konuya detaylı olarak ileride değinilecektir.

Sonuç olarak, öğretilerdeki genel görüşe uygun şekilde, hem TCK sistematığına uygun olması ve kavram birliğinin sağlanabilmesi bakımından, hem de bilişim terimleri konusunda oldukça zengin, tutarlı ve benimsenmiş bir terminolojiye sahip olmamız bakımından isabetli terimin “bilişim suçu” olduğunu düşünmekteyiz. “Bilişim suçu” teriminin uygulamada yetersiz kaldığını gösteren bir veri bulunmaması da yeni kavram arayışına ihtiyacımız olmadığını göstermektedir. Avrupa Konseyi Siber Suç Sözleşmesi’nin (Convention Of Cybercrime) iç hukukumuzda girerken Sanal Ortamda İşlenen Suçlar Sözleşmesi adıyla kabul edilmesi, siber suç deyiminin de yerleşmediğini göstermektedir. Nitekim siber suç kavramı bilişim suçunun yerine geçmek üzere değil, daha çok yabancı ülkelerde ve bilgisayar suçları (computer crimes) teriminin yerine geçmek üzere kapsayıcı bir terim olarak tercih edilmekle, Türk hukukunda kapsayıcı bir terim olan “bilişim suçları”nın çok daha öncesinden kullanılmaya başlandığını gururla ifade etmemiz gerekir.

2.1.2 Tanım ve Kapsam

Kavram olarak genel kabul gören bilişim suçunun tanımı da büyük önem arz etmektedir. Buna karşın isminin belirlenmesi kadar tanımı konusunda da Türk ve yabancı öğretilerde birlik bulunmadığı söylenebilecektir. Türk öğretisinde icra edilen eylemlere veya suçun işlendiği alana öncelik veren veya her iki unsuru da birleştirici tanımların olduğu görülmektedir.

²⁶⁸ Dülger, 2015: 79.

²⁶⁹ Erdoğan, 2013: 45. Dülger, aynı zamanda siber suç kavramının Türkçeleştirilmiş hali olan “sanal suç” kavramının yetersizliğine de vurgu yapmaktadır. Dülger, 2015: 79. Aksi görüşte, Orta, 2015: 77.

²⁷⁰ Çiçek, 2008: 3.

Eylemlere öncelik veren yapılan tanımlar incelendiğinde, Aydın’a göre bilişim suçları “elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların kanuni olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılması”dır²⁷¹. Kurt’a göre ise “verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içinde işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem” bilişim suçlarını oluşturmaktadır²⁷².

Suçun işlendiği alana öncelik veren tanımlara daha yoğun şekilde rastlanmaktadır. Karagülmez, “bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suç” şeklinde bir tarif yapmaktadır²⁷³. Turan, “bilgisayarların, bilgisayar ağlarının ya da elektronik ortamların araç olarak kullanıldıkları ya da bir hedef olarak maruz kaldıkları hukuka aykırı fiiller”i bilişim suçu olarak saymaktadır²⁷⁴. İçel de “bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik eylemler²⁷⁵”i bilişim suçu kapsamında değerlendirmektedir²⁷⁶.

Geniş ve dar anlamda iki farklı tanım yapan yazardan Dülger, geniş anlamda “bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her türlü suç”, dar anlamda ise “verilere ve/veya bilişim sistemlerine veya sistemin/verilerin düzgün ve işlevsel işleyişine, güvenliğine ya da bütünlüğüne karşı işlenen suç” olarak tanımlamıştır²⁷⁷. Erdoğan ise geniş anlamda “herhangi bir suçun icrasında bilişim sistem ya da araçlarının kullanıldığı ya da bilişim sistemlerinin veya içindeki verilerin hedef alındığı suç”, dar anlamda “bilişim sisteminin kendisinin ya da bilişim sistemi içinde bulunan verilerin hedef alındığı ve bilişim teknolojilerinin kullanılması suretiyle ya da bilişim araçlarına doğrudan fiziki müdahaleyle işlenen suç” olarak tanımlamaktadır²⁷⁸.

Yabancı öğretilerde de suçun işlendiği alanda bulunan cihazlara ağırlık verildiği görülmektedir. Katyal, siber suçu, bir suçun işlenmesini kolaylaştırmak veya yürütebilmek için bilgisayarların kullanıldığı suç olarak tanımlamaktadır²⁷⁹.

Tüm bu bilgilerden hareketle, bilişim suçlarını bilişim sistemleri aracılığıyla veya bu sistemleri hedef alan, eylemlerin tümü veya bir kısmının bilişim alanı içerisinde gerçekleştiği suçlar olarak tanımlayabiliriz. Bu şekilde yapılan sade tanımlamanın yeterli olduğu kanaatin-

²⁷¹ Aydın, 1992: 27.

²⁷² Kurt, 2005: 53.

²⁷³ Karagülmez, 2014: 57.

²⁷⁴ Turan, 2016: 43.

²⁷⁵ Gizlilik, bütünlük ve kullanıma açık bulunmasına yönelik eylemler hakkında, Sokullu Akıncı, 2001: 14.

²⁷⁶ İçel, 2001: 3.

²⁷⁷ Dülger, 2015: 83. Aynı şekilde, Akarslan, 2015: 36.

²⁷⁸ Erdoğan, 2013: 52.

²⁷⁹ Katyal, 2001: 12.

deyiz. Çünkü, eylemlerin sayılması veya veri ve bilgisayar gibi bilişim sistemi unsurlarının tanıma ayrıca dahil edilmesi kapsamda kısıtlamalara ve tekrarlamalara neden olmaktadır. Yukarıda açıklandığı gibi, bilişim sistemi zaten bilgisayar ve veri gibi kavramları içinde barındırmaktadır. İç ve dış bağlantı unsurlarının olmadığı yerde bilişim sisteminden, dolayısıyla bilişim suçlarından söz etmek mümkün olmayacaktır. Bu nedenle bilişim suçlarını tanımlarken, bilişim alanı ve bilişim sistemleri kavramlarına atıfta bulunarak, o kavramlara odaklanmak ve içeriğini doğru şekilde doldurmak faydalı olacaktır. Bu noktada geniş ve dar anlamda farklı tanımlara da ihtiyaç bulunmadığını, konunun bilişim suçlarının sınıflandırılması noktasında açıklığa kavuşacağını düşünmekteyiz.

2.1.3 Tarihsel Gelişim

Bilgisayarların tarihi gelişiminden bahsedilirken, doğal olarak bu gelişen teknoloji üzerinde de gelişecek ve farklılaşacak suç tiplerinin varlığından da bahsedilmelidir. Gelişen her teknoloji aynı zamanda yeni suç işleme veya suçluların kendilerini gizlemesi amacıyla da kullanılmıştır. Örneğin 19. yüzyılda ilk telgraf sistemleri kullanılarak işlenen bazı dolandırıcılık suçları ile bilişim suçları arasında uyum gösteren bağlantılar görülmektedir²⁸⁰.

Hacker'lığın tarihi gelişimi ise bilişim suçlarına göre bir miktar farklılık göstermektedir. "Hack" kavramı ilk kez Amerika Birleşik Devletleri'nin Massachusetts Institute of Technology (MIT) Üniversitesinde ortaya çıktığı söylenmektedir. Üniversitede yer alan bir öğrenci kulübü olan Tech Model Railroad Club (TMRC), elektro mekanik sistemler ile yönetilen bir model demiryolu ağı ile ilgilenmekteydi. Bu kulüpte bazı öğrenciler işin görsel kısmıyla ilgilenip modelleri gerçeğe daha yakın yapmak için uğraşırken diğer bir grup da elektronik işlerle ilgilenirdi²⁸¹. İşte bu sistemde yapılan her yeni ilerleme ve iyileştirmeye "hack" adı verilmişti. Bunları yapanlar da "hacker" sayılıyordu²⁸².

Bilinen anlamda ilk bilişim suçunun ise 18 Ekim 1966 tarihli Minneapolis Tribune gazetesinde yer alan "bilgisayar uzamanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı haberde yer alan eylem olduğu ifade edilmektedir²⁸³.

70'li yıllarda John Thomas Draper ile ortaya çıkan phreaking akımı oldukça ünlenmiştir. Telefonlara oldukça meraklı olan görme engelli Joe Engressia bir mısır gevreği paketinden çıkan düdüğün, uzak mesafe görüşmelerinde kullanılan sinyalle aynı tonda olduğunu fark ederek durumu arkadaşı Draper'a söylemiştir. Draper da Blue Box adı verilen ve arama konsollarını taklit ederek uzun mesafe telefon görüşmelerini bedavaya getiren cihazı geliştirmiş-

²⁸⁰ Dülger, 2015: 112.

²⁸¹ Kulübün gelişimi hakkındaki detaylı bilgi için, Levy, 2010: 7.

²⁸² Akdeniz, 2013: 11.

²⁸³ Dülger, 2015: 114.

tir. Draper'in yaptığı denemelerde Beyaz Saray'ın telefonlarına kadar girdiği, hatta başkanla doğrudan telefonla görüşebildiği ifade edilmektedir²⁸⁴. 1971 yılında Ron Rosenbaum'un Esquire dergisindeki makalesinin yayınlanmasıyla iletişim dünyasında suistimallerin olabileceğinin farkına varılması ve Mark Bernay takma adını kullanan phreakerlar gibi kişilerin sadece ücretsiz konuşmakla kalmaksızın aynı zamanda bu bilgiyi sürekli olarak yaygınlaştırmaya çalışması da phreakerların ünlenmesini sağlamıştır²⁸⁵.

80'li yıllarda ise bilgisayar virüslerinin ünlendiği söylenebilir. Sistemlere zarar veren ilk virüsün ARPANet tarafından 1971 yılında Creeper adıyla oluşturulduğu söylenmektedir²⁸⁶. 22 Ekim 1987'de de Delaware Üniversitesinde ilk virüs saldırısı gerçekleşmiş ve virüs birkaç yüz dosyaya bazılarını kullanılamaz hale getirecek şekilde bulaşmıştır²⁸⁷.

90'lı yıllarda internetin günlük kullanımının da yaygınlaşmasıyla bu ortamda işlenen suçların da popüler olduğu söylenebilir. Günümüzde ise daha karmaşık ve daha büyük tehdit içerikli bilişim suçlarının bulunduğunu söylemek yanlış olmayacaktır. Bilişim suçları artık büyük altyapı sistemlerini de hedef alır hale gelmektedir. Bir şehrin tren hatları, elektrik dağıtımı ve su arıtması gibi sistemleri kontrol eden SCADA (Supervisory Control and Data Acquisition – Veri Tabanlı Kontrol ve Gözetleme Sistemi) sistemleri internete bağlı olmasına rağmen büyük çoğunlukla eski nesil teknolojilerden oluşmakta ve saldırılar karşısında zayıf pozisyonda bulunmaktadır²⁸⁸. Örneğin 2011 yılında ABD'nin Illinois eyaletinde sisteme sızan bilişim korsanlarının su pompasını çok hızlı şekilde açıp kapatmak suretiyle binlerce evin temiz su ihtiyacını karşılayan şebekeye zarar verdikleri iddia edilmiştir²⁸⁹.

Öyle görünmektedir bilişim suçları ve bilişim suçlarıyla yapılacak mücadele, hukuksal önemi dışında ekonomik boyutuyla her yıl daha da artacak bütçesiyle geleceğin kritik öneme sahip sektörlerinden biri haline gelecektir. Kamu ve özel sektördeki başlıca kurumların birçoğu şimdiden yapay zekâ ve robotik otomasyonlar gibi ileri düzey teknolojilerle bilişim güvenliğine yatırım yapmaya başlamaktadırlar²⁹⁰.

²⁸⁴ “Dinlediği telefonlarda, ABD Başkanı olan Richard Nixon'un bir ajanla görüşmesine tanık olur. Bir sonraki sefer ajan başkanla görüşmek için “Beni Olimpos'a bağla” der. Ve kendisi de beyaz saraya bağlanarak “Beni Olimpos'a bağla” der, hiç beklenmedik bir şekilde ABD Başkanıyla telefonda karşı karşıya gelen Draper, başkana ulusal bir felaket olduğunu söyler. Başkan durumu sorunca, Draper “Tuvalet kağıdım bitti” şeklinde alaycı bir cevap verir.” Elbahadır, 2016: 22.

²⁸⁵ Kurt, 2005: 54.

²⁸⁶ Yılmaz, 2016: 11.

²⁸⁷ Kurt, 2005: 55.

²⁸⁸ Goodman, 2016: 37.

²⁸⁹ <https://www.bbc.com/news/technology-15817335> (erişim tarihi: 13.02.2019).

²⁹⁰ <http://www.hurriyet.com.tr/teknoloji/kurumların-siber-guvenlige-ayirdigi-butce-artacak-41042734> (erişim tarihi: 13.02.2019).

2.2 Bilişim Suçlarının Sınıflandırılması ve İşlenme Yöntemleri

2.2.1 Sınıflandırma

Bilişim suçlarının yapısının daha iyi anlaşılabilmesi bakımından farklı sınıflandırmaya tabi tutulduğu görülmektedir. Ancak bu ayrımlar da en az bilişim suçlarının tanımı ve kapsamında olduğu kadar görüş ayrılıkları içermektedir. Öyle ki ikili olanlardan on ikili ayrıma kadar çok farklı görüşe rastlamak mümkündür.

2.2.1.1 Bilişim Suçlarının Ayrı Bir Kategori Olmadığı Görüşü

Bu görüşe göre siber uzay ortamında gerçekleşen suçlar ile geleneksel suçlar arasında yapısal bir farklılık bulunmamaktadır. Buradaki farklılık fiziksel gerçeklik noktasında ortaya çıkmaktadır²⁹¹. Buna göre bilişim suçlarında yapılan sınıflandırmaların büyük çoğunluğu bu suçların klasik suçlardaki rolünden kaynaklanmaktadır²⁹². Gerçek dünyada işlenen suçlar ile siber uzayda işlenen suçlar birbirine uyarlanabilir niteliktedir, bilişim suçları geleneksel suçların uzandığı yeni bir alandır²⁹³.

2.2.1.2 Dört veya Daha Fazla Ayrımı Savunan Görüşler

Amerikan öğretisinde bilişim suçları dört ana başlık ve on iki farklı kategoride ifade edilmektedir. Dört ana başlık içerisinde vandalizm, veri ve programlara karşı gerçekleştirilen hırsızlık ve dolandırıcılık, mali ihlaller ve hizmet hırsızlıkları yer almaktadır²⁹⁴.

Carter, bilişim suçlarını dörde ayırmaktadır. İlk kategoride bilgisayarın hedef alındığı suçlar, ikinci kategoride suçun işlenmesinde aracı olarak kullanılan bilgisayarlar, üçüncü kategoride başka suçlara yardımcı olarak bilgisayarlar ve dördüncü kategoride de bilgisayarların yaygınlaşmasıyla ilgili suçlar bulunmaktadır²⁹⁵.

²⁹¹ Sınar, 2001: 71.

²⁹² Karagülmez, 2014: 69.

²⁹³ Brenner, 2001: 14.

²⁹⁴ 12 kategori ise şöyledir:

- Mülkiyete karşı hırsızlıklar,
- Verilere veya hizmetlere karşı gerçekleştirilen hırsızlıklar,
- Giriş ihlalleri,
- Veri sahtekarlığı,
- Şahıslardan kaynaklanan hatalar (hatalardan kaynaklanan ihlaller),
- Gasp,
- Sır aleyhine ihlaller,
- Sabotajlar,
- Maddi kısımlara yönelik hırsızlıklar,
- Varakalarda gerçekleştirilen sahtekarlıklar,
- Bankamatik kartları konusundaki hırsızlıklar,
- Manyetik kartların şifreleri konusunda gerçekleştirilen fiiller. Yazıcıoğlu, 1997: 148.

²⁹⁵ http://www.larryblakeley.com/security_computer_network/computer_crime_categories.htm (erişim tarihi: 25.02.2019).

Türk öğretisinde de dörtlü ayrım örnekleri görülmektedir. Kurt, veri suçları, ağ suçları, yetkisiz giriş suçları ve ilgili suçlar (bilgisayarla bağlantılı diğer suçlar) olarak bilişim suçlarını dörde ayırmaktadır²⁹⁶. Hatta Yılmaz, bilgisayar sistemleri ve verileri üzerine işlenen suçlar, içerik ile bağlantılı suçlar, telif ve marka haklarıyla ilgili suçlar, bilgisayarla bağlantılı geleneksel suçlar ve birleşik suçlar olarak 5’li ayrım yapmaktadır²⁹⁷.

SOİSS’de de bilişim suçlarının bilgisayar veri sistemlerinin ulaşılabilirliği, bütünlüğü ve gizliliğine karşı suçlar, bilgisayar bağlantılı suçlar, içerik bağlantılı suçlar ve telif hakları ve bununla bağlantılı hakların ihlaline ilişkin suçlar olmak üzere dört ana başlıkta değerlendirildiği görülmektedir.

2.2.1.3 Üçlü Ayrımı Savunan Görüşler

Karagülmez, bilişim suçlarını bilgisayarın fiili yapısına zarar verme fiilleri, bilgisayarın tek başına çalışma sistemine ilişkin fiiller ve bilgisayar ağlarına yönelen fiiller olarak üçe ayırmaktadır. Birinci kategori esasen bilişim sisteminin içeriğine yönelik bir suç tipi değildir. İkinci kategori fiziki ortamın değil, elektronik ortamın hedef alındığı eylemlerdir. Üçüncü kategori ise bilişim suçlarının en karmaşık türüdür²⁹⁸.

Demircan, Kurt’un ayrımını benimsemiş, ancak yetkisiz giriş suçlarına yermeden sadece veri suçları, ağ suçları ve ilgili suçlar şeklinde üçlü ayrıma yer vermiştir²⁹⁹.

Yetim, bilişim suçlarını ekonomik değeri olan, güvenlik riski oluşturan ve ahlaka aykırı olan suçlar şeklinde gruplandırmaktadır³⁰⁰.

2.2.1.4 İkili Ayrımı Savunan Görüşler

Interpol’e göre bilişim suçları gelişmiş bilişim suçları (advanced cybercrime) ve sanallaştırılmış bilişim suçları (cyber-enabled crime) olmak üzere iki ana başlık altında incelenmektedir. Gelişmiş bilişim suçları, bilişim sistemlerine yönelik karmaşık saldırıları içerirken, sanallaştırılmış bilişim suçları ile klasik suç tiplerinin internet başta olmak üzere bilişim sistemleri üzerinden gerçekleşmesini ifade etmektedir³⁰¹.

Türk öğretisinde de ikili ayrımın sıklıkla tercih edildiği görülmektedir. İkili ayrımda genel olarak benimsenen görüş, bilişim sistemleri aracılığıyla işlenebilen suçlar ve bilişim sistemlerine özgü suçlar olmak üzere yapılan ayrımdır³⁰². Benzer şekilde Gül, doğrudan ve

²⁹⁶ Kurt, 2005: 79 – 85.

²⁹⁷ Yılmaz, 2016: 21.

²⁹⁸ Karagülmez, 2014: 71.

²⁹⁹ Demircan, 2016: 22.

³⁰⁰ Yetim, 2014: 81.

³⁰¹ <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> (erişim tarihi: 25.02.2019).

³⁰² Aydın, 1992: 27; Erdoğan, 2013: 102; Taşkın, 2008: 10; Gürler, 2015: 82.

dolaylı olarak ikiye ayırmak suretiyle, bilişim sistemlerine özgü suçlara doğrudan suçlar, bilişim sistemleri aracılığıyla işlenen suçlara da dolaylı suçlar ismini vermektedir³⁰³. Akbulut ise dar ve geniş anlamda bilişim suçları olarak ayrım öngörmüş, dar anlamda suçları bilişim teknolojilerinin ortaya çıkardığı suçlar, geniş anlamda suçları ise mevcut suçların bilişim araçlarıyla işlenen suçlar olarak kabul etmiştir³⁰⁴.

2.2.1.5 Değerlendirme

Bilişim suçlarının sınıflandırmasında yaşanan temel ayrılık sanal alana bakış açısı ile ilgilidir. “Gerçek dünya” ve “siber uzay” olarak oldukça iddialı şekilde yapılan bu ayrım, bilişim suçlarının zor bilinir, ölçülür ve tespit edilebilir olduğunu vurgulayarak, bilişim suçlarını ayrı bir kategoriye itmektedir. Halbuki “bilişim sistemleri gibi düşünme” ilkesi uygulandığında, sanal alan “gerçek dışı dünya” gibi bir kavram yerine “alternatif bir yaşam alanı” olarak algılanabilir. Gerçekten de sanal alanda yer alan her bir unsur dünya üzerinde yer alan elementlerin bir ürünüdür ve ona uzak olmamızın tek nedeni insanlık tarihine göre henüz keşfedilmiş sayılmasıdır. Bu bakımdan, bilişim suçlarının zamandan ve mekândan bağımsız olma, sürekli gelişmesi ve sayıca hızla artması gibi özellikleri, ona başlı başına ayrı bir suç sınıfı olma özelliği vermemektedir. Bu noktada bilişim suçlarının geleneksel suçların uzantısı olduğu yönündeki görüşte haklılık payları bulunmaktadır.

Buna karşın, bilişim suçlarının gerçek dünyada yer alan suç tiplerinin uzantısı olması, onlarla bütünüyle aynı unsurları taşıdığını da göstermemektedir. Ayrıca yasa koyucu her zaman belli suç tiplerine verdiği önemi göstermek için ayrı bir bölüm verme ihtiyacı da hissedebilir. Bu bakımdan bilişim suçlarını “dünya dışı” bir varlık imajından çıkarmakla birlikte, ayrıca değerlendirmenin ve sınıflandırmanın önemli pratik faydaları olacaktır.

Bilişim suçlarının sınıflandırılmasında, kavram ve tanımlarda olduğu gibi, gelecekte meydana gelecek değişiklikleri de kapsayacak, öngörülü bir ayrım yapmakta fayda olacaktır. Bu nedenle bilişim suçlarının zarar verdiği alanlar üzerinden yapılan on ikili, altılı veya beşli ayrımlar aradığımız pratik faydayı vermeyebilecektir. Nitekim, günümüzde yapılan sınıflandırmalarda gittikçe öz, az sayıda ve kapsamlı ayrımların yapıldığı görülmektedir.

Bilişim suçlarının ekonomik, güvenlik veya ahlaki tehditleri üzerinden yapılan ayrımın da isabetli olmadığını düşünmekteyiz. Nitekim bilişim suçlarının oluşturduğu ekonomik ve güvenlik riskleri her somut olayda kolayca ayrılabilir durumda değildir. Ayrıca bir suç tipinin ahlaka karşı olarak gruplandırılması ceza yaptırımının temel anlayışına da uygun olmayacaktır.

³⁰³ Gül, 2016: 55.

³⁰⁴ Akbulut, 2017: 69.

Sonuç olarak, bilişim suçlarını öğretide genel kabul gördüğü şekilde salt bilişim suçları (bilişim sistemlerine özgü suçlar) ve bilişim bağlantılı (bilişim sistemleri aracılığıyla işlenebilen) suçlar olarak ayırabiliriz. Salt bilişim suçları, bilişim sisteminin hangi unsuruna (aygıt, veri, ağ) yönelik ve hangi amaçla olursa olsun, bilişim sistemini hedefleyen ve genellikle de yine bir bilişim sistemi aracılığıyla işlenen suçlardır. Bilişim sistemleri aracılığıyla işlenen suçlar ise, bir suçun işlenmesini kolaylaştırmak amacıyla bilişim sistemlerinden faydalanan suçlardır. Bu yönüyle, bilişim sistemi olmaksızın da işlenebilmeleri yönünden salt bilişim suçlarından ayrılırlar. Bilişim sistemleri aracılığıyla işlenen suçlar yasa koyucunun suç politikasına göre genellikle suçun nitelikli hali olarak karşımıza çıkmaktadır.

2.2.2 Bilişim Suçlarının İşlenme Yöntemleri

2.2.2.1 Bilişim Suçlarının Ortak Aşamaları

Teknolojinin ilerlemesi ve bilişim suçları ile mücadelenin gelişmesi neticesinde bilişim suçları da sürekli gelişen ve kendisini farklılaştıran bir yapı göstermektedir. Ancak, bilişim suçlarına vücut veren her eylem bilişim korsanlığının belli aşamalarının dahilinde gerçekleşmektedir. Yöntemler farklılaşsa da bilişim suçlarının genel itibariyle dört³⁰⁵ ortak aşaması olduğu söylenebilir. Bu aşamaların sırasıyla gerçekleşmesi zorunlu olmayıp, seçilen yöntemle göre bazı aşamaların devre dışı bırakılması veya atlanması mümkündür. Bilişim suçlarının gerçekleşmesinde zorunlu olmayan, ancak yön gösteren aşamalar aşağıda incelenecektir.

2.2.2.1.1 Bilgi Toplama

Bilişim korsanı için en değerli şey bilgidir. Yeterli bilgiye sahip olmaksızın hiçbir araç tek başına bilişim suçunun işlenmesini sağlayamaz. Bu nedenle bilişim korsanları öncelikle sızmak istedikleri sisteme ilişkin bilgi toplamak ve sistem açıklarını bu bilgilere göre tespit etmek durumundadır. Böylece yapılacak saldırının açık noktalar üzerine yoğunlaşması ve başarıya ulaşma ihtimali de artmaktadır.

Bilgi toplama aktif ve pasif olmak üzere iki şekilde gerçekleşir. Pasif bilgi toplama, hedef sistem ile doğrudan temasa geçmeden, sistem üzerinde o sistemden bilgi toplandığına dair herhangi bir iz bırakılmadan gerçekleşir. Arama motorları üzerinde gerçekleştirilen sorgular veya whois veritabanı sorgulaması³⁰⁶ gibi bilgi toplama yöntemleri pasif bilgi toplama-ya örnektir. Aktif bilgi toplamada ise sistem üzerinde iz bırakılması ve doğrudan iletişime

³⁰⁵ Aşamaların beş tane olduğuna ilişkin görüş için, Karagülmez, 2014: 89. Keşif ve tarama yapma aşamalarının bilgi toplama aşaması içinde gerçekleşmesi nedeniyle bunları birleştirerek dört aşama şeklinde ifade edilmesinin daha isabetli olduğu düşüncesindeyiz.

³⁰⁶ Genellikle bir sitenin alan adının (domain) daha önce alınıp alınmadığını sorgulamaya yarayan sistem, alan adına dair bazı önemli bilgiler içerdiği için pasif bilgi toplamanın olmazsa olmaz başvuru kaynaklarından birisi olmaktadır.

geçilmesi söz konusudur. Port taraması, TCP ve UDP taramaları gibi işlemler aktif bilgi toplama örneklerini oluşturur³⁰⁷.

Bu aşamada yapılan eylemlerin genel niteliği göz önüne alındığında pasif bilgi toplama “keşif”, aktif bilgi toplamaya ise “tarama” denildiği de görülmektedir. Hatta tarama, yani aktif bilgi toplama eylemlerinin aslında “saldırı hazırlık aşaması” olarak ayrı bir aşama olduğu da ileri sürülmektedir³⁰⁸.

Bilgi toplama aşamasını otomatik hale getiren veritabanları da günümüzde sıklıkla kullanılmaktadır. Örneğin shodan isimli internet sitesi, bilgi toplama işlerinde bir arama motoru gibi işlev görmektedir, gerek bilişim güvenliği uzmanları, gerekse bilişim korsanları tarafından keşif ve tarama amacıyla kullanılmaktadır³⁰⁹.

Bilgi toplama aşamasının bir saldırıdaki en önemli aşama olduğu söylenebilir. Nitekim Carnegie Mellon Üniversitesi’nin yaptığı bir araştırmaya göre sıradan bir ticari yazılımın her bin satırlık kodunda yirmi ila otuz açık bulunduğu tespit edilmiştir. Bu da 50 milyon satır koddan oluşan kaliteli bir programa oranlandığında 1 milyonda fazla açık anlamına gelmektedir³¹⁰. Kusursuz bir yazılımın zorluğu bu denli ortadayken, bilgi toplama faaliyetleri, saldırının başarısını, maliyetini ve gücünü belirleyen temel etken olmaktadır.

2.2.2.1.2 Sisteme Sızma

Yeterince bilgi toplanmasının ardından sistemin zayıf yanlarından sisteme sızılmaya çalışılır. Sistem içerisine virüs yerleştirmekten, verileri toplamak, sahte veriler oluşturmak, zombi bilgisayar oluşturmaya kadar çok farklı amaçlar için yapılan eylemler bu aşamada gerçekleşmektedir³¹¹. Bilişim suçlarının tamamlandığı aşamanın bu aşama olduğundan söz edilebilir, nitekim sonraki aşamalar saldırının devamlılığını veya gizliliğini sağlama amacı gütmektedir.

Günümüzde bir sisteme sızılıp sızılamayacağının anlaşılabilmesi için çeşitli sızma testleri de uygulanmaktadır. Pentest (penetration test) olarak da adlandırılan bu testler, hedef sistem hakkında testi yapacak kişilere önceden bilgi verilmesiyle (white box), bir kısım temel bilgilerin verilmesiyle (grey box) veya hiç bilgi verilmeden (black box) yapılabilir³¹². Yine, PCI güvenlik standartları³¹³  standartların sağlanıp sağlanmadığının kontrolü için sızma

³⁰⁷ Çıtak, 2018: 20.

³⁰⁸ Elbahadır, 2016: 57.

³⁰⁹ <https://www.shodan.io/> (erişim tarihi: 25.02.2019). Shodan veritabanı ile bilişim korsanları arasındaki ilişki hakkında, Goodman, 2016: 40.

³¹⁰ Goodman, 2016: 65.

³¹¹ Karagülmez, 2014: 89.

³¹² <https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/> (erişim tarihi: 17.02.2019).

³¹³ <https://tr.pcisecuritystandards.org/index.php> (erişim tarihi: 17.02.2019).

testlerine başvurulmaktadır. Sızma testlerinde uygulanan eylemler içerisinde hem bilgi toplama hem de sisteme sızma aşamalarına ait eylemler barındırsa da sistem sahiplerinin bilgisi dahilinde yapıldığından suç teşkil etmemektedir.

2.2.2.1.3 Kalıcılığı Sağlama

Sisteme bir kez sızılmış olması, aynı açık kullanılarak ilelebet sisteme sızılabilceği anlamına gelmemektedir. Güvenlik güncellemeleri veya açığın tespit edilerek yama yapılması sonucunda ilgili açık kapanabilir. Bu halde bilişim korsanının en başa dönerek yeniden bilgi toplaması ve başka açıklar araması gerekecek, belki de sisteme bir daha sızamayacaktır. Bu nedenle sisteme istediği zaman girerek kalıcı olmayı amaçlayan bilişim korsanı, bir kez sızdıktan sonra ve çıkış yapmadan önce, güvenlik uygulamalarınca fark edilmeyen ve sadece kendisinin bildiği açıkları bırakır. Bir nevi binaya bir arka kapı veya gizli geçit inşa etmiş olur. Bu eylemlerin niteliği itibarıyla kendilerine aynı zamanda “sistemi sahiplenme” eylemleri de denilmektedir³¹⁴.

2.2.2.1.4 İzleri Yok Etme

Bilişim korsanının da kendi güvenliğini sağlamaya ihtiyacı vardır. Çünkü bilişim sistemlerinin büyük çoğunluğunda yapılan her işlem bazen güvenlik ve bazen de teknolojik ilerlemeyi sağlamak için bilgi toplama amacıyla kayıt altına alınmaktadır. Bu kayıtlar binanın içinde bulunan güvenlik kameraları gibi görülebilir. Eğer bilişim korsanı kamera kayıtlarını temizlemezse, binanın hangi açığından içeriye girdiği, içeride hangi eylemleri yaptığı kolaylıkla görülebilecek ve büyük ihtimalle izleri takip edilerek yakalanacaktır. Yakalanmasa bile yaptığı eylemler görülebildiği için açıklar kolaylıkla kapanacaktır. Bu nedenle işini tamamlayan bilişim korsanı sistemde yer alan log kayıtları ve kayıt defteri girdileri gibi izler başta olmak üzere her türlü izi yok etmeyi amaçlar. Bilişim korsanları ve güvenlik firmaları arasında kayıt teknolojilerini geliştirmek ve tuzaklar kurmak ile bunları yok etmek arasında önemli bir mücadele devam etmektedir³¹⁵.

Log kayıtlarının güvenliğini sağlamak için alınan bir önlem de IP Log İmzalayıcı’dır. Kayıtların elektronik olarak imzalanması sayesinde sahteleri ile değiştirilmesinin önlenmesi amaçlanmaktadır. Mülga İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğin 5/e bendinde “Başkanlık tarafından verilen yazılım ile” log imzalaması yapılacağı öngörülmüş-

³¹⁴ Elbahadır, 2016: 225.

³¹⁵ Karagülmez, 2014: 90.

ken, 11.04.2017 tarihli yeni yönetmelikte bu ibare çıkartılmış ve BTK, IP Log İmzalayıcı ile ilgili soru ve sorunlara destek vermeyeceğini açıklamıştır³¹⁶.

2.2.2.2 Bilişim Suçlarının İşlenmesinde Sık Görülen Yöntemler

Bilişim korsanları, her yeni gelişmeyi kendi saldırıları için bir araca dönüştürmektedir. Bu nedenle yapılan bilişim saldırılarını sınırlı sayıda saymak veya sınıflandırmak mümkün olmamaktadır. Ayrıca bilişim saldırılarında kullanılan yöntemler birden fazla aşamada da kullanılabilir, bu nedenle yöntemlerin saldırı aşamalarına göre sınıflandırılması da sağlanamamaktadır. Örneğin, bilgisayar virüsleri hem sisteme sızma aşamasında hem de izleri yok etme aşamasında kullanılabilir, tek bir aşamaya özgü olmamaktadır. Bu nedenle eserin bu bölümünde sık görülen yöntemlerin sayılması ve kısa bilgilerin verilmesiyle yetinilecek, ayrıca bir sınıflandırmaya girilmeyecektir.

2.2.2.2.1 Zararlı Yazılımlar (Malware)

Zararlı yazılım terimi, İngilizce malicious (kötü niyetli) kelimesinin başı (mal) ve software (yazılım) kelimesinin sonu (ware) alınarak “malware” şeklinde türetilmiştir. Zararlı (kötü niyetli) yazılımların birçok farklı fonksiyonu ve amacı olabilmektedir. Zararlı yazılımlar sisteme izin dahilinde veya izinsiz girmeleri ile metamorfik olup olmadıkları (kendini kopyalayıp kopyalayamadıkları, kodunu kendi kendine değiştirip değiştiremedikleri) göre farklılıklar göstermektedir³¹⁷.

Zararlı yazılımların yayılma biçimleri yıllara göre kullanıcı deneyimi ve bilincinin gelişmesiyle farklılık göstermiştir. İlk zamanlarda basit mesajlarla gönderilen zararlı yazılımlar, kullanıcıların artık mesajlar ve e-mail aracılığıyla gelen bu tür iletilere karşı bilinçlenmesinden sonra daha teknik bir hal almışlardır. Öyle ki bir araştırmaya göre modern zararlı yazılımların yüzde 90’lık bir kesimi daha önce hacklenen popüler bir internet sitesi üzerinden yayılmıştır³¹⁸.

Zararlı yazılımlar en genel haliyle ve niteliklerine göre virüsler, solucanlar ve truva atları olarak üçe ayrılmaktadır³¹⁹. Bununla birlikte günümüzde artık bunların karışımı olarak harmanlanmış tehditler (blended threats) olduğu da bilinmektedir³²⁰. Ayrıca virüsler, solucanlar ve truva atları kullanıldığı amaçlara veya sahip olduğu özel yeteneklere göre bazı özel isimler de alabilmektedir. Bu bölümde zararlı yazılımlar, öğretiler yer alan görüşler ve genel

³¹⁶ <https://www.btk.gov.tr/ip-log-imzalayici> (erişim tarihi: 25.02.2019).

³¹⁷ <https://www.kaspersky.com.tr/resource-center/definitions/metamorphic-virus> (erişim tarihi: 25.02.2019).

³¹⁸ Goodman, 2016: 26.

³¹⁹ Olovsson, 1992: 10.

³²⁰ https://support.symantec.com/en_US/article.TECH98539.html (erişim tarihi: 25.02.2019).

kabul gören bilişim güvenlik (antivirüs) şirketlerinin güncel sınıflandırmaları dikkate alınarak incelenecektir.

2.2.2.2.1.1 Virüsler

Virüsler (bilişim virüsleri), kullanıcının izni ya da bilgisi dahilinde olmaksızın bilişim sisteminin çalışma şeklini değiştiren, küçük farklılıklarla kendisini kopyalayabilen³²¹, gizleyen ve erişilemez olmaya çalışan bir tür zararlı yazılımdır³²². Bulaştığı dosyaları kullanılmaz hale getirebildiği gibi, sisteme yük bindirerek onu yavaşlatma amacı da güdebilir³²³.

Bilişim virüsü terimi ilk kez Fred Cohen'in 1983 yılında Güney Kaliforniya Üniversitesi'ndeki yüksek lisans tezinde kullanılmıştır³²⁴. İlk boot bilişim virüsü saldırısı ise 22 Ekim 1987'de Delaware Üniversitesi'nde kayıt altına alınmıştır³²⁵. Basit Farooq Alvi ve Amjad Farooq Alvi isimlerindeki bilgisayar dükkânı sahibi iki kardeşin, yasadışı dağıtılan bir medikal yazılımı engellemek için korsan kopyasını yaparak yazılımı oldukça yavaş hale getirmeye çalıştığı, ancak programdaki hata nedeniyle daha da zararlı bir kod haline geldiği, böylece ilk bilişim virüsünün oluştuğu söylenmektedir³²⁶. Bu virüse "brain" ismi verilmiştir.

Virüsler bulundukları bölgeye göre boot virüsleri, dosya virüsleri ve makro virüsleri olarak üçe ayrılmaktadır. Boot (ön yükleme) virüsleri, kendisini boot bölümüne kaydeder. İşletim sisteminden farklı bir alanda bulunduğu ve işletim sisteminden önce ön yükleme çalıştığı için, işletim sistemi yeniden kurulsa (formatlansa) da virüs temizlenemez. Bu virüsler sistemin her başlangıcında kendisinin de çalışmasını garanti altına almış olur³²⁷ ve kurtulmak için özel yöntemler gerekir.

Dosya virüsleri işletim sistemi düzeyinde ayrı olarak veya başka bir yazılımın içinde gizlenmiş olarak bulunur ve çalıştırıldıktan sonra genellikle RAM belleğe yerleşerek orada bulunan her dosyaya kendisini bulaştırır ve programlandığı diğer eylemleri yapar³²⁸. Dosya virüsleri de kendi aralarında yerleşik (resident) ve yerleşik olmayan (non-resident) şeklinde ikiye ayrılmaktadır³²⁹.

³²¹ Bülbül/Bingöl, 2018: 34.

³²² Çıtak, 2018: 119.

³²³ Bulaştıkları dosyaya bir daha bulaşmamak için işaret (virus marker) bırakırlar, ekranda şaşırtıcı mesajlar gösterirler ve normal olmayan sistem davranışlarına neden olurlar. Aydın, 1992: 54.

³²⁴ Kurt, 2005: 69; Aynı zamanda Cohen'in kendi kitabının "yazar hakkında" bölümünde de terimin ilk kez 1983'te kullanıldığından bahsedilmektedir. Cohen, 2010: 7.

³²⁵ Dülger, 2015: 129. İlk virüsün ise 1970'li yılların başında yayılab The Creeper olduğu ifade edilmektedir. Ataç Taş, 2010: 14 – 15.

³²⁶ <https://www.cybrary.it/0p3n/first-pc-virus-brain-virus/> (erişim tarihi: 25.02.2019).

³²⁷ Çıtak, 2018: 120.

³²⁸ Gürler, 2015: 87.

³²⁹ Yerleşik virüsler, sistem belleğinde kendine yer edinen ve sistemin açılışında kendisinin de otomatik açılışını sağlayan virüslerdir. Yerleşik olmayan virüsler ise çalıştırıldıkları zaman yerel veya ağ alanlarında kendisine

Makro virüsleri ise ofis programları (word, excel vb.) veya grafik tasarım programları (photoshop, corel draw vb.) gibi yazılımların dosyalarında görülür. Çünkü bu tür kapsamlı yazılımlar, kullanıcıların kolay kullanması için makro desteği ile gelir. Kullanıcılar fazla yazılım bilgisi gerektirmeyen bu makrolar ile yazılımları kendi ihtiyaçlarına uygun şekilde özelleştirebilir. İşte bu makroların kötü amaçlarla kullanılması, dosyayı çalıştıran sistemlerde virüsün yayılmasına neden olur. Bu tür dosyaların sıkça kullanılması nedeniyle makro virüsleri en sık yayılan virüslerden olmaktadır.

Virüslerin işlevlerini daha kolay irdelemek için virüslerin nasıl yapıldığına bakılabilir. Bu noktada yaygın olarak bilinen ve internet üzerinden kolaylıkla bulunabilecek “Terabit Virus Maker” yazılımından bahsetmekte yarar vardır. Bu yazılım, herhangi bir kod bilgisi gerektirmeden, yalnızca istenilen kutucuklar işaretlenerek virüs yapımına olanak sağlamaktadır. İşaretlenebilen kutucuklar arasında ise, bilgisayarı 5 dakika sonra kapat, internet tarayıcısının açılmasını engelle veya açık olanları her 10 saniyede bir kapat, monitörü kapat, sesi kapat, masaüstündeki veya belgelerdeki tüm dosyaları sil, fare tuşlarını yer değiştir, görev yöneticisini veya başlat tuşunu engelle gibi onlarca seçenek bulunmaktadır³³⁰. Görüldüğü üzere bir virüsle yapılacak işlemler tamamen onu oluşturan kişinin hayal gücüne ve becerisine kalmaktadır. Günümüzde farklı işlevlere sahip on binlerce virüsün varlığından söz edilmektedir³³¹. Elbette ki bunlara görevini başarıyla yerine getirip henüz tespit edilememiş diğer virüsleri de eklemek gerekecektir.

Son olarak, virüslerin karakteristik özelliklerine göre dosya bulaşıcı (klasik – file infector), polimorfik³³², metamorfik³³³, gizli (stealth)³³⁴, zırhlı (kaslı – armored)³³⁵, çok bölümlü (multipartited)³³⁶, kamuflaj (camouflage)³³⁷, arkadaş (companion)³³⁸ ve boşluk (cavity)³³⁹ virüsleri olarak ayrıldığı söylenmelidir³⁴⁰.

hedefler aramakta, bellekte yer tutmamaktadır. <https://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms> (erişim tarihi: 25.02.2019).

