

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

YÜKSEK LİSANS TEZİ

**BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ
VERİLERE MÜDAHALE İLE BİLİŞİM SİSTEMİ
ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA
SUÇLARI (TCK M. 244)**

SEDA KOÇOĞLU

2501140494

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ SELMAN DURSUN

İSTANBUL, 2019



T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



YÜKSEK LİSANS
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı : SEDA KOÇOĞLU Numarası : 2501140494
Anabilim Dalı / Anasanat Dalı / Programı : KAMU HUKUKU Danışmanı : DR. ÖĞR. ÜYESİ SELMAN DURSUN
Tez Savunma Tarihi : 11.09.2019 Saati : 11.30
Tez Başlığı : BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE İLE BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇLARI (TCK M. 244)

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin 36. Maddesi uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin **KABULÜNE** OYBİRLİĞİ / **OYÇOKLUĞUYLA** karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATI (KABUL / RED / DÜZELTME)
1- PROF. DR. ADEM SÖZÜER		Kabul
2- DOÇ. DR. VOLKAN DÜLGER		Kabul
3- DR. ÖĞR. ÜYESİ SELMAN DURSUN		Kabul
4- DR. ÖĞR. ÜYESİ MEHMET MADEN		Kabul
5- DR. ÖĞR. ÜYESİ MUHAMMED DEMİREL		Kabul

YEDEK JÜRİ ÜYESİ	İMZA	KANAATI (KABUL / RED / DÜZELTME)
1- DR. ÖĞR. ÜYESİ YUSUF YAŞAR		
2- DR. ÖĞR. ÜYESİ SERDAR TALAS		

ÖZ

BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE İLE BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇLARI (TCK m. 244)

SEDA KOÇOĞLU

Bilişim alanındaki gelişmelerin hukuk alanında da büyük bir etkisi bulunmaktadır. Günlük hayatta sıklıkla karşılaşılan suç tiplerinin bilişim ortamında kolaylıkla işlenebilmesi nedeniyle bazı fiiller suç olarak düzenlenmiştir. Çalışmamızda ilk olarak suçların daha iyi anlaşılabilmesi amacıyla bilişim ve ilgili kavramlar ile suç işleme şekilleri açıklanmaya çalışılmıştır. Ardından TCK m. 244/1-2 çerçevesinde sistem ve veriye müdahale suçları incelenerek suçların unsurları ortaya konulmuştur. Son bölümde ise TCK m. 244/4’de düzenlenen bilişim sistemi aracılığıyla haksız çıkar sağlama suçu incelenmiş ve son olarak çalışmamız kapsamında incelenen suçların TCK’da düzenlenen benzer suçlarla karşılaştırılması yapılarak konunun aydınlatılması amaçlanmıştır.

Anahtar Kelimeler: Bilişim Sistemi, Veri, Bilişim, Bilişim Suçları

ABSTRACT

CRIMES OF INTERVENTION TO THE INFORMATION SYSTEM AND THE SYSTEM DATA AND SECURING UNJUST BENEFIT THROUGH THE INFORMATION SYSTEM (TURKISH PENAL CODE ARTICLE 244)

Seda KOÇOĞLU

The developments in the field of informatics have a great effect on the field of law. As the crime types that are frequently encountered in daily life, can be easily committed in the informatics environment, some of the acts are enacted as crimes. In this study, first, we try to explain informatics and related concepts and pattern of criminality in order to present a better understanding of crimes. Subsequently, system and data intervention crimes are examined within the scope of Turkish Penal Code Article 244/1-2 and elements of crime are discussed. In the last part, crime of unjust benefit that is enacted in Turkish Penal Code Article 244/4 is examined, and finally, it is aimed to clarify the subject by comparing the crimes examined in the scope of this study with similar crimes enacted in Turkish Penal Code.

Keywords: Information System, Data, Informatics, Cyber Crimes

ÖNSÖZ

Bilişim sistemlerinin gelişmesi ve internetin yaygınlaşmasıyla beraber bu sistemler daha çok insan yaşamına girmeye başlamıştır. Birçok ekonomik ve ticari faaliyet internet üzerinden yapıldığı gibi insanlar artık bir iletişim aracı olarak interneti kullanmaya başlamış, sosyal medya ile kitleler arası iletişim öngörülemez şekilde genişlemiştir. Giderek kullanımı artan bu olanakların kötüye kullanılması çeşitli ihlallere yol açmış ve bilişim suçları kavramı ortaya çıkmıştır.

Bilişim suçlarının geçmişi diğer suçlara nazaran yeni sayılabilirse de bu suçların hızlı gelişmesi ve yaygınlaşması nedeniyle bu suçlar ceza hukukun en güncel ve hızlı değişen alanlarından birini oluşturmaktadır. Bilişim suçlarının öngörülemez şekilde yaygınlaşması nedeniyle bu suçların takibi hem kanun koyucu bakımından hem de bu alanda çalışan hukukçular bakımından zorluk arz etmektedir. Suçların daha iyi anlaşılabilmesi için ceza hukuku bilgisinin yanında ayrı bir uzmanlık gerektiren bilişim sistemi ve eklentilerine ilişkin temel teknik bilginin de bulunması gerekmektedir. Bu kapsamda çalışmamızda ilk olarak bu hızlı değişen alanın kapsamı ve tanımı yapılmaya çalışılmıştır. Sonrasında bilişim suçlarının Türk Ceza Hukuku'nda düzenlenmesi ile ilgili yaşanan süreç kısaca ele alınmış ve bilişim suçları bakımından özel öneme sahip işleme biçimleri ile ilgili genel bir bilgi aktarılmaya çalışılmıştır.

Çalışmamız kapsamında incelenen suçlardan olan TCK m. 244/1'de düzenlenen “bilişim sisteminin işleyişinin engellenmesi ve bozulması suçu” ile TCK m. 244/2'de düzenlenen “verileri bozma, yok etme, değiştirme, erişilmez kılma ile sisteme veri yerleştirme veya verileri başka bir yere gönderme suçu” bilişim suçlarının temelini oluşturmaktadır. Bu suçları elimizden geldiği ölçüde ayrıntılı olarak birlikte ama farklılıklarına değinerek açıklamaya çalıştık.

Son incelediğimiz suç tipi olan TCK m. 244/4'te düzenlenen “bilişim sistemi aracılığıyla haksız çıkar sağlama suçu” ise ekonomik değerin sistem içerisinde veri olarak değerlendirilmesinden kaynaklı olarak klasik suçlarla en çok bağlantılı olan

bilişim suçu tipidir. Haksız çıkar sağlama suçunu ilk olarak suçun unsurları kapsamında açıklamaya çalıştık. Sonrasında ise çalışmamızda incelediğimiz üç suç tipini her suç tipi için TCK’da yer alan benzer suçlarla karşılaştırmasını yaparak konunun daha iyi anlaşılmasını amaçladık.

Bu çalışma kapsamında danışmanlığımı üstlenerek tecrübelerini paylaşan değerli hocam Dr. Öğr. Üyesi Selman DURSUN’a teşekkürlerimi sunarım. Lisans döneminden bu yana her konuda yardımcı olan değerli hocam Prof. Dr. Adem SÖZÜER’e de teşekkürü bir çok bilirim.

Hayatım boyunca olduğu gibi bu süreçte de yanımda olan, sevgileri ile bu süreci kolaylaştıran aileme sonsuz teşekkür ederim. Bu süreçte desteklerini her zaman hissettiğim bütün dostlarıma ise teşekkürlerimi sunarım.

İstanbul, 2019

Seda KOÇOĞLU

İÇİNDEKİLER

ÖZ.....	iii
ABSTRACT	iv
ÖNSÖZ.....	v
KISALTMALAR LİSTESİ	xiii
GİRİŞ	1

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMİ VE BİLİŞİM SUÇLARI İLE İLGİLİ KAVRAMLAR İLE HUKUKİ DÜZENLEMELER

I. BİLİŞİM SİSTEMİ İLE İLGİLİ TEMEL KAVRAMLAR.....	5
A. Bilişim	5
B. Bilişim Alanı.....	7
C. Bilişim Sistemi.....	10
D. Bilgisayar	14
1. Bilgisayar Kavramı	14
2. Tarihi Gelişimi.....	18
3. Unsurları.....	20
a. Donanım (Hardware)	20
b. Yazılım (Software).....	22
c. Bilgisayarla Bağlantılı Bazı Tanımlar.....	23
(1) Program	23
(2) Veri.....	23

E. İnternet.....	26
------------------	----

II. BİLİŞİM SUÇU KAVRAMININ ORTAYA ÇIKIŞI VE GELİŞİMİ 30

A. Bilişim Suçu Kavramı.....	30
------------------------------	----

B. Bilişim Suçlarının Tanımı ve Özellikleri.....	36
--	----

C. Bilişim Suçlarının İşlenme Şekilleri (Modus Operandi)	39
--	----

1. Truva Atı (Trojan Horse)	40
2. Salam Tekniği.....	42
3. Ağ Solucanları (Network Worms).....	43
4. Bilişim Virüsleri	44
a. Boot Virüsleri	46
b. File (Dosya) Virüsleri	47
c. Makro/Mail Virüsleri	47
5. İstem Dışı Alınan Elektronik İletiler (Spam)	48
6. Mantık Bombaları (Logic Bombs)	50
7. Çöpe Dalma (Scavenging)	51
8. Gizlice Dinleme (Eavesdropping) – Ağ Koklama (Sniffing)	52
9. Veri (Bilgi) Aldatmacası (Data Diddling).....	52
10. Tarama (Scanning).....	52
11. Süper Darbe (Super Zapping).....	53
12. Gizli Kapılar veya Hile Kapısı (Trap Doors)	54
13. Eş zamansız Saldırıları (Asynchronous Attacks)	54
14. Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme	55
15. Sırtlama veya Yetki Dışı/ Gizlice Girme	56
16. Yerine Geçme (Masquerading)	56
17. Tavşanlar (Rabbits).....	57
18. Bukalemun (Chamelon)	57
19. Casus Yazılımlar (Spyware).....	58

20. Telefon Çeviriciler (Dialers)	59
21. Sahte İleti (Fake/Fault Mail)	59
22. Sazan Avlama/Oltalama (Phishing).....	60
23. Klavye Dinleme Sistemleri (Keyloggers)	61
D. Bilişim Suçlarının Tarihi Gelişimi	62
E. Avrupa Konseyi Siber Suç Sözleşmesi	64
F. Türk Hukukunda Bilişim Sistemine Yönelik Düzenlemeler	69
1. 1989 Tarihli TCK Ön tasarısı	71
2. 3756 Sayılı Kanunla 765 Sayılı TCK'ya Eklenen Düzenleme	72
3. 1997 Tarihli TCK Tasarısı	74
4. 2000 Tarihli TCK Tasarısı	75
5. 2003 Tarihli TCK Tasarısı	77
6. 5237 Sayılı TCK.....	78

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE SUÇLARI

I. BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE SUÇLARI.....	81
A. Kanuni Tanım.....	81
B. Suçlarla Korunan Hukuki Değerler.....	83
C. Suçların Temel Unsurları	90
1. Maddi Unsurlar.....	90
a. Suçların Konusu.....	90
(1) Genel olarak	90
(2) İnternet Oyunlarındaki Özne ve Nesnelerin Durumu	93

b. Fiil	95
c. Netice	98
(1) Bilişim Sistemine Müdahale Suçu	98
i. Bilişim Sisteminin İşleyişini Engellemek.....	98
ii. Bilişim Sisteminin İşleyişini Bozmak.....	104
(2) Bilişim Sistemindeki Verilere Müdahale Suçu	109
i. Verileri Bozmak	110
ii. Verileri Yok Etmek.....	112
iii. Verileri Değiştirmek	116
iv. Verileri Erişilmez Kılmak	118
v. Veri Yerleştirmek	120
vi. Verileri Başka Bir Yere Göndermek.....	121
d. Fail	123
(1) Genel Olarak Bilişim Suçları Bağlamında Fail	123
(2) Suçların Faili.....	127
e. Mağdur	128
(1) Genel Olarak Bilişim Suçları Bağlamında Mağdur	128
(2) Suçların Mağduru.....	130
2. Manevi Unsur	133
3. Hukuka Aykırılık Unsuru.....	135
D. Suçların Nitelikli Unsuru.....	140
E. Suçların Özel Görünüş Biçimleri	145
1. Teşebbüs.....	145
2. İştirak	148
3. İçtima	148
a. Görünüşte İçtima.....	149
b. Zincirleme Suç.....	151
c. Fikri İçtima	153
F. Kusurluluk ve Cezalandırılabilirliğin Diğer Koşulları	158

G. Yaptırım	159
H. Soruşturma ve Kovuşturma	161

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU VE İNCELENEN SUÇLARIN BENZER SUÇLARLA KARŞILAŞTIRILMASI

I. BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU	164
A. Kanuni Tanım.....	164
B. Korunan Hukuki Değerler	167
C. Suçun Unsurları.....	169
1. Maddi Unsurlar	169
a. Suçun Konusu	169
b. Fiil	171
c. Netice	173
d. Fail	176
e. Mağdur	177
2. Manevi Unsurlar	178
3. Hukuka Aykırılık Unsuru.....	180
D. Suçun Nitelikli Unsuru	181
E. Suçun Özel Görünüş Biçimleri.....	181
1. Teşebbüs.....	181
2. İştirak	182
3. İçtima	183

F. Kusurluluk ve Cezalandırılabilirliğin Diğer Koşulları	185
G. Yaptırım.....	186
H. Soruşturma ve Kovuşturma	186
II. SUÇLARIN BENZER SUÇLARLA KARŞILAŞTIRILMASI	188
A. Bilişim Sistemine Girme Suçu Sonucunda Sistemdeki Verilerin Yok Olması veya Değişmesi Suçu.....	188
B. Mala Zarar Verme Suçu.....	189
1. Suçun Konusu.....	189
2. Hareket.....	194
C. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu ...	196
1. Kontör Transferi	198
2. ATM'den Para Çekilmesi veya İnternet Üzerinden Yapılan Havalelerde Durum	200
D. Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu	208
E. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu	216
F. Zimmet Suçu.....	222
G. Kişisel Verilerin Kaydedilmesi Suçu.....	223
H. Güveni Kötüye Kullanma Suçu.....	225
SONUÇ.....	226
KAYNAKÇA.....	234

KISALTMALAR LİSTESİ

a.e.	: Aynı Eser
a.g.e.	: Adı Geçen Eser
a.g.m.	: Adı Geçen Makale
a.g.t.	: Adı Geçen Tez
AKSSS	: Avrupa Konseyi Siber Suç Sözleşmesi
ARPA	: Advanced Reseach Projeckt Agency
Atm	: Automatic Teller Machine
BBS	: Bulletin Board System
Bkz.	: Bakınız
C	: Cilt
CD	: Compact Disc
CD	: Ceza Dairesi
CGK	: Ceza Genel Kurulu
CMK	: Ceza Muhakemesi Kanunu
Çev.	: Çeviren
E.	: Esas
Ed.	: Editör
ENIAC	: Electronic Numerical Integrator and Calculator
FSEK	: Fikir ve Sanat Eserleri Kanunu
HD	: Hukuk Dairesi
HGK	: Hukuk Genel Kurulu
K	: Karar
m.	: Madde
MIT	: Massachusetts Institute of Technology
ÖSYM	: Öğrenci Seçme ve Yerleştirme Merkezi
s.	: Sayfa
S	: Sayı
SBE	: Sosyal Bilimler Enstitüsü

SGK	: Sosyal Sigortalar Kurumu
TAAD	: Türkiye Adalet Akademisi Dergisi
TBBD	: Türkiye Barolar Birlięi Dergisi
TBMM	: Türkiye Büyük Millet Meclisi
TDK	: Türk Dil Kurumu
TCK	: Türk Ceza Kanunu
UYAP	: Ulusal yargı ağı projesi
vb.	: Ve Benzeri
vd.	: Ve Devamı
Y:	: Yıl
YGCK	: Yargıtay Ceza Genel Kurulu

GİRİŞ

Teknolojik gelişmelere bağılı olarak bilişim alanında da yaşanan değışimler hayatın her alanını etkilemiştir. Bilgisayarların ve özellikle en yaygın kullanılan veri iletim ağı olan internetin kullanımının yaygınlaşmasıyla bilişim artık birçok alana hâkim olmaya başlamıştır. Bu süreç hemen hemen her gün yeni bir gelişme ve teknoloji ile insanları tanıştırmaktadır. Öngörülemez yapısı ile teknoloji ilk olarak askeri amaçlarla kullanılmış olsa da günümüzde ekonomik, sosyal ve kişisel hemen hemen her alanda kullanılmaktadır. Bankacılık işlemlerinden ticari alım-satıma sanal da olsa bir topluluğa katılma olanağından güvenlik hizmetine kadar birçok gündelik işlem bu sistemler sayesinde gerçekleştirilmektedir.

Bu süreç, sıradan yazılımların amaçlarını aşarak ortam ve nesne tanıyan yapay zekâlı makineler üretilmesine kadar ilerlemiş bulunmaktadır. İnsanlar artık çok da uzak olmayan bir zamanda mesleklerini yapay zekâlı makinelere kaptırma endişesi duymaktadır. Dış görünüş olarak insanlara da çok benzeyen bu tür robotlar hekim, avukat, aşçı, şoför, hakem, muhasebe uzmanı gibi birçok mesleğin gerektirdiğı bilgi ve beceriye sahip olacak şekilde programlanabilmektedir.

Teknoloji ve bilişim alanındaki ilerlemeler sürerken bu alanlarda suçların işlenebilme olanakları da katlanarak artmış bulunmaktadır. Bu sistemler kullanıldıkça açıkları öğrenilmeye başlanılmış ve kullanıcıları tarafından kötüye kullanımı başlamıştır. Sanal dünyanın gerçek dünyaya göre daha esnek olması, anonimlik, fiziki olmayan yerlerde hareketin gerçekleşebilmesi, sanal iz bırakma endişesinin yaşanmaması, delil ve ispat zorluğu gibi nedenlerle bu suçlar sürekli bir artış göstererek hemen hemen her alandaki işlemlere yayılmıştır.

Bilişim alanında yaşanan gelişmelere bağılı olarak daha önceden düşünülmemiş ve dolayısıyla da mevcut suç tipleri arasında düzenlenmemiş birçok yeni bilişim suçu ortaya çıkmıştır. Bunun yanında bu suçlar, mevcut suç tiplerinde öngörülen fiillerin yeni yöntemlerle işlenmesine de neden olmaktadır.

Bilgisayar kullanımına ve internet erişimine sahip olmak artık temel insan haklarından sayılmaktadır. Her ne kadar kullanıcılar bu suçlara karşı güvenli şifre oluşturma ya da herkese açık internet ağına girmeme gibi önlemler alsın da bu tür önlemler süreci uzatmakta ama sonucu engellememektedir.

Bilişim suçları klasik suçlara göre kendine özgü kavramları ve işleniş biçimleri ile özellik kazanmıştır. Bu nedenle çalışmamız kapsamında ilk olarak ilgili suç tiplerine geçmeden önce bu suçlarla ilgili kavram ve tanım sorunsallarına değinerek bunlar açıklanmaya çalışılacaktır. Özellikle ilgili suç tiplerinin incelenmesinde sıkça karşılaşılabilecek olan bilişim sistemi, veri, bilgisayar, internet kavramları unsurlarına kısaca değinerek açıklanmaya çalışılacaktır. Bilişim suçları karakteristik özelliği gereği bilişim ağlarında işlenebilen bu suçların işleniş tarzları da önem arz etmektedir. Sadece bilişim suçlarına özgü olan bu işleniş biçimleri hakkında geniş bir araştırma yaparak en yaygın olanları kısa da olsa izah edilmeye çalışılmıştır. Devamında bu suçların kanun koyucu tarafından ilk defa düzenlenme çalışmaları ve bu çalışmalar kapsamında hazırlanan ön tasarı ve tasarılar değinerek bu suçların gelişimi hakkında bilgi vermek amaçlanmıştır.

Bilişim suçlarının işleniş tarzı itibarıyla bu suçlar birçok ülkeyi ilgilendirebilmektedir. Kişi aslında bulunmadığı ülkeden başka bir ülkedeymiş gibi hareket ettiği izlenimi vererek üçüncü bir ülkede suç işleyebilmektedir. Bu nedenle bu alanın cezasız kalmaması amacıyla uluslararası işbirliğini gerçekleştirmeye yönelik çalışmalar yapılmıştır. Suçlarla mücadeleyi etkin kılmak için Avrupa Konseyi çeşitli çalışmalar yapmıştır. Sonuç olarak Avrupa Konseyi Siber Suç Sözleşmesi birçok ülke tarafından imzalanmıştır, ülkemizde de 02.05.2014 tarihinden itibaren yürürlüktedir. Sözleşmenin yürürlüğe girmesi ile mevzuat ile sözleşme arasında uyum sağlanması ve uluslararası adli yardımlaşmanın ilerlemesi amaçlanmaktadır.

İkinci bölümde bilişim sistemine müdahale suçu ile bilişim sistemindeki verilere müdahale suçu olmak üzere iki ayrı suç birlikte ama farklılarına dikkat çekerek incelenmiştir. Bu suçlar ile Avrupa Siber Suç Sözleşmesinin 4. maddesinde öngörülen “verilere müdahale” ve 5. maddesinde öngörülen “sistemlere müdahale”

düzenlemelerine paralellik sağlanmaya çalışılmıştır. Bu suçlardan ilki olan sistemin işleyişinin engellenmesi veya bozulması suçu aslında birçok bilişim suçunun da temelini oluşturmaktadır. Özellikle Facebook ve Instagram gibi kullanıcıların paylaştıkları şahsi bilgiler ile gelişen sosyal medya profillerinin kullanıcısı dışında kişilerce giriş şifrelerinin ele geçirilmesi hareketi birçok suça zemin olmaktadır. Sisteme girişin engellenmesi ile suçun serbestçe işlenebileceği özgür alan oluşturulmuş olacaktır.