³³⁰ Yazılım halen güncel olup, indirme seçenekleri ve diğer detayları ayrıca dipnot olarak verilmeyecektir.

³³¹ Kurt, 2005: 69.

³³² Her çoğalmasında aynı zamanda kendi imzasını da değiştiren, bu sayede fark edilmeden dolaşan virüs.

³³³ İçerdiği kodun fonksiyonelliği aynı kalmak şartıyla, her saldırıda kendi kodunu değiştiren, tespit edilmesi zor virüs.

³³⁴ Bellekte yerleşik olmasına karşın, dosyaların temiz halinin kopyasını da tutarak, antivirüs programlarına bu dosyayı gösteren, enfekte edilmiş dosyaları ise başka alanda tutarak gizli kalmayı amaçlayan virüs.

³³⁵ Karmaşık şekilde tasarlanmış, gerçekte bulunduğu yerden başka bir yerde bulunduğu inancını veren virüs.

³³⁶ Dosya uzantılarına ve boot alanına eşzamanlı olarak saldırabilen virüs.

³³⁷ Enfekte edilmemiş dosyaları enfekte edilmiş gibi antivirüs programlarına gösteren virüsler. Son dönemlerde gelişmiş antivirüs yazılımları nedeniyle sayılarının azaldığı söylenmektedir.

³³⁸ Dosyalarda hiçbir değişiklik yapmayan, bunun yerine aynı dosyanın farklı uzantısıyla bulunan virüslerdir. Örneğin .exe uzantılı bir dosyanın .com şeklinde uzantısı olarak bulunur, uzantıya dikkat etmeyen kullanıcının gerçek dosya yerine kendisini aktif hale getirmesini bekler.

³³⁹ Dosyaların sonuna zararlı kodlarını eklemek yerine, çeşitli nedenlerle boşluk olarak bırakılmış alanlara kodları yerleştiren, böylece virüslü dosyanın boyutunun değişmemesini sağlayan ve tespitini zorlaştıran virüsler.

³⁴⁰ <https://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms> (erişim tarihi: 25.02.2019).

2.2.2.2.1.2 Solucanlar (Worm)

Solucanlar veya ağ solucanları, virüslere benzemektedir. Hatta onların bir alt türü olduğu ifade edilmektedir. Solucanlar kendilerini kopyalayabilen ve kullanıcıların izni olmaksızın sistemlere zarar veren, kendisini birçok ağıta kopyalayabilmek için ağlara odaklanan ve bu açıkları kullanan zararlı yazılımlardır. Klasik virüsler bağımsız olarak başka ağıtlara erişemezken, solucanlar ağları kullanarak bulduğu ağıtlara kendilerini kopyalaması yönüyle virüslerden farklılık gösterirler³⁴¹. Sürekli olarak başka ağıtlara erişme çabası onların solucan olarak adlandırılmasına neden olmuştur³⁴². Doğal olarak solucanlar güvenlik duvarı ile karşılaştığında onu aşmak üzere programlanmaktadır³⁴³.

Ağ solucanları ilk kez 2 Kasım 1988'de ARPANET'e yüklenen bir yazılımın hızla diğer ağıtlara yayılmasıyla görülmüştür. O tarihlere göre yüksek bir rakam olan 2000 bilgisayarın bu zararlı yazılımdan etkilendiği ifade edilmiş ve 150.000 dolarlık bir zarar ortaya çıkmıştır³⁴⁴.

2.2.2.2.1.3 Truva Atları (Trojan Horse)

Truva atları ismini Truva savaşıyla almaktadır. Yunan mitolojisinde önemli bir yer tutan³⁴⁵ Truva savaşı, rivayetlere göre 10 yılı aşkın süre boyunca kentin kuşatılması ve çatışmalarla devam etmiştir. Şehrin bu yollarla ele geçirilemeyeceğini anlayan Yunanlılar ise Truva atı fikrini geliştirmişlerdir. Buna göre içerisinde Yunan askerlerinin olduğu büyük bir tahta at şehre hediye edilir. Hediye şehrin içine kabul edildikten sonra gece vakti atın içindeki askerler dışarı çıkarak şehrin kapılarını açar ve böylece Truva şehri ele geçirilmiş olur.

Truva atları ya da bilişim truvaları (computer trojans) da ismini aldığı mitolojik anlatının özüne uygun olarak kullanıcıların kendi rızaları dahilinde sistemlerine dahil etmesinden sonra işlevini yerine getirip sistemlere zarar veren bir tür zararlı yazılımdır. Virüs ve solucanlardan iki temel noktada ayrılmaktadırlar. İlk olarak kendi kendilerini çoğaltma yetenekleri

³⁴¹ Aydın, Dülger ve Kurt, solucanlar ile virüsler arasındaki farklılıklara değinirken, solucanların virüslerden farklı olarak, sisteme zarar verme zorunluluğu olmaksızın hareket etmesinden bahsetmektedir. Ancak zarar verme kavramı, burada soyut kalmaktadır. Teknik olarak zararlı yazılımların tamamı az veya çok bulunduğu sistemlere zarar vermekte, virüsler ve solucanların verdiği zararın ağırlığı konusunda ölçülebilir bir veri de bulunmamaktadır. Bu bakımdan başka ağıtlara kendilerini kopyalama kriteri virüs ve solucanlar arasında daha isabetli bir ayırım yapılabilmesini sağlayacaktır.

³⁴² Çıtak, 2018: 130.

³⁴³ Dülger, 2015: 126.

³⁴⁴ Dülger, 2015: 126.

³⁴⁵ Homeros'un İlyada ve Odysseia eserlerinde savaştan bahsedilmektedir.

yoktur, kullanıcı tarafından indirilip çalıştırılmayı beklerler³⁴⁶. İkinci olarak ise kullanıcıların rızası (kandırılmış dahi olsa) olarak, onun bilgisi dahilinde sisteme yerleşmektedirler³⁴⁷.

Truva atları, faydalı bir programın içine yerleştirilerek veya doğrudan faydalı bir programın kendisiymiş gibi görünerek kullanıcıların kendilerini indirmesini beklerler. Yazılımların resmi internet sitesi yerine başka yerlerden yapılan indirmelerde bu tür zararlı yazılımlara sıkça rastlanmaktadır. Ya da “Facebook Hesabı Ele Geçirme” adıyla aslında olmayan bir özelliği vaat eden yazılımlar, kendilerini indiren kullanıcıların sistemlerine bu yönüyle sızmış olmaktadır³⁴⁸.

Truva atları sistemde arka kapı (backdoor) açmaktan, veri hırsızlığına, klavye ve fare hareketlerini takip ederek tuş kaydetmekten (keylogger), zombi bilgisayar oluşturarak hizmet aksatma saldırılarına kadar pek çok amaçla kullanılmaktadır. Öyle ki günümüzde en sık kullanılan zararlı yazılım türü olduğundan bahsedilmekte, hatta devletler arası meselelerde dahi görülmektedir³⁴⁹.

2.2.2.2.1.4 Mantık Bombaları (Logic Bombs)

Mantık bombaları sistemde âtıl durumda kalan ve programlandığı şartlar oluştuğu zaman eylemlerini gerçekleştiren zararlı yazılımlardır. Bu şartlar belli bir tarihin veya sayısal koşulun gerçekleşmesi (zaman bombası – time bomb) olabileceği gibi, herhangi bir mantıksal koşul da olabilir, bu halde şartın niteliğine göre farklı isimler alabilirler³⁵⁰. Mantık bombalarının ortaya çıkış nedeninin doğru anda maksimum zararı vermek olduğu ifade edilmektedir³⁵¹. Bir personelin işten ayrıldığı zaman faaliyete geçecek şekilde hazırladığı yazılım ile her yıl 26 Nisan’da faaliyete geçen Çernobil virüsü mantık bombalarına örnek verilebilir³⁵².

Mantık bombaları bir görüşe göre yalnızca truva atlarının bir türü olarak değerlendirilmektedir³⁵³. Bizim de katıldığımız diğer bir görüşe göre ise mantık bombaları virüs, solucan veya truva atı formlarında olabilir³⁵⁴, sadece truva atının mirasçısı olarak gösterilerek kısıtlanmaması isabetli olacaktır.

³⁴⁶ <https://www.symantec.com/connect/articles/security-11-part-2-trojans-and-other-threats> (erişim tarihi: 24.08.2018). Gürler, bu durumu “zararsız yazılım olarak görünme” şeklinde açıklamaktadır. Gürler, 2015: 98.

³⁴⁷ Dülger, 2015: 120.

³⁴⁸ Çıtak, 2018: 129.

³⁴⁹ Devletler arasında veri hırsızlığı amacıyla kullanılan Promis adlı truva atı ile ilgili bilgi için, Kurt, 2005: 65; Dülger, 2015: 121.

³⁵⁰ Gürler, 2015: 100.

³⁵¹ Olovsson, 1992: 9.

³⁵² Orta, 2015: 103.

³⁵³ Dülger, 2015: 126; Kurt, 2005: 73.

³⁵⁴ <https://searchsecurity.techtarget.com/definition/logic-bomb> (erişim tarihi: 25.08.2018).

2.2.2.2.1.5 Bukalemun

Bukalemun zararlı yazılımları ismini aldıkları hayvana benzeyen yönlere sahiptir. Kendini saklamakta başarılı olan ve zararsız yazılım gibi görünen, gerçek kimliklerini ise sisteme girdikten sonra ortaya çıkaran zararlı yazılımlardır³⁵⁵. Bukalemunlar bu özellikleri nedeniyle truva atlarına benzemektedir. Başarılı bukalemun yazılımları yasalara uygun yazılımların her hareketini taklit edebilir, sisteme giren tüm kullanıcıların adlarını ve şifrelerini kaydeder ve kendi amaçları için kullanır³⁵⁶.

2.2.2.2.1.6 Salam Tekniği

Salam tekniği küçük ve fark edilmeyen parçalardan büyük bir sonuç ortaya çıkması anlamında kullanılan bir tekniktir. Bu teknik, yazılımın kod alanındaki kendini gizleme başarısına değil, sonuçlarının önemsenmemesi nedeniyle böyle bir araştırmaya gidilmemesi prensibine dayanmaktadır. Genel olarak banka hesaplarında yapılan küçük oynamalar bu tekniğe örnek gösterilir. Buna göre, faiz veya benzeri matematik hesaplarında paranın on binde birlik ya da yüz binde birlik gibi kuruşların da altında kalan rakamların yuvarlanması gerekmektedir. Salam tekniği kullanılarak da zararlı yazılım aracılığıyla bu yuvarlamalar yazılım sahibinin lehine çevrilmekte, ya yuvarlama kriterleri ya da yuvarlanan miktarın aktarılan hesabı değiştirilmektedir. Değişen küçük miktarların banka görevlileri veya hesap sahipleri tarafından fark edilmesi zor olmakta, ancak birçok hesaptan aktarılan paralar zararlı yazılım sahiplerine büyük miktarda fayda sağlamaktadır³⁵⁷. Yapısının uygun olması nedeniyle bu teknik için genellikle truva atları kullanılmaktadır³⁵⁸.

2.2.2.2.1.7 Zararlı Reklam Yazılımları (Adware)

Günümüzde sık görülen zararlı yazılımların başında gelmektedir. Sistemin kendisine veya içindeki dosyalara zarar verme amacı gütmeyenler, internette gezinti sırasında kullanıcının karşısına sürekli reklam çıkarılmasına neden olurlar. Bu reklamlara tıklanma sayesinde de maddi karşılık elde ederler³⁵⁹. Sık görülmeleri nedeniyle sadece reklam yazılımlarını tarayıp silmeye yönelik tasarlanan bilişim güvenlik programları da geliştirilmektedir³⁶⁰.

³⁵⁵ Kurt, 2005: 75; Dülger, 2015: 127.

³⁵⁶ Aydın, 1992: 51.

³⁵⁷ Dülger, 2015: 121.

³⁵⁸ Kurt, 2005: 67.

³⁵⁹ Çıtak, 2018: 131.

³⁶⁰ Dünya üzerinde popüler olan temizleme aracının 200 milyonun üzerinde indirildiği söylenmektedir. <https://blog.malwarebytes.com/malwarebytes-news/2016/10/malwarebytes-acquires-adwcleaner/> (erişim tarihi: 25.08.2018).

En “iyiniyetli” reklam yazılımları dahi, internet trafiğini etkilediği için sistem performansını etkiler ve yavaş çalışmasına neden olur. Bazı zararlı reklam yazılımları ise kendisini koruma altına alarak sistemden temizlenmesini engelleyecek her türlü önlemi almaya çalışarak sistemin birçok özelliğini kısıtlar. Bizim de karşılaştığımız ve kötü deneyimi elde etme imkânı bulduğumuz Lucky Search adlı yazılım zararlı reklam yazılımlarına örnek olarak gösterilebilir. Bu yazılım internette yapılan her arama sırasında ayrıca bir reklam penceresi ortaya çıkartmakta ve görev yöneticisinden işlevi sonlandırılrsa bile sistem içinde ayrıca bulunduğu bir dizinden kendisini yeniden başlatabilmektedir.

2.2.2.2.1.8 Fidyeye Yazılımı (Ransomware)

Zararlı reklam yazılımları gibi günümüzde oldukça popüler olan diğer bir zararlı yazılım da fidye yazılımlarıdır. “Ransomware” veya “CryptoLocker” adıyla bilinen bu tür yazılımlar sistemde bulunan dosyaları şifrelemeyi amaçlar. Sonrasında ise bilişim korsanları mağdur firmalarla iletişim kurarak, şifrenin kaldırılması için para (fidye) talep etmektedirler. Çoğu zaman da firmalar önemli verilerini kaybetmemek için bu teklifi kabul etmekte, hatta itibarları sarsılmasın diye bu saldırıları duyurmamakta ya da şikayetçi olmamaktadırlar. WannaCry, Petya ve Bad Rabbit isimli zararlı yazılımlar fidye yazılımlarına örnek verilebilir³⁶¹.

Bazı bilişim korsanları ise sahte mesajlar göndererek, dosyaların şifrelendiğini söylemektedir. Bu tür sahte fidye yazılımı bildirimleri de gerçekleri kadar sık görülmektedir³⁶².

2.2.2.2.1.9 Arka Kapı (Gizli Kapı) Yazılımları

Bilişim suçlarının işleme aşamalarından birinin sistemde kalıcılığı sağlama (sistemi sahiplenme) olduğundan yukarıda bahsedilmişti. Bunun sağlanması için de bazı zararlı yazılımlardan destek alınması gerekmektedir. Bu yazılımların ortak özelliği sistemde arka kapı (backdoor) açmaları ve sonraki saldırılar için zemin oluşturmalarıdır. Çeşitli backdoor, truva atları, rootkit ve netcat yazılımları hem sistemde arka kapı bırakmak hem de bıraktıkları izleri silmek için kullanılmaktadır³⁶³.

2.2.2.2.1.10 Tuş Kaydediciler (Keylogger)

Keylogger (tuş kaydedici) kelimesi, klavyede bulunan tuş anlamına gelen “key” ile kayıt, raporlama anlamına gelen “log” kelimelerinin birleşiminden oluşmaktadır. İlk, ilkel tuş kaydediciler yalnızca klavyede basılı tuşları kaydetmekteyken, günümüzde klavye girdilerin-

³⁶¹ Çıtak, 2018: 134.

³⁶² <https://www.volico.com/the-difference-between-real-and-fake-ransomware/> (erişim tarihi: 25.08.2018).

³⁶³ Elbahadır, 2016: 237; Çıtak, 2018: 134; Kurt, 2005: 67.

den başka anlık ekran görüntülerini, sistem loglarını, program açılış ve kapanış saatlerini, çalınan müziklerin isimlerini ve hatta sosyal medyada sohbet edilen kişilerin isimlerini bile kaydedebilmektedir³⁶⁴. Tuş kaydediciler her zaman zararlı yazılım olarak kullanılmayabilir, örneğin bir şirketin personellerine veya ebeveynlerin çocuklarına karşı sistem hareketlerini takip edebilmeleri için bu uygulamaları kullandıkları bilinmektedir. Hatta askeri ve benzeri gizlilik gerektiren sistemlerde de bu tür tüm girdilerin kayıt altına alınması mümkündür.

Tuş kaydediciler yazılımsal ve donanımsal olmak üzere ikiye ayrılır. Yazılımsal tuş kaydediciler lisanslı yazılımlar veya truva atları aracılığıyla sistemde yer edindirler. Donanımsal tuş kaydediciler ise genellikle bilişim sistemlerine takılan bir aparat aracılığıyla işlevini yerine getirirler³⁶⁵.

Basit görünmesine karşın bilişim sistemlerine yapılan neredeyse tüm girişlerin klavye ve fare ile sağlanması, özellikle kullanıcı adları ve parolaları gibi kritik verilerin bu aşamada elde edilebilme imkânı vermektedir. Bu nedenle tuş kaydediciler ile ilgili olarak güvenlik uzmanları ve bilişim korsanları arasında mücadele devam etmektedir. Başta bankalar olmak üzere birçok firma sistemlerinde tuş kaydedicilerin bilgi çalmasını engellemek için sanal klavye uygulamasına geçmişlerdir. Bunun üzerine bilişim korsanları farenin tıklandığı koordinatları raporlama yöntemini denediler, bu sayede sanal da olsa klavyede tuşların yeri değişmediği için tuş dizilimine göre parolaları tespit edebilmekteydiler. Bunun üzerine sanal klavyede tuşların rastgele dizilmesini sağlayacak ve koordinat tespitini de geçersiz kılacak bir yöntem geliştirildi. Bunun karşılığında da farenin tıklanma sırasında ekran görüntüsünü alan bir güncelleme de bilişim korsanları tarafından geliştirildi³⁶⁶. Buna cevap olarak da fare imlecinin sanal klavyede sadece tuşun üzerinde durması ve tıklama yapılmaksızın parola girişinin sağlandığı teknoloji devreye alındı. Gelecekte de mücadelenin bu şekilde süreceği tahmin edilmektedir.

2.2.2.2.1.11 İzleme ve Gizlenme (Sniffing ve Spoofing)

Türkçe kelime anlamı “koklama” olan ve dinleme, izleme anlamında kullanılan sniffing, aynı ağa bağlı aygıtların arasındaki veri akışının izlenmesi anlamına gelmektedir. Bu bakımdan izlemenin gerçekleşebilmesi için ilgili ağa giriş sağlanması veya ağ içerisindeki aygıtlardan birisine sızılması gerekmektedir³⁶⁷.

Ağdaki aygıtlar arasında veri aktarımı bütün olarak değil, paketler halinde gerçekleşmektedir. Her bir pakette de hedef aygıtın bilgisi yer alır ve ağ içerisinde dağıtımına çıkarılır.

³⁶⁴ Gürler, 2015: 92; Çıtak, 2018: 124.

³⁶⁵ Elbahadır, 2016: 108.

³⁶⁶ Çıtak, 2018: 124.

³⁶⁷ ARP spoofing hakkında detaylı bilgi için, Usta, 2015: 83 – 90.

Bu esaslara göre paketler ağdaki tüm aygıtlara ulaşır, hedef bilgisi uyumluysa ise o aygıtta kaydedilir, uyumlu değil ise göz ardı edilerek paket kabul edilmez. Ağ içerisinde izleme yapacak olan aygıt ise gelen her paketi, hedef bilgisi fark etmeksizin kabul etmek üzerine yapılandırılmıştır. Bu sayede ağ üzerinde aktarılan her paket, izleme cihazına da kaydedilmektedir³⁶⁸. İzlemenin yazılım veya donanım kaynaklı olması mümkündür³⁶⁹.

Gizlenme (spoofing) ise sızılmış olan sistemde bilişim korsanlarının kendi sistemlerini koruma ve gizleme amacıyla yaptığı işlemlere verilen isimdir. Gizlenme, sistemde fark edilmeden gezinmeyi sağlayabildiği gibi, ağdaki cihazlardan birisi gibi davranmayı sağladığı için ağ trafiğini de izleme şansına sahip olmaktadır³⁷⁰.

2.2.2.2.2 Hizmet Aksatma Saldırıları

Bilişim sistemlerinin tahmin edilenin ötesinde hızlarda işlem gerçekleştirmesi, onların aksatılmasının mümkün olmadığı anlamına gelmez. Sistem ne kadar hızlı çalışırsa çalışsın, kapasitesinin üzerinde yük bindirilmesi her zaman mümkündür. İşte esas amacı, sisteme girmek veya dosyalara zarar vermek yerine, sürekli olarak istem göndererek sistemlerin çalışmasını yavaşlatan veya aksatan eylemler hizmet aksatma saldırılarının konusunu oluşturmaktadır. Hizmet aksatma saldırıları da diğer zararlı yazılımlar gibi önemli maddi zararlara neden olabilmektedir. Özellikle DDOS saldırıları günümüzde oldukça popüler hale gelmiştir³⁷¹.

2.2.2.2.2.1 DOS ve DDOS Saldırıları

DOS (Denial Of Service – Servis Yadsıması) saldırıları, bir bilişim sisteminin, diğer bir sisteme sürekli istek göndererek onu işlevsiz hale getirmeye yönelik yapılan saldırılardır. DDOS (Distributed Denial Of Service – Dağıtılmış Servis Yadsıması) saldırıları ise ismini aldığı üzere dağıtılmış şekilde birden fazla sistem üzerinden bir sisteme yapılan saldırılardır. Görüldüğü üzere bu tür saldırılar, başlangıçta oldukça masum görünen isteklerin sistemin kaldıramayacağı bir yoğunlukta gönderilmesi prensibine dayanmaktadır. Bu nedenle “sistem kaynaklarını tüketme” saldırıları olarak da adlandırılmaktadırlar³⁷².

İlk DOS saldırısı 1974 yılında David Dennis adlı öğrenci tarafından gerçekleştirilmiştir. Bilgisayara verilen “ext” komutunun, dış aygıtlarla bağlantı sağladığı, ancak herhangi bir dış aygıt sisteme bağlı değilse, bu komutun sistemi kilitlediği ve yeniden başlatılması gerektiğini fark eden Dennis, bir program yazarak, birçok bilgisayara eş zamanlı olarak bu komutu

³⁶⁸ Elbahadır, 2016: 208 – 209.

³⁶⁹ Orta, 2015: 104.

³⁷⁰ Elbahadır, 2016: 214.

³⁷¹ DDOS saldırılarının teknik bilgi yerine sadece çok sayıda sistem gerektirmesi nedeniyle DDOS saldırılarının hackerlar arasında “acizlik” olarak görüldüğü söylenmektedir. Çıtak, 2018: 156.

³⁷² Dülger, 2015: 132; Gürler, 2015: 105.

göndermiş ve böylece 31 bilgisayarı kilitleyerek yeniden başlatmaya zorlamıştır³⁷³. 1990'ların ortalarından itibaren internet üzerinden yapılan sohbetlerde (chat) görülen DOS saldırıları, günümüzde şirketlerin internet sitelerinde sunduğu hizmetleri engellemek amacıyla ticari nedenlerle³⁷⁴ ve hatta politik amaçlarla³⁷⁵ dahi kullanılabilir.

Genellikle internet üzerinden yapılan bu saldırılar internet protokolleri (TCP veya UDP gibi) kurallarının kötüye kullanılması suretiyle gerçekleştirilmektedir. Kullanılan yöntemlere göre ICMP Flood, Smurf, Ping Flood, Ping Of Death veya SYN Flood gibi isimler alabilmektedirler³⁷⁶.

Saldırganlar, tespit edilmemek için DOS ve DDOS saldırılarını genellikle kendi sistemlerinden değil, daha önce ele geçirdikleri ve zombi haline getirdikleri bilişim sistemleri üzerinden yapmaktadırlar. Zombi sistemlerinin oluşturduğu bu sisteme aynı zamanda BotNet (Bot Ağı) de denilmektedir.

Hizmet aksatma saldırılarının benzeri sonuçları bazı iyiniyetli durumlarda da görülmektedir. Örneğin, sınav veya yerleştirme sonuçlarının açıklandığı dönemlerde, güçsüz sunuculara binlerce kişinin aynı anda yaptığı istekler sonucu sunucular çoğu zaman kilitlenmektedir. Bu bakımdan öğrenciler başta olmak üzere birçok kişi DDOS saldırılarının oluşturduğu sonuçları farklı yoldan deneyimleme imkânı yakalamaktadır.

2.2.2.2.2 İstenmeyen Posta (SPAM)

SPAM, istem dışı alınan elektronik postalara genel olarak verilen isimdir. Genellikle reklam veya pornografik amaçlı olarak kullanılan bu postalar çok sayıda kişiye ulaştırılabilir. Özelliğiyle bağdaşmayan bir isim olan “Spiced Pork and Ham”'in (baharatlı domuz ve jambon) kısaltması olarak kullanılmış ve aslında 1960'larda İngiltere’de satılan bir konserve markasından ilham alınmıştır³⁷⁷.

E-posta adresleri aracılığıyla internet üzerinde güvenlik kontrolü ve hesap açma gibi birçok işlemin gerçekleştirilmesi, e-posta adreslerinin popülaritesini korumakta, bu adreslere yönelik girişimleri de cazip kılmaktadır. Hangi e-postanın gereksiz, hangilerinin gerçek olduğunun tespiti de oldukça zordur. Tanınmış e-posta firmaları, posta kutularını önemli ve gerek-

³⁷³ <https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/> (erişim tarihi: 06.09.2018).

³⁷⁴ Örneğin, bir otelin rezervasyon sistemine sahte olarak her defasında farklı isimlerle rezervasyon yapılarak, başkalarının kullanmasına engel olunması yoluyla zarar verilebilmektedir. Gürler, 2015: 105.

³⁷⁵ 2008 yılında Rusya – Gürcistan arasındaki uyuşmazlık nedeniyle, Gürcistan hükümetinin birçok resmî sitesi Rus bilişim korsanları tarafından DDOS saldırılarına tabi tutulmuştur. Elbahadır, 2016: 125.

³⁷⁶ Elbahadır, 2016: 118 – 121.

³⁷⁷ 1970'lerde İngiltere’de ünlü komedi programı olan Monty Python’da işlenmiş yemek istemeyen bir çiftin, gittiği lokantada spam içeren ürünlerden başka bir şey bulamayıp yemek zorunda kalmalarını konu eden skeçten ilham alındığı söylenmektedir. <http://www.pau.edu.tr/bidb/tr/sayfa/spam-postalar> (erişim tarihi: 06.09.2018).

siz (spam) olarak ayırmaktaysa da, bunun tüm postaları ayırt etmesi şimdilik mümkün değildir. Bazı firmaların veri tabanlarında bulunan e-posta adreslerini satmaları³⁷⁸, bilişim korsanlarının yaptıkları aktif veya pasif aramalarda elde ettikleri veriler, site içeriklerinde e-posta adresi tarayan yazılımlar³⁷⁹ ve e-posta iletilmesi (forward) de gereksiz postaların çoğalmasına neden olmaktadır.

Tüm bu sakıncalı yönlerine karşın gereksiz postaların oluşturduğu en büyük sorun, internet trafiğini olumsuz yönde etkilemeleridir. İnternet trafiğinin önemli bir bölümünün e-postalardan, posta trafiğinin yüzde yetmişinin de gereksiz postalardan³⁸⁰ oluştuğu düşünüldüğünde, gereksiz postaların önemi daha iyi anlaşılabilir. Bu nedenle gereksiz postalara, hizmet aksatma saldırıları içinde yer vermek daha doğru olacaktır. Gereksiz postaların özel yasalarla düzenlendiği ülkeler bulunmakta, ülkemizde ise genel veya özel olarak herhangi bir düzenlemeye gidilmediği görülmektedir³⁸¹.

2.2.2.2.3 Tavşanlar

Zararlı yazılım olarak kabul edilen tavşanlar, özellikleri bakımından diğer hizmet aksatma yöntemlerine benzerler. Sisteme bir kez girdikten sonra, işlemciye sürekli olarak yük bindirerek, onu yavaşlatarak yapması gereken işlere engel olur ve diskte yer alan tüm alanı doldururlar³⁸². Çok hızlı çoğalması ve istek üretmesi nedeniyle tavşan ismini almıştır³⁸³. Bu bakımdan sisteme içeriden DOS saldırısı yapıyormuş gibi düşünülebilir.

2.2.2.2.3 Sosyal Mühendislik

İnsanların belli konulardaki zaaflarından veya bilgi eksikliklerinden faydalanarak bilgi etme yöntemine sosyal mühendislik denilmektedir. Diğer yöntemlerin arasında muhtemelen en az teknik bilgi gerektiren, buna karşın çoğu ihtimalde oldukça etkili sonuç vermesi nedeniyle günümüzde sosyal mühendislik örneklerine sıklıkla rastlanmaktadır. Her ne kadar teknik bilgi gereksinimi az olsa da, daha detaylı ve teknik desteklenmiş saldırıların başarıya ulaşma ihtimali daha fazladır. Hatta sosyal mühendislik sayesinde sisteme giriş bilgileri ele geçirilirse, sistemin teknik olarak ne kadar güvenli olduğunun pek önemi kalmamaktadır. Ayrıca sistemde açık bulamayan yetenekli bilişim korsanlarının son çare olarak sosyal mühendisliğe

³⁷⁸ 500.000 adet e-posta adresinin 100 dolar civarında satıldığı ileri sürülmektedir. <https://keremkoseoglu.com/2005/04/30/e-posta-adresini-spammerlardan-saklayin/> (erişim tarihi: 06.09.2018).

³⁷⁹ Bu yazılımlar, sitelerde yer alan tüm metinleri inceleyerek ornek@ornek.com formatındaki tüm metinleri otomatik olarak posta listesine ekleyen yazılımlardır. Bu nedenle herhangi bir alanda posta adresinin açıkça yazılmaması önerilmektedir.

³⁸⁰ <http://www.pau.edu.tr/bidb/tr/sayfa/spam-postalar> (erişim tarihi: 06.09.2018).

³⁸¹ Dülger, 2015: 130.

³⁸² Aydın, 1992: 52.

³⁸³ Dülger, 2016: 126.

başvurmaları da sosyal mühendisliğin uzmanlar arasında da yaygın olduğu ve çok geniş bir yelpazede geliştiğinin göstergesidir.

Sosyal mühendislik, aslında Türk Dil Kurumu'nun sözlüğüne girmiş ve halk arasında bilinen haliyle “tokatlama”nın³⁸⁴ ta kendisidir. Bilişim alanında görülen sosyal mühendislik örnekleri de çeşitli yazılımlar kullanılarak veya en sade haliyle basit elektronik postalar aracılığıyla kurbanı etkilemeyi amaçlamaktadır.

Sosyal mühendisliğin sosyolojik ve psikolojik boyutları çalışmamızın kapsamı dışında olsa da, muhatabı etki altına almak için yetkili ve otoriter biriymiş gibi görünüm, yardımsever ve minnet altında bırakan görünüm veya muhatap ile ortak sosyal alanlar (hemşehricilik, spor kulüpleri gibi) bulan sosyal görünüm yöntemlerinin uygulandığı söylenmelidir³⁸⁵.

2.2.2.2.3.1 Oltalama (Phishing)

Phishing, “password” (şifre) ve “fishing” (balık avlama) kelimelerinin birleştirilmesiyle oluşturulmuştur. Şifre avlama anlamına gelen kelime, dilimize oltalama veya yemleme olarak çevrilmiştir³⁸⁶.

Oltalama saldırıları tamamen bilişim korsanının hayal gücüne dayalıdır. Bu nedenle tam bir sınırının çizilmesi mümkün olmamaktadır. Ancak bir sonraki konuda değinilecek sahte ve geçici postalar ile sahte internet siteleri hazırlanması yöntemleri sık karşılaşılan oltalama teknikleridir. Gerçeğine çok yakın tasarlanan internet sitelerine kullanıcıların yönlendirilerek kullanıcı adlarını ve şifrelerini girmelerini sağlamasıyla büyük zararların ortaya çıktığı bilinmektedir. İngiltere polisinin yapmış olduğu ankette işletmelerin üçte birinden fazlasının siber dolandırıcılık girişimlerine maruz kaldığı bildirilmektedir³⁸⁷.

Oltalama, muhatapları yönünden yaygın ve doğrudan olmak üzere ikiye ayrılmaktadır. Yaygın oltalamada, hazırlanan kimlik avı yöntemi birden fazla kişiye aynı anda gönderilir ve yemi yutmaları beklenir. Doğrudan oltalamada (spearphishing) ise tek bir muhatap seçilerek, ona özgü ve daha inandırıcı bilgiler ile ikna edilmeye çalışılmaktadır³⁸⁸. Kredi kartı bilgilerinin ele geçirilmesi için bir bankanın olası tüm müşterileriyle iletişim kurulması için yaygın oltalama yöntemi kullanılır, çünkü bu örnekte önemli olan oltalamanın niteliği değil niceliği-

³⁸⁴ Kemal Sunal'ın bilinen sinema filmi Tokatçı'da, kötü karakterlerin zaaflarından faydalanarak onları dolandırma yöntemleri ele alınmıştır. Tokatlamanın kelime anlamı için, http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5b9398396a6b93.89947248 (erişim tarihi: 08.09.2018).

³⁸⁵ Elbahadır, 2016: 199 – 200.

³⁸⁶ Dülger, 2016: 132.

³⁸⁷ <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/fraud/little-book-of-big-scams-business-edition.pdf> (erişim tarihi: 08.09.2018).

³⁸⁸ <https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/fraud/little-book-of-cyberscams.pdf> (erişim tarihi: 08.09.2018).

dir. Belli bir internet sitesindeki veritabanına erişmek için en zayıf halka olarak seçilen personelle iletişim kurulması için doğrudan ortalama yapılması gerekir, çünkü posta diğer personellere de gönderilirse içlerinden herhangi birinin fark etmesi ve tüm girişimin başarısız olma ihtimali daha da artmaktadır.

Oltalama saldırılarında bulunan internet sitelerine ilişkin bilgiler veritabanlarında toplamakta ve bazı internet siteleri tarafından bir sitenin oltalama (phishing) amaçlı olarak kullanılıp kullanılmadığı sorgulanabilmektedir³⁸⁹.

2.2.2.2.3.2 Sahte ve Geçici Postalar

Esasında bir oltalama tekniği olan sahte ve geçici postalar, sıkça kullanılmaları ve neredeyse her sıradan kullanıcının karşılaşması nedeniyle ayrı bir başlık altında değerlendirilmektedir.

Alan adı (domain) üzerinde yetki sahibi olduğu durumlarda geçici postalar alınabilmektedir. Böyle bir yetki yoksa bilişim korsanları sahte (fake) posta adreslerini geçici adreslere bağlamaktadır. Bu sayede örneğin facebook tarafından e-posta gönderilmiş gibi gösterilerek, verilen yanıtın mailde gösterilen adres yerine bilişim korsanının seçtiği geçici adrese göndermesi sağlanabilmektedir³⁹⁰. Sahte ve geçici e-posta kombinasyonu ile yapılan saldırılar, saldırganın tespitini de zorlaştırmaktadır.

Gönderilen sahte e-postalar ile sistemde sorun olduğu, bakım yapılması gerektiği veya güncelleme yapılması gerektiği gibi gerekçelerle, şifre, anne kızlık soyadı gibi bilgiler istenebilmektedir. Bu yöntemler her ne kadar kolay fark edilebilir gibi görünmekteyse de halen birçok kişi bu tür kimlik avı dolandırıcılıklarının mağduru olmaktadır³⁹¹.

2.2.2.2.4 Diğer Yöntemler

Daha önce bahsedilmiş olduğu gibi, bilişim suçlarının eksiksiz bir tasnifini yapmak oldukça zordur. Sürekli gelişen, birbirinin parçaları haline gelen veya etkisini yitiren birçok yöntem mevcuttur. Bu bakımdan sayılanların dışında yer alan diğer yöntemlere de kısaca değinilmekle yetinilecektir.

Bahsedilecek yöntemlerden ilki, aralarında en az karmaşık olanıdır. Kas gücü (kaba kuvvet – brute force) olarak adlandırılan bu yöntem tüm ihtimallerin denenerek sonuca ulaşılması esasına dayanır. Parola kırma saldırılarında milyonlarca muhtemel parolanın tek tek denenmesi ile sonuca ulaşılabilir. Kas gücü saldırıları, saldırıyı yapacak aygıtın gücü

³⁸⁹ www.phishtank.com (erişim tarihi: 11.04.2019), gibi siteler üzerinden daha önce oltalama saldırısı yaptığı bildirilen siteler içinde arama yapılabilmektedir.

³⁹⁰ Çıtak, 2018: 152.

³⁹¹ Elbahadır, 2016: 108.

ve şifrenin zorluğu ile orantılıdır³⁹² ve basit ve kısa şifrelerde diğer karmaşık yöntemleri denemekten çok daha pratik ve etkilidir. Bu nedenlerle şifrelerde büyük, küçük harf, rakam ve özel karakterler (^+%-&/ gibi) kullanılması önerilmektedir³⁹³. Yapılan araştırmalarda³⁹⁴ kişilerin hesaplarına ait şifreleri neredeyse hiç değiştirmedikleri ve genel olarak kolay bulunabilir şifreler kullandıkları görülmekte, bu da kaba kuvvet saldırılarına rastlanmaya devam edileceğini göstermektedir.

Çöpe dalma veya atık toplama olarak adlandırılan diğer yöntemde, veri işleme sonucu arta kalan bilgilerin toplanması veya silinen bilgilerin çeşitli yöntemlerle geri getirilmesiyle elde edilmesi sonucu bilgi toplanması söz konusudur. Çünkü elektronik veya manyetik ortamda silinme işleminden kasıt biçim değiştirmeden ibarettir ve geri dönüşü her zaman mümkün olabilir³⁹⁵. Bu yöntem çıktı birimlerinden çıkan kâğıt ve mürekkeplerin incelenerek bilgi edilmesi gibi fiziki yöntemleri de kapsamaktadır³⁹⁶. Basit gibi görünse de, bu çöplerde birçok sistemin giriş bilgileri elde edilmiş, hatta filmlere de konu olmuştur. Bugün bizlere gelen kredi kartları ve şifrelerini içeren mektupların kart alındıktan sonra olduğu gibi çöpe atılması da tehlikenin boyutunu ortaya koymaktadır.

Veri aldatmacası olarak adlandırılan başka bir yöntemde verilerin kayıt sırasında değiştirilmesi veya bazı verilerin kasten bırakılması söz konusudur³⁹⁷. Süper darbe yönteminde sistemdeki kullanıcı yetkileri kötüye kullanılır ve aslında sistemin çökmesi gibi tehlike altında sistemi kurtarmaya yarayan özel yetkiler doğrudan bilişim suçu işlemek amacıyla kullanılır³⁹⁸.

Bahsedilen yöntemlerden daha farklı yapıya sahip “omuz sörfü”nden de bahsedilmelidir. Şifrelerin yazılması sırasında fiziki olarak izlenmesi, ajanda ve not kağıtlarının incelenerek şifrelerin tespiti gibi bilgilerin bilişim alanı dışında toplandığı yöntemlerle bilişim suçlarının işlenmesi için zemin hazırlanabilir³⁹⁹.

Son olarak, tüm bunların başarısızlığa uğrayabilen yöntemler olduğu vurgulanmalıdır. Çünkü başarılı yöntemler henüz fark edilmemiş demektir ve muhtemelen onu oluşturan bilişim korsanı tarafından da kolayca açıklanmayacaktır.

³⁹² <https://www.betterbuys.com/estimating-password-cracking-times/> (erişim tarihi: 09.09.2018). İnternet sitesinde ortalama bir işlemciyle şifrelerin ne kadar sürede kırılabilceği hesaplanmaktadır. Elbette bu hesaplama kullanılan algoritmaya göre değişebilmektedir.

³⁹³ Dülger, 2016: 133.

³⁹⁴ Örneğin, Bilek, 2012: 105.

³⁹⁵ Kurt, 2005: 62.

³⁹⁶ Dülger, 2016: 134.

³⁹⁷ Aydın, 1992: 48.

³⁹⁸ Aydın, 1992: 49; Kurt, 2005: 66.

³⁹⁹ İlbaş, 2009: 29.

2.2.2.2.5 Hactivizmin Bilişim Suçu Olup Olmadığı Sorunu

Hactivizm, diğer adlarıyla bilişim aktivizmi ya da bilgisayarlı aktivizm, temel olarak bilişim sistemleri ile politik görüşlerin kitleler üzerinde yayılması veya bir soruna toplumsal tepki gösterilmesi anlamına gelmektedir⁴⁰⁰. Hactivizmin farklı örneklerinin görülmesi, bilişim suçu sayılıp sayılmaması yönünde de tartışmaya neden olmuştur.

Hactivizmin bilişim suçu olarak kabul görüldüğü görüşe göre, hactivist hareketler koleksiyon, yayımlama, diyalog, eylem koordinasyonu ve kulis faaliyetleri olarak beşe ayrılmaktadır. Bu yöntemler ile yayınlara hükümet tarafından konulan sansürlerin aşılabildiği, wikileaks olayında da görüldüğü şekilde devletlere ait gizli belgelerin sızdırılabildiği, bilişim korsanlarının, bilişim suçlarına dair detaylar vererek bu suçları özendirdikleri, internet üzerinden çeşitli eylemler için örgütlenme yapılabildiği söylenmektedir⁴⁰¹. Hactivistlerin adaletsiz bulunduğu konularda hakkı kendinde görerek misilleme amacıyla saldırıda bulunmaları, halkın gözünde iyi bir imaja sahip olmak için de bu eylemlerde ezilenlerin yanında sloganlar kullanmaları da oluşumun nitelendirilmesi için aleyhe kullanılan argümanların başında gelmektedir⁴⁰².

Hactivizmin başlı başına bir suç türü olarak kabul edilmediği görüşe göre ise, bazı hallerde suçların işlenmesinde kullanılan yöntemlerin bütünüyle bir suç modeli olarak tanımlanması ciddi derecede hatalı ve internetin doğasına hatalıdır. Bu tür bir kabul, beraberinde ifade özgürlüğünü ve demokrasiyi kısıtlayıcı tedbirlerin alınmasını beraberinde getirecektir⁴⁰³. Yine, hactivistlerin adaletsizliklere karşı düzenledikleri bazı eylemlerde (Anonymous üyelerinin yasal bir operasyon kapsamında çocuk istismarı sitelerini hedef alması ve bu hizmetleri kullanan on beş bin kişinin bilgilerini afişe etmesi gibi) kitlelerin içten içe kendilerini desteklerken bulması örnek gösterilerek, hactivizmin organize suç veya siber terörist yapılanmalarıyla karıştırılmaması gerektiği şeklinde fikirler de ileri sürülmektedir⁴⁰⁴.