Veri bilgisayardaki bilginin bilgisayar koduna göre işlenmiş halini oluşturduğundan birçok değeri simgeleyebilmektedir. Bu nedenle verinin dışarıdan gelen müdahalelere karşı korunması gerekmektedir. TCK m. 244/2’de düzenlenen bilişim sistemindeki verilere müdahale suçu ile verinin korunması amaçlanmıştır.

Ayrıca günümüzde internet sadece bireylerin iletişimde kullandığı bir araç olmaktan öteye geçerek bireyin devlet ile iletişimi sağlayan en önemli unsur haline gelmiştir. Hemen hemen tüm kamusal işlemlerin internette gerçekleştiriliyor olması karşısında bu alanın tehlikelere açık olduğu açıktır. Bu durumu öngören kanun koyucu TCK m. 244/3’te ilk iki fıkrada düzenlenen suçların nitelikli haline yer vermiştir. Bir bilişim sistemini işleyişini engelleme veya bozma ya da bir bilişim sistemindeki verileri bozmak, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme fiillerinin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali nitelikli hal olarak kabul edilmiştir.

Üçüncü ve son bölümde TCK m. 244/4 bağlamında bilişim sistemleri kullanılarak haksız çıkar sağlama suçunun unsurları açıklanmaya çalışılmıştır. Bilişim sistemi ve veri kullanılmasıyla maddi ya da manevi haksız kazancın elde edilmesini kanun koyucu korumak istemiştir. Başka bir suç oluşturmaması halinde ifadesi kullanılarak aynı fiile gerçekleştirilebilecek hukuka aykırı yarar elde edilmesi ancak bunun başka bir suç tipinde düzenlenmiş olması halinde bu suç tipinin uygulanmayacağı belirtilmiştir.

Veri ve sistemlerin günümüzde her alanda kullanılması gerçeęi karşısında kanunda birçok suç tipinin nitelikli hali olarak bu sistemlerin kullanılması düzenlenmiştir. Bu nedenle konunun iyi anlaşılması amacıyla incelediğimiz her üç suç tipini de kanundaki benzer suç tipleriyle karşılaştırarak suçların kapsamını açıklamaya çalıştık.



BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMİ VE BİLİŞİM SUÇLARI İLE İLGİLİ KAVRAMLAR İLE HUKUKİ DÜZENLEMELER

I. BİLİŞİM SİSTEMİ İLE İLGİLİ TEMEL KAVRAMLAR

A. Bilişim

Bilişim kelimesi Fransızca “*Informatique*” kelimesinin dilimizdeki karşılığı olup, bu kelime de Fransızca “*information* (bilgi)” ve “*automatique* (otomatik)” kelimelerinin birleşmesinden türemiştir¹.

Bilgi vermek kökeninden gelen informatique kelimesinden ayrılarak Türkçe karşılığı olarak bilgi kökeninden gelen bilişim sözcüğünün kullanılması uygun olmuştur².

Bilişim bilgi toplumuyla birlikte hayatımıza girmiş ve hukuk yaşamımızı şekillendirmiştir. Bilginin üretim faktörü olarak ele alınması hukuki açıdan bilgi temelli ekonominin doğmasına ve buna uygun altyapı ihtiyacını ortaya çıkarmıştır. Bilgi ekonomisi yaratmak için bilgiyi küresel ağlarda dolaşıma sokmak zorunluluğu bulunmaktadır. Bilgi ve iletişim teknolojisinin kullanımı ise küresel bilgi dolaşımında mutlaka kullanılması gereken unsurdur. Avrupa Konseyi Siber Suç Sözleşmesi gibi uluslararası düzenlemelerle bilgi toplumunda bu konularda birlik sağlanması amaçlanmaktadır³.

¹ Olgun Değirmenci, “Bilişim Suçları”, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2002, s. 4. Yılmaz Yazıcıoğlu, “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y:1, S:1, İstanbul, Ocak- Mart 2004, s. 175.

² Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 7. bs., Ankara, Seçkin Yayıncılık, 2018, s. 68.

³ Yasin Beceni, “Bilgi Toplumunda Hukukun Değişen Yüzü”, **Bilişim Hukuku**, Der. Mete Tevettoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 68.

Bilişim kavramı verilerin işlenmesiyle beraber bilgi işlem sonucunun aktarılmasını yani veri iletişimini ifade eder⁴. Bilginin otomasyona tabi tutulması sonucunda işlenmesini; verinin saklanması, değerlendirilmesi, nakledilmesini ve çoğaltılması anlamlarını içermektedir⁵.

Bilişim kavramını insanların hemen hemen her alandaki iletişiminde kullandığı bilginin, düzenli bir biçimde işlenmesi, her türden düşünsel sürecin yeniden üretilmesi, bilginin depolanması ve kullanıcıların erişimine açık bulundurulması bilimi olarak tanımlamak mümkündür⁶.

Bilişimin kökenini matematik, fizik ve elektroteknik oluşturur. Bilişim mühendisliği, verileri aktarabilen, depolayabilen ve işleyebilen makineler tasarlamaktadır. Bilişim, diğer bilimlerdeki olguları soyutlaştırıp algoritmalar yardımıyla işlemekte, gerçek süreçlerin simülasyonunu mümkün kılmaktadır⁷.

Doktrinde yapılan tanımlamalar genellikle “*bilginin işlenmesi, aktarılması, depolanması*” noktaları üzerinde durmaktadır⁸. Günümüzde bilişim, belgelemenin yerini alan ve hayatın her alanına giren bilgisayar ve ona bağlı sistemlerle bilginin işlenmesi yerine kullanılan bir kavramdır. Hem verilerin işlenmesini, yani bilgi işlemini hem de bilgi işleminin sonucunun aktarılmasını yani veri iletişimini ifade etmektedir⁹.

⁴ İsmail Ergün, **Siber Suçların Cezalandırılması ve Türkiye’deki Durum**, Ankara, Adalet Yayınevi, 2008, s. 10.

⁵ Yazıcıoğlu, “2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, s. 175; Emin Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yayınları, 1992, s. 3; Faruk Aşıcıoğlu/ Murat Nihat Arslan/ Semih Dokurer, **Meraklılar ve Hevesliler İçin Adli Bilimler**, İstanbul, Türkiye İş Bankası Yayınları, 2012, s. 56.

⁶ Dülger, **a.g.e.**, s. 70.

⁷ Veli Özer Özbek, “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. IX, Özel Sayı, İzmir, 2007, s. 1023.

⁸ Değirmenci, **a.g.t.**, s. 5; Cevat Özel, “Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 342.

⁹ Berrin Akbulut, **Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2017, s. 13.

Bilişim ile ilgili kavram karmaşası, İngilizce “data” ve “information” kelimelerinin Türkçeye “bilgi” olarak çevrilmesinden kaynaklanmaktadır. Aslında bilgi işlem kavramı ile kastedilen veridir ve veri bilgi ile karıştırılmaktadır¹⁰.

Bilişim teknolojisi ise bilgi ve iletişim teknolojileri alanındaki bütün unsurları kapsayan genel bir ifadedir. Bu teknolojinin vücut bulduğu merkez bilgisayar olsa da artık bu teknolojiyi bilgisayarla sınırlamak doğru olmaz¹¹.

Sonuç olarak bilişim; verinin otomatik olarak işlenmesi, saklanması, tasnif edilmesi, terkibi ve aktarılması ile ilgili bilim dalı olarak tanımlanabilir¹².

B. Bilişim Alanı

Bilişim alanı kavramını izah etmeye öncelikle Türk Hukuku’nda bu kavramın hangi aşamalardan geçerek ve ne şekilde tanımlandığı ile başlamak uygun olacaktır. Bilişim alanı kavramına ilişkin ilk tanımlama girişimi, 1989 tarihli Türk Ceza Kanunu Ön Tasarısı’nda yer almaktadır. 1989 tarihli Türk Ceza Kanunu Ön Tasarısı’nda “bilişim alanı” 342. maddenin gerekçesinde “*bilgileri toplayıp depo ettikten sonra bunları otomatik olarak işleme tabi tutma sistemlerinden oluşan alan...*” olarak tanımlanmıştır¹³.

Türk kanun koyucusu, Fransız Ceza Kanunu Projesinden etkilenecek, 6 Haziran 1991 tarih ve 3756 sayılı Kanun ile 765 sayılı Türk Ceza Kanunu’na “Bilişim Alanında Suçlar” başlığı altında on birinci bap olarak 525/a, 525/b, 525/c ve 525/d maddelerini eklemiştir¹⁴.

¹⁰ Değirmenci, **a.g.t.**, s. 7.

¹¹ Hatice Akıncı/ A. Emre Kılıç/ Cüneyd Er, “Türk Ceza Kanunu ve Bilişim Suçları”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s.163.

¹² Değirmenci, **a.g.t.**, s. 7; Levent Kurt, **Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin Yayıncılık, 2005, s.25.

¹³ Değirmenci, **a.g.t.**, s. 6; Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, İstanbul, Alfa Yayınevi, 1997, s. 130.

¹⁴ Değirmenci, **a.g.t.**, s. 53.

“Bilişim Alanında Suçlar” başlıklı on birinci bapta suçları tanımlarken bilgileri otomatik işleme tabi tutan sistem kavramı kullanılmıştır. Bu kavram ile ne kastedildiği açık değildir. Ancak 1991 değişikliğinin gerekçesinde bu kavramın yanında parantez içinde bilgisayar kelimesine yer verilerek kavram açıklanmaya çalışılmıştır. Bilgileri otomatik işleme tabi tutan sistem kavramının içine bilgisayar girmekle beraber, bunu bilgisayarla sınırlandırmak doğru olmaz. Bu kavramın içine, verinin yerleştirildiği, işlendiği, saklandığı ve iletildiği her türlü bilişim sistemini oluşturan aygıtın girdiğini kabul etmek gerekir¹⁵. Esasında bu ibareden yalnızca bilgisayar kavramını değil, bilgisayarın da içerisinde yer aldığı tüm bilişim sistemini anlamak gerekir¹⁶. Bu kavramın içine verilerin manuel veya otomatik olarak girildiği, saklandığı, otomatik olarak işlendiği ve iletildiği her türlü cihazın girmesi gerekmektedir. Bilgisayar kavramı yerine bu ibareye kanun koyucu tarafından yer verilmesi de bunu doğrular niteliktedir¹⁷. Keza banka ve kredi kartları ile para çekilen ATM makineleri bu kavram içinde kabul edilmiştir¹⁸. Bilgileri otomatik işleme tabi tutan sistem ifadesiyle sadece bilgisayarların değil, diğer bilişim cihazları da kanun kapsamına alınmış olunduğunu savunmak, genişletici yorum yapılması değil, aksine mevcut durumun ortaya konulmasıdır¹⁹.

Bilişim alanı 1997 tarihli Türk Ceza Kanunu Tasarısı’nın dokuzuncu bölümde yer alan “Bilişim Alanında Suçlar” başlığı altındaki 347. maddenin gerekçesinde *“Bilişim alanından maksat verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma imkânı veren manyetik sistemelerdir.”* şeklinde tanımlanmaktadır²⁰.

¹⁵ A.e., s. 168-169; Yazıcıoğlu, a.g.e., s. 224.

¹⁶ Ali Karagülmez, **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, 5. bs., Ankara, Seçkin Yayıncılık, 2014, s. 48.