Bu noktada hactivizmin tek başına bir suç türü olmadığı görüşüne katılmakla birlikte, sorunun hactivizmin tam olarak nitelendirilememesinden kaynaklandığını düşünmekteyiz. Aynı durumun bilişim korsanlarının nitelendirilmesinde yaşandığı da göz önüne alınırsa, ön yargılardan uzak ve tarihsel gelişime uygun bir yorum izlenmesinde fayda olacaktır. Hactivizmin ilk olarak eğlence amaçlı olarak ortaya çıkmasının ardından, günümüzde toplumsal ve politik yönlerinin daha ağır bastığı söylenmektedir⁴⁰⁵. Ancak bu durum, birçok hareketi içinde

⁴⁰⁰ Demirkıran, 2013: 28.

⁴⁰¹ Karagülmez, 2014: 82 – 86.

⁴⁰² Goodman, 2016: 46.

⁴⁰³ Dülger, 2015: 136.

⁴⁰⁴ Goodman, 2016: 48.

⁴⁰⁵ Demirkıran, 2013: 27.

barındıran hactivist eylemleri doğrudan suç türleri içerisine almayı gerektirmemektedir. Nasıl ki şiddet içermeyen toplantı ve gösteri yürüyüşleri yapmak Anayasal bir hak ise hactivist eylemler de düşünce özgürlüğü kapsamında aynı çerçevede değerlendirilmeli, bunların içinde ceza yasalarında suç olarak tanımlanan hareketler bulunması halinde ayrıca ele alınmalıdır.

2.3 Karşılaştırmalı Hukukta Bilişim Suçları ve Bu Suçlar ile Mücadele

2.3.1 Uluslararası Örgütler

Bilişim suçlarının çok uluslu, sürekli ve hızlı oranda gelişen yapısı, bilişim suçları ile mücadelede de aynı oranda titizliği ve karşılıklılığı gerektirmektedir. Asya – Pasifik Ekonomik İş Birliği (APEC), Avrupa Konseyi (COE), Avrupa Birliği (EU) ve Amerikan Devletleri Örgütü (OAS) gibi bölgesel; Commonwealth, G8, OECD ve Birleşmiş Milletler gibi çok uluslu topluluklar bilişim suçları ile mücadele konusunda önemli atılımlar gerçekleştirmiştir. Buna karşın iş birliğinin yeterli seviyede olmaması ve bilişim suçları ile mücadelenin kayda değer oranda maddi kaynak gerektirmesi, beklenen sonuçların alınamamasına neden olmaktadır⁴⁰⁶.

Uluslararası örgütlerce uygulanan projelerin niteliği incelendiğinde, genel olarak gelişmiş ülkelerin sınır aşan bir suç tipi olarak bilişim suçlarını kontrol altına alabilmek için, gelişmekte olan ve az gelişmiş ülkelere önemli yatırım ve desteklerde bulunduğu, böylece ülkelere sınır ötesinden gelen tehditleri engellemeye çalıştıkları görülmektedir. Ayrıca uluslararası örgütler tarafından hazırlanan bağlayıcı veya tavsiye niteliğindeki metinlerde ceza sorumluluğu için “haksız” ve “kasıtlı” olma şartı özellikle vurgulanmaktadır⁴⁰⁷.

2.3.1.1 Birleşmiş Milletler

Bilişim teknolojilerinin gelişmesi ve bilişim suçlarının yaygınlaşması ile birlikte Birleşmiş Milletler’in de bu konu üzerine eğildiği görülmektedir. İlk olarak 7. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongresinin ardından 1985 yılında hazırlanan Milan Eylem Planı’nın 224. paragrafında yeni mağdur şekillerinin ortaya çıktığı ifade edilmiş, buna örnek olarak da bilgisayar suçlarından oluşan mağduriyetler gösterilerek konu tartışılmıştır⁴⁰⁸. Bir sonraki (8.) kongre 1990 yılında Havana’da gerçekleştirilmiş ve kongrenin ardından düzenle-

⁴⁰⁶ Yılmaz, 2016: 164.

⁴⁰⁷ Mahmutoğlu, 2001: 40.

⁴⁰⁸ Çeşitli suç türlerinin tartışıldığı bu eylem planında bilişim teknolojilerinin ceza soruşturmasındaki kullanım önerilerine de yer verilmektedir. <https://digitallibrary.un.org/record/114498/files/a-conf-121-22-rev-1-e.pdf> (erişim tarihi: 25.02.2019). Erdoğan, 2013: 64.

nen raporda ise bilgisayar bağlantılı suçlara (computer-related crime) özel bir bölüm verilerek birtakım tavsiyelerde⁴⁰⁹ bulunulmuştur⁴¹⁰.

Birleşmiş Milletlerin bilişim suçları ile ilgili çalışmaları yürüten birçok organizasyonu mevcuttur. Bunlardan 1997 yılında kurulan UNODC (United Nations Office on Drugs and Crime – Birleşmiş Milletler Uyuşturucu ve Suç Ofisi) bilişim suçları ile uzun vadede, ulusal yapılar ile iş birliği içinde, sürdürülebilir bir eylemliliği kendisine misyon edinmiştir⁴¹¹. UNODC’nin yönetim yapısında ise CCPCJ (Commission on Crime Prevention and Criminal Justice – Suç Önleme ve Ceza Adaleti Komisyonu) yer almaktadır. Bu komisyon, BM Genel Kurulunun önerisiyle, Ekonomik ve Sosyal Konseyin 1992/1 sayılı kararı ile kurulmuş ve 2006 yılında görevleri genişletilerek bugünkü halini almıştır. Komisyonun her yıl düzenli olarak hazırlanan raporlarında sınır aşan bir suç tipi olarak ifade edilen bilişim suçları ile mücadele konusundaki açıklamalarına yer verilmektedir⁴¹². Komisyon aynı zamanda 2015 yılında “bilişim suçları deposu” projesini hayata geçirerek, yasal düzenlemeler ve elektronik deliller gibi konularda bilişim suçlarına ilişkin bir veritabanı hazırlamıştır⁴¹³. Adı ünlü dedektif Sherlock Holmes’a benzeyen SHERLOC (Sharing Electronic Resources and Laws on Crime) portalından bu veritabanına erişmek mümkündür⁴¹⁴.

Birleşmiş Milletler, bilişim suçlarının yanında, siber terörizm ve siber savaş konularında da farklı çalışmalar göstermektedir⁴¹⁵. Bu organizasyonlar arasında UNIDIR⁴¹⁶ (United Nations Institute for Disarmament Research – Birleşmiş Milletler Silahsızlanma Araştırmaları Enstitüsü), ITU⁴¹⁷ (International Telecommunication Union – Uluslararası Telekomünikasyon Birliği) ve CTITF⁴¹⁸ (Counter Terörizm Implementation Task Office – Terörle Mücadelede Uygulayıcı Görev Gücü) sayılabilir.

⁴⁰⁹ Üye devletlerden toplu şekilde eforda bulunmalarının istenilmesi, ulusal ceza mevzuatının modernize edilmesi, bilişim güvenliği ve korumasının güçlendirilerek toplumun duyarlı hale getirilmesi, adli süreçte yer alan şüphelilerin yeterli eğitim almasının sağlanması, bilişim suçlarının önlenmesi üzerine yayınların hazırlanarak gelecek yıl bütçelerine dahil edilmesi gibi öneriler getirilmiştir.

⁴¹⁰ <https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf> (erişim tarihi: 25.02.2019).

⁴¹¹ <https://www.unodc.org/unodc/en/cybercrime/index.html> (erişim tarihi: 25.02.2019).

⁴¹² <http://www.unodc.org/unodc/en/commissions/CCPCJ/session/index.html> (erişim tarihi: 25.02.2019).

⁴¹³ <https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html> (erişim tarihi: 25.02.2019).

⁴¹⁴ <https://sherloc.unodc.org/cld/v3/sherloc/> (erişim tarihi: 25.02.2019).

⁴¹⁵ Yılmaz, 2016: 158.

⁴¹⁶ UNIDIR’in hedefleri arasında, ulusal, bölgesel veya çok taraflı düzeyde politika odaklı çalışmalar ile konuyla ilgili araştırma ve analizler bulunmaktadır. <http://www.unidir.org/est-cyber> (erişim tarihi: 25.02.2019). UNIDIR’in siber stabilite ile ilgili model önerilerine ilişkin çeşitli yayınları da bulunmaktadır.

⁴¹⁷ Dünyayı birbirine bağlama konusunda taahhütte bulunan vizyonuyla ITU, yapay zekadan nesnelerin internetine ve bilişim güvenliğine kadar birçok konuda çalışma göstermektedir. Projelerinin arasında çevrimiçi alanda çocuk koruma, ulusal stratejiler, bilişim güvenliğinin standardizasyonu ve radyo iletişiminin korunması gibi farklı çalışmalar bulunmaktadır. <https://www.itu.int/en/action/cybersecurity/Pages/default.aspx> (erişim tarihi: 25.02.2019).

⁴¹⁸ 11 Eylül saldırısının ardından hazırlanan terörizmle mücadele stratejisi kapsamında 2005 yılında kurulan CTITF, 2009, 2001 ve 2018 yıllarında yayımlanan terör amaçlı internet kullanımına ilişkin yayınları ile bu ko-

2.3.1.2 OECD

Ekonomik İşbirliği ve Kalkınma Örgütü (OECD) ilgilendiği eğitim, ekonomi, finans, nükleer gibi konuların yanı sıra bilim ve teknoloji konularına da uzun yıllardır eğilim göstermektedir. İlk olarak 1983 yılında ceza hukuku ile bilişim suçları arasındaki ilişkinin tartışılması amacıyla OECD bünyesinde komite kurulmuştur⁴¹⁹. 1986 yılında yayımlanan “Computer-Related Crime: Analysis of Legal Policy” adlı rapordan⁴²⁰, 1999 yılında e-ticaret içeriklerine ilişkin tüketici rehberine, 2017 yılında bilişim risk yönetiminde sigortacılık rolünün geliştirilmesine kadar farklı alanlarda raporlar hazırlanmıştır⁴²¹.

Araştırma konumuz ile asıl ilgili olan kısmı ise 1992 yılında hazırlanan “Bilişim Sistemleri Güvenliği İçin OECD İlkeleri” adlı rapor oluşturmaktadır⁴²². Öneri niteliğinde olan bu ilkeler daha sonra 2002 yılında güncellenmiştir⁴²³. Birbirini tamamlayıcı toplam dokuz ilke⁴²⁴ üye devletlere önerilmektedir.

Bu konuda ayrıca 2009 yılında hazırlanan “Bilgisayar Virüsleri ve Diğer Zararlı Yazılımlar: İnternet Ekonomisine Bir Tehdit” adlı rapordan bahsedilmesi gerekmektedir. Raporda zararlı yazılım türleri ile bunların ekonomik yönden irdelemesi ve bilişim alanında yer alan

nuda çalışmalar göstermektedir. <https://www.un.org/counterterrorism/ctitf/en/publications> (erişim tarihi: 25.02.2019).

⁴¹⁹ <http://www.webology.org/2007/v4n3/a45.html> (erişim tarihi: 25.02.2019).

⁴²⁰ Erdoğan, 2013: 64.

⁴²¹ https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en#page2 (erişim tarihi: 25.02.2019).

⁴²² <http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm> (erişim tarihi: 10.09.2018). Raporun basılı hali de ayrıca bulunmaktadır.

⁴²³ İlkeler Türkçe dahil olmak üzere birçok dile çevrilmiştir. <http://www.oecd.org/sti/ieconomy/32493366.PDF> (erişim tarihi: 10.09.2018).

⁴²⁴ 1. Bilinç

Kullanıcılar, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabilecekleri konularında bilinçli olmalıdır.

2. Sorumluluk

Tüm kullanıcılar bilgi sistem ve ağlarının güvenliğinden sorumludur.

3. Tepki

Kullanıcılar, güvenlik tedbirlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmelidir.

4. Etik

Kullanıcılar birbirlerinin yasal çıkarlarına saygı göstermelidir.

5. Demokrasi

Bilgi sistem ve ağlarının güvenliği, demokratik toplumun temel değerleri ile uyumlu olmalıdır.

6. Risk Değerlendirmesi

Kullanıcılar risk değerlendirmeleri yapmalıdır.

7. Güvenlik Tasarımı ve Uygulama

Kullanıcılar güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak ele almalıdır.

8. Güvenlik Yönetimi

Kullanıcılar, güvenlik yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.

9. Yeniden Değerlendirme

Kullanıcılar, bilgi sistem ve ağlarının güvenliklerini incelemeli ve yeniden değerlendirmeli, güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri yapmalıdır.

aktörler arasında yapılan anket sonuçlarına yer verilmektedir⁴²⁵. Yine 2009 yılında yayımlanan “Çevrimiçi Kimlik Hırsızlıkları” raporu da ortalama yöntemleri başta olmak üzere kimlik hırsızlıklarına yer vermekte ve bu konudaki OECD politikalarını ve çözüm önerilerini sıralamaktadır⁴²⁶.

2.3.1.3 Commonwealth

Geçmişte Britanya İmparatorluğunun parçası olan devletler ile sonradan eklenen katılımcılarla birlikte toplamda 53 üye devlete sahip Commonwealth, bilişim suçları ve güvenliği konusunda çalışma gösteren topluluklardan biridir. CCI (Commonwealth Cybercrime Initiative – Commonwealth Bilişim Suçları Girişimi) adında bir örgütlenmeye yönelen Commonwealth, gelişmekte olan üye devletlere bu girişim aracılığıyla bilişim güvenliği konusunda destek vermektedir. CCI ayrıca, Commonwealth bilişim suçları mevzuatını gözden geçirmekle, sanal para birimlerinin yaygınlığını denetlemek ve raporlamakla da görevlidir. Commonwealth, ITU Çevrimiçi Çocuk Koruma programının bir katılımcısı olmakla birlikte, Commonwealth Sekreterliği de Avrupa Konseyi Bilişim Suçları Sözleşmesi Komitesinin gözlemcisi olarak bulunmaktadır⁴²⁷.

Commonwealth topluluğunun bilişim suçlarına ilişkin en önemli katkısı ise hazırlamış oldukları model kanundur. “Model Law on Computer and Computer Related Crime” başlıklı bu model yasa, topluluğun 3 – 7 Mayıs 1999 tarihli toplantısında görüşülen girişimci fikirlerin ürünüdür. Öyle ki ilk taslağı 2001 yılında hazırlanan ve 18 – 21 Kasım 2002 tarihli toplantıda sonuç hali kabul edilen model kanun, Avrupa Konseyi Siber Suç Sözleşmesi’nin de temelini oluşturmuştur. Hatta, Commonwealth topluluğunun yalnızca Avrupa değil, birçok kıtada üye devletinin olması nedeniyle, SOİSS prensiplerinin dünyaya hızlıca yayılmasında faydalı olduğundan söz edilmektedir. SOİSS ile kıyaslandığında model kanunun daha geniş ve cesur yükümlülükler barındırdığı görülmektedir⁴²⁸. 2017 yılında model kanunun mevcut hali yayımlanmış ve halen gözden geçirilme aşamasında olduğu belirtilmiştir⁴²⁹.

⁴²⁵ https://read.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page4 (erişim tarihi: 10.09.2018).

⁴²⁶ Özel sektör ile dayanışma, üye ülkelerin ulusal standartlarının belirlenmesi, etkili yasal düzenlemelerin getirilmesi, caydırıcılığı sağlama, mağdur paydaşlara (hükümet, tüketici vb.) eğitim gibi çeşitli çözüm önerileri sunulmuştur. https://read.oecd-ilibrary.org/science-and-technology/online-identity-theft_9789264056596-en#page8 (erişim tarihi: 10.09.2018).

⁴²⁷ <http://thecommonwealth.org/cybercrime> (erişim tarihi: 03.11.2018), Yılmaz, 2016: 162. CCI’nin diğer çalışmaları için, <http://thecommonwealth.org/commonwealth-cybercrime-initiative> (erişim tarihi: 03.11.2018).

⁴²⁸ <http://www.webology.org/2007/v4n3/a45.html> (erişim tarihi: 03.11.2018).

⁴²⁹ http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf (erişim tarihi: 03.11.2018).

2.3.1.4 Karayip Topluluğu (CARICOM – Caribbean Community)

Karayip bölgesinde bilişim suçları sayısında görülen artış, bölge ülkeleri ve gelişen diğer ülkelerin dikkatini çekmiş ve bilişim suçları ile mücadelede uyumluluk bakımından proje geliştirilmesine karar verilmiştir⁴³⁰. ITU ile Karayip Topluluğu arasında gerçekleştirilen HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean) projesi kapsamında bilişim suçlarına ilişkin mevzuattan, yükümlülöklere, eğitim çalışmalarına kadar birçok doküman yayımlanmış ve bu kapsamda çalışmalar gerçekleştirilmektedir⁴³¹.

2.3.1.5 Sekizler Grubu (G8)

Gelişmiş ve dünya ekonomisinin büyük çoğunluğunu yöneten sekiz ülkeden oluşan G8 topluluğu, yalnızca ekonomik iş birliği değil, bilişim suçlarıyla mücadelede de girişimlerde bulunmuştur. İlk kez 1995 yılında Halifax Zirvesinde doğrudan bilişim suçlarından bahsedilmemiş olsa da uluslararası organize suçlarla mücadele konusunda üye devletlerin taahhüdünden bahsedilmektedir. 1996 Lyon Zirvesinde ise bu suçlara yönelik 40 maddelik tavsiye kararı yayınlanmıştır⁴³². 1997 Denver Zirvesinde, daha önceki kararları güçlendirmek için üye devletlere bilişim suçlarının (high tech crime) cezalandırılmasına yönelik odaklanılması, hükümetlerin bu konuda teknik ve yasal yeteneklerinin arttırılması tavsiye edilmektedir⁴³³. Sonraki zirvelerde de bilişim suçlarının önemi ve mücadelesine yönelik tedbirlerden düzenli olarak bahsedilmiştir.

G8 topluluğunun bilişim suçlarına ilişkin mücadelede başlıca katkısı ise yürütmekte oldukları “24/7 Bilişim Suçları Ağı”dır. G8’in farklı konularda oluşturduğu çalışma gruplarından birisi olan Roma – Lyon Grubu’nun Bilişim Suçları (High tech crime) Alt Grubu, Aralık 1997’de kurulan bu ağın sorumluluğunu üstlenmektedir. 70’in üzerinde ülkede çalışma gösteren bu ağ, bilişim suçları konusunda dijital kanıtların ele geçirilmesi ve saklanabilmesini amaçlamaktadır⁴³⁴.

⁴³⁰ Yılmaz, 2016: 161.

⁴³¹ https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/cybercrimes_mpg.pdf (erişim tarihi: 03.11.2018).

⁴³² Yılmaz, 2016: 153.

⁴³³ <http://www.webology.org/2007/v4n3/a45.html> (erişim tarihi: 04.11.2018).

⁴³⁴ <https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%2024.pdf> (erişim tarihi: 04.11.2018).

2.3.1.6 Amerikan Devletleri Örgütü (OAS – Organization of American States)

Amerika kıtasında yer alan 35 üye ve içerisinde Türkiye'nin de bulunduğu gözlemci statüsündeki devletlerle toplam 69 devleti barındıran OAS, diğer bölgesel topluluklar gibi üye devletlerin bilişim suçları karşısındaki teknik ve yasal düzenlemelerle ilgili çalışmalar yürütmektedir. Topluluğun ilk ciddi çalışmasının 2003 yılında hazırlanan “Bilişim Güvenliğine Yönelik Tehditlere Karşı Mücadelede Amerikan Ülkeleri Stratejisi” belgesi olduğu söylenebilir. 2018 yılında CICTE (Inter – American Committee Against Terrorism) ile birlikte hazırlanan raporda toplam 32 ülkede yapılan çalışmalara kronolojik olarak yer verilmiştir⁴³⁵.

2.3.1.7 İnterpol

1923 yılında dünya çapında polis iş birliğini sağlamak için kurulan İnterpol, bilişim suçlarına karşı mücadelede aktif çalışma gösteren organizasyonların başında gelmektedir. İnterpol'ün özellikle son yıllarda terörizm ve organize suçlar ile birlikte bilişim suçlarına da aynı önem derecesinde yer verdiği görülmektedir. Aktif olarak bilişim suçlarına yönelik operasyonlara katılan İnterpol, aynı zamanda araştırma desteği sunmakta, eğitimler düzenlemekte ve dijital kanıtları da toplamaktadır⁴³⁶. İnterpol katıldığı operasyonların bir bölümüne internet sitesinde yer vermektedir. Verilen bilgilere göre, 2012, 2014 ve 2015 yılında düzenlenen operasyonlarda 80'in üzerinde kişi tutuklanmış, merkezi kontrol sunucuları kapatılmış ve 350 parçanın üzerinde elektronik kanıt ele geçirilmiştir⁴³⁷.

2.3.1.8 Avrupa Konseyi (COE)

Bilişim suçlarına ilişkin önemli çalışmalar yapan kurumlardan bir diğeri ise Avrupa Konseyi'dir. Türkiye'nin de taraf olduğu ve bilişim suçlarına ilişkin halihazırda en itibarlı belge olarak kabul gören “Sanal Ortamda İşlenen Suçlar Sözleşmesi”nin dışında konseyin başkaca projeleri de mevcuttur.

Avrupa Konseyi'nin bilişim suçları bakımından ilk girişimi 1976 yılında düzenlenen “Ekonomik Suçların Kriminolojik Yönlerine İlişkin Strazburg Konferansı” olmaktadır. Bu konferansta bilişim suçlarının çeşitli kategorileri tanıtılmıştır. 1985 yılında kurulan başka bir uzman komite, bilişim bağlantılı suçların yasal boyutlarıyla ilgili çalışmalar yapmış, sonucunda 1989 tavsiye kararları sunulmuştur. Bu belgede bilgisayar dolandırıcılığı, sahteciliği, veri ve programlara zarar verme, yetkisiz giriş ve çoğaltma eylemlerinin bir listesine de yer veril-

⁴³⁵ <https://www.oas.org/ext/en/tools/Document-Search> (erişim tarihi: 04.11.2018).

⁴³⁶ Yılmaz, 2016: 163.

⁴³⁷ <https://www.interpol.int/en/Crime-areas/Cybercrime/Operations/Operation-Aces> (erişim tarihi: 04.11.2018).

miş ve üye ülkelere mevzuatın planlanması noktasında seçenekler sunulmuştur⁴³⁸. 11 Eylül 1995'te kabul edilen başka bir tavsiye kararında ise toplam 18 ilke, arama ve el koyma, teknik izleme, soruşturma makamları ile iş birliği, elektronik kanıt, şifreleme kullanımı, araştırma-istatistik-eğitim ve uluslararası iş birliği olmak üzere 7 kategoriye yerleştirilmiştir⁴³⁹.

Bilişim suçları bakımından sözü edilen öncü belgelerin dışında COE'nin tamamlanan ve halen aktif olan projeleri de bulunmaktadır. Bu projeler Romanya'da bulunan C-PROC (Cybercrime Programme Office – Bilişim Suçları Program Bürosu) tarafından yürütülmektedir. Büronun temel görevi, ülkelerin SOİSS çerçevesinde bilişim suçlarına karşı donanımını ve yeterliliğini arttırmaktır⁴⁴⁰.

Devam eden projelerden olan Ahtapot (Octopus) uyarınca COE bünyesinde her 12 – 18 ayda bir düzenli olarak konferans düzenlenmektedir. 80'i aşkın ülkenin temsilcileri ile özel sektör ve akademik alanda katılımcılar ile bilişim suçları alanında en büyük konferanslardan olmakta, her bir konferansta gelişen güncel sorunlara ilişkin özel bir tema seçilmektedir. İlki 11 – 12 Haziran 2007'de düzenlenen konferansın 10.su “bilişim alanında kanıtlar” temasıyla 11 – 13 Temmuz 2018 tarihinde gerçekleşmiştir⁴⁴¹.

Bilişim suçlarına karşı mücadelede Avrupa Konseyi'nin yer aldığı projeler, ülkelerin bulunduğu coğrafi bölgelere göre farklı isimler almıştır. Glacy+ (Global Action of Cybercrime Extended – Bilişim Suçlarına Karşı Genişletilmiş Küresel Hareket) projesi ile COE üyesi ülkelerle birlikte Afrika, Asya – Pasifik ve Latin Amerika bölgelerinde yer alan diğer 12 ülke⁴⁴² ile başta kolluk kuvvetlerinin iş birliği olmak üzere elektronik kanıtlar konusunda gelişim hedeflenmektedir⁴⁴³. CyberSouth (Siber Güney) projesinde ise benzeri amaçlar, güney komşular olarak görülen Cezayir, Ürdün, Lübnan ve Tunus'la iş birliği halinde gerçekleştirilmeye çalışılmakta⁴⁴⁴, PGG (Partnership for Good Governance – İyi Yönetim İçin Ortaklık) projesinde ise doğu bölgesinde yer alan Azerbaycan, Ermenistan, Belarus, Gürcistan, Moldova ve Ukrayna ile iş birliği yapılmaktadır⁴⁴⁵.

⁴³⁸ Schjolberg/Hubbard, 2005: 8.

⁴³⁹ Schjolberg/Hubbard, 2005: 9.

⁴⁴⁰ <https://www.coe.int/en/web/cybercrime/capacity-building-programmes> (erişim tarihi: 11.11.2018).

⁴⁴¹ <https://www.coe.int/en/web/cybercrime/octopus-conference> (erişim tarihi: 11.11.2018).

⁴⁴² Cape Verde, Şili, Kosta Rika, Dominik Cumhuriyeti, Gana, Moritanya, Marokko, Nijerya, Filipinler, Senegal, Sri Lanka ve Tonga.

⁴⁴³ <https://www.coe.int/en/web/cybercrime/glacyplus> (erişim tarihi: 11.11.2018).

⁴⁴⁴ <https://www.coe.int/en/web/cybercrime/cybersouth> (erişim tarihi: 12.11.2018).

⁴⁴⁵ <https://www.coe.int/en/web/cybercrime/cybercrime-eap-2018> (erişim tarihi: 12.11.2018).

2.3.1.8.1 Sanal Ortamda İşlenen Suçlar Sözleşmesi

2.3.1.8.1.1 Genel Olarak

Avrupa Konseyi'nin 185 sayılı uluslararası antlaşması (CETS) olan Sanal Ortamda İşlenen Suçlar Sözleşmesi, bilişim suçlarını ele alan ilk antlaşmadır⁴⁴⁶. 23 Kasım 2001'de imzaya açılmış ve yeterli sayıda ülkenin imzalamasının ardından 1 Temmuz 2004'te yürürlüğe girmiştir. Günümüz itibarıyla sözleşmenin tarafı olan 61 ülke bulunmakta, 4 ülke de sözleşmeyi imzalamakla birlikte henüz onay aşamasını tamamlamamış bulunmaktadır⁴⁴⁷.

Budapeşte Sözleşmesi olarak da bilinen SOİSS'in 46. maddesi uyarınca sözleşmeye taraf devletlerce SOİSS Komitesi (T-CY – Cybercrime Convention Committee) kurulmuştur. Bu komite sözleşmenin genişletilmesi, ek protokollerin düzenlenmesi, düzenli toplantıların yapılması ve bilgi paylaşımının sağlanması gibi görevleri yerine getirmektedir⁴⁴⁸. SOİSS Komitesinin etkin şekilde çalışması, sözleşmenin güncelliğini ve popülaritesini korumasını sağlamaktadır.

Dünya çapında bir referans belge olarak kabul edilen SOİSS, iç hukukumuzda da yer edinmesi sayesinde konumuz bakımından önemini arttırmaktadır. Türkiye sözleşmeyi 10 Kasım 2010⁴⁴⁹ tarihinde Strazburg'da imzalamıştır. Ardından 6533 sayılı kanunla sözleşmenin onaylanması uygun bulunmuş, Bakanlar Kurulu'nun 2014/6656 sayılı kararı ise 9 Ağustos 2014 tarihli resmî gazetede yayımlanmıştır⁴⁵⁰. Buna göre ekli beyan ve çekinceler ile SOİSS iç hukukumuza girmiştir. Dışişleri Komisyonu raporunda sözleşmeye taraf olunması halinde aynı zamanda SOİSS Komitesi'nde de oy hakkına sahip olunacağından bahsedilmesi, sözleşmeye taraf olmanın önemli nedenlerinden birinin bu olduğunu göstermektedir⁴⁵¹.

Sözleşmenin onaylanmasından önceki eserlerde sözleşmeden “Avrupa Konseyi Siber Suç Sözleşmesi” olarak İngilizce başlığının birebir çevirisi şeklinde bahsedilmekteydi. Onay kanununda sözleşmenin başlığı olarak “Sanal Ortamda İşlenen Suçlar Sözleşmesi” ifadesinin kullanılmasıyla bu eserde de sözleşmeden SOİSS olarak bahsedilecektir.

⁴⁴⁶ Erdoğan, 2013: 67.

⁴⁴⁷ Sözleşmenin tarafı olan ülkelerin güncel listesi için https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ZWkdLbJk (erişim tarihi: 12.11.2018).

⁴⁴⁸ <https://www.coe.int/en/web/cybercrime/tcy> (erişim tarihi: 12.11.2018).

⁴⁴⁹ COE internet sayfasında imza tarihini 30 Kasım 2010 olarak gösterse de, hükümet metni ve gerekçesinde imza tarihi 10 Kasım 2010 olarak görülmektedir. <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf> (erişim tarihi: 12.11.2018).

⁴⁵⁰ <http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/08/20140809.htm&main=http://www.resmigazete.gov.tr/eskiler/2014/08/20140809.htm> (erişim tarihi: 12.11.2018).

⁴⁵¹ <https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf> (erişim tarihi: 12.11.2018).

2.3.1.8.1.2 Sözleşmenin Sistematiği

Giriş dışında SOİSS toplam 4 bölümden oluşmaktadır. Birinci bölümde tanımlara yer verilmiş, ikinci bölümde üç kısım altında ulusal düzeyde maddi ve usulü hukuk hükümleri ifade edilmiş, üçüncü bölümde uluslararası iş birliği için hükümlerden bahsedilmiş ve son bölümde yürürlük ve çekincelere ilişkin hükümler yer almıştır.

Tek madde barındıran birinci bölüm, bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi tanımlarına yer vermektedir. Buna ilişkin tartışmalar önceki bölümlerde yapıldığından tekrarlanmayacaktır. Bununla birlikte terimlerin kullanımında orijinal metnin birebir çevirisi yerine terminolojide bütünlük sağlayacak şekilde yer alması (bilgisayar sistemi yerine bilişim sistemi gibi) gerektiğinden bahsedilmelidir. Ayrıca bilişim sistemlerinin geldiği son evre de göz önüne alınarak ihtiyaç duyulan diğer kavram tanımlamalarının tartışılması uygun olacaktır.

Sözleşmenin ikinci bölümü, taraf ülkelerin iç hukuktaki sorumluluğuna ilişkin bir çerçeve çizmektedir. Birinci kısımda iç hukukta cezalandırılması öngörülen dokuz adet suç tipine yer verilmiştir. Bu suç tipleri salt bilişim suçları ve bilişim bağlantılı suçlar ayrımına uygun şekilde sıralanmaktadır. Salt bilişim suç tiplerinde bilişim sistemlerine yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale ve cihazların kötüye kullanımına ilişkin düzenlemeler görülmektedir. Yasadışı erişim ve araya girme suçları, bilişim sistemine yetkisiz giriş ve izleme – dinleme faaliyetlerini kapsamakta, iç hukukumuzda TCK m. 243’e karşılık gelmektedir. Verilere ve sisteme müdahale TCK m. 244’te düzenlenen verilerin tahrip edilmesine ve sistemin engellenmesine ilişkin eylemleri kapsamaktadır. Cihazların kötüye kullanımı ise TCK’ye 2016 yılında eklenen 245/A maddesiyle suç tipleri arasına dahil edilmiştir. SOİSS’de yer alan salt bilişim suç tipleri değerlendirildiğinde, aslında yasadışı erişim ve araya girme eylemlerinin bağlantılı niteliği nedeniyle tek bir maddede düzenlenebileceği görülmektedir. Aynı şekilde veri ve sisteme müdahale eylemlerine de tek maddede yer verilebilecektir. Nitekim iç hukukumuzda da toplamda 5 madde halinde yer verilen suç tiplerinin 3 madde içerisinde daha isabetli şekilde toplandığı görülmektedir.

SOİSS’de yer alan bilişim sistemleri aracılığıyla işlenen suçlar ise bilişim sistemleriyle bağlantılı sahtecilik, dolandırıcılık, çocuk pornografisi ve telif haklarına ilişkin suçlardır. İç hukukumuzda da TCK m. 158/1-f ile bilişim sistemlerinin kullanılması dolandırıcılığın nitelikli hali sayılmış, TCK m. 226’da çocuk pornografisine, FSEK m. 71’de telif haklarına ilişkin suç tiplerine yer verilmiştir.

Sözleşmenin ikinci bölümü yalnızca maddi hükümlere yer vermemiş, ulusal düzeyde alınacak tedbirlerden ve usul hükümlerinden de bahsetmiştir. Bu tedbirler arasında korunma-

sız olan verilerin süratli olarak korunması (m. 16), trafik verilerinin korunması ve açıklanması (m. 17), hizmet sağlayıcıların abone bilgilerini teslim etmesi (m. 18), bilgisayar verilerinin aranması ve el konulması (m. 19), trafik verilerinin gerçek zamanlı kaydedilmesi (m. 20) ve içerik verilerinin kaydedilmesi ve toplanması yer almaktadır.

Üçüncü bölümde, suçlara ilişkin kanıt elde edilebilmesi amacıyla uluslararası alanda alınacak tedbirlerden bahsedilmiştir. Temel ilke olarak, iş birliğine ilişkin uluslararası belgeler ile iç hukuk düzenlemelerinin uygulanması suretiyle mümkün olan en geniş iş birliğinin sağlanması benimsenmiştir (m. 23). Bu noktada, suçluların iadesinden kanıtların depolanması ve saklanmasına, bilgi aktarımına kadar birçok iş birliği hükmü bulunmaktadır. Bunun kolaylaştırılması amacıyla her bir taraf ülkeye 7 gün 24 saat boyunca ulaşılabilecek bir irtibat noktası belirleme yükümlülüğü getirilmiştir⁴⁵² (m. 35).

2.3.2 Ulusal Düzenlemeler

2.3.2.1 ABD

Amerika Birleşik Devletleri bilişim teknolojilerinin ve dolayısıyla bilişim suçlarının gelişiminde önde gelen ülkelerden biridir. Öyle ki bilişim sistemlerine yetkisiz girişe cezai yaptırım getiren ilk ülkedir⁴⁵³ Günümüzde de bilişim teknoloji devlerinin büyük çoğunluğunun ABD kaynaklı olması ve bu sektörün ülke ekonomisine olan etkisi göz önüne alındığında bilişim güvenliğinin sağlanması konusunda önemli çabalar gösterildiği söylenmelidir. Bunun en belirgin örneği olarak, bir Avrupa Konseyi üye ülkesi olmamasına karşın, ABD'nin SOİSS'i imzalayıp onaylayarak sözleşmenin bir tarafı haline gelmesi verilebilir.

Diğer yandan ABD'de gelişmiş sivil toplum hareketlerinin bulunması, bilişim güvenliğini sağlamak için yapılan düzenlemelerde insan hakları ihlali oluşacağı sebebiyle kamuoyu oluşturulmasına, eylemler düzenlenmesine ve mahkemeler tarafından iptal kararı verilmesine de neden olabilmektedir. Bu yönüyle ABD iç hukukundaki düzenlemelerin insan hakları bağlamında da önem arz ettiği söylenebilir⁴⁵⁴.

Federal anlamda yapılan düzenlemelerden biri olan Computer Fraud and Abuse Act (CFAA – Bilgisayar Sahtekarlığı ve Kötüye Kullanılması Yasası) 1984 yılında yürürlüğe girmiş, 1988, 1989, 1990, 1994, 1996, 2001, 2002 ve 2008 yıllarında değişikliğe uğramıştır. Yasa yedi bölüm içerisinde suçların niteliğine göre 1 ila 20 yıl arasında hapis cezaları içermektedir. Bu suç tipleri arasında ulusal güvenlik bilgilerinin edinilmesi, bilişim sistemlerine erişim ve bilgi elde edilmesi, kamuya ait bilişim sistemlerine yetkisiz erişim, şifre kaçakçılığı,

⁴⁵² Türkiye tarafından bildirilen iletişim noktası Emniyet Genel Müdürlüğü – Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı/Bilişim Suçlarıyla Mücadele Şube Müdürlüğü'dür.

⁴⁵³ Erdoğan, 2013: 54; Karagülmez, 2014: 103.

⁴⁵⁴ Dülger, 2015: 213.

kasten veya taksirle bilişim sistemlerine yetkisiz giriş ve zarar verme eylemleri bulunmaktadır⁴⁵⁵.

Telefon Dinleme Yasası'nda (Wiretap Act – 18/2511) 1986 yılında yapılan değişiklik ile tüm elektronik iletişim ağları da suç kapsamında sayıldığından, bilişim suçları ile mücadele kapsamında yapılan düzenlemelerden biri olmuştur. İletişimi durdurma, izleme ve dinleme gibi eylemler bu yasa kapsamında cezalandırılmaktadır⁴⁵⁶.

Son olarak, ABD'de federal kanunların yanı sıra birçok eyalet yasasında da bilişim suçlarına ilişkin düzenlemelerin bulunduğu⁴⁵⁷, hatta bu düzenlemelerin 1984 yılındaki ilk federal kanun çıkmadan önce gerçekleştiği söylenmelidir. Federal kanunlara göre daha geniş hazırlanmasına karşın, aralarında bütünlük bulunmamakta ve farklılıklar göstermeleri nedeniyle eleştirilmektedir⁴⁵⁸.

2.3.2.2 Almanya

Kıta Avrupa'sında bilişim suçları alanında ilk çalışma ve düzenlemeler Almanya'da yapılmıştır⁴⁵⁹. Buna karşın 1997 öncesinde Almanya'da da bilişim ve özellikle internet alanında hukuksal bir belirsizliğin olduğu, bu boşluğun öğreti çalışmalarıyla aşılmaya çalışıldığı görülmektedir. 01.08.1996 yılında yürürlüğe giren Telekomünikasyon Yasası, 12.07.1996 tarihli Telekomünikasyon Hizmeti Girişimleri – Bilgi Koruma Yönetmeliği ve 01.08.1997'de yürürlüğe giren Bilişim ve İletişim Servisleri Yasası bu alandaki ilk gelişmelerdir. Bilgi Koruma Hakkında Yasa, Sayısal İmza Yasası ve Teleservisler Yasası gibi birçok yasayı içinde barındıran Bilişim ve İletişim Servisleri Yasası, özellikle 2001 yılında Teleservisler Yasasında yapılan değişikliklerle içerik, erişim ve servis sağlayıcı ayrımını ve bu aktörlere yüklenen genişletilmiş sorumlulukları düzenlemiştir⁴⁶⁰.

Türk ceza hukukunu da etkileyen Alman hukukunda bilişim suçlarına ilişkin maddi ceza hükümleri esas olarak özel yasalarda değil Alman Ceza Kanunu içerisinde düzenlenmiştir. Kanunun özel hükümler başlığı altında 202/a, 202/b, 202/c, 303/a ve 303/b maddelerinde salt bilişim suçları; 130, 176, 184d, 263a ve 269 maddeleri ile Alman Telif Hakları Yasası

⁴⁵⁵ <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> (erişim tarihi: 25.11.2018).

⁴⁵⁶ <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> (erişim tarihi: 25.11.2018).

⁴⁵⁷ Kurt, 2005: 99.

⁴⁵⁸ Yazıcıoğlu, 1997: 187.

⁴⁵⁹ Dülger, 2015: 220.

⁴⁶⁰ Erman, 2001: 204.