¹⁷ Caner Yenidünya/Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2003, s. 45.

¹⁸ Sinan Esen, **Malvarlığına Karşı Suçlar Belgede Sahtecilik ve Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2007, s. 623.

¹⁹ Akıncı/Alıç/Er, a.g.m., s. 172.

²⁰ Değirmenci, a.g.t., s. 6.

2000 tarihli Türk Ceza Kanunu Tasarısı'nda ise bilişim alanı kavramı tasarının ikinci kısmının dokuzuncu bölümünde düzenlenen 346. maddenin gerekçesinde, yukarıda bahsedilen 1997 tasarısına benzer şekilde “*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler*” olarak tanımlanmıştır²¹. Bu tanımın bilişim alanını tanımlamaktan uzak olması ve aslında bilişim alanını değil de bilgisayarı tanımlanıyor olması bakımından yetersiz olduğunu savunan görüş de bulunmaktadır. Bu görüşe göre, bilgisayarın mutlaka manyetik olması gerekmediği gibi sadece manyetik özellikli bilgisayarları kapsam içine alma riski bu tanımla oluşmaktadır²².

1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı ve 26.09.2014 tarihli TCK'nın 245. maddesinin gerekçesinde “*bilgileri otomatik işleme tabi tutan sistem*” yerine bu tür araçlarla işlenen suçları da kapsayabilmesi ve teknolojinin ilerlemelere açık olması nedeniyle “*bilişim sistemi*” tabiri tasarı ve alt yapı komisyonundaki şekliyle kullanılmıştır²³.

Tezimizin konusunu oluşturan suç tiplerinin de içinde bulunduğu 5237 sayılı TCK'nın topluma karşı suçlar başlıklı üçüncü kısmının onuncu bölümü “Bilişim Alanında Suçlar” başlığını taşıdığından kavramın açıklanması gerekmektedir.

Bilişim alanı, verilerin işlenmesini, saklanmasını, işlenilen verilerin aktarılmasını ve bunların teknolojilerini ifade eder. İletişim ve bilgisayarlar dâhil bütün teknolojileri içine alan bir kavramdır. Bu kavram bilgisayarı da içine alan bir üst kavram olduğundan bilgisayardaki verilere veya bilgisayara karşı işlenen fiiller bilişim alanı kapsamına dâhil olduğu gibi verilerin aktarılmasını sağlayan cihazlardaki ve

²¹ A.e., s. 7; Sulhi Dönmezer, **Kişilere ve Mala Karşı Cürümler**, 17. bs., İstanbul, Beta Yayınları, 2004, s. 626.

²² Yazıcıoğlu, “2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, s. 175; Yavuz Erdoğan, **Türk Ceza Kanunu'nda Bilişim Suçları(Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile)**, İstanbul, Legal Yayıncılık, 2012, s.11.

²³ Kurt, **a.g.e.**, s. 26; Mehmet Burak Kızıltan, “5237 Sayılı TCK'da Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları”, İstanbul Üniversitesi SBE Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2007, s. 4.

sistemlerdeki verilere karşı gerçekleştirilen ihlaller de bilişim suçu kavramı içerisine girmektedir²⁴.

Bilişim alanını; verileri toplama, depo etme, tasnif etme, otomatik işleme tabi tutma özelliklerine sahip elektronik sistem ve sistemler ile bunları tamamlayıcı cihazlardan oluşan alanla beraber bu sistemleri birbirine iletişim unsurları aracılığıyla bağlanmasından oluşan dev ağın bütününe oluşturduğu alan olarak tanımlamak gerekir. Bilişim alanının unsurları olarak temelde bilgisayar ve interneti sayabiliriz²⁵.

Bir fiilin bilişim suçu oluşturup oluşturmayacağının tespiti açısından alanın tespiti çok önemlidir. Bu alan bilgisayar sistemi ile mi temellendirilmelidir yoksa o bilgisayar o fiilde sadece bir yardımcı unsur olarak mı vardır sorusunun cevaplanması gerekmektedir. Bilgisayar sistemleri bir kısım faaliyetlerde ve bunların çeşitli aşamalarında kullanılmakta ise de bunların gerçekleşmesi bilişim temelli değilse bu alan bilişim alanı olarak kabul edilmeyecek ve bu alanda gerçekleşen fiiller de bilişim suçuna sebebiyet vermeyecektir²⁶. Dolayısıyla bilişim alanı sadece bazı bilgisayar suçlarını değil bununla beraber bilgisayar şebekelerinde ve/veya onlara karşı işlenen suçları da kapsayan bir niteliktedir²⁷.

C. Bilişim Sistemi

Teknolojik gelişmelerin sürekli ve çok hızlı biçimde değişmesi karşısında bilişim sisteminin tanımlaması kavramın kısıtlanmasına neden olabilirse de bilişim sisteminin çoğu bilgi işlem faaliyetinin temeli olması dolayısıyla özelliklerini açıklamaya çalıştık.

Bilişim sistemi kavramı dar anlamıyla ele alınıp sadece bilgisayar veya internet gibi sistemlere indirgenmeden bu sistemler de dâhil olmak üzere bir bütün olarak ele

²⁴ Akbulut, **a.g.e.**, s. 110.

²⁵ Kurt, **a.g.e.**, s. 26-27; Akıncı/Alıç/Er, **a.g.m.**, s. 170.

²⁶ Kurt, **a.g.e.**, s. 26.

²⁷ Yazıcıoğlu, “2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, s. 175.

alınmalıdır²⁸. Bilişim sistemi, bilgisayarla kısıtlı olmayan aynı zamanda verinin işlenmesi, depolanması, kullanılması ve nakledilmesi şeklinde ortaya çıkan bir bütündür²⁹. Günümüzde teknolojiye sürekli ilerleme göz önüne alınarak, bilişim sistemini her somut olayın özelliğine göre değerlendirmek daha isabetlidir.

Sadece teknolojinin getirdiği büyük bir yenilik olmak veya elektronik özelliklere sahip bulunmak bir cihazı bilişim cihazı yapmamaktadır. Bu cihazın aynı zamanda bilişim ağıyla iletişim kurması yani iletilen, alınan, işlenen verilerin olması gerekmektedir³⁰.

Veri depolama, işleme, kullanma, nakletme sürecini oluşturan ve bir bilişim sisteminde bu hizmetin gerçekleşmesini sağlayan cihazların bilişim sisteminin bir kısmı olarak kabul edilip edilmeyeceğinin tartışılması gerekmektedir. Modem, ATM cihazı, post işlem makinelerinin durumunu bu açıdan değerlendirmek gerekmektedir. Bu tür cihazlar, bilgisayar özellikleri taşıyan yani çok amaçlı işlem yapabilme özelliğine sahip olan bir sisteme bağlı olarak çalışıyorsa bunları bilişim sisteminin bir parçası olarak görmek gerekir. Bilişim sisteminin en önemli özelliği genel amaçlı kullanım özelliğidir. Belli bir işin yapılmasına özgülenip başka bir fonksiyon ifa etmeyen sistem bilişim sistemi değildir. Mesela otomatik çamaşır makinesi, dalış bilgisayarları, spor aletlerindeki bilgisayarlar, elektronik ev aletleri, televizyonlar bilişim sistemi özelliğine sahip değildir. Şifreli yayınların şifresini çözerek görüntü ve sesi normal yayın haline getiren dekoder cihazı sadece belirli bir işlem yapmak üzere imal edildiğinden, genel amaçlı işlem yapabilme özelliği bulunmadığından, bilişim sistemi olarak kabul edilmezler³¹. Bu husus özellikle belirli fonksiyonları yerine getirmesi için mikro çiplerin yerleştirildiği araçlar bakımından özellik gösterir. Bu tür

²⁸ Veli Özer Özbek/Koray Doğan/Pınar Bacaksız/İlker Tepe, **Türk Ceza Hukuku Özel Hükümler**, 13. bs., Ankara, Seçkin Yayıncılık, 2018, s. 968.

²⁹ Mesih Gözüşirin, “5237 Sayılı Türk Ceza Kanunu’nda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi”, Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Ankara, 2011, s. 5.

³⁰ Akıncı/Alıç/Er, **a.g.m.**, s. 259.

³¹ Kurt, **a.g.e.**, s. 142; Yazıcıoğlu, “2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, s. 176.

araçlarda genel olarak bilginin işlenmesi yerine, belirli işlemlerin otomatik olarak yapılması esas olduğundan bunlar bilişim sistemi sayılmazlar³².

İçinde hangi malzemenin bulunduğunu haber veren ve ihtiyaca göre internet sitelerinden ihtiyaç olan malzemeleri sipariş eden buzdolabı, sebzeyi besin değerini kaybetmeyeceği sıcaklıklara göre pişiren fırın, kumaşların cinsini fark ederek ısını ona göre ayarlayan ütü ilerleyen yıllarda yaygınlaşacak ürünlerdendir. Bu cihazlar, bir kısım manyetik devreler ve programların eklenmesiyle bu hale gelen cihazlardır. Bu cihazlar bilgisayara ilişkin bir kısım özellikler gösterebilir de genel amaçlı işlem yapamadıklarından yani sadece kendi hafızalarına yüklenmiş bir veya iki program çerçevesinden hareket ettiklerinden bilişim sistemi sayılmazlar. Oysa bilişim sistemi, uygun programlar yüklenmesiyle beste yapmaktan en karışık mimari hesapların yapılmasına kadar birçok farklı işlem yapabilme özelliğine sahiptir³³.

Bilişimin temel özelliğinin veri işleme, depolama ve veri iletişimi olduğunu kabul eden görüş, bilişim sisteminin belirlenmesinde genel amaçlı kullanım unsurunun kriter olarak kabul edilmesini kabul etmez. Buna gerekçe olarak da teknolojinin sürekli gelişimi karşısında genel amaçlı kullanımın soyut ve belirsiz bir kavram olmasını göstermektedirler³⁴.

İnternete bağlantı yapabilen cep telefonlarının bilişim sistemi olarak kabul edilebilmesi için bu telefonların bilgisayar özelliklerine sahip olması gerekmektedir. Yani genel amaçlı işlem yapabilme özelliğine sahip bir bilgisayar aynı zamanda cep telefonu ise bunu bilişim sistemi olarak kabul etmek mümkündür. Telefon asıl kullanım amacı bakımından iletişim temelli bir cihaz olmakla beraber bilgileri otomatik olarak işleme tabi tutabilme özelliğinin kazandırılması ile bilişim sistemi sayılabilecektir³⁵.

³² Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008, s. 19; Yazıcıoğlu, **a.g.e.**, s. 216.

³³ Kurt, **a.g.e.**, s. 144.

³⁴ Erdoğan, **a.g.e.**, s. 12.

³⁵ Kurt, **a.g.e.**, s. 143.

5237 sayılı TCK'nın ikinci kitabının üçüncü kısmının onuncu bölümünde bilişim alanında suçlar düzenlenmiştir. 5237 sayılı TCK ile Türk hukuk mevzuatında ilk defa bir kanun metninde bilişim sistemi kavramına yer verilmiştir. Üst kavram olarak da kabul edilebilen bilişim sistemi kavramının içine öncelikle bilgisayar girmekte ise de bunun yanında teknolojinin ilerlemesi ile başka cihazların da ileride bu kavrama dâhil olacağını söyleyebiliriz³⁶.