108/b ve Federal Veri Koruma Yasası 34. maddelerinde ise bilişim bağlantılı suçlara ilişkin düzenlemeler bulunmaktadır. Buna göre⁴⁶¹;

- Hak sahibi olmayan kişilerin girişine karşı korunan bilişim sistemlerine kendisi veya başkası adına yetkisiz giriş sağlayan kişi 3 yıla kadar hapis veya adli para cezası ile cezalandırılır. (202/a)

- Teknik araçlarla kendisi veya başkası için aleni olmayan verileri sağlayan kişi, eylem daha ağır başka bir suçu gerektirmedikçe 2 yıla kadar hapis veya adli para cezası ile cezalandırılır. (202/b)

- 202/a ve 202/b maddelerinde düzenlenen suçların işlenmesi amacıyla şifre ve benzeri güvenlik kodları ile bilgisayar programlarını üreten, satan, veren, yayan veya herhangi bir şekilde ulaşılabilmelerini sağlayan kişi 1 yıla kadar hapis veya adli para cezası ile cezalandırılır. (202/c)

- Verileri hukuka aykırı şekilde silen, erişilmez hale getiren, kullanılamaz hale getiren veya değiştiren kişi 2 yıla kadar hapis veya adli para cezası ile cezalandırılır. (303/a)

- Başkası için önemli değer taşıyan bilgi işlem sürecini 303/a maddesinde sayılan eylemlerden biriyle, başkasına zarar vermek amacıyla verileri sisteme dahil ederek veya ileterek veya bilişim tesisatı veya veri taşıyıcı aleti tahrip ederek engellerse 5 yıla kadar hapis veya adli para cezası ile cezalandırılır. Ağır hallerde ise ceza 6 aydan 10 yıla kadar hapis cezasıdır. Çok miktarda malvarlığı kaybı olması, durumun meslek veya sanat haline getirilerek bir çetenin üyesi sıfatıyla hareket edilmesi, toplum için hayati önem taşıyan malların temin edilmesi veya halka hizmet edilmesinin engellenmesi ile Almanya Federal Cumhuriyeti'nin güvenliğine zarar verilmesi halinde kural olarak ağır hal gerçekleşmiş sayılır. (303/b)

- Halkı kin ve düşmanlığa tahrik suçunda içeriğin radyo veya telekomünikasyon medyaları aracılığıyla yayılmasını sağlayan kişi 3 yıla kadar hapis veya adli para cezası ile cezalandırılır. (130)

- Çocukların cinsel istismarında, bilişim teknolojisi kullanılarak veya bu teknolojiler ile pornografik içerikleri ulaşılabılır hale getirerek çocuğu cinsel davranışlarda bulunmak amacıyla etkileyen kişi 3 aydan 5 yıla kadar hapis cezası ile cezalandırılır. (176)

- Pornografik içeriğe radyo veya telekomünikasyon medyaları yoluyla hukuka aykırı şekilde bir başka kişinin veya kamunun erişimini sağlayan kişi 184 ila 184c maddeleri uyarınca cezalandırılır. Telekomünikasyon medyaları aracılığıyla çocuk pornografisi konulu bir içe-

⁴⁶¹ Yenisey/Plagemann, 2015: 311;

https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23legislation@country_label_s%22,%22value%22:%22Germany%22%7D,%7B%22fieldName%22:%22en%23_el.legislation.crimeType%22,%22value%22:%22Cybercrime%22%7D%5D,%22match%22:%22%22,%22sortings%22:%22%22%7D (erişim tarihi: 07.12.2018).

riğe erişmeye girişen kişi 184b maddesi uyarınca, genç pornografisi konulu bir içeriğe erişmek isteyen kişi ise 184c maddesi uyarınca cezalandırılır. (184d)

- Dolandırıcılık suçlarında, kendisinin veya üçüncü kişinin malvarlığında hukuka aykırı bir artış sağlama amacıyla bilgisayarı hatalı bir sonuç verecek şekilde programlayan veya bir şekilde yetkisiz olarak bilgisayar programının işleyiş sürecine müdahale eden kişi 5 yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu amacı taşıyan bilgisayar programlarını imal veya temin eden, satışa sunan, bulunduran veya başkasına bırakan kişi ise 3 yıla kadar hapis veya adli para cezası ile cezalandırılır. (263a)

- Sahtecilik suçlarında, ispat değeri taşıyan verileri aldatma amacıyla kayıt eden, değiştiren veya bu şekilde bulunan verileri kullanan kişi 5 yıla kadar hapis veya adli para cezası ile cezalandırılır. (269)

- Yetkisiz şekilde hak sahipleri tarafından konulmuş telif haklarını kaldıran, değiştiren veya eseri izinsiz dağıtan, yayımlayan veya herkesçe erişilebilir hale getiren kişi bir yıla kadar hapis veya adli para cezası ile cezalandırılır. Suçun ticari ölçekte gerçekleşmesi halinde ise üç yıla kadar hapis veya adli para cezası ile cezalandırılır. (Alman Telif Hakları Yasası m. 108/b)

Bu düzenlemeler incelendiğinde, Alman hukukunda bilişim suçlarına ilişkin düzenlemelere genel olarak doğrudan ceza kanununda yer verildiği, ancak bunun Türk hukukunda olduğu gibi bilişim suçlarına özgü ayrı bir bölüm olarak yer verilmesi şeklinde değil, dolandırıcılık, sahtecilik, cinsel dokunulmazlık, özel hayatın gizliliğine ilişkin suçlar bölüm başlıkları altında ilgili yerlerde düzenlendiği görülmektedir. Bu da somut olay değerlendirilirken ilgili bölümün ilkelerinin esas alınmasını gerektirecektir⁴⁶².

2.3.2.3 Fransa

Diğer ülkelerde olduğu gibi Fransa’da da bilişim suçlarına özgü düzenlemelerden önce eylemler eski FrCK’deki hırsızlık (m. 379), inancı kötüye kullanma (m. 408) ve dolandırıcılık (m. 405) gibi bazı suçlarla karşılanmaya çalışılırdı. Bu boşluğun giderilmesi için yapılan önemli düzenlemelere 05.01.1988 tarih ve 88 – 19 sayılı “Relative a la fraude informatique” isimli kanun, bilişim alanında gizliliğin korunmasına ilişkin 06.01.1978 tarih ve 78 – 17 sayılı “Relative a l’informatique, Aux Fichiers et aux Libertés” isimli kanun ve telif haklarına ilişkin 03.07.1985 tarih ve 85 – 660 sayılı “Relative aux Droits d’auteur et aux Phonogrammes et de Videogrammes et des Entreprises de Communication Audiovisuelle” isimli kanunlar örnek verilebilir⁴⁶³.

⁴⁶² Erdoğan, 2013: 59; Kurt, 2005: 106.

⁴⁶³ Yazıcıoğlu, 1997: 198.

Yeni FrCK'den önce bilişim suçları konusunda yaşanan en önemli gelişme ise 88 – 19 sayılı kanunla yapılan düzenlemedir. Daha önce öngörülen tedbirleri değiştirmeyen ve belirli bilişim suçlarına yer veren bu değişiklik kanunun 462. maddesinde yer alan beş tip suç öngörmektedir. Bunlar hukuka aykırı şekilde bilişim sistemine girilmesi veya kalınması; verilerin tahribi, değiştirilmesi, yok edilmesi veya başka veriler yüklenmesi; sistemin işleyişinin engellenmesi ve bozulması; bilgisayar belgelerinde sahtekarlık yapılması ve bu tür belgenin bilerek kullanılmasıdır⁴⁶⁴.

Günümüzde de yürürlükte olan ve 01.03.1993'te yürürlüğe girmiş yeni FrCK'de salt bilişim suçları 323/1 – 7 maddelerinde, bilişim bağlantılı suçlar ise 226/16 – 23, 227/23 maddelerinde düzenlenmiştir⁴⁶⁵. Ayrıca Fransız Para ve Finans Yasası ile Fransız Fikri Mülkiyet Yasası'nda cezai düzenlemeler bulunmaktadır. Buna göre⁴⁶⁶;

- Hileli şekilde bilişim sistemlerinin tamamına veya bir parçasına giren veya kalmaya devam eden kişi 2 yıla kadar hapis ve 30.000 € para cezası ile cezalandırılır. Bu eylemin sistemde fonksiyon değişikliğine veya modifikasyona (gizleme-tutma-bastırma-kesme) neden olması halinde 3 yıla kadar hapis ve 45.000 € para cezası verilir. (m. 323/1)
- Bilişim sistemlerinin fonksiyonelliğini engelleyen veya müdahale eden kişi 5 yıla kadar hapis ve 75.000 € para cezası ile cezalandırılır. (m. 323/2)
- Bilişim sistemi içerisindeki verileri değiştiren, silen veya sahte gösteren kişi 5 yıla kadar hapis ve 75.000 € para cezası ile cezalandırılır. İlk üç maddedeki eylemleri gerçekleştirmek amacıyla bilgisayar programı veya cihaz ithal eden, üreten, bulunduran veya teklif eden kişi en ağır ceza ile cezalandırılır. (m. 323/3)
- İlk üç maddedeki suçları işlemek için örgüt kuran veya üye olan kişiye, en az bir veya daha fazla eylemin içinde bulunması halinde en ağır ceza verilir. (m. 323/4)
- Hukuka aykırı şekilde kişisel verileri veya kimlik numaralarını elde eden, işleyen – yönlendiren kişi, ihmalen gerçekleşmiş bile olsa, 5 yıla kadar hapis ve 300.000 € para cezası ile cezalandırılır. (m. 226/16 – 23)
- Çocuğun pornografik içeriğe sahip bir fotoğrafı veya benzer bir temsilini edinen, kaydeden yayımlayan, ithal veya ihraç eden kişi 3 yıla kadar hapis ve 45.000 € para cezası ile cezalandırılır. Eylemin iletişim altyapısı kullanılarak herkesçe erişime açık hale getirilmesi

⁴⁶⁴ Yazıcıoğlu, 1997: 199.

⁴⁶⁵ Kangal, 2001: 228.

⁴⁶⁶ https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldNa-me%22:%22en%23legislation@country_label_s%22,%22value%22:%22France%22%7D,%7B%22fieldName%22:%22en%23_el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22match%22:%22%22,%22sortings%22:%22%22%7D (erişim tarihi: 08.12.2018).

halinde 5 yıla kadar hapis ve 75.000 € para cezası verilir. Suça teşebbüs de aynı cezaya tabiidir. (m. 227/23)

- Aynı yasanın 163/3 maddesinde yer alan sahtecilik suçlarının işlenmesi amacıyla bilgisayar programları veya her nevi veriyi üreten, erişen, saklayan veya veren kişi 7 yıla kadar hapis ve 750.000 € para cezası ile cezalandırılır. (Fransız Para ve Finans yasası m. 163/4)

Terminolojik yönden bakıldığında, eTCK’de ve mehz kanunu olan eski FrCK’de yer alan “bilgileri otomatik işleme tabi tutan sistem” kavramının yeni FrCK’de de kullanılmaya devam edildiği, “bilişim sistemi” veya başka bir ifadeye yer verilmediği görülecektir⁴⁶⁷.

Fransız Ceza Kanunu sistematigi incelendiğinde TCK’de olduğu gibi salt bilişim suçlarına ayrı bir bölüm verildiği, ancak bölüm başlığının “Bilgileri Otomatik Olarak İşleyen Sistemlere Yetkisiz Giriş” olarak kısıtlı kapsamda bırakıldığı görülmektedir. Halbuki bu bölümün içerisinde yalnızca giriş değil, sistem içerisindeki verilere zarar verme de cezalandırılmaktadır. Bu yönüyle bölüm başlığının madde içeriklerini kapsamadığı söylenebilecektir. Aynı şekilde bir eylemin FrCK’nin 323/1-2-3 maddelerinde yer alan suç tiplerinin hangisine uyduğunun tespiti, suç tiplerinin birbirine yakınlığı nedeniyle zorluk göstermektedir.

2.3.2.4 Japonya

Japonya da bilişim teknolojilerinin gelişimiyle birlikte tehlike gösteren bilişim suçlarını erken fark eden ve düzenlemeler yapan ülkelerdendir. Japon Parlamentosu 22.06.1987 yılında “Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun”u yürürlüğe sokmuştur. 1990’lı yılların ortalarında siber pornografi eylemleri uygulamada JpCK 175. paragrafi kapsamında kabul edilmiş, 13.02.2000 tarihinde yürürlüğe giren “İnternete Haksız Girmenin Yasaklanması Hakkında Kanun”da ayrıntılı bir düzenleme getirilmiştir⁴⁶⁸.

Japon hukukunda salt bilişim suçları 03.02.2000 tarihinde yürürlüğe giren “Bilgisayarlara Yetkisiz Giriş Kanunu”nda düzenlenmiştir⁴⁶⁹. JpCK’de ise bilişim bağlantılı suçlar 162-2, 163-2,3,4,5, 234-2, 258 ve 259. maddelerinde düzenlenmiştir. Buna göre⁴⁷⁰;

- Başka bir kişinin hakları, görevleri veya durumunun belgelendirilmesi ile ilgili izinsiz olarak elektromanyetik kayıt oluşturan kişi 5 yıla kadar hapis (ve çalışma) veya 500.000 Yen’e kadar para cezası ile cezalandırılır (m. 161-2/1). Bu eylemin resmi makamlarda veya

⁴⁶⁷ https://sherloc.unodc.org/res/cld/document/french_penal_code_html/french_penal_code.pdf (erişim tarihi: 08.12.2018).

⁴⁶⁸ Ünver, 2001: 76.

⁴⁶⁹ Karagülmez, 2014: 138.

⁴⁷⁰ Resmi olmayan İngilizce metin üzerinden incelenmiştir.

https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23legislation@country_label_s%22,%22value%22:%22Japan%22%7D,%7B%22fieldName%22:%22en%23_el.legislation.crimeType_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22match%22:%22%22,%22sortings%22:%22%22%7D (erişim tarihi: 08.12.2018).

resmi görevlilerce gerçekleştirilmesi halinde 10 yıla kadar hapis (ve çalışma) veya 1.000.000 Yen'e kadar para cezası verilir (m. 162-2/2). Bu kayıtları kullanan da üreten gibi cezalandırılır (m. 162-2/3). Suça teşebbüs cezalandırılır (m. 162-2/4).

- Yetkisiz olarak başkasının finansal durumunu uygunsuz yönetmek amacıyla ödeme aracı olarak kredi kartı veya başka bir kart yapan kişi 10 yıla kadar hapis veya 1.000.000 Yen'e kadar para cezası ile cezalandırılır. Bu ceza para çekme amacıyla kart üreten kişiler için de geçerlidir (m. 163-2/1). Önceki fıkrada belirtilen amaçlarla kartı kullanan, veren, transfer veya ithal eden kişi de aynı şekilde cezalandırılır (m.163-2/2,3).

- 163-2 maddesi uyarınca üretilen kartları bahsedilen amaçla bulunduran kişi 5 yıla kadar hapis (ve çalışma) veya 500.000 Yen'e kadar para cezası ile cezalandırılır. (m.163-3)

- 163-2 maddesinde bahsedilen kartlara ilişkin bilgileri edinen kişi 3 yıla kadar hapis (ve çalışma) veya 500.000 Yen'e kadar para cezası ile cezalandırılır. Bilgileri bu amacı bilmesine rağmen sağlayan kişi de aynı şekilde cezalandırılır. (m. 163-4)

- 163-2/1 ve 163-4/1 fıkralarında yer alan suçlara teşebbüs cezalandırılır. (m. 163-5)
- İş için kullanılan bilgisayarlara zarar veren veya bilgisayar veya elektronik kayıtlarla yanlış veri veya sahte komut girişi gibi her türlü yolla ticaretin engellenmesine neden olan kişi 5 yıla kadar hapis (ve çalışma) veya 1.000.000 Yen'e kadar para cezası ile cezalandırılır. (m. 234-2)

- Dolandırıcılık suçları kapsamında, sahte elektromanyetik kayıt, sahte veri veya yetkisiz komutların üretilmesi veya kullanılmasıyla mülkiyet hakkının edinilmesi, kaybı veya değişikliğine neden olan kişi 10 yıla kadar hapis (ve çalışma) cezası ile cezalandırılır. (m. 246-2)

- Resmi makamlarca kullanılan bir belge veya elektromanyetik kayda zarar veren kişi 3 aydan 7 yıla kadar hapis cezası (ve çalışma) ile cezalandırılır. (m. 258)

- Özel amaçlarla kullanılan bir belge veya elektromanyetik kayda zarar veren kişi 7 yıla kadar hapis cezası (ve çalışma) ile cezalandırılır. (m. 259)

Bilgisayarlara Yetkisiz Giriş Kanunu m. 3'te suç tipi açıklanmış, m. 8 ve 9'da yaptırım hükümlerine yer verilmiştir. İhlali halinde 1 yıla kadar ağır hapis (penal servitude) veya 500.000 Yen'e kadar para cezası öngörülen bilgisayarlara yetkisiz erişimin ne olduğu ise üç başlık halinde sınırlı sayıda belirlenmiştir. Bunlar:

1. Sınırlı şekilde erişimde bulunan ve şifre ile erişim sağlanan bilgisayara telekomünikasyon ağı üzerinden başka bir kişinin bilgileri aracılığıyla girilmesi, (sistem yöneticisinin (admin) yapmış olduğu giriş işlemleri hariç)

2. Sınırlı şekilde erişimde bulunan bilgisayara telekomünikasyon ağı üzerinden, giriş önlemlerinden sıyrılacak tedbirleri uygulayarak erişim sağlanması, (sistem yöneticisinin (admin) yapmış olduğu giriş işlemleri hariç)
3. Başka bir bilgisayar ile kontrol edilen ve girişi sınırlı bulunan bilgisayara telekomünikasyon ağı üzerinden sistemin yetkisiz olarak erişilebilir hale getirilmesi.

Japon hukukunda diğer ulusal düzenlemelere göre suç tiplerinin oldukça detaylı şekilde açıklandığı görülmektedir. Öyle ki ceza kanununun ilgili bölümlerinde eklenen maddeler (234-2, 246-2 gibi) suçun klasik haline atıf yapmak veya yalnızca nitelikli halini belirtmek yerine suç tipini ve yaptırımı içerir tam bir ceza hükmü içermektedir. Yine Japon hukukunda bilişim suçlarının ticari yaşamla ilgili yönüne önem verildiği ve sıkı kurallar getirildiği görülmektedir.

2.3.2.5 İngiltere (Birleşik Krallık)

İngiltere bilişim suçlarını farklı yönleriyle ele alan ve düzenleme yapan ülkelerden biridir. Bu düzenlemelere örnek olarak, 1907 tarihli Bermuda Ceza Kanunu⁴⁷¹, 1959 tarihli Müstehcen Yayınlar Kanunu, 1978 tarihli Çocuk Koruma Kanunu, 1988 tarihli Telif, Tasarım ve Patent Kanunu, 1990 tarihli Bilgisayarların Kötüye Kullanımı Kanunu, 1998 tarihli Veri Koruma Kanunu, 2003 tarihli Cinsel Suçlar Kanunu, 2006 tarihli Dolandırıcılık Kanunu, 2006 tarihli Terörizm Kanunu ve 2008 tarihli Tüketicilerin Haksız Ticaretten Korunması Düzenlemesi verilebilir⁴⁷².

Bu düzenlemelerin içerisinde çalışma konusu bakımından en önemli bulunanı 29.08.1990'da yürürlüğe giren Bilgisayarların Kötüye Kullanımı Kanunu'dur (Computer Misuse Act). 2006 yılında çıkarılan Polis ve Adalet Kanunu (Police and Justice Act) ve 2015 yılında çıkarılan Ciddi Suçlar Kanunu (Serious Crime Act) ile iki kez değişikliğe uğramıştır. CMA üç bölüm (kötüye kullanım suçları, yargılama, çeşitli hükümler) ve 21 kısımdan oluşmaktadır⁴⁷³. Birinci bölümde yer alan kötüye kullanım suçları ise ikisi Ciddi Suçlar Yasası ile sonradan eklenmek üzere beş kısma ayrılmıştır. Bunlar:

1. Bilgisayar (ve ekipmanına) yetkisiz erişim. (Unauthorised Access to computer material)

Bilgisayarda yer alan herhangi bir program veya veriye erişim sağlamak için eylemde bu-

⁴⁷¹ Kanunda 07.05.2008 tarihinde yürürlüğe giren değişiklikler ile.

⁴⁷² https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#c=%7B%22filters%22:%5B%7B%22fieldNa-me%22:%22en%23legislation@country_label_s%22,%22value%22:%22United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%22%7D,%7B%22fieldName%22:%22en%23_el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22match%22:%22%22,%22sortings%22:%22%22%7D (erişim tarihi: 09.12.2018).

⁴⁷³ <http://www.legislation.gov.uk/ukpga/1990/18> (erişim tarihi: 09.12.2018); Yazıcıoğlu, 1997: 194. Kanunun ilk halinde 18 kısım bulunmaktadır.

lunulması, bu eylemin yetkisiz olarak gerçekleşmesi ve failin eylemin gerçekleştiği anda yetkisiz girişin bilincinde olması halinde suç vücut bulmaktadır. Bu eylemin herhangi bir tür program veya veriye karşı gerçekleşmesi yeterli sayılmaktadır. Bu suçun faili 12 aya kadar⁴⁷⁴ hapis cezası veya para cezası veya her iki ceza ile cezalandırılabilir.

2. Başka suçların işlenmesini sağlamak veya kolaylaştırmak amacıyla izinsiz erişim. (Unauthorised access with intent to commit or facilitate commission of further offences) Bir önceki kısımdaki suçu, bu kısımda yer alan başka suçların işlenmesini sağlamak veya kolaylaştırmak amacıyla (kendisi veya üçüncü bir kişi için) işleyen kişi cezalandırılmaktadır. Bu suçun gerçekleşmesi için başka suçların henüz gerçekleşmemiş olması veya imkânsızlık bulunması önem arz etmez. 21 yaşını doldurmuş ve başka bir suçtan mahkûm olmamış kişiler 5 yıla kadar hapis⁴⁷⁵ veya para cezası veya her iki ceza ile cezalandırılabilir.

3. Çeşitli yetkisiz eylemler. (Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc) Yetkisiz olduğunu bilerek bilgisayar üzerinde pervasızca herhangi bir eylemde bulunan kişi bu kısım uyarınca cezalandırılmaktadır. Sistem işleyişini bozmak, program veya verilere erişimi engellemek veya bunları gizlemek, veri güvenilirliğini bozma bu eylemler arasında sayılmaktadır. Bu kısım uyarınca fail 10 yıla kadar hapis⁴⁷⁶ veya para cezası veya her iki ceza ile cezalandırılabilir.

3ZA. Ciddi zarar riski oluşturan veya neden olan yetkisiz eylemler. (Unauthorised acts causing, or creating risk of serious damage) Bir önceki kısımda yer alan eylemlerin ciddi zarar verme riski cezalandırılmaktadır. Zarar verilebilecek alanlar, insan refahı, çevre, herhangi bir ülke ekonomisi veya ulusal güvenliği olmak üzere dört başlıkta belirlenmiştir. İnsan refahına verilen zararlar ise hayat kaybı, hastalık veya yaralanma, yiyecek, içecek veya enerji kaynaklarının bozulması, iletişim veya ulaşım imkanlarının bozulması veya sağlık servislerinin bozulması olarak sınırlı sayıda belirlenmiştir. Suçun gerçekleşmesi için yetkisiz eylemlerin zararın esas kısmını oluşturması şart olmayıp, tali zarar halinde de suçun vücut bulduğu kabul edilmektedir. Suçun faili hakkında 14 yıla kadar hapis cezası, para cezası veya her iki cezaya da hükmedilmektedir. Eğer bu suç ile yaşam kaybı, hastalık veya yaralanma ile ulusal güvenliğe yönelik bir zarar meydana gelir ise fail hakkında müebbet hapis cezası veya para cezası veya her iki cezaya da hükmedilmektedir.

⁴⁷⁴ Kanunun ilk halinde 6 aya kadar olan hapis cezası 01.10.2008 tarihinden itibaren 12 aya çıkarılmıştır.

⁴⁷⁵ “Summary conviction” için 12 aya kadar, “Conviction on indictment” için 5 yıla kadar ceza öngörülmektedir.

⁴⁷⁶ “Summary conviction” için 12 aya kadar, “Conviction on indictment” için 10 yıla kadar ceza öngörülmektedir.

3A. Önceki kısımlarda yer alan suçların işlenmesi için “eşya” yapılması, sağlanması veya edinilmesi. (Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA) Bu kısım uyarınca önceki kısımlarda yazılı suçların işlenmesi veya iştirak edilmesi için bir “eşya”nın yapılması, uyarlanması, sağlanması veya sunulması da suç olarak tanımlanmıştır. Bu kısım kapsamında eşyadan kastedilenin ise elektronik form halinde bulunan her türlü program veya veri olduğu söylenmektedir. Bu suçun faili hakkında 2 yıla kadar hapis⁴⁷⁷ veya para cezası veya her iki cezaya da hükmedilmektedir.

2.3.2.6 İtalya

İtalya da bilişim suçlarına ilişkin düzenlemeleri ceza kanunu içerisinde yapan ülkelerden biridir. İtCK’nin 392, 461, 491, 615, 616, 618, 621, 635 ve 640. maddelerinde çeşitli hükümlere rastlanmaktadır⁴⁷⁸. Buna göre özetle;

- Bilgi teknolojileri veya telematik sistemlere yetkisiz erişim (m. 615-ter). (1) Güvenlik önlemleri ile korunan bir bilgi teknolojileri sistemi veya elektronik sisteme kendisini uygun-suz şekilde tanıtan (bu şekilde giren) veya kendisini çıkarma yetkisine sahip kişilerin açık veya zımnî niyetine karşı sistemde kalmaya devam eden kişi 3 yıla kadar hapis cezası ile cezalandırılır. (2) Eylemin 1) Kamu görevlisi veya kamu hizmetlerinden sorumlu kişinin görevini kötüye kullanarak, 2) Fail tarafından nesnelere veya kişilere cebir uygulanarak veya silahlı halde, 3) Eylem, sistemin, verinin veya programlarının tamamının veya bir bölümünün yok edilmesi, zarar görmesi veya engellenmesi ile sonuçlanırsa 1 yıldan 5 yıla kadar hapis cezası verilir. (3) Eğer bu bölümdeki eylemlerin askeri alanı, toplum düzenini, kamu güvenliği, sağlığını veya yararını ilgilendirmesi halinde sırasıyla (fıkralara göre) 1 yıldan 5 yıla kadar ve 3 yıldan 8 yıla kadar ceza verilir. (4) Birinci fıkra kapsamındaki suçlar şikâyeteye tabiidir.

- Bilgisayar veya telekomünikasyon sistemleri giriş kodlarının yasadışı yayılması (m. 615-quater). Kendisine veya bir başkasına yarar sağlamak veya başkasına zarar vermek için, telematik sistemlere giriş için uygun olan ve korunan kodları sakıncalı şekilde sağlayan, çoğaltan, yasadışı yayan veya veren kişi 1 yıla kadar hapis ve 5164 €’ya kadar para cezası ile cezalandırılır.

- Bilgi teknolojileri veya telematik sistemleri kesen veya onlara zarar veren malzeme, cihaz veya bilgisayar programlarının yayılması (m. 615-quinquies). Bilgi teknolojileri sistem-

⁴⁷⁷ “Summary conviction” için 12 aya kadar, “Conviction on indictment” için 2 yıla kadar ceza öngörülmektedir.

⁴⁷⁸ Ünver, 2001: 67;

https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23legislation@country_label_s%22,%22value%22:%22Italy%22%7D,%7B%22fieldName%22:%22en%23_el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22match%22:%22%22,%22sortings%22:%22%22%7D (erişim tarihi: 10.12.2018).

leri, bilgi, veri veya bilgisayar programlarının bir kısmına veya tamamına yasadışı şekilde zarar vermek amacıyla, başkaca ekipman veya bilgisayar programlarını üreten, temin eden, yayan veya başka bir şekilde kullanıma uygun hale getiren kişi 2 yıla kadar hapis ve 10.329 €'ya kadar para cezası verilir.

- Veri, bilgi veya bilgisayar programlarına zarar verilmesi (m. 635-bis). Eylem daha ağır bir cezayı gerektirmediği takdirde, veri veya bilgisayar programını yok eden, bozan, silen, değiştiren veya durduran kişi hakkında mağdurun şikâyeti üzerine 6 aydan 3 yıla kadar hapis cezası verilir. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise şikâyet aranmaksızın 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılır.

- Kamu bünyesinde veya kullanımında bulunan veri, bilgi veya bilgisayar programlarına zarar verilmesi (m. 635-ter). Eylem daha ağır bir cezayı gerektirmediği takdirde, herhangi bir şekilde kamu bünyesi veya kullanımında olan veri, bilgi veya bilgisayar programını yok eden, zarar veren, değiştiren veya durduran kişi 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılır. Eylem yok etme, zarar verme, değiştirme, silme veya durdurma ile sonuçlanmış ise 3 yıldan 8 yıla kadar hapis cezası verilir. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise verilecek ceza arttırılır.

- Bilgi sistemleri veya telematik sistemlere zarar verilmesi (m. 635-quater). Eylem daha ağır bir cezayı gerektirmediği takdirde, 635-bis maddesindeki eylemleri gerçekleştirerek veya veri aktarımı-bulaştırması yoluyla bilgi teknolojisi veya diğer telekomünikasyon sistemlerinin bütününe veya bir parçasını kullanılamaz hale getiren veya fonksiyonlarını ciddi şekilde geciktiren kişi 1 yıldan 5 yıla kadar hapis cezası ile cezalandırılır. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise verilecek ceza arttırılır.

- Kamu kullanımında olan bilgi sistemleri veya telematik sistemlere zarar verilmesi (m. 635 quinquies). 635-quater maddesinde belirtilen eylemlerin kamu kullanımında olan bilgi sistemleri veya telematik sistemlerin bütünü veya bir bölümüne gerçekleştiren kişi 1 yıldan 4 yıla kadar hapis cezası ile cezalandırılır. Eylem, sistemlerin yok edilmesi, zarar verilmesi veya kullanılamaz hale getirilmesi ile sonuçlanırsa fail hakkında 3 yıldan 8 yıla kadar hapis cezası verilir. Eylem, sistem operatörünün kötüye kullanımıyla gerçekleşmiş ise verilecek ceza arttırılır.

- Kişisel nedenlerle keyfi uygulama sonucu mala zarar verme (m. 392). Mahkemeye başvurarak iddia ettiği haklarını kullanabilecek olan kişi, hakkı keyfi olarak kendi kullanıp mala zarar verdiği takdirde, şikâyetçinin davası ile 516 €'ya kadar para cezası ile cezalandırılır. Bu kapsamda bir bilgi teknolojileri programının bütününe veya bir bölümünün de-ğişti-

rilmesi, modifiye edilmesi, kaldırılması veya telekomünikasyon sistemlerinin engellemesi veya aksatılması da mala zarar verme sayılır.

- Sahte para, damga pulu veya filigran üretme veya bulundurma (m. 461). Eylem daha ağır bir cezayı gerektirmediği takdirde, sahte para, pul veya filigranlı kâğıt elde etmek için, filigran, bilgisayar programı veya materyal imal eden, satın alan, bulunduran veya devreden kişi 1 yıldan 5 yıla kadar hapis ve 103 – 516 € para cezasına çarptırılır.

- Gizli doküman içeriklerinin açığa çıkarılması (m. 621). İçerikten habersiz olarak, gizli kalması gereken içerikleri kendi çıkarına veya herhangi bir sebep olmaksızın kullanan kişi, 3 yıla kadar hapis veya hapis ile birlikte 103 – 1032 € arasında para cezasına çarptırılır. Bu kapsamda, bilişim teknolojileri kapsamındaki her türlü veri, bilgi veya program da suçun konusu içerik olarak varsayılır.

Ceza kanunundaki düzenlemelerin dışında, İtalya’da ayrıca sorun oluşturan mafya türü örgütlü suçlulukla mücadele parçası olarak suç gelirlerinin aklanması suçuyla etkin mücadele edilebilmesi için 356/1992 sayılı yasa kabul edilmiş ve bilişim sistemlerini de kapsar şekilde suç gelirlerinin aklanması suçunda kolaylık sağlayan hazırlık hareketlerinin dahi cezalandırılması öngörülmüştür⁴⁷⁹.

2.4 Türk Hukuku’nda Bilişim Suçlarının Niteliği ve Bu Suçlarla Mücadelenin Gelişimi

2.4.1 Tarihçe

Ülkemizde bilişim suçlarına ilişkin düzenlemelerin iskeletini TCK’nin oluşturduğu, bunun yanı sıra bazı özel kanunlarda farklı suç tiplerinin düzenlendiği ve özellikle internet ağına ilişkin sorumlulukların belirlendiği görülmektedir. Bu bakımdan Türkiye’de bilişim suçlarının düzenlenmesinde genel yaklaşımın Kıta Avrupa’sında yer alan sisteme benzerlik gösterdiği söylenebilir.

Bilişim suçlarına ilişkin düzenlemelerin Türk hukukuna girişi 1989 TCKÖT ile olmuştur. 1987 tarihinde düzenlenen ilk metnin 342 – 346. maddelerinde bilişim suçlarına yer verilmiştir. Düzenlendiği yer itibarıyla “Topluma Karşı Suçlar” başlıklı ikinci kısmın dokuzuncu bölümünde 5 madde halinde yer almaktadır. Ön tasarıda suç tiplerinin yanı sıra tüzel kişiler ve teşebbüse ilişkin de hükümlerin bulunmakta, teşebbüs halinde tamamlanan suçun cezasının verileceği belirtilmektedir⁴⁸⁰.

1989 tarihli TCKÖT bütünüyle yasalaşmamış olsa da, bilişim suçlarına ilişkin bölümü önemli değişikliklere uğramaksızın TCK’ye girmiştir. 14.06.1991 RG tarihli ve 3756 sayılı kanunla, 765 sayılı TCK’ye 525/A, B, C ve D maddeleri eklenmiştir. 525/A maddesinde bil-

⁴⁷⁹ Dülger, 2015: 225.

⁴⁸⁰ Kurt, 2005: 120.

gileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme suçu, 525/B maddesinde bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru tahrip etme suçu, 525/C maddesinde delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sistemi kullanma suçu düzenlenmiş, 525/D maddesinde ise 525/A ve B maddeleri uyarınca ayrıca verilecek hak yoksunluklarına yer verilmiştir.

1997, 2000 ve 2003 tarihli TCKÖT’lerde de bilişim suçlarında güncel gelişmeler ele alınmıştır. 1997 TCKÖT’de ilk kez “bilgileri otomatik olarak işleme tabi tutmuş sistem” verine “bilişim sistemi” ifadesinin kullanıldığı ve “Topluma Karşı Suçlar” başlıklı ikinci kısmın “Bilişim Alanında Suçlar” başlıklı dokuzuncu bölümünde 347 – 352. maddeleri arasında toplam 6 maddede düzenlendiği görülmektedir. 2000 tarihli TCKÖT’de bilişim suçlarının bulunduğu yer ve bölüm başlıkları korunmuş, yalnızca müstakil olarak “Banka ve Kredi Kartlarının Kötüye Kullanımı” başlıklı 349. madde eklemesi dikkat çekmektedir. Yine 2003 tarihli TCKÖT’de ufak değişiklikler ve para miktarlarında güncellemeler görülmektedir⁴⁸¹.

2.4.2 Güncel Durum

5237 sayılı TCK’nin yürürlüğe girmesinden itibaren salt bilişim suçları, kanunun ikinci kitabının “Topluma Karşı Suçlar” başlıklı üçüncü kısmının “Bilişim Alanında Suçlar” başlıklı dokuzuncu bölümünde yer almaktadır. İlk kabul edildiği haliyle bilişim sistemine girme suçu (m. 243), sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu (m. 244), banka ve kredi kartlarının kötüye kullanılması suçu (m. 245) düzenlenmiş ve 246. maddede tüzel kişiler hakkında güvenlik tedbiri hükümlerine yer verilmiştir.

Günümüze kadar gelinen süreçte ise bölüm üç kez değişikliğe uğramıştır. İlk olarak 08.07.2005 RG tarihli ve 5377 sayılı kanunun 27. maddesi uyarınca, banka ve kredi kartlarının kötüye kullanılması suçu yeniden düzenlenmiş, suçun kapsamı genişletilmiş ve bazı akrabalar hakkında cezaya hükmolunamayacağı kabul edilmiştir. İkinci değişiklik 19.12.2006 RG tarihli ve 5560 sayılı kanunla getirilmiş ve banka ve kredi kartlarının kötüye kullanılması suçunu düzenleyen 245. maddeye 5. fıkra eklenmiştir. Buna göre aynı maddenin birinci fıkra kapsamına giren hallerde, malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümlerinin uygulanacağı belirtilmiştir. Üçüncü ve en kapsamlı değişikliğin ise 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 30. maddesiyle getirildiği görülmektedir. Buna göre bilişim sistemine girme suçunda girme ve kalmaya devam etme olarak tanımlanan eylemde, “ve” ibaresi isabetli olarak veya şeklinde değiştirilmiş, sisteme girme veya kalmaya devam etmek ayrı ayrı

⁴⁸¹ Kurt, 2005: 132.

cezalandırılabilir hale getirilmiştir. Aynı maddeye eklenen 4. fıkra ile dinleme ve izleme olarak tabir edilen bilişim suçları ceza kanunu kapsamına dahil edilmiştir. Son olarak 245/A maddesi kanuna eklenerek, yasak cihaz ve bilgisayar programlarına ilişkin cezalara hükmedilmiştir.

Bilişim bağlantılı suçların ise çoğunluğu TCK’de bulunmakla birlikte bazı özel kanunlarda da hüküm bulunduğu görülmektedir. TCK’nin nitelikli hırsızlık (m. 142), nitelikli dolandırıcılık (m. 158), kumar oynanması için yer ve imkân sağlama (m. 228) suçlarında bilişim sistemlerinin kullanılması suçun nitelikli hali olarak yer almaktadır. Yine, haberleşmenin engellenmesi suçu (m. 124) ve hakaret suçu (m. 125) gibi bazı suçlarda doğrudan bilişim sisteminden bahsedilmemiş olsa da, madde içeriğinden eylemin bilişim sistemi aracılığıyla da kolaylıkla gerçekleştirilebileceği anlaşılabilmektedir⁴⁸².

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 17. maddesinde, kişisel verilere ilişkin suçların TCK 135 ile 140. maddeleri arasındaki hükümler uyarınca cezalandırılacağı, bu kanuna göre kişisel verileri silmeyen veya anonim hale getirmeyen kişilerin TCK 138. maddesi uyarınca cezalandırılacağı belirtilmiştir.

5846 sayılı Fikir ve Sanat Eserleri Kanunu’nun 71. maddesinde bir eserin çeşitli şekillerde izinsiz olarak çoğaltılması suç olarak kabul edilmişken, 72. maddesinde bilgisayar programlarının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üretmek, vermek, kullanmak veya bulundurmak suç kapsamına alınmıştır.

5809 sayılı Elektronik Haberleşme Kanunu’nun 63. maddesinde cezai hükümlere yer verilmiş, ilgili kanuna aykırı olan eylemlerle ilgili hapis ve adli para cezaları öngörülmüştür.

5070 sayılı Elektronik İmza Kanunu’nun 16. maddesinde ilgilinin rızası dışında imza oluşturma aracını elde etme veya izinsiz elektronik imza oluşturma suçu, 17. maddesinde sahte olarak elektronik imza oluşturma suçu düzenlenmiş, ayrıca 19. maddede tüzel kişilerle ilgili güvenlik tedbirlerine yer verilmiştir.

2.4.3 Değerlendirme

Karşılaştırmalı hukuk göz önüne alındığında ülkemizde bilişim suçlarına ilişkin mevzuatın önemli aşamalar kaydettiğini söylemek mümkündür. Özellikle yTCK ve son değişiklikler ile Sanal Ortamda İşlenen Suçlar Sözleşmesi hükümlerine uyum sağlanma çabası içinde olduğu, sözleşmede bahsedilen suç tiplerinin tamamının TCK’de yer aldığı görülmektedir. Ayrıca “bilgileri otomatik olarak işleme tabi tutan sistem” gibi kalabalık ifadeler yerine bili-

⁴⁸² Suç unsurlarının bilişim sistemleri yönüyle incelemesi için, Taşkın, 2008: 114.

şim hukuku alanında dil zenginliğimizin kullanılarak yalın, anlaşılabilir ve aynı zamanda kapsayıcı niteliği olan ifadeler kullanılabilmesi ve bu anlamda birçok ülkeden önde bulunulması memnuniyet vericidir. Ancak çocuk pornografisine ilişkin TCK m. 226’da içeriğin yalnızca basın ve yayın yolu ile yayılmasına yer verilmekle, açık şekilde bilişim sistemlerinden bahsedilmemiş olması bir eksiklik olarak değerlendirilebilecektir.

Tüm bunların yanı sıra bilişim suçlarının geçirdiği evrim, günlük hayatın her alanında yaygın şekilde karşılaşılabilmesi göz önünde alındığında artık bilişim suçlarının “Topluma Karşı Suçlar” kısmı yerine “Kişilere Karşı Suçlar” kısmı içerisinde düzenlenmesi gerektiğini düşünmekteyiz. Suçtan kaynaklanan baskın zararın kişiler üzerinde oluşması ve TCK sisteminde “Kişilere Karşı Suçlar”a verilen önem nedeniyle, bilişim alanında suçlara da aynı önemin verildiğinin gösterilmesi amacıyla bu bölüm içerisinde yer alması uygun olacaktır. Nitekim TCK m. 245/5’e göre malvarlığı suçlarına ilişkin etkin pişmanlık hükümlerinin uygulanması, malvarlığına ilişkin suçların da “Kişilere Karşı Suçlar” kısmında düzenlenmesi, bilişim alanında suçların “Kişilere Karşı Suçlar”la olan yakın bağlantısını da ortaya koymaktadır.

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİN ENGELLENMESİ, BOZULMASI, VERİLERİN YOK EDİLMESİ VEYA DEĞİŞTİRİLMESİ SUÇU (TCK m. 244)

3.1 Genel Olarak

Bilişim suçlarına ilişkin düzenlemelerin özel kanunlarda değil, doğrudan 5237 sayılı TCK’de yer aldığından bir önceki bölümde bahsedilmişti. Türk Ceza Kanunu’nun ikinci kitap, üçüncü kısımda yer alan “Topluma Karşı Suçlar” kısmının onuncu ve son bölümünde “Bilişim Alanında Suçlar” yer almaktadır. Bu bölümde ise suç tipleri dört maddeye ayrılmış, beşinci ve son maddede uygulanacak güvenlik tedbirlerine yer verilmiştir. Suç tipleri arasında bilişim sistemine girme (m. 243), sistemi engelleme, bozma, verileri yok etme veya değiştirme (m. 244), banka veya kredi kartlarının kötüye kullanılması (m. 245), yasak cihaz veya programların (m.245/A) bulunduğu görülmektedir.

İlgili madde Adalet Komisyonunda kabul edildiği haliyle 3 fıkradan oluşmakta ve birinci fıkra tüm eylemler sayılarak diğer fıkralarda nitelikli haller gösterilmekteydi⁴⁸³. Ancak kanun metninde bu eylemlerin iki fıkraya ayrılarak maddenin toplam 4 fıkra haline getirildiği, bilişim sistemlerine yönelik suçların birinci fıkra, verilere yönelik suçların ise ikinci fıkra yer aldığı ve farklı yaptırımlara bağlandığı görülmektedir. Bilişim sistemlerine yönelik suçlara ilişkin cezanın, verilere yönelik suçlara ilişkin cezalardan daha ağır olması, yasa koyucunun bilişim sistemlerine karşı eylemleri daha önemli gördüğü şeklinde yorumlanmaktadır⁴⁸⁴.

eTCK’nin 525B maddesi ve Sanal Ortamda İşlenen Suçlar Sözleşmesi’nin 4, 5 ve 8. maddelerine karşılık gelen TCK m. 244, içerisinde üç farklı suç tipi barındırmaktadır. Bunların incelemesine geçilmeden önce madde metnine yer vermekte fayda vardır:

“Madde 244 – Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

- (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.

⁴⁸³ <https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c059/tbmm22059119ss0664.pdf> (erişim tarihi: 23.12.2018).

⁴⁸⁴ Dülger, 2015: 432.