Bilişim sistemi kavramının kullanılması, veri iletişimi sağlayan tüm araç ve sistemleri kapsayacağından isabetlidir. Bu suretle veri saklanması mümkün olan gelişmiş cep telefonlarına hukuka aykırı erişim fiili de suç olarak düzenlenmiştir³⁷.

Kanun koyucu 243. maddenin gerekçesinde bilişim sistemi kavramını şu şekilde tanımlamıştır; “*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemleri tabi tutma imkânı veren manyetik sistemlerdir.*”³⁸ Bu tanım, bilişim sistemlerinin veriyi saklayan, saklanan veriyi işleyen, değerlendiren, düzenleyen ve aktaran sistemler olduğu açık olarak belirtmediğinden yetersiz kalmaktadır³⁹.

Gerekçedeki tanıma göre bir sistemin bilişim sistemi olarak kabul edilebilmesi için şu üç unsurunun arandığını söyleyebiliriz; verileri gönderebilen, alabilen, depolayabilen bir sistem olması, otomatik işleme tabi tutma özelliğinin bulunması ve manyetik olması⁴⁰.

Avrupa Siber Suç Sözleşmesinde “bilişim sistemi” ifadesi tanımlar kısmında yer almasa da “bilgisayar sistemi”nin tanımı şu şekilde yapılmıştır; “*Herhangi bir cihaz ve birbiriyle bağlantılı bir grup veya cihazlar yoluyla bir veya birden fazla*

³⁶ Kurt, **a.g.e.**, s. 139.

³⁷ Olgun Değirmenci, “2004 Türk Ceza Kanunu’nun Bilişim Suçları Bakımından Değerlendirilmesi”, **TBB Dergisi**, S:58, Mayıs/Haziran 2005, s. 198-199.

³⁸ Kurt, **a.g.e.**, s. 139.

³⁹ Değirmenci, **a.g.m.**, s. 199.

⁴⁰ Kurt, **a.g.e.**, s. 140; Tunç Demircan, **Bilişim Alanında Suçlar**, İstanbul, Legal Yayıncılık, 2016, s. 40.

program tarafından devam ettirilen verinin otomatik olarak işlenmesi, bu işlemin yerine getirilmesi.”⁴¹

28060 sayılı Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkındaki Yönetmelik’in 3. maddesinin ilk fıkrasının b bendinde bilişim sistemi şu şekilde tanımlanmıştır; “*Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi ifade eder.*” Bu tanım bilişim sisteminin bilgisayardan ibaret olmaması sebebiyle isabetsizdir⁴².

Öğretide bilişim sistemi kavramını tanımlamak için kullanılan kriterleri üç başlık altında özetlersek, ilk ölçüt bilgisayarı temel alır, bilgisayar temelli çalışan sistemi bilişim sistemi kabul etmektedir. İkinci ölçüt 765 sayılı TCK’daki yasal düzenlemeden kaynaklanmaktadır. Buna göre sistem eğer bilgileri otomatik işleme koyabiliyor ve işleyebiliyorsa o sistem bilişim sistemidir. Otomatik işleme koymaktan kasıt, sistemin veri gönderip alabilmesi yani manyetik olmasıdır. Son ölçüt ise sistemin belli bir amaç için özgülenmemesi ve genel amaçlı olarak programlanabilmesini sistemin bilişim sistemi kabul edilmesi için gerekli olduğunu belirtmektedir⁴³.

D. Bilgisayar

1. Bilgisayar Kavramı

TCK’da yer alan bilişim suçları ya bilişim sistemlerine karşı ya da bilişim sistemleri aracılığıyla işlenir. Bilişim sisteminin en önemli unsuru olan bilgisayar ise suçların işlenmesinde önemli bir fonksiyona sahiptir⁴⁴.

Gelişen teknoloji karşısında bilgisayarın kalıcı tanımını yapmak güçtür. Doktrinde birçok tanım yapılan bilgisayarın, programlara göre işlem yapma, verilen

⁴¹ Kurt, **a.g.e.**, s. 139.

⁴² Erdoğan, **a.g.e.**, s. 16.

⁴³ Şaban Cankat Taşkın, “Bilişim Hukuku Uluslararası Uyuşmazlıklar”, **TBB Dergisi**, S. 85, 2009, s. 333-334.

⁴⁴ Akbulut, **a.g.e.**, s. 5.

komutlara göre işlem yapma, verileri depolama, verileri işleme tabi tutma, veri iletişimini sağlama, sonuçlar üretme özellikleri olduğunu söyleyebiliriz⁴⁵.

“Elektronik beyin”, “sayısal makine”, “elektronik hesaplayıcı”, “bilgi işlem donanımı”, “matematiksel makine”, “otomatik makine” gibi birçok isimle adlandırılan bilgisayarın kapsayıcı tanımını yapmak gelişen teknoloji nedeniyle zordur. Daha önceden bilgisayar olarak nitelendirilmesi bile düşünilemeyen birçok cihaz artık bu kapsamdadır. Değişik tanımları yapılmakla birlikte bilgisayarı, dış ortamdan çeşitli yöntemlerle aldığı verileri sisteminde bulundurduğu programlar doğrultusunda depolayan, işleyen, bu verilerden yeni sonuçlar üreten ürettiği sonuçları kullanıcıya sunan ve bu suretle veri iletişimini sağlayan makine olarak tanımlamak mümkündür⁴⁶. Kısaca bilgisayar olarak kabul edilebilecek cihazların veri alma, saklama ve gönderme özelliklerinin olduğunu söyleyebiliriz⁴⁷. Bu tanım hem bilgisayarın somut ve soyut unsurlarını birlikte içermesi hem de veri depolama özelliğine işaret etmesi bakımından isabetlidir. Çünkü bilgisayar her türlü veriyi depolama işlevi üstlendiği gibi dijital arşiv olarak da hizmet verebilmektedir⁴⁸.

İngilizcede bilgisayar sözcüğü, “to compute” “hesaplayarak sonuca ulaşma, sayma, toplama, hesaplama, hesap etme” kelimesinden türetilerek “computer” olarak isimlendirilmiştir. Türkçede ise “bilgisayar” sözcüğünün yalnızca hesaplayıcı anlamına gelen nitelendirmeden öte bilgi işlemek kökünden türetilerek “*bilgi saymak, bilgi vermek*” anlamlarına gelmesi dilimiz açısından yerinde bir seçimdir⁴⁹. Bilgisayarlar kendi mantığına göre sisteme yüklenen veriye uygun işlem sonucu veren programlarla donatılmıştır. Yüklenmiş olan işletim sistemi sayesinde girilen verileri düzenler, bilgileri birleştirir, depolar ve aktarırlar⁵⁰.

⁴⁵ Kurt, **a.g.e.**, s. 28.

⁴⁶ Yenidünya/Değirmenci, **a.g.e.**, s. 18-19; Karagülmez, **a.g.e.**, s. 49.

⁴⁷ Erdoğan, **a.g.e.**, s. 24.

⁴⁸ Dülger, **a.g.e.**, s. 61.

⁴⁹ Dülger, **a.g.e.**, s. 59.

⁵⁰ Kurt, **a.g.e.**, s. 29.

Bir bilgisayardan bahsedilmek için bilgisayarda şu özelliklerin bulunması gerektiğini söyleyebiliriz; öncelikle fiziksel bir yapısının yani donanımın olması gerekir. Bilgisayarın diğer özelliği ise verilen bir işi ya da girilen problemi bir program aracılığıyla yapabilmesi ve çözebilmesine yönelik olarak yazılımın unsurunun olmasıdır⁵¹.

Bilgisayar aslında temel olarak bir bilişim sistemidir. Verilerin saklanması, işlenmesi ve iletilmesi bakımından en yaygın kullanılan sistemdir. Bazen öğretilme ve uygulamada aynı anlamda kullanıldıkları görülse de aynı şey değildir, bilişim bilgisayara oranla daha geniş kapsamlıdır⁵². Bu karışıklık bilgisayarın en yaygın bilişim sistemi olmasından kaynaklanmaktadır⁵³.

Bilişimin bilgisayara göre daha kapsayıcı bir kelime olduğunu kabul etmekle beraber bilişimin bir bilim dalı, bilgisayarın ise bu bilim dalının kullandığı araçlardan sadece biri olması nedeniyle karşılaştırmayı uygun bulmayan görüşlere de rastlamak mümkündür⁵⁴.

Bilgisayarların bazı işlevlerini yerine getiren ancak bilgisayar tanımına uymayan akıllı cep telefonları, cep bilgisayarları, kişi ya da araçları elektronik olarak tanıyan güvenlik araçları gibi cihazların bilişim suçlarına konu olması mümkündür⁵⁵.

Bilgisayarı kendisine benzer diğer cihazlardan ayırt edici fonksiyonunun ne olduğu konusunda tam olarak bir netlik bulunmamaktadır. Bilgisayarın işlemini 4-5 temel işleme dayanarak yapması ayırt edici olarak nitelendirilemez zira gelişmiş hesap makineleri de bu özelliğe sahiptir. Programlanabilme özelliği, bilgisayarı diğer elektronik aletlerden ayırt eden önemli bir fark olsa da tek başına yeterli değildir. Zira

⁵¹ Ketizmen, **a.g.e.**, s. 16; Aslı Deniz Helvacıoğlu, “Avrupa Konseyi Siber Suç Sözleşmesi- Temel Hükümlerin İncelenmesi”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 280.

⁵² Ali İhsan Erdağ, “Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S. 2, 2010, s. 278.

⁵³ Aslı Bayındır, “Türk Ceza Kanunu’nda Düzenlenen Bilişim Suçları”, **Suç ve Ceza Hukuku Dergisi**, S. 2, 2010, s. 57.

⁵⁴ Erdoğan, **a.g.e.**, s. 8.

⁵⁵ Dülger, **a.g.e.**, s. 70.

günümüz teknolojilerini içeren buzdolabı, fırın ve çamaşır makinelerinin de bu tür programlanabilme özellikleri vardır⁵⁶.

Bilgisayarı elektronik hesap makineleri, programlanabilir buzdolaplarından ayıran en önemli husus, bilişim yeteneğidir. Bu bilgisayarın belli bir fonksiyonu gerçekleştirmeye yönelik olmaması yani genel amaçlı olması anlamına gelir⁵⁷. Bilgisayar iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıttır⁵⁸.

Bilgisayarı yüklenen programlar aracılığıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen verileri başka yerlere iletmek, başka yerlerdeki verilere ulaşmak gibi amaçlarla kullanılan ve ayrıca depolanmış bir programı işletebilen ve işlem akışı sayesinde sırasını otomatik olarak değiştirebilen aygıtlar olarak da tanımlayabiliriz⁵⁹.

Bilgisayar 1 ve 0 sayısı ile çalışır. Bilgisayar verilen her komutu iki değerli olarak değerlendirir. Bilgisayar verilen komutu “evet” ve “hayır” gibi iki değerli olarak işlem yapmaktadır⁶⁰. Bu ikililerin bir araya gelmesiyle oluşan temel veri birimi olan bitlerdeki açık veya kapalı olma durumlarına göre elektrik akımı devrelerden geçmekte ya da geçmemektedir. Devrelerin açık ya da kapalı olmasının bilgisayar kullanıcısı için anlam ifade ettiği yer devrelerin oluşturduğu yazılar, grafikler, sesler ve görüntülerdir. Aslında çok karmaşık görünen bilgisayarlar elektrik devrelerinin açık ve kapalı olmasına dayalı olarak klasik mantık kurallarına göre çalışan cihazlardır⁶¹.

Çok fazla tanımı yapılan bilgisayarın, bütün fonksiyonlarını belirten bir tanımının yapılması zordur. Hızla gelişen bilgisayar dünyası karşısında yapılan tanım da kısa sürede yetersiz hale gelecektir⁶². Örneğin teknolojik gelişmeler sonucu ortaya

⁵⁶ Yazıcıoğlu, **a.g.e.**, s. 28; Kurt, **a.g.e.**, s. 29.

⁵⁷ Değirmenci, **a.g.t.**, s. 10; Akbulut, **a.g.e.**, s. 10; Yazıcıoğlu, **a.g.e.**, s. 28; Kurt, **a.g.e.**, s. 29.

⁵⁸ Yazıcıoğlu, **a.g.e.**, s. 26.

⁵⁹ Akbulut, **a.g.e.**, s. 10; Yazıcıoğlu, **a.g.e.**, s. 28; Dülger, **a.g.e.**, s. 66,67.

⁶⁰ Yazıcıoğlu, **a.g.e.**, s. 28.

⁶¹ Dülger, **a.g.e.**, s. 67, 68.

⁶² Değirmenci, **a.g.t.**, s. 9.

ıkan akıllı evler olarak da anılan binalardaki telefon yoluyla komuta edilen sistemlere yapılan saldırılarda bu cihazlar bilgisayar olarak kabul edilmektedir⁶³.

2. Tarihi Gelişimi

Bilgisayarın bugünkü teknolojik özelliklerine ulaşması uzun zaman almıştır. Bilgisayarlar hesap makinelerinin üretilmeye başlanması sonrasında hızlı gelişen bir süreçte insan hayatında gittikçe daha çok yer almaya başlamıştır⁶⁴.

İngiliz matematikçi Charles Babbage 1812’de fark makinesi üzerinde çalışmaya başlamıştır. 1871’de bu analitik makine istenilen seviyeye gelemese de Babbage’nin yaptığı hesaplamalar ve çizimler hesap makineleri ve bilgisayarların temelini oluşturmuştur⁶⁵.

Bilgisayarların gelişim dönemi temelde dörde ayrılır; 1940-1958 arası birinci dönem, 1958-1964 arası ikinci dönem, 1965-1971 arası üçüncü dönem ve 1971’den günümüze kadar uzanan dördüncü dönem⁶⁶.

İlk bilgisayar sayılan “ALTAIR 8800”den “ENIAC (Electronic Numerical Integrator and Calculator)” a kadar birçok bilgisayar bu tarihlerde üretilmiştir. ENIAC, 1946’da Philadelphia’daki Pennsylvania Üniversitesi’nde tamamlanıp işlevini gerçekleştiren ilk bilgisayardır⁶⁷.

⁶³ Karagölmez, **a.g.e.**, s. 49.

⁶⁴ Akbulut, **a.g.e.**, s. 5.

⁶⁵ Aysan Şentürk/Neşe Korcuklu/Mustafa Balay, **Bilgisayar Kullanımı ve İnternet**, Bursa, Ekin Kitapevi, 2005, s. 3.

⁶⁶ Yazıcıoğlu, **a.g.e.**, s. 34.

⁶⁷ Daha önce geliştirilen makinelerin aksine bu bilgisayar, hiçbir mekanik parçası olmadan tamamen elektronik unsurlardan oluşmaktadır. Ekranı da olmayan bu bilgisayar beş bin rakamı saniyenin beşte biri kadar zaman diliminde sayabilme özelliğine sahiptir. 30 ton ağırlığında ve 180 metre karelik bir alan üzerine kurulu bu dev cihaz, 18.000 vakum tüpten oluşmaktadır. Çalıştığından fazla ısıttığı için hem pahalı soğutma sistemlerine hem de makinenin yapısını çok iyi bilen uzmanlara ihtiyaç duyulmaktadır. Şu an Washington müzesinde sergilenmekte olan bu cihaz, son kez kullanıldığı 2 Ekim 1955 tarihine kadar başta Amerikan ordusunun topçu bataryalarının hazırlanması, mermi ve bombaların isabetleri, menzil ve hidrojen bombası hesaplamaları olmak üzere birçok üniversite araştırmasında kullanılmıştır.

Yazıcıoğlu, **a.g.e.**, s. 35; Akbulut, **a.g.e.**, s. 6; Aydın, **a.g.e.**, s. 8.

ENIAC'ın üretilmesiyle başlayan ve elektron lambalı bilgisayarlar dönemi adı verilen ilk kuşak bilgisayarlar dönemi elektro-mekanik makinelere göre daha fazla işlem yapabilen, bellek kapasitesinin fazla olduğu bilgisayarların üretildiği dönemdir⁶⁸.

İkinci kuşaktaki bilgisayarların ise en önemli yeniliği programlamaya yenilik getirmeleridir. Bu dönemde, programcının makinenin yapısını bilmek zorunda kalmadan program yapabilmesini sağlayan ve İngilizceye biraz da olsa benzeyen program dilleri ile bilgisayarın donanımı ve bu diller arasında köprü olan işletim sistemi geliştirilerek, kavramsal program dilleri ortaya çıkmıştır⁶⁹.

İkinci kuşak bilgisayarlar döneminde, transistör denilen elektronik devre elemanının ortaya çıkmasından sonra üretilen bilgisayarların dönemini kapsar. İlk transistörlü bilgisayarın üretilmesiyle başlar ve 1964 yılına kadar devam eder. Bu dönemde ilk defa manyetik disk kullanılmış, işlem hızı arttırılmış, bellek kapasitesi yükseltilmiş ve çoklu programlama uygulamaya konulmuştur⁷⁰.

Üçüncü kuşak döneminde ise transistörlerin yerini tümleşik devreler almıştır⁷¹. Üçüncü kuşak dönemi entegre devreler kullanılarak imal edilen bilgisayarlar dönemini ifade etmek amacıyla kullanılmaktadır. Bu dönemde bellek kapasitesi ve hızın artırılması dışında ilk defa mikro bilgisayarlar üretilmektedir. İkinci kuşak döneminde ilk defa ortaya çıkan çoklu kullanımın geliştirilmesi de bir diğer önemli gelişmedir⁷².

Dördüncü kuşak bilgisayarlar döneminde ise mikro işlemcilerin kullanılmaya başlanmasıyla bilgisayarların küçülmesi ve ucuzlaması sağlanmıştır. RAM ve ROM bellek üretilerek yarı iletken ürünler dönemi başlamıştır⁷³. Mikro bilgisayarların

⁶⁸ Akbulut, **a.g.e.**, s. 6; Mustafa Topaloğlu, **Bilişim Hukuku**, Ankara, Karahan Kitapevi, 2005, s. 2.

⁶⁹ 1959 yılında, International Business Machine (IBM) vakum tüpleri- katodik tüpler yerine transistörler kullanmak suretiyle önemli derecede enerji tasarrufu sağlayan ilk bilimsel bilgisayar olan "IBM 7090"ı üretti. Yazıcıoğlu, **a.g.e.**, s. 36.

⁷⁰ Akbulut, **a.g.e.**, s. 7.

⁷¹ Kızıltan, **a.g.t.**, s. 7.

⁷² Akbulut, **a.g.e.**, s. 7.

⁷³ **A.e.**, s. 8.

1980'lerin sonunda pazara girmesiyle kişisel bilgisayarlar geniş kitlelerin kullanımına sunulmuştur⁷⁴.

Bu dönemden günümüze kadar bilgisayarlar insan hayatında gittikçe artan bir konuma sahip olmuştur. Bilgisayar ve internet kullanımının yaygınlaşmasıyla elektronik ticaret mümkün hale gelmiş, e-miting imkânları doğmuş⁷⁵, eğitim, kütüphanecilik, sağlık hizmetlerinde önemli değişiklikler meydana gelmiştir. Ekonomik ve sosyal hayatı değiştiren bilişim teknolojisinin ceza hukukuna da etkisi büyük olmuştur⁷⁶.

Beşinci dönem olarak bireylerin aktif olarak internet sitelerinin yapım süreçlerine katılmalarını, herkesin kendi sitesini yapabilecek hale gelmesini gösterebiliriz. Altıncı dönem olarak mobil cihazların yaygınlaşması suretiyle insanların sürekli olarak interneti kullandığı dönemi, yedinci dönem olarak ise nesnelerin internetini yani insanlara ihtiyaç kalmaksızın nesnelerin birbiriyle iletişimde olacağı dönemi sayabiliriz. Sekizinci dönem olarak ise yapay zekanın geliştiği dönemi şimdilik varsayım olarak söylemek mümkündür. Bu dönemlere tarih verilmemesinin nedeni bunların iç içe geçmiş olmalarından ve halen de gelişmeye devam etmelerinden kaynaklanmaktadır⁷⁷.

3. Unsurları

a. Donanım (Hardware)

Bir bilgisayarın fiziksel kısımlarına verilen genel isimdir. Klavye, fare, ekran, yazıcı, sabit disk, bellek, mikro işlemci, tarayıcı gibi harici parçaları da ifade eder⁷⁸.

⁷⁴ Bilgisayara gösterilen bu ilgi karşısında 1983'te Time dergisi "yılın adamı" olarak bilgisayarı seçti. Yazıcıoğlu, **a.g.e.**, s. 39.

⁷⁵ Türkiye'de ilk e-miting için bkz: <http://www.hurriyet.com.tr/gundem/e-miting-yapacak-40846416> (Çevrimiçi) 20.06.2018.

⁷⁶ Akbulut, **a.g.e.**, s. 25.

⁷⁷ Dülger, **a.g.e.**, s. 91.

⁷⁸ Yazıcıoğlu, **a.g.e.**, s. 31; Karagülmez, **a.g.e.**, s. 50.

Mikro işlemci (merkezi işlem birimi) giriş birimlerinden gelen veriler üzerinde işlemler yapan, yapılan işlemleri denetleyen ve sonuçlarını saklayan, bilgisayarın geçici olarak tüm işlemlerini yapan birimdir⁷⁹.

Rom (read only memory-salt okunur bellek), bilgisayarın temel işlevlerini yerine getirmesi ve açılması için gerekli olan diğer deyişle donanımın çalışma düzenini sağlamak amacıyla programlanan bellektir. Burada bulunan veriler bilgisayarın yapılması sırasında üretici tarafından yerleştirilirler. Salt okunur oldukları için silinmeleri ve değiştirilmeleri söz konusu değildir⁸⁰.

Bilgisayarın bu parçasına herhangi bir kayıt yapmak mümkün olmayıp, bu hafıza sadece okuma işlemi yapan veri kaydedilmeyen birimdir⁸¹. Veri kaydedilmediğinden deformasyona uğramaz⁸².