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

Görüleceği üzere 244/1 ve 244/2’de suç tiplerine yer verilmiş ve 244/3’te arttırıcı neden olarak nitelikli hale yer verilmiştir. 244/4 düzenlemesinin hukuksal niteliğinin ayrı bir suç tipi mi, yoksa nitelikli hal mi olduğu öğretilerde tartışmalı olup, konu ilerleyen bölümde ele alınacaktır.

3.2 Korunan Hukuksal Değer

Öğretilerde korunan hukuksal değerlerin tartışmalı olduğu görülmektedir. Bunun başlıca nedeni, bilişim sistemlerinin günlük yaşamda önemli bir pay edinmesi ve birçok farklı değerle iç içe geçmiş bulunmasıdır. Bu durum TCK m. 244’ün birden fazla ve farklı yapıda suç tipini içeren düzenlemesinde de kendisini göstermektedir. Bunlar arasında tercih ve önem sıralamasında bulunmak da çeşitli güçlükler göstermektedir. Bu nedenle suçun koruduğu hukuksal değerlerin karma yapıda olduğu görüşü hakimdir⁴⁸⁵.

Bu suçla korunan hukuksal değerler arasında mülkiyet ve fikri mülkiyetin korunması sayılmaktadır. eTCK’nin 525B maddesindeki düzenlemenin mala zarar verme suçuyla olan ilişkisinin üzerinde durulması, bilişim suçlarının bu yönüyle klasik mala zarar verme suçunun özel bir şekli olduğunu ve bu suç yönünden de mülkiyet – malvarlığı hakkının korunduğu ileri sürülmüştür⁴⁸⁶. Özellikle TCK m. 244/4 hükmünün haksız menfaat temin etmeyi içermesi, mülkiyet hakkının korunduğunun önemli argümanlarından biri olmuştur⁴⁸⁷. 244/2 hükmünde önemle vurgulanan veri kavramının aynı zamanda fikir ve sanat eserleri kapsamındaki içerikleri de koruduğu, bu nedenle fikri mülkiyetin de korunan bir değer olduğu ifade edilmektedir⁴⁸⁸.

Suçun bilişim sistemlerinin bütünlüğü ve güvenliği ile toplum çıkarlarını koruduğu da söylenmektedir. Düzenlemenin “Topluma Karşı Suçlar” kısmında yapılmış olması, toplumun, özellikle de bilişim sistemlerine hâkim olmayan kişilerde bu sistemlere karşı güvenin olumsuz

⁴⁸⁵ Dülger, 2015: 411.

⁴⁸⁶ Tezcan/Erdem/Önok, 2016: 954; Kurt, 2005: 161; Karagülmez, 2014: 237.

⁴⁸⁷ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 931. Mülkiyet hakkının korunduğunu kabul etmekle birlikte, düzenlemenin “eylemin başka bir suça sebebiyet vermemesi halinde” bölümünden hareketle TCK m. 244/4’ün, verilerin kişi veya mal olarak kabul edilemeyecek olması nedeniyle dolandırıcılık vb. düzenlemelerden farklı olduğu, çıkar sağlanabilecek her türlü değer koruma altına alındığı ifade edilmektedir. Erdoğan, 2013: 251.

⁴⁸⁸ Erdoğan, 2013: 216.

yönde etkilenmesinin önüne geçilebileceği vurgulanmaktadır⁴⁸⁹. Yargıtay da bir kararında benzer ifadeler kullanmıştır⁴⁹⁰.

Bilişim sistemlerinin günlük hayatın her alanında ve kişiler tarafından sıklıkla kullanılması, suçun bu yönüne de dikkat edilmesini sağlamıştır. Düzenlemenin bu nedenlerle bilişim sistem sahibi ve kullanıcısının maddi ve manevi çıkarlarını koruduğu öne sürülmüştür⁴⁹¹. Bu noktada, eylemlerin bilişim sistemlerinin hem donanımına hem yazılımına zarar verebilecek nitelikte olduğu vurgulanmakta ve sistemin uygun şekilde işletilme hakkı korunmaktadır⁴⁹².

Bilişim sistemlerinin fonksiyonları dikkate alınarak, özel hayatın gizliliği ve haberleşme özgürlüğü, teknolojik gelişim özgürlüğü⁴⁹³ gibi hakların da korunduğu ifade edilmektedir⁴⁹⁴. Bir görüş ise, kişisel veriler ve dolayısıyla özel yaşamın TCK m. 125 – 136 aracılığıyla korunduğunu söylemekle, bilişim suçlarının bunun dışında kalan veri ve hakları koruduğunu iddia etmektedir⁴⁹⁵.

SOİSS açıklayıcı raporunda (explanatory report) koruma altına alınan hakkın veri ve bilgisayar programlarının bütünlüğü ve fonksiyonelliği olduğu belirtilmiştir⁴⁹⁶. Bu açıklama öğretide mülkiyet hakkının veya veri gizliliği ve dokunulmazlığının korunduğu konusunda farklı şekillerde yorumlanmaktadır⁴⁹⁷.

Tüm bu açıklamalar birlikte değerlendirildiğinde, dar ve geniş anlamda iki farklı korunan değer tespit edilebilecektir. Dar anlamda korunan değer, geliştirici ve kullanıcıların bilişim sistemleri üzerindeki mülkiyet hakkıdır. Bilişim sistemlerinin seri üretime tabi olmasına karşın kişiselleştirilebilir olma özelliği, onlara “diğerlerinden ayırt edilebilir eşya” niteliği katmakta ve bu da mülkiyet hakkının esasını oluşturmaktadır. Gerek donanım ve yazılım gerekse sistem içinde bulunan verilerin maddi bir değer taşıdığı konusunda bir tereddüt bulunmamaktadır ki çoğu zaman verilerin, duyu organlarıyla algılanabilen parçalardan değer bakımından daha öncelikli bir hedef haline geldiği gözetilmelidir.

⁴⁸⁹ Erdoğan, 2013: 184.

⁴⁹⁰ “... Bilişim sistemlerinin veya verilerin zarar görmesi halinde, kişinin malvarlığında bir azalma meydana geleceği gibi toplumun, bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişi etkilendiği, bilişim sistemlerinin zarar görmeden işler durumda bulunmasında toplumsal yarar olduğu için yasanın topluma karşı işlenen suçlar kısmına alınmıştır...” Yargıtay, 11. CD. 2009/1616 E. 2009/11328 K. 07.10.2009 T.

⁴⁹¹ Erdoğan, 2013: 184.

⁴⁹² Artuk/Gökçen/Yenidünya, 2010: 718; Dülger, 2015: 411. Benzer şekilde “ekonomik yaşamın korunması” deyiimiyle de yer verildiği görülmektedir. Kurt, 2005: 162.

⁴⁹³ Kurt, 2005: 162.

⁴⁹⁴ Artuk/Gökçen/Yenidünya, 2010: 724.

⁴⁹⁵ Apaydın, 2015: 16.

⁴⁹⁶ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b> (erişim tarihi: 16.12.2018).

⁴⁹⁷ Erdoğan, 2013: 215.

Geniş anlamda korunan değer ise bilişim sistemlerinin bütünlüğü ve güvenliğidir. Bu koruma tek tek bilişim sistemi unsurlarının üzerinde olmaktan çok, uzayı kapsayan bilişim alanının parçaları olarak düşünülmelidir. Yaşam destek ünitelerinden, eğlence ve iletişim araçlarına kadar insan yaşam standartlarını koruyan ve kalitesini arttıran paralel bir düzlem olan bilişim sistemlerinin herhangi birine yönelen tehdit, bilişim alanının bütününe tehdit edeceğinden aslında bu düzlemin tamamının korunmasının amaçlandığı söylenebilecektir.

3.3 Suçun Maddi Unsurları

3.3.1 Konu

Bilindiği üzere hareketin yöneldiği kişi ya da şey suçun konusunu oluşturmaktadır. Bu konu bir eşya olabileceği gibi bir şahsın fiziki, maddi yapısı veya bünyesi de olabilir. Bu kapsamda suçun konusu ile mağdur bazı suç tiplerinde iç içe geçmiş halde bulunabilse de mağdur suçun konusunun sahibi olan kimse olarak konudan farklılık göstermektedir⁴⁹⁸. Yine suçun konusu, korunan hukuksal değerden farklıdır. Korunan hukuksal değer ihlal edilen hukuki varlık veya menfaati ifade eder. Bu nedenle korunan değere hukuksal konu, suçun işlendiği şeye ise maddi konu da denilmektedir⁴⁹⁹. Konusuz bir suç düşünülemeyeceği gibi, suçun konusu arttırma ve eksiltme nedenlerinin uygulanması sırasında cezanın ferdileştirilmesinde önem göstermektedir⁵⁰⁰.

TCK m. 244'te yer alan suçun hukuksal konusu 1. ve 2. fıkralar bakımından ayrı ayrı değerlendirilmelidir. Bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunda (m. 244/1) suçun konusunun bilişim sistemi olduğu konusunda bir tartışma bulunmamaktadır⁵⁰¹. Burada önem gösteren esas nokta ise bilişim sisteminin tanımlanması ve sınırlarının belirlenmesidir.

TCK m. 244'ün gerekçesi suç konusunun tanımlanmasında soru işaretleri oluşturmuştur. Tartışmayı değerlendirmeden önce gerekçenin ilk paragrafını aktarmakta fayda vardır:

“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 ızzar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır.”

⁴⁹⁸ Örneğin, kasten yaralama suçunda mağdur yaralanan kişi, konu ise bu kişinin vücududur. Yine hakaret suçunda mağdur hakaret edilen kişi, konu ise o kişinin şerefidir.

⁴⁹⁹ Toroslu, 2008: 93.

⁵⁰⁰ Artuk/Gökçen/Yenidünya, 2015: 284 – 285.

⁵⁰¹ Tezcan/Erdem/Önok, 2016: 956; Artuk/Gökçen/Yenidünya, 2010: 720.

Gerekçe incelendiğinde “fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları” deyiminden bilişim sisteminin somut parçalarına, diğer ifadeyle donanımına ağırlık verildiği düşünülebilir. Nitekim bu durum öğretilerde eleştirilmiş ve gerek yazılım gerekse donanımın suçun konusu olabileceği ifade edilmiştir⁵⁰². Diğer bir görüş ise gerekçede diğer unsurlardan da açıkça bahsedilmesi karşısında gerekçenin zaten suçun konusunu yalnızca donanım ile kısıtlamadığını söylemektedir⁵⁰³.

Bize göre de gerekçeye ilk bakışta suçun konusu yalnızca donanım gibi anlaşılabilir makteyse de, bütününe bakıldığında ayırım gözetmeksizin bilişim sisteminin tüm unsurları anlatılmak istenmiştir. Ancak unsurların tam olarak nitelendirilememesi nedeniyle genel ifadeler ile yetinildiği görülmektedir. Bu noktada önceki bölümde bahsettiğimiz bilişim sistemi unsurlarına (duyuya yönelen aygıt – iç bağlantı – dış bağlantı) ilişkin ayırımımızın sorunu çözeceğini düşünmekteyiz. Aksi halde klasik donanım – yazılım ayırımı ile her zaman doğru sonuçlar elde edilemeyecektir. Bilişim sisteminin bozulması veya engellenmesi duyuya yönelen aygıtta fiziksel olarak verilecek bir zarar aracılığıyla olabileceği gibi iç bağlantı veya dış bağlantıya zarar verilmesi suretiyle de olabilir. Bilişim sistemi unsurları ve bilişim suçlarının işleme yöntemi bölümlerinde diğer açıklamalara yer verildiği için onlara atıf yapmakla yetinilmektedir.

Öğretilerde yer alan diğer bir tartışma ise içinde veri bulunmayan bilişim sistemlerinin suçun konusunu oluşturup oluşturmayacağıdır. Bir görüşe göre bu tür bir bilişim sistemi çalışabilir durumda olmadığından suçun konusunu oluşturamayacaktır. Örneğin, bir mağazanın vitrininde bulunan bir bilgisayara zarar verilmesi durumunda TCK’nin 244. maddesi değil 151. maddesindeki mala zarar verme suçunun konusu gündeme gelmektedir⁵⁰⁴. Diğer görüş ise içerisinde veri bulunmasa dahi bilişim sisteminin temel özellikleri olan veri alma, depolama ve gönderme özelliklerine sahip sistemlerin birinci fıkra kapsamında korunması gerektiğini, aksi halde bilişim sisteminin hukuksal güvenceden yoksun bırakılmış sayılacağını söylemektedir⁵⁰⁵. Bu noktada sadece suçun konusundan hareketle TCK m. 244 ve m. 151 arasındaki bağlantının çözülemeyeceğini düşünmekteyiz. Bu konu ileride kast unsurunda ve içtima bölümünde tartışılacaktır. Şimdilik bir şeyin sadece tek bir suçun konusunu oluşturmak zorunda olmadığını, farklı suç tiplerinin konusunu aynı şeyin oluşturabileceğini ve diğer unsur-

⁵⁰² “Her ne kadar gerekçe aksi yönde bir eğilim içerisinde olsa bile, kanaatimizce bir bilişim sisteminin işleyişi bakımından unsur niteliği taşımak koşulu ile gerek yazılım gerekse donanım unsurları bu suçun hukuki konusunu teşkil ederler” Özbeke/Kanbur/Doğan/Bacaksız/Tepe, 2015: 933.

⁵⁰³ Erdoğan, 2013: 194.

⁵⁰⁴ “Çünkü bu maddenin düzenlenme 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.” Dülger, 2015: 415.

⁵⁰⁵ Erdoğan, 2013: 197.

larla suç tipine karar verilmesi gerektiği söylenmelidir. Aksi takdirde bilişim sisteminin iç bağlantı unsuru olan verinin varlık ve yokluk tartışması hem gerçekçi değildir hem de teorik bir sonuç elde etmeyi zorlaştırmaktadır. Örneğin, banka ATM'sine kartını kaptıran kişinin öfkeyle ATM'yi parçalayarak sistemin işleyişini bozması, içinde veri bulunmasına karşın bilişim sistemini bozma değil mala zarar verme suçu olarak değerlendirilmelidir.

TCK m. 244/2'nin açık lafzı karşısında suçun konusunu veriler oluşturmaktadır⁵⁰⁶. Birinci ve ikinci fıkralar arasındaki belki de en önemli ayrım suçun konusunda meydana gelmektedir. Öğretide bir görüş bilişim sistemlerinin de suça konu olduğunu belirtmekteyse de bizim de katıldığımız diğer görüş, açıkça verilerden bahsetmekte olduğundan, suçun konusunu yalnızca verilerin oluşturduğunu söylemektedir⁵⁰⁷. Elbette yazılımlar ve programlar gibi verilerden oluşan her türlü bütün de suça konu olabilecektir⁵⁰⁸ ki veriye ilişkin açıklamalara ilk bölümde yer verilmiştir. Son dönemde özellikle oyunlarda ve diğer veritabanlarında ortaya çıkan verinin mülkiyetinin kime ait olduğu konusu ve bunun suçun unsurlarına olan etkisi ise ileride hukuka aykırılık bölümünde tartışılacaktır.

3.3.2 Mağdur

Her suçun bir konusu olduğu gibi bir mağdur da bulunur. Mağdur, suçun maddi konusunun ait olduğu kişidir. Suçtan zarar gören kişi ise mağdura göre daha kapsamlıdır. Suçun işlenmesiyle hukuksal menfaatleri dolaylı veya doğrudan zarar gören kişiler suçtan zarar gören olarak kabul edilir. Her mağdur aynı zamanda suçtan zarar gören de sayılmakla birlikte, mağdur ve fail özellikleri aynı kişide birleşemez⁵⁰⁹. Tüzel kişilerin suçun mağduru olup olmayacağı ise tartışmalıdır. Bir görüş tüzel kişilerin mağdur olabileceğini öne sürerken, diğer bir görüş ise tüzel kişilerin ancak suçtan zarar gören konumunda olabileceğini söylemektedir⁵¹⁰.

TCK m. 244 kapsamında bilişim sisteminin engellenmesi veya verilerin yok edilmesi veya değiştirilmesi suçları mağdur yönünden bir özellik göstermemektedir. Herkes bu suçların mağduru olabilir. Öyle ki suçun mağdurunun mutlaka bilişim sisteminin veya verilerin maliki veya zilyedi olması da gerekmemektedir. Öğretide “hak sahibi” kavramının kullanıldığı ve

⁵⁰⁶ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 934; Tezcan/Erdem/Önok, 2016: 955. Artuk/Gökçen/Yenidünya, 2010: 736.

⁵⁰⁷ Erdoğan, 2013: 229.

⁵⁰⁸ Dülger, 2015: 415.

⁵⁰⁹ Artuk/Gökçen/Yenidünya, 2015: 288.

⁵¹⁰ Artuk/Gökçen/Yenidünya, 2015: 288.

kapsamın geniş tutulduğu görülmektedir⁵¹¹. Sisteme veya verilere herhangi bir engel olmaksızın ulaşılmasında çıkarı bulunan ve sistem üzerinde tasarruf yetkisi bulunan kişi suçun mağduru olabilecektir⁵¹².

TCK m. 244/3'te düzenlenen nitelikli hal bakımından öğretide hâkim görüş, banka veya kredi kurumu ya da kamu kurum ve kuruluşlarının suçtan zarar gören değil, mağdur oldukları yönündedir⁵¹³. Yine m. 244/4 uyarınca mağdur, eylemler nedeniyle malvarlığı itibarıyla zarara uğrayan kişidir⁵¹⁴.

Yargıtay, aynı bankanın farklı şubelerdeki hesapları arasında internet aracılığıyla yapılan aktarmalarda, bankanın doğrudan suçtan zarar görmediğini ve hükmü temyiz hakkı bulunmadığını karara bağlamıştır⁵¹⁵.

Bu suçta mağdurun birbirinden bağımsız birden fazla kişi olması mümkündür. Özellikle bulut sistemlerin yaygınlaşmasından sonra veritabanlarını başka bir sunucuda barındıran şirket veya serbest meslek sahiplerinin verilerine karşı gerçekleşen eylemde hem ilgili sunucunun hak sahibinin hem de verilerin hak sahibinin ayrı ayrı mağdur sıfatı taşıyacağı kabul edilmelidir.

Öğretide bir görüş, bu suç bakımından tüzel kişilerin ancak suçtan zarar gören sıfatını taşıyabileceğini kabul etmekteyse de⁵¹⁶ bu görüşe katılmamaktayız.

3.3.3 Fail

İradi olarak hareket edebilme yetisi -şimdilik- sadece insana özgü olduğu için ancak bir insanın suç faili olabileceği kabul edilmektedir. Kanunun özel bir yükümlülük altında bulunan veya belli niteliklere sahip kişiler tarafından işlenebileceğinin öngörüldüğü hallerde özgü (mahsus) suçlardan, herhangi bir ayırt edici ibarenin yer almadığı durumlarda ise herkes tarafından işlenen suçlardan bahsedilmektedir. TCK'ye göre tüzel kişilerin suç faili olmaya- cıkları açıkça belirtilmiş ve ancak güvenlik tedbiri niteliğindeki yaptırımlar saklı tutulmuştur.

⁵¹¹ Artuk/Gökçen/Yenidünya, 2010: 720; Tezcan/Erdem/Önok, 2016: 955. "Bilişim sistemi üzerinde hak sahibi olmak, ya mülkiyet hakkı sahibi olmakla ya da başka bir kısım sözleşmelerle (kira, ariyet, finansal kiralama gibi) elinde bulundurmakla olabilir." Kurt, 2005: 242.

⁵¹² Dülger, 2015: 414; Yılmaz, 2016: 192.

⁵¹³ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2016: 935.

⁵¹⁴ Tezcan/Erdem/Önok, 2016: 955.

⁵¹⁵ "... Sanıklar hakkında müşteki ...'ın ...A.Ş şubesinde bulunan hesaptan, aynı bankanın bir başka şubesindeki hesabına internet aracılığıyla 16.500 TL tutarında havale ettiği iddiasıyla açılan kamu davasında müşteki bankanın doğrudan suçtan zarar görmediği ve mahkemece katılma kararı verilmiş olması da hükmü temyiz hakkı vermeyeceğinden katılan vekilinin temyiz isteminin CMUK'un 317. maddesi uyarınca istem gibi reddine..." Yargıtay, 2. CD. 2014/25924 E. 2016/10421 K. 01.06.2016 T.

⁵¹⁶ Apaydın, 2015: 20.

Öğretide de tüzel kişilere karşı cezai nitelikte olmasa da idari, inzibati ve mali nitelikte yaptırımlarla, güvenlik tedbiri niteliğindeki yaptırımların da uygulanabileceği söylenmektedir⁵¹⁷.

TCK m. 244'te yer alan suç tipi, mağdurda olduğu gibi failde de bir özellik göstermez. Bu suçun faili herhangi bir kişi olabilir⁵¹⁸. Bilişim suçlarının doğal yapısı gereği teknik bilgi gerektirdiği ve herkes tarafından işlenemeyeceği gibi bir kanı bulunsa da, kanunda aranan bir özellik olmadığından suçun herkes tarafından işlenmesine engel değildir⁵¹⁹. Ayrıca günümüzde büyük maharetlerle gerçekleştirilen bilişim suçlarının genele oranla çok küçük bir kısmı oluşturduğunu, çoğu suçun orta düzey bilgisayar ve telefon kullanıcıları tarafından gerçekleştirildiğini söylemeliyiz.

Öğretide bir görüşe göre failin tespiti ve zararı kimin getirdiğinin açıkça ortaya konulması, başka bir kişiye ait bir bilişim sisteminde bulunan kendine ait verilere zarar verilmesi halinde faillik sıfatının oluşmayacağı⁵²⁰ ifade edilmekteyse de bu görüşe katılmamaktayız. Öncelikle, verilerin bilişim sisteminden bütünüyle bağımsız olduğu düşünülmemelidir. Başkasına ait bir bilişim sisteminde yapılan verilere müdahale eylemi kendiliğinden hak alma kapsamında değerlendirilmelidir. Örneğin bir filmin sahibinin, kendisine ait olmayan bir sunucudaki korsan kopyaları silmesi halinde, sırf verinin gerçek sahibi olduğundan bahisle faillik sıfatının oluşmayacağı düşünülmemelidir. Kişinin başkalarına ait sistemlerdeki kendine ait veriler üzerinde işlem yapması halinde faillik sıfatının değil, hukuka uygunluk nedenlerinin tartışılması gerekmektedir.

Bilişim suçlarının fail yönünden özellik gösteren diğer bir yanı, bu suçların faillerinin özel bir isimle anılmasıdır. “Bilişim korsanları” veya “hacker” olarak halk arasında sıklıkla kullanılan bu terimler önceki bölümlerde incelendiğinden yeniden konu edilmeyecektir.

Son olarak TCK m. 246 gereğince yararına haksız çıkar sağlanan tüzel kişiler hakkında güvenlik tedbirleri uygulanacağı söylenmelidir.

3.3.4 Eylem

TCK m. 244'teki düzenlemenin, 244/1 ve 244/2 fıkralarında iki ayrı suç tipi barındırdığından daha önce bahsedilmişti. Bu nedenle eylemler aşağıda ayrı başlıklar halinde ele alınacaktır. TCK 244/4'te yer alan düzenlemenin suçun nitelikli hali olduğu görüşüne katıldığımızdan dolayı ilgili düzenleme ise suça etki eden nedenler başlığı altında incelenecektir.

⁵¹⁷ Artuk/Gökçen/Yenidünya, 2015: 284.

⁵¹⁸ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 935. Dülger, 2015: 414.

⁵¹⁹ Erdoğan, 2013: 144; Kurt, 2005: 241.

⁵²⁰ Dülgeri 2015: 414.

3.3.4.1 Bilişim Sisteminin İşleyişini Engellemek veya Bozmak (TCK m. 244/1)

TCK m. 244/1, “bir bilişim sisteminin işleyişini engellemek veya bozmak”tan bahsetmekte ve bu eylemi cezalandırmaktadır. Eylemin eTCK’deki karşılığı olan m. 525/B düzenlemesi ise “sistemin işlemesine engel olma veya yanlış şekilde işlemesini sağlama” şeklindedir. Görüleceği üzere engel olma – engelleme eylemi aynen korunmuş, yanlış şekilde işlemesini sağlama eylemi ise yerini bozma ifadesine bırakmıştır. Yanlış şekilde işlemesini sağlama nispeten belirsiz ve işleyiş engelleme eyleminden de her zaman kolay ayrılabilir bulunmadığından⁵²¹ yTCK’nin düzenlenmesi öğretide bizim de katıldığımız şekilde isabetli olarak karşılanmıştır.

Bu suç esas olarak ani suçtur. Bilişim sisteminin işleyişinin engellenmesi veya bozulması genellikle eylemin yapıldığı anda netice verir ve eylemin sonlandırılması ile sona erer. DDOS saldırıları bu suç tipinin tipik bir örneğidir, hedef sisteme istek gönderilerek işleyiş engellenir veya durdurulur, eylem kesildiği veya tamamlandığı zaman sistem hizmet ve fonksiyonları anında baştaki haline döner. Yine, bu suç tipi durum suçlarına⁵²² da örnek gösterilebilir, nitekim bu suç tiplerinin klasik hali olduğu söylenen mala zarar verme suçu da durum suçlarına örnek gösterilmektedir⁵²³. Örneğin, sistem kaynaklarını tüketme saldırılarında, sistem soğutmasının iyi olmaması ve aşırı yüklenme nedeniyle işlemci gibi bazı donanım parçalarının yanarak bozulması halinde durum suçundan bahsedilebilecektir. Tüm bunlara karşın suçun kesintisiz (mütemadi) şekilde işlenmesi de mümkündür⁵²⁴. Suçun ani şekilde de işlenbilmesinden dolayı zorunlu kesintisiz suç değil, muhtemel kesintisiz suç değerlendirilecektir. Örneğin elektriğin kesilmesi veya veri taşıma araçlarının saklanması halinde kesintisiz suçtan bahsedilmektedir⁵²⁵. Aynı şekilde arka kapı (backdoor) bırakma ve bu kapı üzerinden sistemin engellenmeye devam edilmesi durumunda da kesintisiz suç oluşacaktır.

Hareketin şeklinde göre bu suç tipi genellikle icrai hareketle işlenen suçlardandır. Ancak bazı durumlarda ihmal suretiyle de gerçekleştirilebilir. Örneğin, sistem güvenliğinden sorumlu failin, sistemi bilerek savunmasız bırakması halinde suç ihmali davranışla işlenmiş olacaktır⁵²⁶.

Öğretide sistemin işleyişini engelleme veya bozma eylemlerinin seçimlik hareketli suç olup olmadığı konusunda tartışma bulunmaktadır. Baskın görüşe göre engelleme veya bozma

⁵²¹ Erdoğan, 2013: 185.

⁵²² Durum suçları (iz bırakan suçlar), neticenin tamamlanmasına karşın, zararın giderilmesinin vakit aldığı suçlardır. Yaralama suçu örnek olarak gösterilmektedir, yaranın uzun süre kapanmaması neticenin tamamlanmış olmasını engellememektedir. Artuk/Gökcen/Yenidünya, 2015: 248 – 249.

⁵²³ Özbek, 2006: 135.

⁵²⁴ Erdoğan, 2013: 185.

⁵²⁵ Erdoğan, 2013, 185.

⁵²⁶ Erdoğan, 2013: 185; Dülger, 2015: 418.

eylemleri seçimlik hareketlerdir ve bunlardan herhangi birinin gerçekleşmesi halinde suç oluşacaktır⁵²⁷. Yine eTCK döneminde de seçimlik hareket olduğu görüşü benimsenmiştir⁵²⁸. Diğer görüşe göre ise engelleme ve bozma eylemin hareket değil, netice unsurunu oluşturmaktadır. Bu nedenle engelleme veya bozma neticesi herhangi bir hareketle gerçekleşebileceğinden serbest hareketli suçtan bahsedilmelidir⁵²⁹. Bize göre engelleme ve bozma halleri eylemlerin neticesi olmayıp seçimlik hareketli suç oluşturmuştur. Çünkü söz konusu unsurların hareket değil de netice olduğunun kabulü halinde, suçun seçimlik hareketli değil, seçimlik neticeli olduğu varsayılmalıdır ki bu durum TCK sistematığına aykırı olacaktır. Yasa koyucu da madde gerekçesinde "... Fıkırdaki seçimlik hareketli bir suç meydana getirilmiştir." demekle hükmün düzenleniş amacını ortaya koymaktadır.

TCK m. 244/1'de neticenin ayrıca gerçekleşmiş olması aranmadığından suç sırf hareket suçu niteliği taşımaktadır⁵³⁰.

3.3.4.1.1 İşleyişi Engellemek

Engellemek kelime anlamıyla bir şeyin gerçekleşmesini veya yapılmasını önlemek anlamına gelmektedir⁵³¹.

Öğretide de bu tanım üzerinden bilişim sisteminin bazı özelliklerinin eklenmesiyle eylem yorumlanmaktadır. Bilişim sistemlerinin varlık sebebi olan görevlerini yapamaz hale getirilmesi⁵³², normalde yerine getirdiği fonksiyonlarını ifa etmesinin engellenmesi⁵³³, sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılması⁵³⁴, dışarıdan gerçekleşen bir müdahale ile kısmen veya tamamen önlenmesi⁵³⁵, veri işleme faaliyeti yapmasının önlenmesi⁵³⁶ şeklinde tanım yapıldığı görülmektedir.

Öğretideki bu tanım ve açıklamalar incelendiğinde engelleme ile bozma eylemleri arasındaki farkın iki şekilde açıklandığı görülecektir. İlk olarak sistemin durdurulması veya yavaşlatılması geçici ise engelleme, kalıcı ise bozma eylemlerinin gerçekleştiği söylenmekte-

⁵²⁷ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 937 – 938; Tezcan/Erdem/Önok, 2016: 955; Ar-tuk/Gökçen/Yenidünya, 2010: 719; Dülger, 2015: 417; Karagülmez, 2014: 237; Yılmaz, 2016: 195; Taşkın, 2008: 44; Gürler, 2015: 138; Demircan, 2016: 101.

⁵²⁸ Yazıcıoğlu, 1997: 262; Yenidünya/Değirmenci, 2003: 96.

⁵²⁹ Erdoğan, 2013: 186.

⁵³⁰ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 938.

⁵³¹ http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1e8823ec0d10.99241874 (erişim tarihi: 22.12.2018).

⁵³² Erdoğan, 2013: 189.

⁵³³ Kurt, 2005: 164.

⁵³⁴ Yılmaz, 2016: 194.

⁵³⁵ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 935.

⁵³⁶ Tezcan/Erdem/Önok, 2016: 955.

dir⁵³⁷. İkinci olarak ise sistemin bir kısmının etkilendiği hallerde engelleme, bütünün etkilenmediği halde bozma söz konusu olmaktadır.

Bize göre bu iki kıstas da eylemleri net olarak ortaya koymakta yetersiz kalmaktadır. Bu konudaki en isabetli ölçüt, fen bilimlerinde yer edinen fiziksel değişim – kimyasal değişim ayrımı esas alınarak yapılabilir. Bilindiği gibi fiziksel değişimde maddenin iç yapısında değişme olmadan, süreç tersine çevrilerek tekrar eski hale getirilebilecek (buzun eritilmesi – suyun dondurulması) bir değişim söz konusuyken, kimyasal değişimde maddenin yapısı değişikliğe uğradığından aynı şekilde eski hale dönmek mümkün olmamaktadır. Bilişim sistemlerinin engellenmesi ve bozulmasında da bu kıstasları ele alırsak, yapılan eylem sona erdirildikten sonra sistem eski halinde çalışabiliyorsa engellenme, yapısal değişikliğe uğramış ve teknik önlemler (format atma, kurtarma vb.) gerektiriyorsa bozulma söz konusudur.

Tüm bu bilgilerden yola çıkarak bilişim sisteminin engellenmesini, işlevlerin yapısal olmayan ve sona erdirildiğinde başka bir şeye gerek kalmaksızın olağan şekilde devam ettirilebilecek şekilde önlenmesi olarak tanımlayabiliriz.

Bu ayrıma göre sistem kaynaklarını tüketme saldırıları (DDOS, tavşanlar vb.) sona erdirildikten sonra sistem normal çalışmasını sürdürebildiğinden sistemin engellenmesi söz konusudur. Bu saldırıların geçici veya kalıcı olması ile sistemin bir bölümünü veya tamamını etkilemesinin bir önemi bulunmamaktadır. Bununla birlikte zararlı yazılımlarla işletim sisteminin kritik dosyalarının tahrip edilmesi örneğinde zararlı yazılım temizlense bile geri dönüş imkânı bulunmadığından sistemin bozulduğu kabul edilecektir. Yine sistemi açıp kapatmakla giderilebilecek sorunlara ilişkin eylemlerin de bozma değil, engelleme olduğu ifade edilmelidir.

Yasa koyucunun kavramı geniş tutmuş olması, öğretide her türlü eylemin dahil edilmesi gerektiği şeklinde yorumlanmaktadır. Bu anlamda bilişim sistemleri, başka bilişim sistemleri veya zararlı yazılımlar aracılığıyla engellenebileceği gibi, elektriğinin kesilmesi, kabloların çıkarılması gibi somut unsurlara yönelik eylemlerle de engellenebilecektir⁵³⁸. Yine önemsiz gibi görünse de veri işlem hızını düşüren her türlü eylem engelleme kapsamında düşünülmelidir⁵³⁹.

Öğretide bilişim sistemi dışındaki unsurlara yapılan müdahalenin, örneğin taşınabilir bilgisayarın yere atılarak kırılması durumunda m. 244 anlamında engelleme değil mala zarar verme suçunun olduğu ifade edilmiştir. Ayrıca bilgisayar şifresinin değiştirilerek girişin

⁵³⁷ Erdoğan, 2013: 190.

⁵³⁸ Dülger, 2015: 418.

⁵³⁹ Kurt, 2005: 164.

engellenmesi engelleme suçuna örnek verilmiştir⁵⁴⁰. Bu görüşlere katılmamaktayız. Öncelikle sistemlere fiziksel zarar verilmesi durumunda failin amacının saptanması önem taşımaktadır. Örneğin teknik bilgisi bulunmayan ve bilgisayarın o anda yaptığı işlemin tamamlanmasını istemeyen birinin bu amaçla bilgisayarı parçalaması mala zarar verme suçu olarak değil, bilişim sistemini engelleme veya bozma suçu olarak değerlendirilmelidir⁵⁴¹. Yine, bilgisayar şifresinin değiştirilerek girişin engellenmesi, sistemin engellenmesi suçunu değil, ikinci fıkradaki verilerin değiştirilmesi suçunu oluşturmaktadır⁵⁴². Yargıtay da bu görüştedir⁵⁴³. Çünkü sistemin varsayılan işleyişinin engellenmesi söz konusu değildir, sistem halen doğru şifrenin girilmesi halinde açılmak üzerine olan işlevini yerine getirmektedir.

3.3.4.1.2 İşleyişi Bozmak

Bozmak, kelime anlamıyla bir şeyi kendisinden beklenen işi yapamayacak duruma getirmektir⁵⁴⁴.

Öğretide de TDK'nin tanımına uygun olarak, bilişim sistemlerinin veri işleme faaliyeti yapamayacak hale getirilmesi ya da doğru sonuçlara ulaşmasına engel olacak şekilde müdahalede bulunulması⁵⁴⁵, kısmen ya da tamamen işlemez hale getirilmesi⁵⁴⁶, tamamıyla çalışamaz hale getirilmesi⁵⁴⁷, kendisinden beklenen işi yapamayacak şekilde kısmen veya tamamen tahrip edilmesi⁵⁴⁸, kalıcı surette sistemden istifadenin engellenmesi⁵⁴⁹ şeklinde tanımlar mevcuttur. Sistemin bozulmasında, engellenmesinde olduğu gibi yasa koyucunun kavramı geniş tuttuğu, farklı şekillerde sistemin bozulmasının mümkün olduğu yönünde bir görüş birliği bulunmaktadır.

Sistemin engellenmesi bölümünde yaptığımız ayırım geçerli olarak, geri dönülemez şekilde ve yapısal değişikliğe neden olan her türlü eylemin sistemi bozma kapsamında değerlendirilmesi gerektiğini düşünmekteyiz. Bu eylem bütün bir işletim sistemini etkileyebileceği

⁵⁴⁰ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 936.

⁵⁴¹ Bu konuda iki suçun da olduğu ve konunun TCK m. 44 hükmü uyarınca çözüleceği de ifade edilmektedir. Artuk/Gölcen/Yenidünya, 2010: 719. İctima bölümünde bu konuya değinilecektir.

⁵⁴² Aynı görüşte, Tezcan/Erdem/Önok, 2016: 956.

⁵⁴³ "... Katılana ait hotmail adresine hukuka aykırı olarak giren ve yeni şifre oluşturup katılanın erişimini engelleyerek e-mail adresini kullanan sanığın eylemine uyan TCK'nin 244/2 madde ve fıkrası uyarınca cezalandırılması gerektiği gözetilmeden yazılı şekilde yasal ve yeterli olmayan gerekçeyle beraatına hükmolunması..." Yargıtay, 8. CD. 2013/771 E. 2014/15833 K. 23.06.2014 T. Aynı yönde, Yargıtay, 8. CD. 2013/11478 E. 2014/8887 K. 08.04.2014 T.

⁵⁴⁴ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1ea0ee74fc31.41993145 (erişim tarihi: 22.12.2018).

⁵⁴⁵ Erdoğan, 2013: 193; Tezcan/Erdem/Önok, 2016: 955.

⁵⁴⁶ Dülger, 2015: 419.

⁵⁴⁷ "Çalışamaz hale getirilmesi; sistemin çökertilmesi, program akışının değiştirilmesi, bozulması, sistemin soyut unsurlarının yani yazılımlarının virüsler vasıtasıyla işlemez hale getirilmesi şekillerinde gerçekleştirilebilir." Kurt, 2005: 164.

⁵⁴⁸ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 934.

⁵⁴⁹ Artuk/Gökçen/Yenidünya, 2010: 720.

gibi basit bir program üzerinde de tesir etmiş olabilir. Yine, engellemede olduğu gibi bozma suçunda da fiziksel müdahaleler ile suçun oluşması mümkündür.

3.3.4.2 Bilişim Sistemindeki Verileri Bozmak, Yok Etmek, Değiştirmek, Erişilmez Kılmak, Veri Yerleştirmek veya Verileri Başka Yere Göndermek (TCK m. 244/2)

TCK m. 244/2’de sistemi engelleme ve bozma suçunun dışında, veriler üzerinde gerçekleşen suç tiplerine yer vermiştir. Birinci fıkra uyarınca yapılan açıklamalar ile uyumlu olmak üzere, bu suçta da seçimlik hareketlere yer verildiği görülmektedir⁵⁵⁰. Nitekim kanunun gerekçesi yalnızca birinci değil ikinci fıkrayı da kapsayacak şekilde seçimlik hareketler olduğunu belirtmektedir. Suçun seçimlik hareketli olmasının sonucu olarak, gösterilen eylemlerden herhangi birinin gerçekleştirilmesi halinde suç tamamlanmış sayılacak, birden fazla eylemin gerçekleşmiş olması ise cezanın belirlenmesinde alt sınırdan uzaklaşmayı gerektirebilecek bir etken olarak ele alınacaktır⁵⁵¹.

Yasa koyucunun düzenleme tekniği açısından, bu suç tipi için kapsamı geniş tutmak istediği ve boşluk bırakmamak amacıyla tespit edebildiği her türlü eylemi suç tipine dahil ettiği görülmektedir⁵⁵². Bu durum her ne kadar kanunilik ve belirlilik ilkelerine uygun bir yasa yapma tekniği olsa da, eylemlerin birbirine olan benzerliği ve bazı durumlarda ayırt edilmeleirindeki zorluğu ortaya koymaktadır. Kanunun bu fıkradaki ele alınış biçimi, bilişim suçları konusunda henüz yerleşmiş bir sistematığe sahip olmadığımızı ve şimdilik suç tipine uymayan eylemlerin kalmaması yönünde bir politika izlendiğini göstermektedir.

Birinci fıkraya paralel olarak bu suç tipinin de ihmali hareketle işlenmesi mümkündür. Örneğin bir saldırı sırasında gerekli önlemleri alması gereken sorumlunun, kasıtlı olarak eylemde bulunmaması sonucunda verilerin zarar görmesi halinde ihmali hareketle suçun gerçekleştiği varsayılmaktadır⁵⁵³.

Uygulamada sıklıkla görülen başkasına ait e-posta veya sosyal medya gibi hesapların şifrelerinin ele geçirilmesi ve akabinde gerçekleştirilen kullanıcı adına paylaşım yapma, şifreyi değiştirerek kullanıcının erişmesini engelleme gibi eylemler Yargıtay tarafından bu fıkra kapsamında suç olarak değerlendirilmektedir⁵⁵⁴. Konuya içtima bölümünde ayrıca değinilecektir.

⁵⁵⁰ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 938. Bu unsurların seçimlik hareket değil netice olduğu, birden fazla netice meydana gelse de tek suç oluştuğu görüşü için, Erdoğan, 2013: 217.

⁵⁵¹ Artuk/Gökçen/Yenidünya, 2010: 724.

⁵⁵² Erdoğan, 2013: 219; Dülger, 2015: 429.

⁵⁵³ Erdoğan, 2013: 219.

⁵⁵⁴ Tezcan/Erdem/Önok, 2016: 956.

3.3.4.2.1 Verileri Bozmak

Bozmanın kelime anlamının bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek olduğundan yukarıda bahsedilmişti⁵⁵⁵. Öğretide de bozma eyleminin verinin içeriğine veya yapısına müdahale ederek veriyi kısmen veya tamamen kullanılamaz hale getirmek olduğu söylenmektedir⁵⁵⁶.

Bilişim sistemlerinin bozulması konusunda yaptığımız açıklamalar burada da geçerlidir. Verinin yapısal olarak, olağan şekilde geri döndürülemez şekilde zarara uğratılması bozmak olarak düşünülmelidir. Bu eylem zararlı yazılımlar veya doğrudan fiziksel müdahale ile gerçekleştirilebilecektir⁵⁵⁷.

Bozmak eylemi yok etmekten farklıdır. Yok edilme eyleminde verinin varlığına son verilmekte, bozma halinde ise veri bulunmakla birlikte kullanılamaz halde bulunmaktadır⁵⁵⁸. Yine, bozmak eylemi değiştirmekten de farklılık gösterir. Değiştirme eyleminde veri yine kullanılabilir başka bir biçime bürünmekteyken, bozma halinde meydana gelen değişim veriyi kullanılamaz hale getirmektedir.

3.3.4.2.2 Verileri Yok Etmek

Yok etmek kelime anlamıyla ortadan kaldırmak, varlığına son vermek demektir⁵⁵⁹. Öğretide ise verilerin gerçek anlamda varlığına son verilemeyeceği kabul edilmekle, soyut anlamda teknik ve mantıksal bir yok etme eyleminden bahsedilmektedir⁵⁶⁰.

eTCK'nin 525/B maddesinde verilerin silinmesinden bahsedilmekte, yTCK'de ise bu eylem ayrıca yer almayıp yok etme kapsamında değerlendirilmiştir. Böylece gereksiz tekrar önlenmiştir⁵⁶¹.

Öğretide veriye tekrar ulaşılabilme imkanının varlığının suçun oluşmasını engellemeceği isabetli olarak ifade edilmektedir. Verinin barındığı donanım fiziksel olarak geri dönüştürülemeyecek bir hasara uğramadığı sürece verinin farklı ve ileri düzey tekniklerle geri getirilebilmesi mümkündür⁵⁶². Kaldı ki bu teknikler de her gün gelişmektedir. Bu nedenle verilerin kalıcı olarak yok edilmesi çok iddialı bir ifade olduğundan öğretide, veriye erişim

⁵⁵⁵ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1f66217ece51.76515473 (erişim tarihi: 23.12.2018).

⁵⁵⁶ Artuk/Gökçen/Yenidünya, 2010: 724; Erdoğan, 2013: 220.

⁵⁵⁷ Dülger, 2015: 420; Kurt, 2005: 167.

⁵⁵⁸ Aynı görüşte, Erdoğan, 2013: 220.

⁵⁵⁹ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1f66246ce5b7.05920229 (erişim tarihi: 23.12.2018).

⁵⁶⁰ Erdoğan, 2013: 222; Dülger, 2015: 420.

⁵⁶¹ Erdoğan, 2013: 223.

⁵⁶² Bu tekniklerle ilgili detaylı bilgi için Dülger, 2015: 421.

için verilen komutun sonuçsuz kalmasına neden olacak şekilde kayıtlardan silinmesi ile suçun tamamlandığı kabul edilmektedir⁵⁶³.

Öğretide ayrıca verilerin geri dönüşüm kutusuna gönderilmesi halinde verinin yok edilip edilmemiş olduğu tartışılmıştır. Bir görüş verilerin kolaylıkla yeniden eski yerlerine alınabileceğinden hareketle yerinin değiştirilmiş olmasının yok etme suçunu oluşturmadığını söylemektedir. Diğer görüş ise verilerin geri dönüşüm kutusunda bulunduğu sürece kullanılamayacağını, veri sahibinin veriyi bıraktığı yerde bulamayacağından verilerin yok edildiğinin kabul edilmesi gerektiğini belirtmektedir⁵⁶⁴. Bize göre bu tür eylemlerin veriyi yok etme suçunu oluşturması mümkün değildir. Verilerin geri dönüşüm kutusuna taşınması, teknik olarak verilerin bütünlüğü bozulmaksızın başka herhangi bir klasöre taşınmasından farklı değildir, burada değiştirilen verinin kendisi değil, onun konumunu gösteren referansıdır (dizin – anahtar veri). Bu durumda olsa olsa verileri başka yere gönderme eyleminin tartışılması gerekecektir.

Yok etme eylemi, ortada değerlendirilebilir bir veri bırakılmaması yönüyle diğer eylemlerden ayrılmaktadır⁵⁶⁵.

3.3.4.2.3 Verileri Değiştirmek

Değiştirmek kelime anlamıyla başka bir biçime sokmak, bir şeyi bulunduğu bir yerden başka bir yere götürmek demektir⁵⁶⁶. Diğer eylemler arasında en kapsamlı olanın değiştirmek olduğu söylenebilir. Verileri başka yere göndermek kanunda ayrıca bir hareket olarak tanımlandığından bunun dışında kalan değiştirme eylemleri bu kapsamda değerlendirilmelidir.

Bize göre verileri değiştirmek esas olarak üç şekilde mümkündür. İlk olarak verilerin içeriğinin değiştirilmesi bu eylemi oluşturur. Bir verinin yerine başka verinin konulması da bu kapsamda düşünülmelidir. İkinci durum verinin biçiminin (tipinin) değiştirilmesi şeklindedir⁵⁶⁷. Veri içeriğinin değişmemekle birlikte uzantısının değiştirilmesi, sertifika veya benzeri nitelikte orijinallliğini etkileyecek değişiklikler bu kapsamdadır. Üçüncü ve son durumda ise verilerin niceliğinin değiştirilmesinden bahsedilmelidir. Kopyalamak gibi verilerin sayısını etkileyecek her türlü hareket bu eylem kapsamında değerlendirilir. FSEK m. 71’de yer alan

⁵⁶³ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 939.

⁵⁶⁴ Erdoğan, 2013: 222; Dülger, 2015: 421; Apaydın, 2015: 22.

⁵⁶⁵ Kurt, durumdan ortada tamir edilebilecek bir unsurun kalmaması şeklinde bahsetmektedir. Kurt, 2005: 168.

⁵⁶⁶ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1f667154fb10.96378208 (erişim tarihi: 23.12.2018).

⁵⁶⁷ “Burada verinin değiştirilmesinden kastedilen şey, bir verinin bulundurulma ve kullanma amacı dışında, başka bir formata dönüştürülmesidir.” Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 939.

suç tipleri içerisindeki eserin değiştirilmesi ve çoğaltılması da bu eylemlerle paralellik gösterecek şekilde düşünülmelidir⁵⁶⁸.

Günümüzde film, müzik gibi medya içerikleri *codec* denilen çeşitli sıkıştırma yöntemleriyle farklı formatlarda piyasada bulunmaktadır. Bu *codec*'ler az yer kaplayan ama içeriğin kalitesini bir miktar azaltacak şekilde tasarlanmış olabileceği gibi yüksek kalitede ve çok yer kaplayan bir biçime sahip olabilir. Bu biçimler arasında yapılacak çevirme işlemleri de bu eylem kapsamında değerlendirilmelidir.

Öğretide bazı yazarlar kötü amaçlı kodların veriye yerleştirilmesinin, verileri değiştirme eylemi içinde değerlendirmesine karşın⁵⁶⁹, kanunda veri yerleştirmek şekilde ayrı bir eylem belirlenmiş olduğu dikkate alındığında, veri içeriğinden herhangi eksiltme yapmaksızın yalnızca üzerine fazladan veri eklenmesi durumlarında veri yerleştirme eyleminin tartışılması gerektiğini düşünmekteyiz.

3.3.4.2.4 Verileri Erişilmez Kılmak

Erişmek kelime anlamıyla varılması zamana, emeğe bağlı olan veya uzakta bulunan bir amaca varmak, ulaşmak demektir⁵⁷⁰. Bu eylem ile verileri yok etmeksizin veya değiştirmeksizin erişilmez kılınan tüm eylemler vurgulanmaktadır. Zararlı yazılım kullanılması, şifre koyulması vb. yöntemler başta olmak üzere birçok şekilde bu eylem gerçekleştirilebilir⁵⁷¹. Öğretide erişilmez kılmanın geçici veya kalıcı olması arasında bir fark olmadığı belirtilmektedir⁵⁷². Verilerin erişilmez kılınması için verinin mevcut sistemde halen bulunuyor olması şarttır⁵⁷³.

Erişilmez kılmak, verilerin halen bulunması yönüyle yok etmekten, veri içerik veya yapısının ya da niceliğinin değişmemesi yönüyle değiştirme eylemlerinden ayrılmaktadır. Verilerin erişilmez kılınması aynı zamanda bilişim sistemini de erişilmez kılmak suretiyle engellemişse TCK m. 244/1'in uygulanması gerekecektir⁵⁷⁴.

Bilişim suçlarının işleme yöntemlerinde detaylı olarak bahsedilmiş olan fidye yazılımları bu eylemin tipik örneğini oluşturmaktadır.

⁵⁶⁸ Bilgisayar programları ile ilgili çoğaltma ve yayma eylemleri hakkında detaylı bilgi için, Öztan, 2008: 355.

⁵⁶⁹ Erdoğan, 2013: 224.

⁵⁷⁰ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1f670ca83ac0.87203298 (erişim tarihi: 23.12.2018).

⁵⁷¹ Dülger, 2015: 422.

⁵⁷² Erdoğan, 2013: 225.

⁵⁷³ Aynı görüşte, Artuk/Gökçen/Yenidünya, 2010: 725.

⁵⁷⁴ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 939. “Ancak 1. fıkra bilişim sisteminin işleyişi korunduğu için, tek başına bir sistem olmayıp bir sistemin parçası olarak kullanılabilen veri taşıma araçlarındaki verilerin erişilmez kılınması için bozulması ya da çalışmasının engellenmesi halinde ise 2. fıkradaki hükmün uygulanması gerekir.” Dülger, 2015: 422.

3.3.4.2.5 Veri Yerleřtirmek

Yerleřtirmek kelime anlamıyla yerine koymak, yerleřmesini saęlamak demektir⁵⁷⁵. Veri yerleřtirme eylemi sistemdeki verilere bir zarar vermemesine karřın, verilerin gvenilirlięinin zarar grmesi nedeniyle cezalandırılmaktadır⁵⁷⁶. Veri yerleřtirmenin iki řekilde meydana geleceęini dřnmekteyiz. İlk halde sistemin ierięine baęımsız bir veri bloęunun aktarılmasından, ikinci halde ise mevcut verilerde bir eksiltme yapılmaksızın veri ierięine yeni verilerin eklenmesinden bahsedilebilir. Eęer verilerde eksiltme ve arttırma aynı anda gerekleřmiřse bu halde veri yerleřtirme deęil, veri deęiřtirme eyleminin gerekleřtięinin kabul gerekmektedir.

Veri yerleřtirme bir řekle baęlı deęildir. Yerleřtirilen veri biliřim aęları zerinden veya sisteme eklenecek bir donanım zerinden ya da bařkaca bir yntemle de saęlanabilir.

İřletim sistemleri kendi yapıları gereęi bazı verileri kendilięinden retebilmektedir. Sistem gvenlięi veya yapılan iřlemlerin raporlanması iin tutulan bu veriler oęunlukla kullanıcının farkında olmaksızın gerekleřmektedir. Bu řekilde bir hareketin dolaylı sonucu olarak sisteme eklenmiř bulunan veriler, eylem ynnden veri yerleřtirme tipine uysa da suun manevi unsurunu tařımayabilir. Byle durumlarda failin kastının deęerlendirilmesi gerekir.

Yargıtay bir kararında bilgisayar ortamında sahte iře giriř bildirgesi verilmesinin veri yerleřtirme eylemi olduęundan bahsetmektedir. Karara eylemin m. 244'te yer alan suu oluřturmaması nedeniyle katılmamakla birlikte, isabetli olarak veri deęiřtirme yerine yerleřtirme eyleminden bahsedilmesinin nem arz ettięini dřnmekteyiz⁵⁷⁷.

3.3.4.2.6 Verileri Bařka Yere Gndermek

Gndermek kelime anlamıyla yollamak, bir yere doęru yola ıkarmak, yetki vererek gitmesini saęlamak demektir⁵⁷⁸.

ęretide verileri bařka bir yere gnderme eyleminin kapsamı tartıřmalıdır. Bir grř, verinin mevcut biliřim sistemi dıřında bařka bir yere gnderilmesi gerektięini sylerken, dięer grř ise kanun metninde bir sınırlama bulunmadıęından aynı sistem ierisinde bařka bir

⁵⁷⁵ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1f671b7e1405.63535627 (eriřim tarihi: 23.12.2018).

⁵⁷⁶ Artuk/Gkcen/Yenidnya, 2010: 725.

⁵⁷⁷ "... Sanıkların fikir ve eylem birlięi ierisinde hareket edip sahte iře giriř bildirgesi dzenleyerek iřyerinde alıřmayan kiřileri sigortalı olarak gsterdikleri iddiasıyla aılan kamu davasında; e-bildirge, imza ve řifre ile bilgisayar ortamında iře giriř bildirgelerinin verilmesi eyleminde, sahte oluřturulmuř maddi varlıęı haiz, somut bir belge olmadıęından sbutu halinde eylemin TCK'nın 244/2. maddesinde dzenlenen sisteme veri yerleřtirme suunu oluřturacaęı cihetle..." Yargıtay, 11. CD. 2015/1571 E. 2017/1828 K. 13.03.2017 T.

⁵⁷⁸ http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c1f67645b3936.30207068 (eriřim tarihi: 23.12.2018).

yere göndermenin de suç oluşacağını söylemektedir⁵⁷⁹. Bize göre “başka bir yer” ifadesi belirsizdir ve bilişim suçları terminolojisine de uygun değildir⁵⁸⁰. Bununla birlikte “başka” ifadesinin kullanılması mevcut sistemin dışına çıkılması gerektiğini çağrıştırmaktadır. Bu nedenle ifadenin yeniden ele alınma ihtiyacını belirtmekle birlikte⁵⁸¹ mevcut sistemin dışına gönderilmesi gerektiği görüşüne katılmaktayız.

Göndermek ile değiştirmek eylemleri arasında kes – kopyala ayrımı olduğu söylenebilir⁵⁸². Eğer veri bulunduğu yerde kalmak suretiyle kopyalama yoluyla nicelik olarak arttırılmışsa veri değiştirme, verinin bulunduğu yerden alınarak nicelik olarak aynı kalmak koşuluyla başka bir yere taşınması halinde verileri başka yere gönderme eyleminden söz edilmelidir.

Öğretide verilerin sadece bilişim alanında gönderilmesi değil, örneğin yazıcı vb. çevre elemanlarından çıktı alınması halinde de gönderme eyleminin gerçekleştiği söylenmektedir⁵⁸³.

3.4 Suça Etki Eden Nedenler

TCK m. 244 kapsamında herhangi bir cezayı hafifletici neden düzenlenmediğinden, genel hükümlere göre indirim nedenleri takdir edilecektir. Cezayı ağırlaştırıcı üç neden bulunmaktadır. Bunlardan ikisi TCK m. 244/3 ve 244/4’te, diğeri ise 3713 sayılı Terörle Mücadele Kanunu’nun 4. ve 5. maddelerinde düzenlenmiştir. Bunların sırasıyla incelenmesi gerekmektedir.

3.4.1 Eylemin Bir Banka veya Kredi Kurumuna ya da Bir Kamu Kurum veya Kuruluşuna Ait Bilişim Sistemi Üzerinde İşlenmesi (m. 244/3)

TCK m. 244/3’e göre bu maddede yer alan eylemlerin banka veya kredi kurumu ya da kamu kurum veya kuruluşuna ait bilişim sistemleri üzerinde işlenmesi halinde verilecek ceza yarı oranında arttırılmaktadır.

Banka ve kredi kurumlarını kapsamı 5411 sayılı Bankacılık Kanunu’nda belirtilmiştir. Kanunun 157. maddesinde bu kanuna tabi kuruluşların TCK 244 kapsamında banka veya kredi kurumu olarak kabul edileceği ifade edilmektedir. Aynı kanunun 2. maddesinde ise kapsam, “Türkiye’de kurulu mevduat bankaları, katılım bankaları, kalkınma ve yatırım bankaları, yurt dışında kurulu bu nitelikteki kuruluşların Türkiye’deki şubeleri, finansal holding şirketleri, Türkiye Bankalar Birliği, Türkiye Katılım Bankaları Birliği, Bankacılık Düzenleme ve

⁵⁷⁹ Artuk/Gökçen/Yenidünya, 2010: 725; Erdoğan, 2013: 227.

⁵⁸⁰ “Verilerin başka bir yere gönderilmesine dair bu cümle ... sunulan tasarıda yer almamaktadır. TBMM Adalet Komisyonu tarafından bu madde değiştirilmiş ve maddeye eklenmiştir.” Erdoğan, 2013: 227.

⁵⁸¹ “Kanaatimizce bu seçimlik hareketin düzenleniş şekli maddenin “ratio legis”ine hizmet etmekten uzaktır.” Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 940.

⁵⁸² Aynı görüşte, Dülger, 2015: 428.

⁵⁸³ Erdoğan, 2013: 228.

Denetleme Kurumu ve Tasarruf Mevduatı Sigorta Fonu” olarak belirlenmiştir⁵⁸⁴. Kanunun açık hükmü karşısında Bankacılık Kanunu kapsamı dışında kalan kuruluşların banka veya kredi kuruluşu olarak değerlendirilmesine imkân yoktur. Bankacılık Kanunu’nun 157. maddesi, özünde ceza kanunu niteliği dahi taşımayan bir kanunun, TCK’ye açıklama getirmeye çalışması ve ileride yapılacak değişikliklerin sistematik sorunlara yol açacağı nedeniyle eleştirilmektedir⁵⁸⁵. Bize göre söz konusu düzenlemede uygulamada yaşanacak sorunların giderilmesi için kapsamın belirlenmesi amaçlanmaktadır. Ancak söz konusu düzenlemenin kanun yapma tekniğine aykırı olduğunu, böyle bir atıfta bulunulması gerekli ise, atfın Bankacılık Kanunu’nda değil, TCK’nin tanımlar başlıklı 6. maddesinde yapılmasının uygun olacağı düşüncesindeyiz. Nitekim TCK’nin 158/1-j maddesinin gerekçesinde, “Kredi kurumu deyiminden banka olmamasına karşın, kanunen borç para vermeye yetkili kılınan kurumlar anlaşılır.” denilmekte, aynı kavramın TCK m. 158 ve m. 244’te farklı kapsama tabi tutulması belirlilik ilkesini zedelemektedir.

Fıkra da yer alan kamu kurum ve kuruluşları ifadesinden ise devletin merkez ve taşra teşkilatları ile yerel yönetimler ve KİT’ler yani geniş anlamda devlet aygıtı anlaşılmalıdır⁵⁸⁶.

Fıkra metni incelendiğinde banka veya kredi kuruluşlarına, kamu kurum ve kuruluşlarından önce yer verildiği görülmektedir. Bu durum da son dönemde karşılaştırmalı hukukta da görülen, bilişim suçlarının neden olduğu ekonomik sonuçlara verilen önemi göstermektedir.

Düzenlemede bilişim sistemine, yerine veya zamanına dair bir ayırım yapılmadığı görülmektedir. Buna göre bilişim sisteminin mutlaka banka, kredi kuruluşu veya kamu kurumlarına ait binalarda yer alması şart olmadığı gibi, sisteme uzaktan müdahalede de yer şartı aranmamaktadır. Yargıtay Millî Eğitim Bakanlığına ait olan e-okul sisteminin şifrelerinin ele geçirilerek devamsızlık ve not durumunun değiştirilmesini arttırıcı neden olarak görmüştür⁵⁸⁷. Yine bilgisayar, ATM ve benzeri her türlü bilişim sisteminin suça etki eden neden kapsamında olduğu söylenmelidir.

⁵⁸⁴ Bankacılık Kanunu’nun “Tanımlar ve Kısaltmalar” başlıklı 3. maddesinde,

Banka: Mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını,

Mevduat bankası: Bu kanuna göre 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: Bu kanuna göre 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 ifade etmektedir. Türkiye Bankalar Birliği Risk Merkezi Yönetmeliği’nde de kredi kuruluşları aynı şekilde tanımlanmıştır.

⁵⁸⁵ Erdoğan, 2013: 199.

⁵⁸⁶ Apaydın, 2015: 25.

⁵⁸⁷ “... Sanıkların okul ders notlarını ve devamsızlık durumlarını değiştirmek için bilişim sisteminin Millî Eğitim Bakanlığına bağlı okullarda kullanılan e-okul bilişim sistemi şifreleri ele geçirmek suretiyle yükletilen suçu işledikleri kabul edilmesi nedeniyle hükmolunan cezasının sitenin kamu kurumuna ait olması nedeniyle TCK’nin 244/3. maddesi gereğince cezaların arttırılması gerektiği gözetilmeden yazılı şekilde hükümler kurulması...” Yargıtay, 8. CD. 2016/3794 E. 2017/1405 K. 15.02.2017 T.

Suçun kamu kurum ve kuruluşlarına ait bilişim sistemleri üzerinde işlenmesi nitelikli hal olarak kabul edilmişken, kamu görevlisinin işlemesine yönelik bir nitelikli hale yer verilmemiştir. Öğretide kamu görevlisi ya da banka veya kredi kurumu görevlisinin suçu işlemesi halinde de ağırlaştırıcı neden yapılması gerektiği söylenmektedir⁵⁸⁸. Bilişim sistemlerinin güvenilirliğini daha ağır şekilde etkilemesi ve karşılaştırmalı hukukta da genellikle ağırlaştırıcı neden olarak düzenlenmesi nedeniyle bu öneriye katılmaktayız.

3.4.2 Eylemin İşlenmesi Suretiyle Kişinin Kendisinin veya Başkasının Yararına Haksız Çıkar Sağlaması (m. 244/4)

TCK m. 244/4'te “Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamanın başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.” denilmektedir.

Fıkra metninde “başka bir suç oluşturmaması” ifadesinin yer almasıyla, öğretide düzenlemenin bir tali norm olduğu kabul edilmektedir. Buna göre asli – tali norm ilişkisi çerçevesinde tali norm sonra uygulanacaktır. Ancak bu durum hükmün özel norm olma özelliği ile çelişmektedir⁵⁸⁹. Diğer yandan madde metninde başka bir suç oluşturmamasının belirtilmesine karşın, gerekçede daha ağır bir cezayı gerektiren başka bir suç oluşturmamasından bahsedilmesi ayrı bir çelişkidir. Gerekçe ile hükmün çelişmesi karşısında gerekçenin bağlayıcı olması nedeniyle gerekçeye itibar edilmemeli, cezanın daha ağır veya hafif olmasına bakılmaksızın eylemin başka bir suç oluşturmaması halinde TCK m. 244/4 uygulanmamalıdır⁵⁹⁰.

3.4.2.1 TCK m. 244/4'ün Nitelikli Hal Olarak Kabul Edilip Edilemeyeceği Sorunu

Öğretide TCK m. 244 kapsamında en tartışmalı konulardan biri, 244/4 hükmünün ayrı bir suç tipi mi teşkil ettiği yoksa nitelikli hal mi oluşturduğu yönündedir. Bir görüşe göre TCK m. 244/4 bağımsız bir suç tipi teşkil etmektedir⁵⁹¹. Bu görüşün savunucularına göre hükümde “başka bir suç oluşturmaması” ibaresinin bulunması yasa koyucunun bağımsız bir suç yaratmak istediğinin kabulünü gerektirir. Yoksa yasa koyucunun bir ağırlaştırıcı nedenle bir suçu karşılaştırması ve birini diğerine tercih etmesi kabul edilemez⁵⁹². Yine, hüküm nitelikli hal olarak kabul edilirse, çıkarın elde edilememesi halinde teşebbüs hükümlerinin de tatbik

⁵⁸⁸ Erdoğan, 2013: 197; Dülger, 2015: 434; Apaydın, 2015: 26.

⁵⁸⁹ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 942.

⁵⁹⁰ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 942.

⁵⁹¹ Tezcan/Erdem/Önok, 2016: 957; Artuk/Gökçen/Yenidünya, 2010: 728.

⁵⁹² Erdoğan, 2013: 247.

edilemeyeceği söylenmektedir⁵⁹³. Ayrıca, yasa koyucunun abesle iştigal etmeyeceği, suçun tüm unsurlarına yer verildiği ve artırım oranı belirlenmesi yerine doğrudan ceza belirlenmiş olması da bu görüşün savunucularının kullandığı argümanlardır⁵⁹⁴.

TCK m. 244/4 hükmünün nitelikli hal olarak değerlendirilmesi gerektiğini savunan diğer görüşe göre, suçun nitelikli hali düzenlenirken temel suç tipine bağlılık devam etmektedir. “Yukarıda tanımlanan fiillerin işlenmesi suretiyle” denilmiş olması da suç tipine bağlılığın devam ettiğinin göstergesidir⁵⁹⁵.

Bu sorunun çözümü ile ilgili olarak madde gerekçesi incelendiğinde birinci ve ikinci fıkralar için “suç olarak tanımlanmıştır”, dördüncü fıkra için ise “ceza yaptırımına altına alınmıştır” ifadelerinin bulunduğu görülmektedir. Dördüncü fıkra için gerekçede suç olarak tanımlanma veya netice sebebiyle ağırlaştırıcı neden olarak bahsedilmemiş olması, gerekçenin bu sorunun çözümünde yardımcı olmayacağı anlamına gelmektedir. Benzer şekilde Yargıtay kararlarında da ilk üç fıkradaki hallerin gerçekleşmemesi halinde dördüncü fıkranın uygulanamayacağından bahsedilmekte, ancak bunun nitelikli hal mi yoksa suçun maddi unsurunun gerçekleşmemesi nedeniyle mi olduğu açıklanmamaktadır⁵⁹⁶.

Biz, TCK m. 244/4 hükmünün nitelikli hal oluşturduğunu kabul etmekle, bunu birbirini tamamlayan üç nedene dayandırmaktayız.

İlk olarak yasa koyucunun amacının ağırlaştırıcı neden olduğunu düşünmekteyiz. Üçüncü fıkrada nitelikli hale yer vermiş yasa koyucunun dördüncü fıkrada yeniden bağımsız bir suç ihdas etmek istemesi kanun yapma tekniğine uygun düşmemektedir. Kaldı ki söz konusu fıkralar gerek hükümet tasarısında gerek adalet komisyonu metninde istikrarlı şekilde aynı sırayla yer almıştır.

İkinci olarak, ceza normu lafzi olarak yorumlandığında da hükmün nitelikli hal oluşturduğu görülmektedir. TCK’de genel düzenlenme biçimi olarak “...(bir eylemi)...(yapan/gerçekleştiren) kişi, ... ile cezalandırılır” kalıbı uygulanmaktadır. TCK 244/4 ise bu kalıp değil, genellikle nitelikli hallerde görülen “... cezasına hükmolunur” ibaresi yer almaktadır. Bu nedenle karşıt görüş taraftarlarınca ileri sürülen suçun tüm unsurlarına yer verildiği görüşüne de katılmamaktayız.

Üçüncü neden teşebbüs haline dayanmaktadır. 244/4 hükmünün bağımsız bir suç oluşturduğu kabul edildiği takdirde, ilgili suça teşebbüs de mümkün olacaktır. Bu da hakkaniyet-

⁵⁹³ Erdoğan, 2013: 244.

⁵⁹⁴ Erdoğan, 2013: 247.

⁵⁹⁵ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 941; Esen, 2007: 636.

⁵⁹⁶ “... Katılan şirketin sistemine hukuka aykırı olarak girerek, sistemin işleyişini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme şeklindeki TCK’nin 244/1-3. madde ve fıkralarında yazılı hallerin gerçekleşmemesi nedeniyle, anılan maddenin 4. fıkrasının uygulanamayacağı...” Yargıtay, 8. CD. 2016/104 E. 2016/7753 K. 13.06.2016 T.

siz sonuçlar doğuracaktır. Örneğin, üst sınırdan ceza verilmesi gereken bir olayda bilişim sisteminin işleyişini bozan kişiye 5 yıl ceza verilmesi gerekirken, aynı kişi aynı eylemlerle haksız çıkar da elde etmeye çalışmışsa 6 yıl olan ceza teşebbüs indirimiyle⁵⁹⁷ 3 yıla düşecektir. Böylece daha ağır olan netice hakkında daha hafif bir cezaya hükmedilmiş olmaktadır. Bu da düzenlemenin nitelikli hal amacıyla getirildiğini ortaya koymakta, suçun temel halinin 244/1 ve 2. fıkralarda düzenlendiğini göstermektedir.

Bu açıklamalarımız dışında ilgili hükmün bağımsız bir suç olduğu görüşünü savunan yazarların sunduğu bazı argümanların da geçerli olmadığını düşünmekteyiz. Örneğin ceza kanunumuzda nitelikli hal olarak artırımların tamamı oransal olarak belirlenmemiştir, TCK 87/2, 94/2-3, 96/2, 142/1-2 ve 149/1 maddelerinde oransal olarak değil, alt ve üst sınırlı ceza artırımı veya indirimi öngörülmektedir⁵⁹⁸. Bu durumda cezanın alt ve üst sınırının tayin edilmiş olması tek başına hükmün bağımsız bir suç olduğunu ispatlamamaktadır.

TCK 244/4 hükmünün nitelikli hal olarak kabulü bazı önemli sonuçlar da doğurmaktadır. Buna göre temel suç tipi oluşmadığı takdirde (244/1 veya 2) nitelikli halin de uygulanması mümkün değildir. Ayrıca nitelikli hale teşebbüsten de söz edilemeyecek, neticenin oluşmadığı halde yalnızca suçun basit şeklinden ceza verilebilecektir⁵⁹⁹.

Öğretide bir görüş TCK 244/3 fıkrasının, 244/4'e uygulanmayacağını ifade etmektedir⁶⁰⁰. Bu görüş, m. 244/4 metninde yer alan “yukarıda fıkralarda tanımlanan fiillerin işlenmesi suretiyle” ifadesi ve üst sırada yer alan 244/3 fıkrasına ayrıca bir atıf bulunmamasını gerekçe olarak göstermektedir⁶⁰¹. Diğer görüş ise TCK 244/3 ve 4. fıkralarının ayrı ayrı uygulanabileceği yönündedir. Biz, 244/4 düzenlemesinin nitelikli hali oluşturması ve 3. ve 4. fıkraların ikisinde de ilk iki fıkroda belirtilen eylemlere atıf yapılması karşısında ilk görüşe ait gerekçe-ye itibar etmemekte, artırım nedenlerinin somut olaya göre ayrı ayrı veya birlikte uygulanabileceği düşüncesindeyiz.

3.4.2.2 TCK m. 244/4 Kapsamında Haksız Çıkarın Kapsamı ve Niteliği Sorunu

Öğretide TCK m. 244/4 kapsamında tartışılan diğer konu ise elde edilen haksız çıkarın niteliğidir. Buna ilişkin bir görüş, haksız çıkardan bahsedilenin yalnızca maddi yararlar oldu-

⁵⁹⁷ Teşebbüs halinde dörtte birden dörtte üçüne kadar olan indirim oranının ortalama olarak yarısı suretiyle uygulanması halinde.

⁵⁹⁸ Artuk/Gökçen/Yenidünya, 2016: 894.

⁵⁹⁹ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 941.

⁶⁰⁰ Artuk/Gökçen/Yenidünya, 2010: 731.

⁶⁰¹ Erdoğan, 2013: 256.

ğunu⁶⁰², diğer görüş ise hukuken tasvip edilmeyen her türlü çıkarın kapsama dahil olduğunu ifade etmektedir⁶⁰³.

Bu tartışmaya ilişkin SOİSS’e bakmakta yarar vardır. TCK m. 244/4 hükmü, SOİSS’in 8. maddesinin karşılığını oluşturmaktadır. İlgili maddede “haksız yere maddi menfaat” sağlamanın cezalandırılması gerektiği belirtilmiş, ibare TCK’de “haksız bir çıkar” olarak yer almıştır. Bu durum, çıkar kavramının geniş yorumlanmasını savunan tarafça, madde metninde kısıtlamaya yer verilmediği için maddi – manevi her türlü çıkarın bu hüküm uyarınca değerlendirileceği şeklinde açıklanmaktadır⁶⁰⁴.

Mevzuatta daha önce de haksız çıkar kavramının kullanıldığı düzenlemelerin bulunduğu görülmektedir. Mülga 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu’nun 1. maddesinde, içinde “kendilerine veya başkalarına haksız çıkar sağlamak amacı” dahil olmak üzere birçok eylem sayılmaktadır⁶⁰⁵. Bu kanunla getirilen amacın belli ekonomik menfaatlere elde edilmesi için uygulanan yöntemlerle mücadele olduğu yasa koyucu tarafından da belirtilmiştir⁶⁰⁶.

Bize göre çıkar kapsamının belirlenmesi pratik öneme sahip bulunmaktadır. Kapsam çok daraltılırsa, bilişim suçları aracılığı ile hırsızlık ve dolandırıcılık suçları ayrıca düzenlenmiş bulunduğundan m.244/4 uygulama alanı bulamayabilecek, kapsamın çok geniş tutulması halinde ise suçun temel şeklinden ceza verilme ihtimali oldukça zorlaşacaktır. TCK m. 244/4’te maddi ve manevi özelliklerine değinmeksizin yalnızca çıkardan bahsedilmiş olması, kanunun bir ara çözüm getirdiği, kapsamı çok dar veya geniş tutmak istemediği şeklinde yorumlanabilir.

TCK m. 244/4 düzenlemesinin, ekonomik suçlarla bilişim suçları arasındaki köprü görevini görmesi, SOİSS’in ve iç hukuktaki haksız çıkara ilişkin önceki düzenlemelerin “parasal bir karşılığı olan” ihlalleri konu etmiş olduğu düşünüldüğünde, biz çıkar kapsamının manevi çıkarları da kapsadığı görüşüne katılmıyoruz. Buna göre sadece bilişim korsanları arasında popülarite kazanmak amacıyla bu eylemin gerçekleştirilmiş olması TCK m. 244/4 kapsamında değil, eylemin niteliğine göre 244/1 veya 2 kapsamında değerlendirilmelidir. Bu-

⁶⁰² Tezcan/Erdem/Önok, 2016: 957.

⁶⁰³ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 942; Kurt, 2005: 175.

⁶⁰⁴ Erdoğan, 2013: 250.

⁶⁰⁵ 4422 sayılı kanun m. 1: “Doğrudan veya dolaylı biçimde bir kurumun, kuruluşun veya teşebbüsün yönetim ve denetimini ele geçirmek, kamu hizmetlerinde, basın ve yayın kuruluşları üzerinde, ihale, imtiyaz ve ruhsat işlemlerinde nüfuz ve denetim elde etmek, ekonomik faaliyetlerde kartel ve tröst yaratmak, madde ve eşyanın azaltılmasını ve darlığını, fiyatların düşmesini veya artmasını temin etmek, kendilerine veya başkalarına haksız çıkar sağlamak, seçimlerde oy elde etmek veya seçimleri engellemek maksadıyla tehdit, baskı, cebir veya şiddet uygulamak suretiyle yıldırma veya korkutma veya sindirme gücünü kullanarak suç işlemek için örgüt kuranlara ... ağır hapis cezası verilir.”

⁶⁰⁶ Dönemin Adalet Bakanı Hikmet Sami Türk’ün kanun hakkındaki konuşması, <http://www.yayin.adalet.gov.tr/adaletdergisi/03.sayi/1hikmet.pdf> (erişim tarihi: 28.12.2018).

nunla birlikte haksız çıkar kavramı yalnızca piyasada belli bir değeri olan ürünler üzerinden düşünülmemelidir. Örneğin, bir veritabanından toplu şekilde e-posta bilgilerinin para karşılığı satılmak üzere ele geçirilmesi halinde haksız çıkar şartının gerçekleştiği söylenmelidir.

Yargıtay m. 244/4'ün uygulamasında titiz davranmakta, haksız menfaatlerin ne olup kim tarafından sağlandığının açıklanıp tartışılmasını istemektedir⁶⁰⁷. Ayrıca dolaylı olarak uğranılan veya gecikmeden kaynaklanan zarar m. 244/4 kapsamında değerlendirilmemektedir. Bir kararda, hayali reçeteyle kamu kurumunun alacağının geciktirilmesinin alacağı tamamen ortadan kaldırmadığı, bu nedenle de haksız bir çıkar edilmediğinden m. 244/4'ün uygulanmayacağı kabul edilmiştir⁶⁰⁸.

3.4.3 Suçun Terör Örgütü Faaliyeti Çerçevesinde İşlenmesi

3713 sayılı Terörle Mücadele Kanunu'nda TCK m. 244'e atıf yapılmaktadır. Buna göre TMK'nin 4. maddesi uyarınca TCK m. 244 kapsamındaki suçların suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlenmesi halinde suç terör suçu sayılmaktadır ve aynı kanunun 5. maddesi uyarınca tayin edilecek hapis ve adli para cezası yarı oranında artırılarak uygulanacaktır. Bu artırma nedeniyle cezanın üst sınırının aşılabilmesi mümkündür.

3.5 Suçun Manevi Unsuru

Manevi unsur, öğretilerde işlenen eylem ile fail arasındaki psikolojik bağ olarak tanımlanmaktadır. Bu bağ kusurluluktan farklı bir olgu olduğundan, manevi unsur olmaksızın suçun varlığından da söz edilemeyecektir⁶⁰⁹. TCK m. 21 suçun oluşmasını kast unsurunun varlığına bağlamakta, m. 22 ise taksirle işlenen eylemlerin ancak kanunda belirtildiği hallerde cezalandırılabilirliğini hüküm altına almaktadır. Türk hukukunda kural olarak suçlarda bulun-

⁶⁰⁷ Yargıtay, 8. CD. 2016/3794 E. 2017/1405 K. 15.02.2017 T.

⁶⁰⁸ "... Sanık ...'nın ... Eczanesi sahibi, sanık ... ile ...'ün ise kalfa olarak çalıştıkları, Medula sistemini kullanmaya yetkili sanıklar ... ile ...'ün olay tarihlerinde kendi çalıştıkları ... Eczanesi'nin şifresi ve katılan ...'ya ait ... Eczanesi'nin haksız şekilde elde ettikleri Medula sistemine giriş şifresi ile önce hayali bir reçetenin eczanelerden birinin şifresiyle Medula Eczane sistemine giriş yapıldığı, hayali reçete Medula Eczane Sistemine kayıtlı iken bu kez diğer eczanenin sisteminden giriş yapılarak gerçek reçetenin sisteme kaydedildiği, hayali reçetenin sisteme kaydedilmesi ile hasta muayene ücretinin çıktığı, ancak hayali reçete sistemde kayıtlı bulunduğu halde diğer eczaneden gerçek reçetenin girişi yapıldığında muayene ücretinin çıkmadığı ve reçetenin karşılandığı, bu kez gerçek reçete karşılandıktan sonra hayali reçetenin sistemden silindiği ve hastaya ait muayene ücretinin bu işlemle bir sonraki ilaç alışıma kadar ötelenerek bilişim sistemindeki verileri bozma, yok etme, sisteme veri yerleştirme suçunu işlediklerinden bahisle açılan davada; sanıkların sübut bulan eylemlerinde, dosya kapsamından yapılan işlemlerin katılan kurumun alacağını geciktirmekten ibaret olduğu, ortadan kaldırmadığı, bu surette bir haksız menfaat elde edilmediğinin anlaşılması karşısında, katılan ...'ya ait eczanenin şifresini haksız ele geçirip bunun vasıtasıyla ...'na ait bilişim sistemine giriş yapıp sahte veri yerleştirip amacına ulaştıktan sonra silmek şeklindeki eylemin TCK'nun 244/2 ve 3. maddelerindeki suç kapsamında değerlendirilmesi gerektiği gözetilmeden anılan maddenin 4. fıkrasıyla hüküm kurulması..." Yargıtay, 8. CD. 2016/12437 E. 2017/6369 K. 31.05.2017 T.

⁶⁰⁹ Artuk/Gökçen/Yenidünya, 2016: 293.

ması gereken genel kast bilme ve isteme unsurlarının gerçekleşmesini ararken, bazı hallerde failin belli bir saikle hareket etmesi de aranmakta, bu halde özel kastın varlığından söz edilmektedir.

TCK m. 244 incelendiğinde suçun taksirli şekline yer verilmemiştir. Bu nedenle suçun taksirle işlenmesi halinde failin cezalandırılması mümkün olmayacaktır. Benzer şekilde kanun suçun işlenmesi için bir saik de aramadığından, m. 244'ün genel kastla işlenebilen bir suç olduğu söylenebilecektir. Yine, doğrudan kasta işaret eden bir ibare bulunmadığından suçun olası kastla gerçekleşmesi mümkün bulunmaktadır⁶¹⁰.

TCK m. 244/4'te yer alan düzenleme ise öğretide tartışmalıdır. Bir görüş bu unsurları genel kast kapsamında kabul etmektedir⁶¹¹. Diğer görüş ise haksız çıkar elde etme unsurunu saik olarak değerlendirmekte ve özel kast aramaktadır⁶¹². Bize göre, hukuka aykırılık unsuruyla yapılan açıklamalara paralel şekilde haksız çıkar elde etme kastın unsurlarına dahil olmakla birlikte bu suç genel kastla işlenebilen bir suçtur.

Öğretide suçun manevi unsuru ile ilgili diğer unsurlara oranla pek tartışma olmamakla birlikte bazı önerilerin bulunduğu görülmektedir. Bunlardan ilki, suçun taksirle işlenmesi halinde en azından şikâyeteye bağlı olacak şekilde cezalandırılması için düzenleme yapılmasıdır⁶¹³. Bir diğer öneri ise suçun özel kast ile işlenmesinin daha doğru olacağı yönündedir⁶¹⁴. Bu görüşlerin ikisine de katılmamaktayız. İlk olarak, gerek bilişim sistemi unsurları gerekse TCK m. 244 uyarınca yapılan açıklamalar doğrultusunda suçun geniş bir yelpazede düzenlendiğini ve haksız cezaların ortaya çıkacağını düşünmemektediriz. Diğer yönden bilişim suçlarında özel kastın ispat zorluğunun da göz ardı edilmemesi gerekmektedir. Diğer yönden bilişim suçlarının taksirli halinin ceza değil tazminat yaptırımını altında düzenlenmiş olmasını da uygun bulmaktayız. Nitekim bilişim sistemlerinin tamiri için teslim edilen kişilerin taksiri sonucu verilere zarar verilmesi halinde, özellikle suçun şikâyeteye bağlı olması halinde, uygulamada ceza yaptırımını baskısı altında artırılmış tazminat sorumluluğu gündeme gelecektir. Bu yaptırımların da uzun vadede toplumun bilişim alanına çekingen ve mesafeli davranması sonucunu doğuracağını düşünmekteyiz.

⁶¹⁰ Erdoğan, 2013: 200; Dülger, 2015: 435.

⁶¹¹ Tezcan/Erdem/Önok, 2016: 957; Artuk/Gökçen/Yenidünya, 2010: 730; Erdoğan, 2013: 258; Gürler, 2015: 157. Daha önce özel kast görüşünde olmakla, sonradan görüş değiştirerek genel kast görüşünü savunan, Dülger, 2015: 450.

⁶¹² Kurt, 2005: 175; Karagülmez, 2014: 240; Taşkın, 2008: 52. Özel kast olarak açıkça bahsetmemekle birlikte, "TCK 244/4 fıkra failde, genel kastın yanında kendisine veya başkasına haksız bir çıkar sağlama kastı da bulunmalıdır." Yılmaz, 2016: 200.