Ram (random access memory-rastgele erişimli bellek) ise bilgisayara girilen verilerin üzerine yazıldığı, okunabildiği ve saklandığı, üzerindeki verilerin silinebildiği ya da değiştirilebildiği, bilgisayarın üzerinde işlem yaptığı bellektir⁸³.

Giriş birimleri, bilgisayara dışarıdan veri girmek için kullanılan her türlü parçayı içerir⁸⁴. Bilgisayara veri girişinin yapıldığı klavye, tarayıcı, kamera, mikrofon, mouse, CD-ROM gibi unsurlar ile işlenen verilerin sonuçlarının görülebildiği monitör, yazıcı gibi unsurları içerir⁸⁵.

Çıkış birimleri, bilgisayarın verileri işledikten sonra bunları algılayabilecek ve saklayabilecek şekilde manyetik ortama kâğıt üzerinde veya bir ekrana aktaran parçaların tümüne verilen genel addır. Monitör, yazıcı ve hoparlör bunlara örnek verilebilir⁸⁶.

⁷⁹ Kurt, **a.g.e.**, s. 31.

⁸⁰ Dülger, **a.g.e.**, s. 63; Akbulut, **a.g.e.**, s. 8.

⁸¹ Kurt, **a.g.e.**, s. 32.

⁸² Yenidünya/Değirmenci, **a.g.e.**, s. 23.

⁸³ Dülger, **a.g.e.**, s. 63; Akbulut, **a.g.e.**, s. 8.

⁸⁴ Akbulut, **a.g.e.**, s. 11.

⁸⁵ Değirmenci, **a.g.t.**, s. 13.

⁸⁶ Akbulut, **a.g.e.**, s. 11.

Teknolojinin gelişmesiyle eskiden kullanılan bazı giriş çıkış birimlerinin kullanımı da azalmaktadır. Disket ya da disket sürücüsü kullanılmamakta, masaüstü bilgisayarlarda kasa kullanımına az rastlanılmaktadır⁸⁷. Teknolojinin ilerlemesiyle yeni çevre giriş çıkış birimleri de olacaktır. Gözün hareketlerini izleyen sensörler, insan sesini bilgisayara aktaran cihazlar ve beyin dalgalarını bilgisayar komutu haline getiren sistemler bunlara örnek olarak verilebilir⁸⁸.

b. Yazılım (Software)

Bilgisayarın soyut bileşenidir. Her türlü bilgisayar programı, bilgisayar için gerekli olan bütün program parçaları ve yazılım dilleri bu kategoriye girmektedir⁸⁹. Donanımı oluşturan fiziki parçaların ne şekilde çalışacağını belirleyen fiziki olmayan soyut kısımdır⁹⁰. Belirli işlem ya da işlemleri yapmak için bilgisayara kurulurlar⁹¹.

Yazılımlar sistem yazılımı ve uygulama yazılımı olmak üzere ikiye ayrılır:

Sistem (işletim) yazılımı, bulunduğu bilişim sisteminin çalışmasını ve en temel fonksiyonlarını yerine getirmesini sağlamaları nedeniyle sistemin olmazsa olmaz unsurudur⁹². Sistemin çalışmasını ve en temel fonksiyonlarını yerine getirmesini sağladıkları gibi belleğin bir kısmında yerleşik kalarak diğer yazılımların çalışmalarını yönlendirir⁹³. Windows, MacOS veya Linux bunlara örnek olarak verilebilir⁹⁴.

Uygulama yazılımı ise belirli bir fonksiyonu gerçekleştirmek veya herhangi bir problemi çözmek için yazılan ve bilgisayarda kurulu bulunan işletim sistemine uyumlu olarak çalışan program türleridir. Bunlar kullanıcının özel ihtiyacını karşılar ve spesifik işlemler yaparlar. Tablo çizmek, yazı yazmak gibi⁹⁵.

⁸⁷ Dülger, **a.g.e.**, s. 64.

⁸⁸ Gözüşirin, **a.g.t.**, s. 14.

⁸⁹ Yazıcıoğlu, **a.g.e.**, s. 32.

⁹⁰ Kurt, **a.g.e.**, s. 31.

⁹¹ Karagülmez, **a.g.e.**, s. 50.

⁹² Akıncı/Alıç/Er, **a.g.m.**, s. 171; Yenidünya/Değirmenci, **a.g.e.**, s. 23.

⁹³ Akıncı/Alıç/Er, **a.g.m.**, s. 171.

⁹⁴ Akbulut, **a.g.e.**, s. 12.

⁹⁵ Kurt, **a.g.e.**, s. 36; Akıncı/Alıç/Er, **a.g.m.**, s. 172.

Sistem yazılımı üzerinde kullanılmak üzere hazırlanmış ve belirli konulardaki problemlerin çözümüne yönelik olarak yazılmış programlardır. Bilgisayarların özel bir sahada işlem yapmasını sağlarlar. Örnek olarak Microsoft Word, Internet Explorer ve anti virüs programları verilebilir⁹⁶.

c. Bilgisayarla Bağlantılı Bazı Tanımlar

(1) Program

Sistemin soyut unsurlarını oluşturur. Kullanıcı ile makine arasındaki iletişimi sağlar. Kullanıcı programlar aracılığıyla cihazı kontrol edebilmekte, denetleyebilmekte ve yönlendirebilmektedir. Her konuda program yazılabilir, yazılımlar da aslında birer programdır. Verileri işleme ve sonuçları alabilmek veya sisteme belli yöndeki faaliyetleri yaptırabilmek amacıyla ihtiyaç duyulan komutların bütünüdür⁹⁷. Kullanıcı ile sistem arasındaki bağlantıyı sağlayan unsurdur⁹⁸.

Bilgisayara verilen işin yapılması ya da belirli bir algoritmaya göre problemin çözülmesi anlamında bir görevin nasıl yerine getirileceğine ilişkin yönerge olarak da tanımlanabilir⁹⁹.

Bilgileri işleme yeteneği dolayısıyla kendisine özgü bir işlevleri gerçekleştirme olanağı veren seri bilgiler topluluğudur¹⁰⁰.

(2) Veri

Bilişim sisteminde işlenen, depolanan, iletilen, kullanılan temel unsur olarak veri; rakamsal, alfabetik ve simgesel nitelik taşıyan kullanıcı için bir anlam ifade

⁹⁶ Akbulut, **a.g.e.**, s. 12; Kurt, **a.g.e.**, s. 36.

⁹⁷ Değirmenci, **a.g.t.**, s. 169, 170; Kurt, **a.g.e.**, s. 39.

⁹⁸ Yazıcıoğlu, **a.g.e.**, s. 225.

⁹⁹ Ketizmen, **a.g.e.**, s. 16; Yazıcıoğlu, **a.g.e.**, s. 31

¹⁰⁰ Dönmezer, **a.g.e.**, s. 617.

etmese de sistemin anlayabildiği bilgi formatıdır¹⁰¹. Veriler bilgisayarın kendilerine göre çalıştığı bilgilerdir¹⁰².

Veri, bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı olarak sonuçlar üretebildiği, saklayabildiği, sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgi olarak tanımlanabilir¹⁰³. Veri, bilgilerin formata dönüştürülmüş hali, formatlanmış bilgidir¹⁰⁴. Bilginin bilişim alanında kullanılabilecek şekilde işlenmesini ve dolayısıyla bilgileri ulaşılabilir, okunabilir ve işlem yapılabilir hale gelmesini sağlarlar¹⁰⁵.

Veriye ekonomik olma özelliği veren şey, verinin bu ortaya çıkma ve saklanma şeklidir. Görüldüğü üzere veri aslında somut bir şey değildir, sanal bir varlığı ifade eder. Somutlaşması ekrana yansması ya da verinin kağıt üzerine basılması ile gerçekleşir¹⁰⁶.

Veri işlem ise, bilginin işlenmesi, saklanması ve işlenen bilgilere erişilmesi gibi sistematik süreçleri kapsar. Veri işlem teknolojisi verinin içeriğiyle değil, alınması, işlenmesi, saklanması, iletilmesi süreciyle ilgilenir¹⁰⁷.

TCK'nın 243. maddesinin gerekçesinde belirttiği üzere, sistem içerisindeki bütün unsurlar veri niteliğindedir¹⁰⁸. Bir bilişim sistemindeki yazı, resim, program dâhil olmak üzere saklanan her şey veridir¹⁰⁹.

¹⁰¹ Kurt, **a.g.e.**, s. 39.

¹⁰² Dönmezer, **a.g.e.**, s. 617.

¹⁰³ Dülger, **a.g.e.**, s. 79.

¹⁰⁴ Yazıcıoğlu, **a.g.e.**, s. 29, 30; Değirmenci, **a.g.m.**, s. 200.

¹⁰⁵ Andreas Popp, Bilgi Teknolojisi ve Ceza Hukuku, Çev. Hakan Hakeri, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 89; Özgür Uçkan, Yasin Beceni, "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s.389.

¹⁰⁶ Veli Özer Özbek, "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi", **İÜHFİM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 184.

¹⁰⁷ Yazıcıoğlu, **a.g.e.**, s. 30.

¹⁰⁸ Erdağ, **a.g.m.**, s. 290.

¹⁰⁹ Yenidünya/Değirmenci, **a.g.e.**, s. 48; Kurt, **a.g.e.**, s. 37

Veri, bilişim sisteminin bir anlamda yaratılış amacıdır¹¹⁰. Veri işleminin temeli olan veri, bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ifade eder. AKSSS m. 1’de tanımlanan “*bilgisayar verisi*” teriminin, bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dâhil olmak üzere işlenmeye uygun nitelikteki her türlü bilgiyi ifade ettiğini söyleyebiliriz¹¹¹. Bunun kapsamına rakamlar, harfler, virgöl, nokta, noktalı virgöl, tırnak işareti gibi özel işaretler de dâhildir¹¹².

İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik’in 3. maddesinin 1-m bendinde veri “*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*” olarak tanımlanmıştır. Aynı maddenin (b) bendinde bilgi “*verilerin anlam kazanmış biçimi*” olarak tanımlanmıştır.

Kişisel Verilerin Korunması Kanunu’nun 3. maddesinde verilerin işlenmesi; “(Kişisel) verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi” şeklinde tanımlanmıştır. Bugün veri işlem denildiğinde genelde bilgisayar ve ona bağlı sistemlerle yapılan veri işlemi kastedilmektedir¹¹³.

Burada son olarak 765 sayılı TCK’da kullanılan diğer herhangi bir unsur kavramına değinmek gerekir. Kanunun gerekçesinde kanun koyucunun bu kavram ile neyi kastettiğine dair bir açıklama yoktur. Hâkim olan görüşe göre, kanun koyucu bilişim teknolojisindeki gelişmeler sonucunda ileride ortaya çıkabilecek ve ne oldukları şimdiden belli olmayan unsurları da bu madde ile kapsama almak için bu

¹¹⁰ Değirmenci, **a.g.t.**, s. 170.

¹¹¹ Değirmenci, **a.g.m.**, s. 200.

¹¹² Akbulut, **a.g.e.**, s. 14; Helvacıoğlu, **a.g.m.**, s. 281; Sacit Yılmaz, “5237 sayılı TCK’nın 244. Maddesinde Düzenlenen Bilişim Alanında Suçları”, **TBB Dergisi**, 2011, s. 71; Aydın, **a.g.e.**, s. 3.