⁶¹³ Erdoğan, 2013: 230.

⁶¹⁴ Bilişim sistemine hukuka aykırı veri sokulmasının geniş bir yelpazede söz konusu olması ve istenmeyen mail veya reklam gibi nedenlerle kişilerin sorumlu olabileceği gerekçe olarak gösterilmektedir. Doğan, 2005: 305.

3.6 Hukuka Aykırılık Unsuru

Eylemin tipe uygun olması, tek başına suçun gerçekleştiğini göstermemektedir. Bu eyleme aynı zamanda hukuk düzenince cevaz verilmemesi gerekmektedir. Ceza Kanunu veya başka kanunlarda eylemin hukuka aykırı olmasını önleyen kurallara hukuka uygunluk sebepleri denilmektedir. Tipe uygunluk eylemin hukuka aykırı olduğu yönünde karine teşkil ettiğinden eylemin hukuka aykırı olduğu değil, hukuka uygunluk nedenlerinin olup olmadığı araştırılmalıdır. Hukuka aykırılık unsurunun araştırılması için kanunda açıkça yazmasına gerek yoktur, ancak bazı suç tiplerinde “hukuka aykırı olarak” gibi ifadelere de yer verilmiştir. Bu hallerde hukuka aykırılık tipikliğe ait bir unsur özelliği kazanmakta ve failin hukuka aykırılık yönünden de doğrudan kastla hareket etmesi gerekmektedir. Hukuka uygunluk nedenleri, eylemi baştan itibaren hukuka uygun hale getirip, kamu davası açılmamasını veya açılmışsa beraat kararı verilmesini gerektirmektedir. Hukuka uygunluk nedenleri toplumsal hayat ile iç içe olduğu için, sosyal değerlerin değişmesi sonucu yeni hukuka uygunluk nedenleri ortaya çıkabilir, bu nedenle tüm hukuka uygunluk nedenlerinin önceden tespit edilmesi mümkün değildir⁶¹⁵. TCK’de hukuka uygunluk nedenleri, kanunun hükmü, meşru savunma, hakkın kullanılması ve ilgilinin rızası olmak üzere dört başlıkta düzenlenmiştir⁶¹⁶.

TCK m. 244 kapsamında hukuka uygunluk nedeni olarak kanunun hükmü düşünülebilir. Öğretide yasadışı örgütlerin propaganda amacıyla kullandığı internet siteleri ile mücadele kapsamında görevlendirilen personelin imha faaliyetlerinin kanunda açık hüküm bulunması karşılığında suç olarak kabul edilmemesi gerektiği söylenmektedir⁶¹⁷. Bu görüşe, 5651 sayılı kanunda yöntemin gösterildiği, herhangi bir kurum ya da kişiye özel görev verilmediği nedenleriyle karşı çıkılmaktadır⁶¹⁸. Bizim de katıldığımız görüşe göre, 5651 sayılı kanunda biri koruma tedbiri diğeri idari yaptırım olarak iki farklı erişimin engellenmesi eylemi bulunmaktadır. Bu yöntemler ayrıca tartışmaya açık olsa da hukuka uygunluk nedeni oluşturduğunun kabulü gerekmektedir⁶¹⁹.

CMK m. 134 ve 135 başta olmak üzere Türk hukukunda uygulanan bazı kontrol tedbirleri de tip olarak TCK m. 244’te yer alan tanıma uymaktadır. Bu tedbirlerde gerçekleşen eylemler yasal koşullara uygun olduğu müddetçe hukuka uygunluk sebebi oluşturacaktır⁶²⁰. Bu noktada sistemin işleyişinin engellenmesi veya verilerin incelemeye uygun şekilde çoğal-

⁶¹⁵ Artuk/Gökçen/Yenidünya, 2015: 374 – 380.

⁶¹⁶ Özbek, 2006: 151.

⁶¹⁷ Erdoğan, 2013: 201.

⁶¹⁸ Dülger, 2015: 436.

⁶¹⁹ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 946. Aynı yönde, Tezcan/Erdem/Önok, 2016: 957.

⁶²⁰ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 947; Dülger, 2015: 436. Kurt da 4422 sayılı kanun döneminde çıkar amaçlı suç örgütleri hakkındaki soruşturmalarda kanuna uygun olarak yapılan eylemleri örnek vermektedir. Kurt, 2005: 174.

tilması veya değiştirilmesi hukuka uygunluk sebebi oluştursa da verilerin bozulması, yok edilmesi veya yerleştirilmesi halinde kanunun hükmü aşılabacağından hukuka uygunluk nedeninden bahsedilmesi mümkün olmayacaktır⁶²¹.

Bilişim sistemlerine yönelik saldırı karşısında meşru savunmanın mümkün olup olmadığı, öğretide saldırının niteliğine bakılarak karar verilmesi şeklinde açıklanmaktadır. Bir görüş, bu suç tipi bakımından meşru savunmanın mümkün olmadığını söylemekte ise de⁶²² bize göre teoride meşru savunma şartlarının oluşması mümkündür⁶²³. Saldırının ağırlığı ve bunun hangi yöntemlerle engellenebileceği önem taşımaktadır. Karşı sisteme zarar vermeksizin yalnızca savunma gereçleriyle saldırının bertaraf edilmesi mümkünse, bu halde meşru savunmadan söz edilemeyecektir. Bununla birlikte sisteme fiilen temasta bulunulmakta ise, diğer şartların varlığı halinde meşru savunmanın oluşacağı kabul edilmektedir⁶²⁴. Meşru savunmanın belirlenmesi sırasında tarafların teknik bilgi ve becerilerinin de göz önüne alınması eylemler arasındaki orantının belirlenmesinde faydalı olacaktır. Dünyaca ünlü bilişim şirketlerine gerçekleşecek bir saldırının önlenmesinde, yerel bir firmaya yönelecek aynı saldırıya oranla eylemlerin daha orantılı olmasının beklenmesi doğal olacaktır.

Öğretide ayrıca, kişilerin kendileri hakkında hakaret veya suçlayıcı içerik bulunduran internet sitelerine karşı verileri bozma veya değiştirme eylemleri halinde meşru savunma halinin gerçekleştiği ve suçun oluşmadığı yönünde görüş bulunmaktadır⁶²⁵. Bu görüşe, 5651 sayılı kanun ile müdahale imkanının bulunması, içeriklerin niteliğinin kişiden kişiye değişmesi ve meşru savunmanın diğer unsurlarının da gerçekleşmemesi nedeniyle katılmamaktayız⁶²⁶.

Bu suç tipinde muhtemelen en çok karşılaşılan hukuka uygunluk nedeni ise hak sahibi kişinin rızasıdır. Bu rızanın açık veya zımni şekilde verilmesi mümkün olmakla birlikte, rıza eylem öncesinde elde edilmiş olmalıdır⁶²⁷. Buna göre bilişim sistemlerinin onarım veya geliştirilmesi kapsamında teslim edilmesi üzerine sistem üzerine yapılan faaliyetler suç teşkil etmemektedir. Elbette, bu tür tamirat durumlarında rızanın sınırları aşıldığı takdirde suç oluşacağından rızanın kapsamının tespit edilmesi önem göstermektedir⁶²⁸. Bununla birlikte, uygulamada bilgisayarların zararlı yazılımlardan temizlenmek üzere teslim edildiğinde, çoğu za-

⁶²¹ Aynı yönde, Kurt, 2005: 174.

⁶²² Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 947.

⁶²³ Aynı yönde, “Örneğin, saldırıdan zarar görenin bazı saldırı programları kullanarak karşı tarafı rahatsız etmek ve saldırıları önlemek amacıyla yapacağı sisteme girme (engelleme) eylemi örnek olarak gösterilebilir.” Taşkın, 2008: 51.

⁶²⁴ Erdoğan, 2013: 201.

⁶²⁵ Öngören’den aktaran, Erdoğan, 2013: 231.

⁶²⁶ Aynı yönde, Erdoğan, 2013: 231.

⁶²⁷ “Suç şikâyetine bağlı olmadığından, mağdurun rızası eylem öncesinde elde edilmiş olmalıdır. Eylem sonrası onaylama, şikâyetçi olmama oluşan suçu ortadan kaldırmaz ve oluşan suçun soruşturması ve kovuşturmasını engellemez.” Erdoğan, 2013: 201.

⁶²⁸ Dülger, 2015: 435; Yılmaz, 2016: 199.

man kısmen müdahale ile diğer verilerin kurtarılabilir olmasına karşın, işletim sisteminin bütünüyle yenilendiği (format atıldığı) görülmektedir. Bu tür teknik bilgi veya donanım eksikliği ya da sadece daha az emek sarf etmek için format atılarak kolay yoldan tüm verilerin yok edilmesi halinde rızanın kapsamı ve failin kastı incelenmelidir. Eğer mağdur, bazı verilerin önemli olduğunu ve kesinlikle saklanması gerektiğini, aksi halde sistemin onarılmadan olduğu şekilde bırakılmasını belirtmiş ise, format atma eyleminin diğer unsurların da varlığı halinde suçu oluşturduğu söylenebilecektir.

İnternet kafe vb. bilişim sistemlerinin kullanım haklarının devredildiği yerlerde, sistemin kasten zarara uğratılmasında da rızanın sınırları aşılmış olduğundan hukuka uygunluk nedeninden bahsedilemeyecektir⁶²⁹.

Lisanslı programların süresinin sona ermesi veya ücretinin ödenmemesi sonucunda erişimin engellenmesi veya verilerin yok edilmesi de öğretide hukuka uygunluk nedeni yönünden tartışılmıştır. Bir görüş, bu tür hallerde kanunda yapılacak düzenleme ile suçun temel haline göre indirim yapılması gerektiğini belirtmektedir. Hırsızlık, dolandırıcılık veya yağma suçlarında kişinin hukuksal alacağını tahsil etmek amacıyla hareket etmesinin indirim nedeni olarak düzenlenmesine karşın, bilişim suçlarında bu hükmün yer almamış olması eksiklik olarak görülmektedir⁶³⁰. Bu noktada tarafların arasındaki sözleşmeye uygun olmak kaydıyla, diğer tarafın edimini yerine getirmemesi nedeniyle sistem veya veriler üzerindeki eylemin suç oluşturmayacağını düşünmekteyiz. Ancak bu eylemler lisanslı programın işleyişine yönelik olmalıdır. Yani kullanıcının programa girişi veya programdan istifade ederek veri üretmesinin engellenmesi mümkündür. Buna karşın kullanıcının halihazırda ürettiği verilerin zarar görmesi halinde hukuka uygunluk nedeninin bulunmadığı gözetilmelidir. Nitekim bu veriler, programdan bağımsız olarak kullanıcıya aittir ve kullanıcı belki de lisansını yenileyerek bu veriler üzerinde yeniden işlem yapmak isteyebilecektir. Böyle bir sözleşmenin hiç bulunmaması halinde ise haksızlık içeriğinin daha az olması nedeniyle cezadan indirim yapılması gerektiği yönündeki düşünceye katılmaktayız.

İlgilinin rızası kapsamında uç bir örnek olmak üzere bir bilgisayar oyunundan bahsedilmelidir. Lose/lose (kaybet/kaybet) isimli oyun, uzaylı yok etmeye dayanmaktadır. Normal oyunlardan farklı olarak ise, her bir uzaylı yok edildiğinde, bilgisayardan rastgele seçilen bir dosyayı kalıcı olarak silmektedir. Silinen dosya basit bir fotoğraf veya ikon olabileceği gibi işletim sistemine ilişkin kritik bir dosya da olabilir. Oyun kaybedildiğinde ise kendisini silmektedir. Taşıdığı büyük risklere karşın, oyun açılışı sırasında kullanıcılara gerekli bilgilendirme

⁶²⁹ Erdoğan, 2013: 231; Dülger, 2015: 435.

⁶³⁰ Kurt, 2005: 174 – 175; Taşkın, 2008: 51.

dirmeyi ve uyarıları yapmaktadır⁶³¹. Hangi verilere zarar verileceği önceden bilinmemesine karşın, duruma ilişkin açık uyarı yapılması karşısında, dosyaların silinmesi hatta sistemin çalışamaz hale gelmesi durumunda hukuka uygunluk nedeni bulunduğundan, failin bu eylemlerden dolayı cezalandırılması mümkün olmayacaktır.

Son olarak, hukuka uygunluk nedenlerindeki genel açıklamalarımıza uygun şekilde TCK m. 244/4 hükmünde “haksız” çıkardan bahsedilmesi sonucunda, hukuka aykırılığın artık tipikliğe ait bir unsur haline geldiği ve failin kastının haksızlık unsurunu da kapsamı gerektiği ifade edilmelidir.

3.7 Suçun Özel Görünüş Biçimleri

3.7.1 Teşebbüs (Kalkışma)

Suçun teşebbüse elverişli olması yönünde öğretide fikir ayrılığı bulunmamaktadır⁶³². Gerek m. 244/1 uyarınca sistemin engellenmesi veya bozulması suçunda gerek m. 244/2 uyarınca verilerin bozulması suçunda hareket netice ile bitişik olmadığından suça teşebbüsten söz edilebilecektir.

Suç seçimlik hareketlerle gerçekleştiği için hareketlerden herhangi biri sonucunda neticenin gerçekleşmesi halinde suç tamamlanmış sayılacaktır⁶³³. Örneğin bir sistemdeki verileri kendi bilgisayarına kopyaladıktan sonra herhangi bir nedenle hedef sistemdeki veriyi yok etmeyi başaramayan fail hakkında sırf bu nedenle suçun teşebbüs aşamasında kaldığından bahsedilemez.

Bu suçta netice failin eylemlerinin etkisi altında kalan mağdur veya bir başka kişinin hareketleri neticesinde de gerçekleşmemiş olabilir. Örneğin, sistemleri kapatarak farkındalık oluşturmayı amaçlayan failin, hedef sistemlere zararlı yazılımlar (mantık bombası) yükleyerek, onları belirlenen günde bilgisayarlarını kapatmamaları durumunda sistemdeki verileri yok edeceğini söyleyen bir uyarı vermesi bu kapsamda düşünülebilir. Burada neticenin gerçekleşmemesi, kullanıcının bilgisayarını kapatması sonucunda mantık bombasının eylemde bulunmamasına bağlıdır. Bu şekilde kullanıcıların iradeleri veya irade dışı eylemleriyle neticenin gerçekleşmediği hallerde de failin teşebbüs sorumluluğundan söz edilmelidir.

Teşebbüsün mümkün olması dolayısıyla suçtan gönüllü vazgeçme de mümkündür. Bu noktada failin icra hareketlerine başladıktan sonra güç kaynağının kesilmesi gibi elinde olmayan nedenlerden dolayı neticenin oluşmadığı durumlarda fail teşebbüs hükümleri uyarınca

⁶³¹ <http://malware.wikia.com/wiki/Lose/Lose> (erişim tarihi: 29.12.2018).

⁶³² Bununla birlikte, 765 sayılı TCK’de yer alan bazı bilişim suçları yönünden tam teşebbüsün mümkün olmadığı, eksik teşebbüsün ise hareketin parçalara bölünebildiği hallerde mümkün olabileceği görüşleri bulunmaktaydı. Yazıcıoğlu, 1997: 264; Ersoy, 1999: 177; Yenidünya/Değirmenci, 2003: 78.

⁶³³ Erdoğan, 2013: 232.

sorumlu tutulacaktır. Ancak icra hareketlerine başlayan fail, kendi iradesiyle eylemini sonlandırırsa gönüllü vazgeçme hükümleri uygulanacaktır. Yine de tüm bu ihtimallerde TCK 243. madde uyarınca sisteme yetkisiz giriş suçu tamamlandığı için fail bu suçtan dolayı sorumlu tutulacaktır⁶³⁴.

Failin verileri değiştirdikten sonra vazgeçerek eski hale getirmesi halinde gönüllü vazgeçme hükümlerinin uygulanıp uygulanmayacağı konusunda farklı görüşler mevcuttur. Bir görüşe göre bu konuda failin cezalandırılmayacağı öne sürülmektedir⁶³⁵. Bizim de katıldığımız diğer bir görüş ise bu durumda artık eylem tamamlanmıştır ve gönüllü vazgeçme değil, etkin pişmanlık hükümleri uygulanabilir. Etkin pişmanlık halinin uygulanması için kanunda hüküm bulunması gerektiğinden ve TCK m. 244'e ilişkin bir etkin pişmanlık hali öngörülmediğinden faile tam ceza verilmelidir⁶³⁶.

Gönüllü vazgeçme ile ilgili olarak log kayıtlarından da bahsedilmelidir. Bilişim korsanı, sisteme girip istediği eylemi gerçekleştirdikten sonra kendisini veya yaptığı işi gizlemek amacıyla log kayıtlarını silmektedir. Bu noktada, yapmış olduğu iş sırasında gönüllü olarak vazgeçen failin, sistemi bulduğu gibi bırakmak amacıyla yarım bıraktığı işlemlerini kaydeden log kayıtlarını silmesinin gönüllü vazgeçme kapsamında tartışılması gerekir. Çünkü bir yandan sistem, bilişim korsanının yaptığı tüm eylemler olmamış gibi eski haline döndürülmekte, diğer yandan bu eylemler nedeniyle üretilmiş verilen yok edilmesi meydana gelmektedir. Her ne kadar failin kendi eylemleri nedeniyle oluşan verileri yok ederek gönüllü vazgeçme kurumunun niteliğine uygun davrandığı söylenebilecekse de, log kayıtlarının oluşturulmasının failin eyleminden çok bilişim sisteminin bir özelliği olması nedeniyle bu verilerin silinmesinin TCK m. 244'teki suçu oluşturduğunu düşünmekteyiz. Gönüllü olarak vazgeçen bilişim korsanı, eylemlerini derhal kesmeli ve herhangi bir düzeltme eylemine girişmemelidir. Zaten log kayıtları incelendiğinde yapmış olduğu eylemler ve neticesi ortaya çıkacağından fail gönüllü vazgeçme hükümleri uyarınca cezalandırılmayacaktır.

Teşebbüs konusunda hangi eylemlerin hazırlık aşamasında, hangi eylemlerin ise icra aşamasında kaldığının ayırt edilmesi de önem taşımaktadır. Bilindiği gibi Türk hukukunda hazırlık ve icra hareketleri ayrılmakta, fail hazırlık hareketlerinden dolayı teşebbüsten sorumlu tutulmamaktadır⁶³⁷. Yukarıda bilişim suçlarının aşamalarından aktif ve pasif bilgi toplama eylemlerinin hazırlık aşaması olduğu ve teşebbüs sorumluluğu doğurmayacağı düşüncesindeyiz. Benzer şekilde kötü amaçlı yazılım üretilmesi de tek başına teşebbüs sorumluluğu gerek-

⁶³⁴ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 948; Erdoğan, 2013: 202.

⁶³⁵ Kurt, 2005: 265-266.

⁶³⁶ Erdoğan, 2013: 234.

⁶³⁷ Artuk/Gökçen/Yenidünya, 2015: 594.

tirmemektedir⁶³⁸. Çünkü bu eylemler başka türlü anlaşılamayacak şekilde bilişim suçuna yönelik bir hareketin varlığına işaret etmemektedir. Sistem bilişim güvenliğinin iyiniyetli olarak test edilmesi veya bazı istatistiklerin toplanması gibi birçok başka amaç çerçevesinde de bu eylemlerin gerçekleşmesi mümkündür. İcra hareketlerinin dar anlamda düşünülmesi, bilişim teknolojilerinin hızlı gelişimini açısından da faydalı olacaktır.

3.7.2 İştirak

TCK m. 244'te düzenlenen suçlar iştirak yönünden özellik göstermemektedir. TCK'nin iştirake ilişkin m. 37 – 41 arasındaki genel hükümler, bu suç için de uygulanacaktır.

Günümüzde uygulamada sıkça görülen “zombi bilgisayarlar” suça iştirak yönünden değerlendirilmelidir. Çoğunlukla zararlı yazılımlar yoluyla ele geçirilen ve “sanal bilgisayar” olarak da ifade edilen bilişim sistemleri üzerinden bilişim suçlarının işlendiği görülmektedir. Bu sayede gerçek fail kendi bilişim sistemini gizleme imkânı yakalamakta, yapılan soruşturmalar sonucunda “zombi bilgisayar” sahiplerinin ceza mahkemelerinde yargılandıklarına sıkça rastlanmaktadır. Bu noktada bilişim korsanının zombi sistemin sahibi kişi ile olan bağlantısını, sistem sahibi kişi ile aralarında bir kullanım anlaşması olup olmadığını, var ise - Bilgisayarların açık tutulması ve dolayısıyla işlem gücünün kullanılması dolayısıyla belli bir ücret ödenmesi gibi durumlarda- bu kastın suç içerikli eylemi kapsayıp kapsamadığının araştırılması gerekecektir.

Öğretide suçun iştirak halinde işlenmesinin cezayı arttırıcı neden olarak kanuna eklenmesi önerilmektedir. Öneride, karşılaştırmalı hukukta benzeri düzenlemelerin olduğundan bahsedilmiş, Bulgaristan ve Belçika Ceza Kanunlarından örnekler verilmiştir⁶³⁹. Bu öneriye örgütlü suçlar ile iştirak hükümlerinin mevcut düzenlemelerinin yetersiz kaldığına dair bir bilgi bulunmaması ve bilişim suçlarının esasının toplu halde işlenmesinden çok bilgi ve bireyselliğe dayalı olması nedenleriyle katılmamaktayız.

3.7.3 İçtima

Ceza hukukunda kaç eylem varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır kuralı geçerlidir. Bu kurala yasa koyucu belli suçlar bakımından mağdur sayısı uyarınca istisna getirmiş olduğu gibi, suçların içtimaı durumunda da her suçtan ayrı ayrı ceza verilip toplanmasının önüne geçilmiştir. Suçların içtimaı bileşik suç, zincirleme suç, aynı veya farklı neviden fikri içtima olmak üzere değişik şekiller göstermektedir. Öğretide özel-genel ve asli-

⁶³⁸ Erdoğan, 2013: 234.

⁶³⁹ Karagülmez, 2014: 283 – 284.

tali norm ilişkileri görünüşte içtima olarak değerlendirilmekte ve içtimaa ilişkin hükümler uygulanmamaktadır⁶⁴⁰.

Bu açıklamalar ışığında TCK m. 244 kapsamında içtimanın tüm halleri mümkündür. Fail, aynı suç işleme kararını yerine getirmek için farklı zamanlarda aynı mağdura ait sistem veya veri üzerinde eylemlerden birini veya birkaçını gerçekleştirmesi halinde Yargıtay tarafından da isabetli olarak ifade edildiği üzere⁶⁴¹ zincirleme suç hükümlerinin uygulanması gerekecektir⁶⁴². Bu noktada DDOS gibi sistem kaynaklarını tüketme saldırılarının istek gönderme eylemlerinden oluştuğu düşünülerek, bu tür birbirinin tekrarı olan eylemler tek bir eylem olarak kabul edilmeli ve suçun temel şeklinden cezalandırılmalıdır. Ancak bu eylemler herhangi bir nedenle kesintiye uğradıktan sonra farklı zamanlarda yeniden yapılmış ise zincirleme suç hükümleri tatbik edilmelidir.

TCK m. 244'te yer alan suç tiplerinin aynı eylemle birden fazla mağdura karşı işlenmesi de mümkündür. Bu halde aynı neviden fikri içtima (TCK m. 43/2) hükümleri uygulanarak bir cezaya hükmedilmeli ve ceza $\frac{1}{4}$ 'ünden $\frac{3}{4}$ 'üne kadar artırılmalıdır. Bu duruma zararlı yazılımların internet gibi bilişim ağları üzerinden sistemlere bulaştırılması örnek olarak gösterilebilir⁶⁴³. Burada fail tek bir eylemle (virüsü tedavüle sokmayla), sistemlere veya verilere zarar vermekte, kaç mağdura ait sistemin etkileneceği ise virüsün teknik kapasitesi ve toplumsal duyarlılık gibi diğer bazı faktörlere bağlı olarak değişmektedir. Elbette ki fail, farklı eylemlerle farklı bilişim sistemlerine saldırılar düzenlemiş ise gerçek içtima hükümleri uygulanacak, her bir eylem için ayrı cezaya hükmedilecektir. Bu nedenle bilişim ağları üzerinden yapılan zararlı yazılım saldırılarında failin eylemlerinin ve kontrol edemediği diğer olguların doğru olarak tespiti içtima kurallarının uygulanmasında önem göstermektedir.

Bir bilişim sisteminin veya verilerin birden fazla sahibi olması da mümkündür. Bu nedenle bilişim sistemine ve/veya verilere yönelen tek eylemin birden fazla mağdura karşı işlenmiş olması gündeme gelecektir. Diğer şartların da varlığı halinde TCK m. 43/2'nin (aynı neviden fikri içtima) uygulanmasında bir engel bulunmamaktadır⁶⁴⁴.

Tek bir eylemle birden fazla hükmün ihlal edilmesi (farklı neviden fikri içtima) durumu farklı ihtimallere göre ayrı ayrı değerlendirilmelidir.

⁶⁴⁰ Artuk/Gökçen/Yenidünya, 2016: 682 – 683.

⁶⁴¹ "... Sanığın bir suç işleme kararının icrası kapsamında değişik zamanlarda ve kısa zaman aralıkları içinde katılanın hesabından internet yoluyla başka kişi ve şirketlere ait banka hesaplarına birden fazla kez para havalesi yaptığının anlaşılması karşısında; cezasının TCK'nın 43. maddesi uyarınca artırılması gerektiğinin gözetilmemesi..." Yargıtay, 22. CD. 2015/13422 E. 2016/1679 K. 09.02.2016 T.

⁶⁴² Erdoğan, 2013: 235.

⁶⁴³ Aynı yönde, Dülger, 2015: 437; Dülger, 2014a: 19.

⁶⁴⁴ Artuk/Gökçen/Yenidünya, 2010: 716.

TCK m. 244/1 ve 244/2 hükümlerinin aynı anda ihlal edilmesi mümkündür. Örneğin, bir verinin yok edilmesi, sistemde kritik bir veri olması nedeniyle bilişim sisteminin bozulmasına da neden olabilir. Bir görüş, birinci ve ikinci fıkraların gerçekleşmesi halinde kastın göstereceği fıkranın uygulanması gerektiğini söylemektedir. Diğer görüş ise, birinci fıkrada düzenlenen durumun daha ağır olduğunu ve iki durumun da gerçekleşmesi halinde birinci fıkranın uygulanması gerektiğini ifade etmektedir⁶⁴⁵. Biz de bu halde farklı neviden fikri içtima kuralının uygulanarak TCK m. 244/1'den hüküm verilmesi gerektiğini düşünmekteyiz. Nitekim birinci ve ikinci fıkranın aynı anda gerçekleştiği olaylarda kastın nereye yöneldiğinin belirlenmesi neredeyse imkansızdır. Üstelik verilere zarar verme amacı taşıyan failin, sistemin engellenmesi veya bozulması noktasında en azından olası kast ile hareket edeceği açık olduğundan birinci fıkrada kast unsurunun gerçekleşmediği bir örnek bulmak oldukça güçtür.

TCK m. 244/4'ün suçun nitelikli hali olduğundan daha önce bahsedildiğinden, bu suçun gerçekleşmesi halinde TCK m. 244/1 ve/veya 2 suçun unsuru haline dönüştüğünden bileşik suç söz konusu olacak ve yalnızca m. 244/4'ten ceza verilecektir⁶⁴⁶. Yine TCK m. 244/4 ile başka bir suç tipinin çatışması durumunda madde metninde “başka bir suç oluşturmaması” ifadesi yer aldığından, asli – yardımcı norm ilişkisi değerlendirilecektir⁶⁴⁷. Bu halde görünüşte içtima olduğundan dolayı TCK m. 244/4'ün değil, ilgili diğer hükmün uygulanması gerekecektir. Örneğin, Yargıtay vermiş olduğu bir kararda kredi kartı bilgilerinin ele geçirilip kullanılarak alışveriş yapılması eyleminin m. 244/4'teki değil, 245/1'deki hükmü ihlal ettiğini belirtmiştir⁶⁴⁸.

TCK m. 243 ile 244 arasındaki içtima ise daha tartışmalıdır. Burada bir görüş, fikri içtima kuralının uygulanmasını ve cezası daha ağır olan m. 244 hükmünün uygulanacağını söylemektedir⁶⁴⁹. Diğer bir görüş, burada geçit suçu oluşmadığını, m. 244'te yer alan suçların mutlaka m. 243'ün ihlalini gerektirmeyeceğini söyleyerek her iki suçtan ayrı ceza verilmesi gerektiğini söylemektedir⁶⁵⁰. Başka bir görüş, geçitli suç kurumunu kabul etmemekle birlikte failin kastı ile çözümlenmesi gerektiğini, m. 244'te yer alan suç tipi olduğu takdirde m. 243'ten ayrıca ceza verilmeyeceğini söylemektedir⁶⁵¹. Daha başka bir görüş, amaç – araç suç

⁶⁴⁵ Erdoğan, 2013: 236.

⁶⁴⁶ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 948.

⁶⁴⁷ Görünüşte içtima hallerinden asli – yardımcı norm hakkında detaylı bilgi için, Artuk/Gökçen/Yenidünya, 2015: 683.

⁶⁴⁸ “... Sanığın, katılanlar ve mağdurların kredi kartı bilgilerini ele geçirip kullanmak suretiyle internet üzerinden değişik zamanlarda birden fazla alışveriş yapmaktan ibaret eyleminin TCK'nin 245/1 ve 43. maddelerinde yazılı suçu oluşturduğu halde, suç vasfında yanılığa düşülerek yazılı şekilde TCK'nin 244/4, 43. maddeleri uyarınca hükümler kurulması...” Yargıtay, 8. CD. 2014/32245 E. 2015/16317 K. 15.04.2015 T.

⁶⁴⁹ Erdoğan, 2013: 171. Fikri içtima kurumunun uygulanması gerektiğine ilişkin başkaca bir görüş, Akbulut, 2017: 211.

⁶⁵⁰ Dülger, 2015: 438.

⁶⁵¹ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 929.

kavramına girerek m. 243'ün geçit olma özelliğini vurgulamakta ve sadece m. 244'ün uygulanacağını belirtmektedir⁶⁵². Bizim de katıldığımız görüş ise fikri içtima kuralının uygulanmayacağı, bununla birlikte tüketen – tüketilen norm ilişkisi çerçevesinde TCK m. 243'ten ayrıca ceza verilemeyeceği, tipe göre m. 244/1, 2 veya 4'ten hüküm verileceği yönündedir⁶⁵³. Yargıtay veri üzerindeki suçlarda bu eylemlerin bir bütün olarak m. 244/2 fıkrasını ihlal edeceğini belirtmektedir⁶⁵⁴.

TCK m. 244 ile kişisel verileri ele geçirmeyi düzenleyen m. 136 arasındaki ilişkiye değinmek gerekmektedir. Kişisel verilerin bilişim ortamında ele geçirilmesi için bilişim sisteminde verilere dair bir eylemde (değiştirmek veya başka yere göndermek gibi) bulunmak şarttır. Bu eylem çoğu zaman kişisel verilerin bedel karşılığında satılması amacıyla gerçekleştiğinden m. 244/2 değil, 244/4 gündeme gelecektir. Bu halde fikri içtima olduğu kabul edilirse daha ağır ceza olan m. 244/4, özel – genel norm kapsamında görünüşte içtima olduğu kabul edilirse m. 136'nın uygulanması gerekecektir. Bize göre bu durumda görünüşte içtima bulunduğundan TCK m. 136 uygulanmalıdır. Yargıtay da kredi kartı bilgilerini kopyalamak için ATM'ye sistem kurma eyleminin m. 244/2-3 değil, m. 136'da yer alan suçu oluşturduğunu ifade etmektedir⁶⁵⁵. Ancak bu durumda failin haksızlık unsuru daha ağır olan eylemi karşısında daha hafif cezayla cezalandırıldığı görülmektedir. Bu nedenle kişisel verilere ilişkin suçların bilişim alanında veya haksız çıkar amacıyla işlenmesinin nitelikli hal olarak ayrıca düzenlenmesi gerektiğini düşünmekteyiz.

TCK m. 244/1 ve m. 124'te düzenlenen haberleşmenin engellenmesi suçları da tek bir eylemle aynı anda işlenebileceğinden bu suçlar arasında fikri içtima ilişkisi kurulabilir⁶⁵⁶.

TCK m. 244 ile m. 142'de yer alan bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık suçları arasında da bağlantıdan söz edilebilir. Yargıtay bir kararında, bir telefon şirketine ait kontörlerin giriş kodu ve şifreyle transfer edildiği bir internet sitesinden, yetkili kişinin bilgisi dışında yapılan kontör aktarımının m. 244'te değil, m. 142/2-e'de yer alan suçu oluşturduğunu ifade etmektedir⁶⁵⁷. Yine öğreti ve Yargıtay'a göre banka hesaplarından müş-

⁶⁵² Artuk/Gökçen/Yenidünya, 2010: 716.

⁶⁵³ Tezcan/Erdem/Önok, 2016: 950 – 951.

⁶⁵⁴ "... Sanığın, katılanın e-mail ve Facebook hesabına izinsiz girip hesapların şifrelerini değiştirmek suretiyle bilişim sistemine görmesini engellediğinden bahisle açılan davada; bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme ile bilişim sistemindeki verileri bozma, yok etme, erişilmez kılma, var olan verileri başka bir yere gönderme suçlarında, gerçekleşen eylemlerin bir bütün olarak TCK'nin 244/2 maddesinde düzenlenen suçu oluşturacağı..." Yargıtay, 8. CD. 2015/14287 E. 2016/4903 K. 12.04.2016 T.

⁶⁵⁵ "... Bankanın ATM cihazına banka ve kredi kartları bilgilerini kopyalamak için sistem kuran, ancak ihbar edilmeleri neticesinde herhangi bir kartın kopyalamasını yapamadan yakalanan sanığın eyleminin TCK'nin 136, 35 maddelerine uyan suçu oluşturduğu gözetilmeden yazılı şekilde TCK'nin 244/2-3 maddeleri uyarınca hüküm kurulması..." Yargıtay, 8. CD. 2014/23 E. 2014/17639 K. 07.07.2014 T.

⁶⁵⁶ Özbek/Kanbur/Doğan/Bacaksız/Tepe, 2015: 948.

⁶⁵⁷ "... şirketine ait kontörleri internet üzerinden ve işyerine ait bilgisayar aracılığıyla ilgili siteler vasıtasıyla transfer ve fatura tahsilatı yapan, bahse konu siteler tarafından giriş kodu ve şifresi verilen katılanın kontör yük-

tekilerin bilgi ve rızası haricinde para aktarılması veya çekilmesi eylemleri m. 142/2-e uyarınca cezalandırılmaktadır⁶⁵⁸.

Yine TCK m. 244 ile malvarlığına yönelik bir diğer suç olan dolandırıcılık suçları arasındaki ilişkiden de bahsedilmelidir. Yargıtay bir kararında sosyal medya ve e-mail adresine girilip şifrenin değiştirilmesi eyleminin TCK m. 244/2'de yer alan suçu, hesabın geri verilmesi için kontör istenmesi eyleminin ise ayrıca dolandırıcılık suçu olduğuna karar vermiştir⁶⁵⁹.

Verilerin değiştirilmesi ve görevi kötüye kullanma suçları arasında da bazı ortak noktalar bulunmaktadır. Nitekim Yargıtay bir kararında kamu görevlilerinin bilgi işlem üzerinden araçlar hakkında borcu yoktur yazısı düzenlemeleri eylemini görevi kötüye kullanma suçu olarak değil, TCK m. 244'teki verileri değiştirme suçu olarak görmektedir⁶⁶⁰.

Yargıtay belgede sahtecilik suçları ile bilişim suçları arasında yaptığı değerlendirmede, fiziki ortamda ve bilişim alanında gerçekleşen eylemlerin ayrı olduğunu kabul etmekte ve

lediği siteye girilerek bilgisi dışında, hattına kontör aktarımı yaptığı anlaşılan sanığın eyleminin TCK'nin 142/2-e. maddesinde düzenlenen suçu oluşturacağı gözetilmeden suç vasfında yanılığa düşerek yazılı şekilde hüküm kurulması..." Yargıtay, 8. CD. 2017/23361 E. 2018/2812 K. 14.03.2018 T.

⁶⁵⁸ Koca/Üzülmez, 2018: 877. "TCK'nın 244/4. maddesinde, Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde... biçimindeki ifadede bu fıkradaki düzenlemenin tali norm niteliğinde olduğunun anlaşılması, buna göre öncelikle yasada düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığı değerlendirildikten sonra gerçekleştirilen eylem bu suçlardan hiçbirisinin tanımına uygun değil ise, bu durumda eylemin TCK'nın 244/4. maddesi kapsamında suç oluşturacağı düşünülecek; müştekinin banka hesabına internet üzerinden ulaşan sanığın, müştekiye ait 1000 TL'yi, EFT yoluyla kendi hesabına havale ederek aynı gün içinde çekmesi eylemindeki kastın, müştekinin banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi hesaplarına geçirmeye, müştekinin rızasına aykırı olarak mal varlığında azalmaya neden olmaya, var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olması nedeniyle, Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 sayılı kararında açıklandığı üzere; sanığın fiilinin TCK'nın 142/2-e maddesinde öngörülen bilişim suretiyle hırsızlık suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi..." Yargıtay, 13. CD. 2013/19796 E. 2014/18903 K. 27.05.2014 T. "... İnternet üzerinden müştekilerin yetkilisi oldukları şirket banka hesaplarından bilgi ve rızaları dışında suç tarihlerinde sanıklara ait ve belirledikleri hesaplara paraların aktarılması, çekilmesi veya bu hesaplardan alışveriş yapılması eyleminin TCK'nın 142/2-e. maddesindeki suçu oluşturduğu gözetilmeyerek yazılı şekilde TCK'nın 244. maddesi uyarınca hüküm kurulması..." Yargıtay, 13. CD. 2017/2912 E. 2017/7281 K. 15.06.2017 T. Benzer yönde, internet üzerinden para aktarma eyleminin m. 142/2-e hükmünü ihlal ettiğine ilişkin, Yargıtay, 2. CD. 2017/2209 E. 2017/5340 K. 10.05.2017 T; Yargıtay, 2. CD. 2014/30086 E. 2016/12564 K. 19.09.2016 T.

⁶⁵⁹ "... Şikayetçiye ait e-mail adresi ve Facebook profilini haksız olarak şifre- sinin ele geçirilip değiştirildiği, daha sonra internet ortamında 100 kontör göndermesi istendiği, kontör göndermediği takdirde her şeyin elinde olduğunu, ekran kartını yakacağını, maddi hasara uğratacağını bildirmesi üzerine şikayetçinin 100 kontör gönderdiğinden bahisle açılan davada ... e-mail şifresinin ele geçirilmesi ve değiştirilmesi eyleminin TCK'nın 244/2 maddesi kapsamındaki suçu, kontör talebinde bulunulmasının ise dolandırıcılık suçunu oluşturacağı da dikkate alınarak sonucuna göre tüm deliller yeniden değerlendirilip hukuki durumun tayin ve takdiri gerekirken..." Yargıtay, 8. CD. 2015/11682 E. 2015/24706 K. 18.11.2015 T.

⁶⁶⁰ "... Sanıkların 2006-2008 yılları arasında sistem üzerinde iddianameye konu bir kısım araçlarla ilgili bilgi işlem silsilesini bozarak usulsüz biçimde tescil işlemlerini tahrif ettikten sonra ilişik kesme veya fenni muayene belgelerini düzenleyerek araçlar hakkında borcu yoktur belgesi düzenledikleri; bir kısım araçlar hakkında ise geçerli bir terkin sebebi olmaksızın kendilerine ait şifreler ile kayıtları değiştirmek sureti ile ... sistemi üzerinde henüz belge çıktısı alınmadan usulsüz olarak terkin ve tescil işlemi yapmaktan ibaret eylemlerinin TCK 244 madde de düzenlenen bilişim sistemlerindeki verileri değiştirme suçunu oluşturmalarına rağmen suç vasfında yanılığ sonucunda görevi kötüye kullanmak suçundan mahkumiyetlerine karar verilmesi..." Yargıtay, 21. CD. 2015/3466 E. 2015/5897 K. 03.12.2015 T.

fiziki ortamdaki eylemlerin m. 204 – 205, bilişim alanındaki eylemlerin m. 244 uyarınca ayrı ayrı cezalandırılması gerektiğine hükmetmektedir⁶⁶¹.

Şifreli yayınların kırılarak bedelsiz izlenmesi eylemlerinde Yargıtay tek eylemle m. 163/2’de yer alan karşılıksız yararlanma ile m. 243 veya 244’te yer alan suçların ihlal edildiğini ve farklı neviden fikri içtima kurumunun işletileceğini karara bağlamıştır⁶⁶².

3.8 Muhakeme

TCK m. 244 uyarınca yapılacak yargılamalarda 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun’un 10, 11, 12 ve 14. maddeleri uyarınca görevli mahkeme Asliye Ceza Mahkemeleridir.

Suç şikâyeteye tabi olmadığından re’sen soruşturma ve kovuşturmayaya tabiidir.

3.9 Yaptırım

TCK m. 244/1’e göre bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun işlenmesi halinde faile bir yıldan beş yıla kadar; 244/2 uyarınca verilerin yok edilmesi veya değiştirilmesi suçunun işlenmesi halinde faile altı aydan üç yıla kadar hapis cezası verilmektedir. Suçun temel şeklinde yalnızca hürriyeti bağlayıcı cezalara yer verilmesine karşın, nitelikli hal olan m. 244/4 uyarınca ayrıca haksız çıkar elde edilmesi durumunda faile iki yıldan altı yıla kadar hapis ve ayrıca beş bin güne kadar adli para cezasına hükmedilmektedir.

TCK m. 246 uyarınca bu suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler uyarınca güvenlik tedbirleri uygulanacaktır.

⁶⁶¹ “... Sanık U. K.’nin azmettirmesi ile hareket eden T. K.’nin iki ayrı soruşturma dosyasını adliyeden çıkarıp bu kişiye teslim etmesi yanında bu dosyalarla ilgili olarak UYAP ortamında gerçeğe aykırı işlemler yapması şeklindeki eylemlerinde, TCK’nin 142, 204, 281. maddelerinde düzenlenen suçların unsurlarının bulunmadığı, buna karşın bilişim sistemindeki verileri değiştirme suçunun işlenmesi için fiziki evrakın da yok edilmesi veya gizlenmesinin zorunlu olmaması nedeniyle hukuki anlamda tek bir fiilden söz edilemeyecek ve TCK’nin 44. maddesi uyarınca fikri içtima kuralının uygulanamayacak olması karşısında, sanıkların unsurları oluşan resmi belgeyi gizleme ve bilişim sistemindeki verileri değiştirme suçları dolayısıyla TCK’nin 205/1-son ve 244/2. maddeleri uyarınca ayrı ayrı cezalandırılmaları gerektiği ve anılan suçları oluşturan eylemlerin aynı zaman diliminde aynı suçun işlenmesine matuf kesintisiz birer fiil olarak gerçekleştirilmiş olmaları sebebiyle anılan Yasanın 43/1. maddesinde düzenlenen zincirleme suç hükümlerinin uygulanma imkanının da bulunmadığı, gizlenen resmi belge adedi ile UYAP ortamında yapılan işlem sayısının ancak sübuta eren suçlar dolayısıyla verilecek temel cezaların belirlenmesinde dikkate alınabileceği gözetilmeden sadece resmi belgeyi gizleme ve bu fiile azmettirme suçlarından yazılı şekilde mahkumiyet hükümleri kurulması...” Yargıtay, 5. CD. 2014/6872 E. 2014/7366 K. 03.07.2014 T.

⁶⁶² “... Bedeli karşılığında izlenmesi gereken şifreli televizyon yayınlarının, sahibinin rızasına aykırı olarak bedelsiz şekilde izlenmesini sağlamak eyleminde TCK’nin 163/2 maddesinde düzenlenen karşılıksız yararlanma suçunun unsurlarının oluştuğu, ancak TCK’nin 44. maddesinde yazılı işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır hükmü gereğince, sanığın eyleminin TCK’nin 243 veya 244. maddelerinde gösterilen suçu oluşturduğunun belirlenmesi durumunda, eylemin tek olduğu ancak iki farklı suçun oluştuğu da gözetilip, eyleminin uyduğu maddedeki cezalar ile TCK’nin 163/2. maddesinde yazılı cezanın karşılaştırılması suretiyle TCK’nin 44. maddesi de gözetilerek sonucuna göre sanığın hukuki durumunun belirlenmesi gerektiğinin gözetilmemesi...” Yargıtay, 11. CD. 2012/439 E. 2013/16403 K. 11.11.2013 T.

SONUÇ

Bilişim sistemlerinin başlangıcından bu yana geçirdiği teknik değişimler, aynı zamanda geniş kitlelerin de kolaylıkla bu sistemlerle ilişkide bulunabilmeleri sonrasında bilişim suçlarında bir artış görüleceği ve bunun ceza hukukunda da yoğun derecede tartışılmaya başlanacağı bundan çok uzun süre önce dahi öngörülebilmekteydi.

Bununla birlikte öğretilerde bilişim suçlarına yönelik yaklaşımların bir bölümünde belirlenemezlik çekincesi bulunduğu dikkat çekmektedir. Bu nedenle genel geçer tanım ve tespitlerden kaçınıldığı görülmektedir. Halbuki, bilişim sistemlerinin tümünü kapsayacak genel ilkelerin ortaya konulması ve hukuk disiplini içerisinde değerlendirilmesi öncelikli çalışmaların arasında yer almalıdır. Benzer şekilde bilişim sistemlerinin yalnızca bilgisayar veya internetten oluşmadığı net bir şekilde ifade edilmeli ve bu konudaki karışıklık giderilmelidir.

Ne kadar karmaşık olursa olsun, bilişim sisteminin yegâne sınırı insan algısıdır. Her bir bilişim sistemi algılanabilmeye muhtaçtır. Algılanabilen sistemler de “sihrini” üstün becerileriyle gösterirler. Bu beceri genellikle kaba kuvvetten oluşur, basit bir devrenin milyonlarcasının küçük hacimlerde bir araya gelebildiği sistemler bilişim suçlarının günümüzdeki konusu olmuştur.

Bilişim sistemlerinin bu yaygınlığı ve kuvveti bilişim suçlarına da yansımıştır. Genel kabule uygun olarak bilişim suçları da kendi içlerinde salt bilişim suçları ve bilişim sistemleri aracılığıyla işlenen geleneksel suçlar olarak ayrılmaktadır.

Bilişim suçlarının sözü edilen bu özellikleri gerek uluslararası gerek ulusal düzeylerde de birçok çalışmanın yapılmasını sağlamıştır. Ülkemizde de bazı yönleriyle birçok ulusal hukuk sistemlerinden önde bir yapının bulunduğu, bununla birlikte bir o kadar da tartışılması ve geliştirilmesi gereken noktalar bulunduğu görülmektedir.

TCK m. 244’te düzenlenen suç tipi, salt bilişim suçları arasında yer almakta, bilişim suçları arasında sık görülen suç tiplerini içinde barındırmaktadır. Hem bilişim sistemlerinin hem de salt verilerin çeşitli suretle bozulması, engellenmesi ve değiştirilmesi eylemlerini içermektedir. Bu anlamda m. 243’te yer alan bilişim sistemine girme suçunun bir adım sonrası içeren eylemlerin tanımlandığı söylenebilecektir.

TCK m. 244, teknolojik yönden oldukça kapsamlı olmakla birlikte, mali yönden tamamlayıcı norm görevi görmektedir. Ekonomik amaçla bu suçun gerçekleşmesi ancak başka bir suçun işlenmemiş olması durumunda cezalandırılmaktadır.

Bunlarla birlikte kaleme alınış şekli itibarıyla TCK m. 244/4 fıkrasının ayrı bir suç tipi mi, yoksa suçun nitelikli hali mi olduğu geniş tartışmalara neden olmuştur. Yine kamu kuru-

luşlarına ait bilişim sistemleri üzerinde işlenen suçların nitelikli hal sayılmamasına karşın, kamu görevlilerinin işlediği suç hakkında bir nitelikli hal öngörülmemiş olması düzenlemenin eleştirilebilecek yönlerindendir.

Bilişim suçlarının, özel hayata karşı işlenen suçlar ve kişisel verilere karşı suçlarla olan ilişkisi de karmaşık sonuçlar doğurabilmektedir. Öğretide yer alan farklı öneriler de dikkate alınarak, içtima kurallarında da hakkaniyetli sonuç doğuracak şekilde bilişim suçlarının yakın nitelikteki suçlarla olan bağlantısının daha net ortaya konulması gerekmektedir.

Yine daha geniş kapsamda değerlendirildiğinde, bilişim suçlarına ait bölümün topluma karşı suçlar değil, kişilere karşı suçlar kısmında düzenlenmesinin daha isabetli olacağını düşünmekteyiz.



KAYNAKÇA

- Akarıslan, H. (2015). *Biliřim Suçları*. Seçkin Yayınevi, Ankara.
- Akbulut, B. (2017). *Biliřim Alanında Suçlar*. Adalet Yayınevi, Ankara.
- Akçam, B. K. (1999). *Suçla Mücadele Edenler İçin İnternet*. Türkiye Biliřim Derneęi Yayınları, Ankara.
- Akdeniz, G. (2013). “Hacker Etięi”. A.R. Keleş, Y. Sal (Ed.). *Hack Kültürü ve Hactivizm: Yeni Bir Siyaset Biçimi, Mustafa Akgül’e Armaęan*. Alternatif Biliřim Derneęi, İstanbul, s. 9 – 15.
- Akın, H. L. (2006). “Robotbilim”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Biliřim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 671 – 674.
- Alaca, B. (2008). *Ülkemizde Biliřim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile)*. Yayımlanmamış Yüksek Lisans Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Apaydın, C. (2015a). “Biliřim Sisteminin İşleyiřini Engelleme ve Bozma Suçları”. *Ceza Hukuku Dergisi*, 29: 205 – 264.
- Apaydın, C. (2015b). “Biliřim Sistemindeki Verileri Yok Etme, Bozma, Eriřilmez Kılma, Deęiřtirme, Hukuka Aykırı Olarak Verileri Yerleřtirme veya Gönderme Suçu ile Bu Suretle Hukuka Aykırı Yarar Elde Etme Suçunun İncelenmesi”. *Terazi Hukuk Dergisi*, 10(111): 14 – 41.
- Artuk, M. E., Ahmet, G., Yenidünya, A. C. (2010). *Ceza Hukuku Özel Hükümler*. Turhan Yayınevi, Ankara.
- Artuk, M. E., Ahmet, G., Yenidünya, A. C. (2015). *Ceza Hukuku Genel Hükümler*. Adalet Yayınevi, Ankara.
- Atalıç Tař, K. (2010). *Biliřim Suçları ve Adana İlinde 2006 – 2009 Yılları Arasında Meydana Gelen Biliřim Suçlarının Deęerlendirilmesi*. Yayımlanmamış Yüksek Lisans Tezi. Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü, Adana.
- Avřar, B. Z. ve Öngören, G. (2010). *Biliřim Hukuku*. Türkiye Bankalar Birlięi Yayınları, İstanbul.
- Aydın, E. D. (1992). *Biliřim Suçları ve Hukukuna Giriř*. Doruk Yayınevi, Ankara.
- Bahtiyar, B. (2007). *Mikro İşlemciler ve Mikro Denetleyiciler*. Nobel Yayınevi, Ankara.
- Baran, P. (1964). *Introduction to Distributed Communications Networks*. Rand Corporation, California.

- Başbüyük, İ. (2010). “Hırsızlık ve Dolandırıcılık Suçlarının Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle İşlenmesi”. *Ceza Hukuku Dergisi*, 14: 151 – 192.
- Bıçkın, İ. (2006). “Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanunu’nda Bilişim Suçları”. *Yargıtay Dergisi*, 32(1 – 2): 145 – 168.
- Bilek, B. T. (2012). *Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri*. Yayımlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
- Bozkurt Yüksel, A. E. (2016). *Bulut Bilişimde Kişisel Verilerin Korunması*. Yetkin Yayınevi, Ankara.
- Brenner, S. W. (2001). *Is There Such A Thing As “Virtual Crime”*. California Criminal Law Review, Volume 4. (<http://ssrn.com/abstract=1611839>, (erişim tarihi: 01.03.2017).)
- Bülbül, İ. ve Bingöl, P. E. (2018). *Etik Hackerlığa Giriş*. Hayy Kitap, İstanbul.
- Can, S. Z. (2015). İşlemci Yapılarının Hatalara Karşı Hassasiyetini Karşılaştırmak İçin Yeni Bir Bit Etki Katsayısı Tanımlanması ve Kullanılması. Yayımlanmamış Yüksek Lisans Tezi. TOBB Ekonomi ve Teknoloji Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Can, H. ve Akın, E. (2006). “Akıllı Ev Aygıtları”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 73 – 78.
- Çakıcı, M. (2014). “Türk Ceza Kanunu m. 243 ve m. 244’te Düzenlenen Bilişim Suçları”. *Ceza Hukuku Dergisi*, 24: 308 – 349.
- Çıtak, Ö. (2018). *Offensive & Defensive Ethical Hacking*. Abaküs Yayınevi, İstanbul.
- Çiçek, İ. (2008). *Ülkemizde Adli Bilişim Laboratuvarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları*. Yayımlanmamış Yüksek Lisans Tezi. Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Cohen, F. (2010). *Digital Forensic Evidence Examination*. ASP Press, California.
- Çölkesen, R. (2006). “Veri Yapıları ve Modelleri”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 892 – 897.
- Dayar, T. (2006). “Web Hizmet Başarımı”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 913 – 917.
- Defense Advanced Research Projects Agency. (1981). *A History of The Arpanet: The First Decade*. Bolt Beranet and Newman Inc, Virginia. (www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA115440, (erişim tarihi: 01.03.2017).)

- Değirmenci, O. (2005). “2004 Türk Ceza Kanunu’nun Bilişim Suçları Bakımından Değerlendirilmesi”. *Türkiye Barolar Birliği Dergisi*, 58: 195 – 208.
- Demircan, T. (2016). *Bilişim Alanında Suçlar*. Legal Yayınevi, İstanbul.
- Demirkıran, P. (2013). “Hactivizm”. A.R. Keleş, Y. Sal (Ed.). *Hack Kültürü ve Hactivizm: Yeni Bir Siyaset Biçimi, Mustafa Akgül’e Armağan*. Alternatif Bilişim Derneği, İstanbul, s. 27 – 33.
- Dijle, H. (2006). *Türkiye’de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı*. Yayımlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Dilek, H. İ. (2007). *Bilişim Suçları ve Türk Hukukundaki Yeri*. Yayımlanmamış Yüksek Lisans Tezi. Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Diyarbakır.
- Doğan, K. (2005). “Bilişim Suçları ve Yeni Türk Ceza Kanunu”. *Hukuk ve Adalet Eleştirel Hukuk Dergisi*, 6-7.
- Doğu, A. H. (2016). *Bilişim Hukuku*. Ekin Yayınevi, Bursa.
- Dülger, M. V. (2014a). “Suçların Birleşmesine İlişkin Tanımlar, Sorunlar ve Çözüm Önerileri”. *Leges Ceza Hukuku Dergisi*, 1: 4 – 87.
- Dülger, M. V. (2014b). “Türk Borçlar Kanunu, Türk Ticaret Kanunu ve Hukuk Muhakemeleri Kanunu’ndaki Bilişim Alanına İlişkin Düzenlemelerin Ceza Hukukuna Yansımaları”. *Ankara Barosu Dergisi*, 1: 111 – 144.
- Dülger, M. V. (2015). *Bilişim Suçları ve İnternet İletişim Hukuku*. Seçkin Yayınevi, Ankara.
- Efe, A. ve Çölkesen, R. (2006). “Ağ Programlama ve TCP/IP”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 55 – 60.
- Eker, Ö. U. (2006). “Türk Ceza Hukukunda Bilişim Suçları Eski TCK Bağlamında Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu’nun İlgili Hükümlerinin Yorumu”. *Türkiye Barolar Birliği Dergisi*, 62: 101 – 131.
- Ekşioğlu, Ş. (Ed.). (Kasım 2018). “Makinelerin Yükselişi, Yapay Zekâ ve Robotik Dünyayı Nasıl Değiştirecek?”. *How It Works*, 1: 14 – 21.
- Erdağ, A. İ. (2010). “Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)”. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, 14(2): 275 – 303.
- Erdoğan, Y. (2013). *Türk Ceza Kanunu’nda Bilişim Suçları*. Legal Yayınevi, İstanbul.
- Erem, F. (1993). “Bilgisayar Suçları ve Türk Ceza Kanunu”. *Türkiye Barolar Birliği Dergisi*, 2: 178 – 186.
- Erman, R. B. (2001). “Alman Hukukunda İnternette Kaynaklanan Ceza Sorumluluğu”. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59(1-2): 203 – 225.

- Ersoy, Y. (1999). “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”. *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 49(3): 178 – 186.
- Esen, S. (2007). *Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar*. Adalet Yayınevi, Ankara.
- Goodman, M. (2016). *Geleceğin Suçları, Dijital Dünyanın Karanlık Yüzü*. Timaş Yayınevi, İstanbul.
- Gözüşirin, M. (2011). *5237 Sayılı Türk Ceza Kanunu’nda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi*. Yayımlanmamış Yüksek Lisans Tezi. Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara.
- Gül, A. (2016). *Doğrudan Dolaylı Bilişim Suçları*. Seçkin Yayınevi, Ankara.
- Gürler, F. (2015). *Yargıtay Kararları Işığında Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar*. Yetkin Yayınevi, Ankara.
- Harmancı, A. E. (2006). “Ağ Mimarisi”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 49 – 55.
- Hawking, S. (2013). *Zamanın Kısa Tarihi*. (Çev. B. GÖNÜLŞEN), Alfa Yayınevi, İstanbul.
- Henkoğlu, T. ve Külcü, Ö. (2013). “Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme”. *Bilgi Dünyası Dergisi*, 14(1): 62 – 86.
- İçel, K. (2001). “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri”. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59(1-2): 3 – 10.
- İlbaş, Ç. (2009). *Bilişim Suçlarının Sosyo – Kültürel Seviyelere Göre Algı Analizi*. Yayımlanmamış Yüksek Lisans Tezi. Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- İnan, A. T. (2006). “Ağ Standartları”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 60 – 67.
- Jamil, T. (1995). *RISC Versus CISC*. IEEE Potentials, Ağustos/Eylül 1995. (https://www.researchgate.net/profile/Tariq_Jamil5/publication/3227233_RISC_versus_CISC/links/5641fcfa08ae24cd3e42a889/RISC-versus-CISC.pdf. (erişim tarihi: 12.01.2019).)
- Kangal, Z. T. (2001). “Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu”. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59(1-2): 227 – 240.
- Karagülmez, A. (2014). *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*. Seçkin Yayınevi, Ankara.
- Karakehya, H. (2009). “Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu”. *Türkiye Barolar Birliği Dergisi*, 81: 1 – 24.

- Kartan, N. (2007). *İntranetin Örgütsel İletişime Etkileri ve İntranetin Bir Alt Sistemi Olarak Datashare Teknoloji Ltd. Şti. Uygulaması*. Yayımlanmamış Yüksek Lisans Tezi. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.
- Katyal, N. K. (2001). *Criminal Law in Cyberspace*. Georgetown University Law Center, 2000 Working Paper Series. (http://papers.ssrn.com/paper.taf?abstract_id=249030. (erişim tarihi: 16.08.2018).)
- Keleş, A. R. ve Sal, Y. (ed.). (2013). *Hack Kültürü ve Hactivizm*. Alternatif Bilişim Derneği, İstanbul.
- Kızıltan, M. B. (2007). *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*. Yayımlanmamış Yüksek Lisans Tezi. İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Koca, M. ve Üzülmüş, İ. (2018). *Türk Ceza Hukuku Özel Hükümler*. Adalet Yayınevi, Ankara.
- Köksal, A. (2010). *Adı Bilgisayar Olsun*. Cumhuriyet Yayınevi, İstanbul.
- Kurt, L. (2005). *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulaması*. Seçkin Yayınevi, Ankara.
- Laudon, K. C. ve Laudon, J. P. (2014). *Management Information Systems*. Pearson Yayınevi, Edinburgh.
- Levy, S. (2010). *Hackers: Heroes Of The Computer Revolution*. O'Reilly Media, Kaliforniya.
- Mahmutoğlu, F. S. (2001). "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu". *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59(1-2): 39 – 49.
- Manas, O. (2006). "Bilgisayar Ağları Tarihçesi". T. Ören, T. Üney, R. Çölkese (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 189 – 193.
- Nakov, S. ve Kolev, V. (2013). *Fundamentals of Computer Programming With C#*. Svetlin Nakov & Co., Sofia. (Ücretsiz E-kitap versiyonu: <http://www.introprogramming.info/wp-content/uploads/2013/07/Books/CSharpEn/Fundamentals-of-Computer-Programming-with-CSharp-Nakov-eBook-v2013.pdf>. (erişim tarihi 14.04.2019).)
- Olovsson, T. (1992). *A Structured Approach to Computer Security*. Chalmers University of Technology, Sweden. (http://publications.lib.chalmers.se/records/fulltext/local_166411.pdf. (erişim tarihi: 25.08.2018).)
- Orta, M. (2015). *Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması (Adli Bilişim)*. Yetkin Yayınevi, Ankara.

- Önok, M. (2013). “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”. *Hukuk Araştırmaları Dergisi Özel Sayı: Prof. Dr. Nur Centel’e Armağan*, (19)2: 1229 – 1269.
- Özbek, V. Ö. (2006). *Yeni Türk Ceza Kanunu’nun Anlamı*. Seçkin Yayınevi, Ankara.
- Özbek, V. Ö., Kanbur, M. N., Doğan, K., Bacaksız, P., Tepe, İ. (2015). *Türk Ceza Hukuku Özel Hükümler*. Seçkin Yayınevi, Ankara.
- Öztan, F. (2008). *Fikir ve Sanat Eserleri Hukuku*. Turhan Yayınevi, Ankara.
- Pallı, H. (2008). *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi. Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Peker, B. (2010). *Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu*. Yayımlanmamış Yüksek Lisans Tezi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.
- Polat, Z. (2006). “Optik Ağlar: Bilişim Otoyolları”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 620 – 623.
- Saka, E. (2013). “Hackerlık Üzerine Birkaç Gözlem”. A.R. Keleş, Y. Sal (Ed.). *Hack Kültürü ve Hactivizm: Yeni Bir Siyaset Biçimi, Mustafa Akgül’e Armağan*. Alternatif Bilişim Derneği, İstanbul, s. 34 – 41.
- Sarı, O. (2013). *Uluslararası Hukuk ve Türk Ceza Hukuku Bağlamında Siber Güvenlik ve Bilişim Sistemine Yönelik Suçlar*. Yayımlanmamış Yüksek Lisans Tezi. Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul.
- Schjolberg, J. S. ve Hubbard A. M. “Harmonizing National Legal Approaches on Cybercrime”.
https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (erişim tarihi: 10.11.2018).
- Sınar, H. (2001). *İnternet ve Ceza Hukuku*. Beta Yayınevi, İstanbul.
- Sokullu Akıncı, F. (2001). “Avrupa Konseyi Siber Suç Sözleşmesi’nde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi”. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59(1-2): 11 – 38.
- Şentürk, A. (2009). *Reduced Instruction Set Processor Design*. Yayımlanmamış Yüksek Lisans Tezi. Çukurova Üniversitesi Doğal ve Uygulamalı Bilimler Enstitüsü, Adana.
- Taş, İ. M. (2013). *Bilgisayar Tabanlı Bilişim Suçlarının Adli Bilişim Çerçevesinde İncelenmesi ve Analizi*. Yayımlanmamış Yüksek Lisans Tezi. Marmara Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- Taşkın, Ş. C. (2008). *Bilişim Suçları*. Beta Yayınevi, İstanbul.

- Taşkın, Ş. C. (2009). “Bilişim Hukuku Uluslararası Uyuşmazlıklar”. *Türkiye Barolar Birliği Dergisi*, 85: 332 – 372.
- Tezcan, D., Erdem, M. R., Önok, R. M. (2016). *Teorik ve Pratik Ceza Özel Hukuku*. Seçkin Yayınevi, Ankara.
- Toker, A. ve Zeki, A. (2006). “Bellekler”. T. Ören, T. Üney, R. Çölkesen (Ed.). *Türkiye Bilişim Ansiklopedisi*. Papatya Yayınevi, İstanbul, s. 116 – 124.
- Toroslu, N. (2008). *Ceza Hukuku Genel Kısım*. Savaş Yayınevi, Ankara.
- Turan, M. (2016). *Bilişim Hukuku*. Seçkin Yayınevi, Ankara.
- Turhan, O. (2006). *Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar)*. Yayımlanmamış Planlama Uzmanlığı Tezi. Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara.
- Tutkun, H. K. (2013). *Telekomünikasyon Sistemleri Sistem Uzmanı El Kitabı*. Seçkin Yayınevi, Ankara.
- Türk, Ö. (2011). *ARM İşlemciler ile Tek Kullanımlık Şifre Uygulamasının Gerçekleştirilmesi*. Yayımlanmamış Yüksek Lisans Tezi. Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
- Ukşal, M. (2015). *Mobil Cihazlarda Adli Bilişim*. Yayımlanmamış Yüksek Lisans Tezi. Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Usta, G. (2015). *Bilgisayar Ağlarında Saldırı ve Savunma*. Seçkin Yayınevi, Ankara.
- Ünver, Y. (2001). “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi”. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, 59(1-2): 51 – 153.
- Yaycı, E. (2007). *Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.
- Yazıcı, Y. (2016). *Sanallaştırılmış Grafik İşlemci Birimlerinin Maliyet Etkinlik Analizi*. Yayımlanmamış Yüksek Lisans Tezi. Türk Hava Kurumu Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- Yazıcıoğlu, R. Y. (1997). *Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle*. Alfa Yayınevi, İstanbul.
- Yazıcıoğlu, R. Y. (1999). “Şifreli Yayınların Bilişim Suçları Karşısındaki Konumu”. *Marmara Üniversitesi Hukuk Araştırmaları Dergisi: Prof. Dr. Selâhattin Sulhi Tekinay’ın Hatırasına Armağan*, 11(1 – 3): 645 – 667.
- Yenidünya, A. C. ve Değirmenci, O. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. Legal Yayınevi, İstanbul.

- Yenisey, F. ve Plagemann, G. (2015). *Alman Ceza Kanunu*. Beta Yayınevi, İstanbul.
- Yetim, S. (2014). “Bilişim Suçları ve Etkin Mücadele Yöntemleri”. *Terazi Hukuk Dergisi*, 9(95): 80 – 86.
- Yılmaz, S. (2011). “5237 Sayılı TCK’nin 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar”. *Türkiye Barolar Birliği Dergisi*, 92: 62 – 100.
- Yılmaz, S. (2016). *Türk Ceza Hukuku Sisteminde Siber Suçlar*. Adalet Yayınevi, Ankara.

İNTERNET KAYNAKLARI

- <http://tdk.gov.tr/> (erişim tarihi: 25.02.2019).
- <http://enformatik.akdeniz.edu.tr/enformatik-bolumu-hakkinda/> (erişim tarihi: 25.02.2019).
- <http://enformatik.aku.edu.tr/bolum-hakkinda-2/enformatik-nedir/> (erişim tarihi: 25.02.2019).
- <http://www.ed.ac.uk/informatics/about/what-is-informatics> (erişim tarihi: 25.02.2019).
- <http://ii.metu.edu.tr/> (erişim tarihi: 25.02.2019).
- http://enformatik.en.ankara.edu.tr/?page_id=46 (erişim tarihi: 25.02.2019).
- <http://www2.tbmm.gov.tr/d22/1/1-0593.pdf> (erişim tarihi: 25.02.2019).
- <http://mevzuat.tbmm.gov.tr/mevzuat/faces/sorgu.jsp?> (erişim tarihi: 25.02.2019).
- <http://be.gazi.edu.tr/posts/view/title/bilisim-sistemleri-98744> (erişim tarihi: 25.02.2019).
- http://www.chip.com.tr/haber/ilk-islemci-intel-4004-40-yasina-girdi_30334.html (erişim tarihi: 25.02.2019).
- <http://www.sabah.com.tr/dunya/2013/04/09/evrenin-760-bin-yasindaki-sesi> (erişim tarihi: 25.02.2019).
- <https://www.youtube.com/watch?v=rME1yJ4xEeE> (erişim tarihi: 25.02.2019).
- [http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/intranet-\(i%C3%A7-a%C4%B1-ve-extranet-\(d%C4%B1-C5%9F-a%C4%B1\)\)](http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/intranet-(i%C3%A7-a%C4%B1-ve-extranet-(d%C4%B1-C5%9F-a%C4%B1))) (erişim tarihi: 25.02.2019).
- <https://www.umitegrioglu.com/intranet-portal-nedir-olmasi-gerekenler/> (erişim tarihi: 25.02.2019).
- <https://www.turkcebilgi.com/ekstranet> (erişim tarihi: 25.02.2019).
- <http://www.darpa.mil/about-us/about-darpa> (erişim tarihi: 25.02.2019).
- <http://www.rand.org/about/history/baran.html> (erişim tarihi: 25.02.2019).
- <https://www.ibiblio.org/pioneers/baran.html> (erişim tarihi: 25.02.2019).
- <http://www-net.cs.umass.edu/653-04/documents/cerfkahn.pdf> (erişim tarihi: 25.02.2019).
- https://en.wikipedia.org/wiki/Internet_protocol_suite (erişim tarihi: 01.03.2016).
- https://tr.wikipedia.org/wiki/Fiziksel_katman (erişim tarihi: 01.03.2016).
- https://tr.wikipedia.org/wiki/World_Wide_Web (erişim tarihi: 01.03.2016).
- <http://shiftdelete.net/hackerlar-ddos-saldirisi-icin-buzdolabi-kullanmis-76351> (erişim tarihi: 25.02.2019).
- <https://ed.ted.com/lessons/how-transistors-work-gokul-j-krishnan> (erişim tarihi: 25.02.2019).
- <http://www.regencytr1.com/> (erişim tarihi: 25.02.2019).
- <http://www.kimnezamanicatetti.com/entegre-devre/> (erişim tarihi: 25.02.2019).
- <https://www.edn.com/electronics-blogs/edn-moments/4412805/Noyce-receives-1st-IC-patent-April-25--1961-> (erişim tarihi: 25.02.2019).
- <http://www.bilim-teknoloji.com/uc-boyutlu-islemciler/> (erişim tarihi: 25.02.2019).

<https://tr.wikipedia.org/wiki/Anakart> (erişim tarihi: 06.03.2016).

<https://www.youtube.com/watch?v=IPX58C2lrEk> (erişim tarihi: 25.02.2019).

https://tr.wikipedia.org/wiki/Yazma%C3%A7_%C3%B6be%C4%9Fi (erişim tarihi: 11.03.2016).

<https://www.turkcebilgi.com/yazma%C3%A7> (erişim tarihi: 25.02.2019).

http://megep.meb.gov.tr/mte_program_modul/moduller_pdf/Bellek%20Birimleri.pdf (erişim tarihi: 25.02.2019).

<http://bidb.itu.edu.tr/sevirdefteri/blog/2013/09/06/bellek-turleri> (erişim tarihi: 25.02.2019).

<http://teknolojirojeleri.com/teknik/onbellek-cache-nedir> (erişim tarihi: 25.02.2019).

<http://www.elektrikport.com/teknik-kutuphane/bios-nedir-bios-ayarlar-nasil-yapilir/15085#ad-image-0> (erişim tarihi: 25.02.2019).

<https://tr.wikipedia.kim/wiki/BIOS> (erişim tarihi: 30.01.2016).

<https://informationisbeautiful.net/visualizations/million-lines-of-code/> (erişim tarihi: 25.02.2019).

https://www.chip.com.tr/haber/system-on-chip-hakkinda-bilmeniz-gerekenler_40217.html (erişim tarihi: 25.02.2019).

<http://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/say%C4%B1sal-ve-analog-ileti%C5%9Fim-ve-internet-eri%C5%9Fim-teknolojileri> (erişim tarihi: 25.02.2019).

<https://www.investopedia.com/terms/a/atm.asp> (erişim tarihi: 25.02.2019).

<https://www.webtekno.com/yazilim/bankamatiklere-yakinda-windows-10-isletim-sistemi-gelecek-h8015.html> (erişim tarihi: 25.02.2019).

<https://www.atmia.com/news/is-your-atm-prepared-for-the-windows-10-migration/5760/> (erişim tarihi: 25.02.2019).

<https://prezi.com/zr2bjeshzcot/atmlerin-isletim-sistemleri/> (erişim tarihi: 25.02.2019).

<https://www.bostondynamics.com> (erişim tarihi: 25.02.2019).

https://www.nasa.gov/mission_pages/msl/index.html (erişim tarihi: 25.02.2019).

<https://azure.microsoft.com/tr-tr/overview/what-is-virtualization/> (erişim tarihi: 25.02.2019).

<https://www.webtekno.com/sosyal-medya/icloud-nasil-hacklendi-h2966.html> (erişim tarihi: 13.01.2019).

<http://teknolojituru.com/2017/07/05/uygulama-magazalarinda-kac-milyon-uygulama-var/> (erişim tarihi: 16.02.2018).

<http://yetkilendirme.btk.gov.tr/> (erişim tarihi: 11.04.2019).

<https://www.esb.org.tr/biz-kimiz> (erişim tarihi: 28.07.2018).

<https://www.btk.gov.tr/ticari-amacli-hizmet-verenler-yer-saglayici-listesi> (erişim tarihi: 28.07.2018).

<https://isttelkom.istanbul/hizmetlerimiz/ibb-wifi-hizmetleri/> (erişim tarihi: 01.08.2018).

<http://www.ankara.bel.tr/haberler/buyuksehirden-ucretsiz-wi-fi-hizmeti/#.W2IKObihmUk> (erişim tarihi: 01.08.2018).

<https://www.haberturk.com/ekonomi/teknoloji/haber/762100-internet-kafeler-azaliyor> (erişim tarihi: 01.08.2018).

<https://stuartsierra.com/2006/07/12/the-three-types-of-computer-user> (erişim tarihi: 07.08.2018).

<http://eski.tbd.org.tr/index.php?sayfa=sozluk&mi1&tipi=entr&harf=H> (erişim tarihi: 02.08.2018).

<https://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html> (erişim tarihi: 11.02.2019).

<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/> (eriřim tarihi: 03.08.2018).

<https://www.bbc.com/news/technology-15817335> (eriřim tarihi: 13.02.2019).

<http://www.hurriyet.com.tr/teknoloji/kurumların-siber-guvenlige-ayirdigi-butce-artacak-41042734> (eriřim tarihi: 13.02.2019).

http://www.larryblakeley.com/security_computer_network/computer_crime_categories.htm (eriřim tarihi: 25.02.2019).

<https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime> (eriřim tarihi: 25.02.2019).

<https://www.shodan.io/> (eriřim tarihi: 25.02.2019).

<https://www.bgasecurity.com/2017/09/10-soruda-sizma-testi/> (eriřim tarihi: 17.02.2019).

<https://tr.pcisecuritystandards.org/index.php> (eriřim tarihi: 17.02.2019).

<https://www.btk.gov.tr/ip-log-imzalayici> (eriřim tarihi: 25.02.2019).

<https://www.kaspersky.com.tr/resource-center/definitions/metamorphic-virus> (eriřim tarihi: 25.02.2019).

https://support.symantec.com/en_US/article.TECH98539.html (eriřim tarihi: 25.02.2019).

<https://www.cybrary.it/0p3n/first-pc-virus-brain-virus/> (eriřim tarihi: 25.02.2019).

<https://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms> (eriřim tarihi: 25.02.2019).

<https://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms> (eriřim tarihi: 25.02.2019).

<https://www.symantec.com/connect/articles/security-11-part-2-trojans-and-other-threats> (eriřim tarihi: 24.08.2018).

<https://searchsecurity.techtarget.com/definition/logic-bomb> (eriřim tarihi: 25.08.2018).

<https://blog.malwarebytes.com/malwarebytes-news/2016/10/malwarebytes-acquires-adwcleaner/> (eriřim tarihi: 25.08.2018).

<https://www.volico.com/the-difference-between-real-and-fake-ransomware/> (eriřim tarihi: 25.08.2018).

<https://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/> (eriřim tarihi: 06.09.2018).

<http://www.pau.edu.tr/bidb/tr/sayfa/spam-postalar> (eriřim tarihi: 06.09.2018).

<https://keremkoseoglu.com/2005/04/30/e-posta-adresini-spammerlardan-saklayin/> (eriřim tarihi: 06.09.2018).

<http://www.pau.edu.tr/bidb/tr/sayfa/spam-postalar> (eriřim tarihi: 06.09.2018).

<https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/fraud/little-book-of-big-scams-business-edition.pdf> (eriřim tarihi: 08.09.2018).

<https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/fraud/little-book-of-cyberscams.pdf> (eriřim tarihi: 08.09.2018).

www.phishtank.com (eriřim tarihi: 11.04.2019).

<https://www.betterbuys.com/estimating-password-cracking-times/> (eriřim tarihi: 09.09.2018).

<https://digitallibrary.un.org/record/114498/files/a-conf-121-22-rev-1-e.pdf> (eriřim tarihi: 25.02.2019).

<https://digitallibrary.un.org/record/1296532/files/a-conf-144-28-rev-1-e.pdf> (eriřim tarihi: 25.02.2019).

<https://www.unodc.org/unodc/en/cybercrime/index.html> (eriřim tarihi: 25.02.2019).

<http://www.unodc.org/unodc/en/commissions/CCPCJ/session/index.html> (eriřim tarihi: 25.02.2019).

<https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html> (erişim tarihi: 25.02.2019).

<https://sherloc.unodc.org/cld/v3/sherloc/> (erişim tarihi: 25.02.2019).

<http://www.unidir.org/est-cyber> (erişim tarihi: 25.02.2019).

<https://www.itu.int/en/action/cybersecurity/Pages/default.aspx> (erişim tarihi: 25.02.2019).

<https://www.un.org/counterterrorism/ctitf/en/publications> (erişim tarihi: 25.02.2019).

<http://www.webology.org/2007/v4n3/a45.html> (erişim tarihi: 25.02.2019).

https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en#page2 (erişim tarihi: 25.02.2019).

<http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm> (erişim tarihi: 10.09.2018).

<http://www.oecd.org/sti/ieconomy/32493366.PDF> (erişim tarihi: 10.09.2018).

https://read.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software_9789264056510-en#page4 (erişim tarihi: 10.09.2018).

https://read.oecd-ilibrary.org/science-and-technology/online-identity-theft_9789264056596-en#page8 (erişim tarihi: 10.09.2018).

<http://thecommonwealth.org/cybercrime> (erişim tarihi: 03.11.2018).

<http://thecommonwealth.org/commonwealth-cybercrime-initiative> (erişim tarihi: 03.11.2018).

http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf (erişim tarihi: 03.11.2018).

<https://www.dwt.com/files/uploads/documents/publications/What%20You%20Should%20Know%20About%20The%202024.pdf> (erişim tarihi: 04.11.2018).

<https://www.oas.org/ext/en/tools/Document-Search> (erişim tarihi: 04.11.2018).

<https://www.interpol.int/en/Crime-areas/Cybercrime/Operations/Operation-Aces> (erişim tarihi: 04.11.2018).

<https://www.coe.int/en/web/cybercrime/capacity-building-programmes> (erişim tarihi: 11.11.2018).

<https://www.coe.int/en/web/cybercrime/octopus-conference> (erişim tarihi: 11.11.2018).

<https://www.coe.int/en/web/cybercrime/glacyplus> (erişim tarihi: 11.11.2018).

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ZWkdLbJk (erişim tarihi: 12.11.2018).

<https://www.coe.int/en/web/cybercrime/tcy> (erişim tarihi: 12.11.2018).

<https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf> (erişim tarihi: 12.11.2018).

<http://www.resmigazete.gov.tr/main.aspx?home=http://www.resmigazete.gov.tr/eskiler/2014/08/20140809.htm&main=http://www.resmigazete.gov.tr/eskiler/2014/08/20140809.htm> (erişim tarihi: 12.11.2018).

<https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf> (erişim tarihi: 12.11.2018).

<https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf> (erişim tarihi: 25.11.2018).

https://sherloc.unodc.org/res/cld/document/french_penal_code_html/french_penal_code.pdf (erişim tarihi: 08.12.2018).

<http://www.legislation.gov.uk/ukpga/1990/18> (erişim tarihi: 09.12.2018).

<https://www.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c059/tbmm22059119ss0664.pdf> (erişim tarihi: 23.12.2018).

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b> (eriřim tarihi: 16.12.2018).

<http://www.yayin.adalet.gov.tr/adaletdergisi/03.sayi/1hikmet.pdf> (eriřim tarihi: 28.12.2018).

<http://malware.wikia.com/wiki/Lose/Lose> (eriřim tarihi: 29.12.2018).

YARGI KARARLARI

Anayasa Mahkemesi, 2014/87 E. 2015/112 K. 08.12.2015 T. RGT: 28.01.2016, RGS: 29607.

Yargıtay, CGK, 1996/6-151 E. 1996/152 K. 25.06.1996 T.

Yargıtay, CGK, 2001/6-30 E. 2001/57 K. 10.04.2001 T.

Yargıtay CGK. 2007/6-136 E. 2007/150 K. 19.06.2007 T.

Yargıtay, 2. CD. 2014/25924 E. 2016/10421 K. 01.06.2016 T.

Yargıtay, 2. CD. 2014/30086 E. 2016/12564 K. 19.09.2016 T.

Yargıtay, 2. CD. 2017/2209 E. 2017/5340 K. 10.05.2017 T.

Yargıtay, 5. CD. 2014/6872 E. 2014/7366 K. 03.07.2014 T.

Yargıtay, 8. CD. 2013/771 E. 2014/15833 K. 23.06.2014 T.

Yargıtay, 8. CD. 2013/11478 E. 2014/8887 K. 08.04.2014 T.

Yargıtay, 8. CD. 2014/23 E. 2014/17639 K. 07.07.2014 T.

Yargıtay, 8. CD. 2014/30037 E. 2015/14023 K. 18.03.2015 T.

Yargıtay, 8. CD. 2014/32245 E. 2015/16317 K. 15.04.2015 T.

Yargıtay, 8. CD. 2015/11682 E. 2015/24706 K. 18.11.2015 T.

Yargıtay, 8. CD. 2015/14287 E. 2016/4903 K. 12.04.2016 T.

Yargıtay, 8. CD. 2016/104 E. 2016/7753 K. 13.06.2016 T.

Yargıtay, 8. CD. 2016/3794 E. 2017/1405 K. 15.02.2017 T.

Yargıtay, 8. CD. 2016/12437 E. 2017/6369 K. 31.05.2017 T.

Yargıtay, 8. CD. 2017/23361 E. 2018/2812 K. 14.03.2018 T.

Yargıtay, 11. CD. 2009/1616 E. 2009/11328 K. 07.10.2009 T.

Yargıtay, 11. CD. 2012/439 E. 2013/16403 K. 11.11.2013 T.

Yargıtay, 11. CD. 2015/1571 E. 2017/1828 K. 13.03.2017 T.

Yargıtay, 13. CD. 2013/19796 E. 2014/18903 K. 27.05.2014 T.

Yargıtay, 13. CD. 2017/2912 E. 2017/7281 K. 15.06.2017 T.

Yargıtay, 21. CD. 2015/3466 E. 2015/5897 K. 03.12.2015 T.

Yargıtay, 22. CD. 2015/13422 E. 2016/1679 K. 09.02.2016 T.

ÖZGEÇMİŞ

Adı ve SOYADI	Mehmet Can KARAGÖZ
Doğum Yeri - Tarihi	Alanya – 05.11.1989
EĞİTİM DURUMU	
Mezun Olduğu Lise	Alanya Ayşe Melahat Erkin Anadolu Lisesi
Lisans Diploması	Ankara Üniversitesi Hukuk Fakültesi
Tezsiz Yüksek Lisans Diploması	
Proje Konusu	
Yüksek Lisans Diploması	
Tez/ Dönem Projesi Konusu	
Doktora Diploması	
Tez/Dönem Projesi Konusu	
Yabancı Dil / Diller	İngilizce
BİLİMSEL FAALİYETLER	
İŞ DENEYİMİ	
Stajlar	Av. Ali Mustafa CAN (Avukatlık Stajı)
Projeler	
Çalıştığı Kurumlar	Karagöz Avukatlık Bürosu
E-Posta	av.mcankaragoz@gmail.com