¹¹³ Akbulut, **a.g.e.**, s. 13, 14.

kavramı kullanmıştır¹¹⁴. Terimlerin özenle seçilmemesi, teknik kelimelerin yeterince bilinmemesi gibi nedenlerle sonuç amacı aşmış durumdadır¹¹⁵.

“*Diğer herhangi bir unsur*” kavramının bilgileri otomatik işleme tabi tutan sistemin donanımına mı yoksa yazılımına mı ait olduğu tartışılmışsa da 5237 sayılı Kanunda hem kanun metninde hem de gerekçesinde bu terime yer verilmemiştir. Ancak 243. maddenin gerekçesinden sistem içerisindeki bütün soyut unsurların fıkra da geçen veri kavramının içinde olduğu belirtilerek açıkta kalan bir husus bırakılmamaya çalışılmıştır¹¹⁶. Dolayısıyla bu terimin sistemin soyut unsuru olan yazılım unsuruna ilişkin olduğunu söyleyebiliriz¹¹⁷. Diğer unsurlar terimi verinin kapsayıcı olması sebebiyle gereksiz kullanılmıştır, sadece veri kelimesinin kullanılması yeterli olacaktır¹¹⁸.

E. İnternet

Bilgisayarların çeşitli yöntemlerle birbirine bağlanabilir hale gelerek bilgisayar ağlarını oluşturmaya başlaması bilişim teknolojisinde devrim yaratmıştır. Fakat önemli olan büyüklü küçüklü ağların kurulması değil bütün bilgisayar ağlarını kapsayan internetin tesis edilmesidir¹¹⁹.

“International” ve “network” kelimelerinin birleşmesinden oluşan internet, dünya üzerinde bulunan bilişim ağlarının ve bilgisayarların birbiri ile bağlantı kurdurularak kendine özgü bir dille iletişimlerinin mümkün kılınmasıdır¹²⁰. İnternet geniş anlamda bilişim sistemi, bilgi ve verileri otomatik olarak işleyen bir sistemleri de kapsayan niteliktedir¹²¹.

¹¹⁴ Değirmenci, **a.g.t.**, s. 171.

¹¹⁵ Yüksel Ersoy, “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”, **Ankara Üniversitesi SBF Dergisi**, C. XLIX, 1994, s. 169, 170.

¹¹⁶ Kurt, **a.g.e.**, s. 144.

¹¹⁷ Yenidünya/Değirmenci, **a.g.e.**, s. 49.

¹¹⁸ Akıncı/Alıç/Er, **a.g.m.**, s. 220.

¹¹⁹ Akıncı/Alıç/Er, **a.g.m.**, s. 166.

¹²⁰ Yenidünya/Değirmenci, **a.g.e.**, s. 36, 37; Değirmenci, **a.g.t.**, s. 23.

¹²¹ Zakir Avşar, Gürsel Öngören, **Bilişim Hukuku**, İstanbul, Türkiye Bankalar Birliği, 2010, s. 30.

Ağ sistemleri içerisinde kullanımı en kolay, en ucuz ve en çok tercih edilen sistem internettir. İnternet, bilgiyi iletmenin yanında teknolojinin ilerlemesine paralel olarak geleneksel usullerle gerçekleştirdiğimiz faaliyetlerin bir kısmını rahatlıkla gerçekleştirilebilen ve daha önce keşfedilmemiş birçok faaliyetin de uygulanabildiği yepyeni bir dünyanın kapılarını açmıştır¹²². Yeni suç tipleri ortaya çıktığı gibi geleneksel suçların yeni teknolojiler aracılığıyla gerçekleştirilmesine de sebebiyet vermiştir. Bu suçların sonuçları klasik suçlar gibi ulusal sınırlar içerisinde kalmamakta, bir virüsün bütün dünyaya yayılması gibi hiçbir coğrafi sınır tanımaksızın tüm insanları etkileyebilmektedir¹²³. Böylesine gelişen internetin kontrol altına alınma ihtiyacı da bununla birlikte gelmiştir. İnternetin belki de en önemli özelliği sınırsız özgürlüğe sahip olunan bu sahanın denetlenmemesi, bir yönetenin olmaması ve belirli bir merkezinin bulunmamasıdır¹²⁴.

Bunun yanında diğer iletişim araçlarından mümkün olmayan yasak bazı faaliyetlerin mümkün olabilmesi internetin diğer yönüdür. İnternet ortamı da “hukukun tanımadığı” veya “hukuk tanımayan” bir alan olamaz. Bu alanın da belirli bir kuralları ve düzeni olmalıdır¹²⁵. Dünya üzerindeki binlerce servis ve erişim sağlayıcının denetlenmesi ciddi bir teknik sorun haline gelmektedir ve bu denetim de oldukça maliyetlidir¹²⁶.

İnternet kullanımı konforlu olsa da bir takım riskler de içermektedir. Örneğin ev kullanıcıları kablosuz erişimlerine parola koymazlarsa aynı erişim noktası üzerinden 253 bilgisayar daha internete ulaşabilmektedir. Burada izinsiz olarak kablosuz erişimi kullanan kişi, internete erişimde başkasına ait olan hesabını ve başkasına tahsis edilmiş IP numarasını kullanmış olacaktır. Bunun sonucunda internet

¹²² Uçkan/Beceni, **a.g.m.**, s. 363.

¹²³ Mahmut Koca, “Avrupa Konseyi Siber Suç Sözleşmesi’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku”, **Bilgi Toplumunda Hukuk**, Ünal Alptekin’e Armağan, C. III, İstanbul, Beta Yayınları, 2003, s. 785, 786; Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul, Beta Yayınları, 2001, s. 78.

¹²⁴ Kurt, **a.g.e.**, s. 41.

¹²⁵ Veli Özer Özbek, “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. IV, S. 1, 2002, s. 104-105.

¹²⁶ Şaban Cankat Taşkın, **Bilişim Suçları**, İstanbul, Beta Yayınevi, 2008, s. 15.

üzerinde yasa dışı gerçekleştirilecek bir işlemde IP numarası üzerinden takip yapıldığında hesap sahibi ve IP tahsis edilen kişi şüpheli konumuna düşecektir. Bu yolla işlenecek bilişim suçlarında suçlunun tespiti oldukça zor hale geleceği gibi suç ile doğrudan ilgisi olmayan kişilerin de şüpheli konumunda olacağı açıktır¹²⁷.

İnternet uluslararası ağa bağlı bilgisayarlar arasındaki veri aktarımı olup teknik bir araç olmaktan öteye gitmemekle birlikte her geçen gün yaygınlaşması önemini artırmış ve her yönden tartışılan bir kavram haline getirmiştir¹²⁸.

İnternetin kesin tarihçesi bilinmemekle beraber askeri menşeli olduğu bilinmektedir. 1969 yılında mevcut ağların savaş durumunda güvenli olmadığı, bu nedenle büyük bilgisayarların güvenilir bir ağla birbirlerine bağlanması görüşü Amerika Birleşik Devletleri Savunma Bakanlığını harekete geçirmiş ve bakanlık kendisine bağlı ARPA (Advanced Reseach Projeckt Agency- Savunma Departmanı İleri Araştırma Projeleri Kurumu) kuruluşu aracılığıyla ARPANET adlı bilgisayar ağını kurmuştur. Bu ağın kurulmasının nedeni bilgisayarlardan herhangi birinin devre dışı kalma durumunda diğer bilgisayarların işlevlerini yerine getirmeye devam edebilmesidir¹²⁹. Hem ABD’de hem de dünyanın başka yerlerinde diğer şebekelerle bağlı olan bu sisteme bir noktadan giriş yapmak bütün sisteme girmek anlamına gelmektedir¹³⁰.

İnternet ziyaret edilen her web sayfasını internette sürekli bağlı olan bir bilgisayarın içeriğine ulaşmasından başka bir şey değildir. Ağa o an için bağlı bulunan bilgisayarların içeriklerinden karşılıklı olarak faydalanması anlamına gelen bir işleyiş tarzına sahiptir¹³¹.

¹²⁷ Mesut Orta, **Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)**, Ankara, Yetkin Yayınları, 2015, s. 58; Değirmenci, **a.g.t.**, s. 39; Orta, **a.g.e.**, s. 68; İsmet Yiğitbaşı, Fatih Gürsul, “Online Bankacılık Suçlarının İncelenmesi: İstanbul Örneği”, **Enformatik, Toplum ve Hukuk**, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016, s. 185; Avşar/Öngören, **a.g.e.**, s. 35.

¹²⁸ Ketizmen, **a.g.e.**, s. 20; Akıncı/Alıç/Er, **a.g.m.**, s. 167.

¹²⁹ Akbulut, **a.g.e.**, s. 19.

¹³⁰ Paul Mungo, Byran Clough, **Sıfıra Doğru Veri Suçları ve Bilgisayar Dünyası**, İstanbul, İletişim Yayınları, 1999, s. 82.

¹³¹ Kurt, **a.g.e.**, s. 42, 43.

İnternete bağı bir bilgisayar artık dış dünyaya açılmıştır, dünyanın neresinde olursa olsun diğer bir bilgisayara erişebilir hale gelmiştir dolayısıyla hem saldırı yapabilecek hem de saldırıya uğrayabilecek konumdadır. Kullanıcının kendisi işlem yapmamış olsa da başkası bilgisayar ağına girip işlem yapabilir¹³². İnternete bağı bulunduğu sürece hiçbir sistem tamamıyla güvenilir değildir ve yeterince uğraşıldığı takdirde kırılmayacak şifre ya da girilemeyecek sistem yoktur. İnternetin yaygınlaşmasıyla failler için bu fırsat alanı da genişlemiştir¹³³.

İnternetin kısa sayılan tarihine bakıldığında çok hızlı bir ilerlemenin olduğu açıktır. Bu kadar hızlı ilerlemesinin nedeni basit, hızlı, pratik şekilde verilere ulaşma imkânı getirmesi, işlemlerde kolaylık sağlamasıdır. Ekonomiden borsaya, askeri alandan kişilerin sosyal hayatına kadar her alana yayılmış durumdadır¹³⁴.

Günümüz dünyasında artık “temel insan hakları” arasında sayılan internet, iletişimde önemli bir mecra halini almıştır. İnternet üzerinden radyo- televizyon yayıncılığı uydu yayıncılığın önüne geçmiş, kitap, dergi, gazete artık web siteleri üzerinden yayımlanmaya başlanmıştır. İnsanlar Facebook, Twitter, Instagram gibi uygulamalar üzerinden iletişim kurmakta buradaki paylaşımlar küresel etki yaratabilmektedir. İnsanlar artık elektronik bankacılık sistemini kullanmakta, pek çok ülkede devlet hizmetleri büyük ölçüde sanal ortamda sunulmaya başlanmıştır. Ülkemizde e-devlet hizmeti uygulamasına buna örnek olarak verilebilir¹³⁵.

Türkiye’de ilk internet bağlantısı 1994 yılında ODTÜ’de gerçekleştirilmiştir¹³⁶. Bu hat çok uzun bir süre tüm ülkenin tek çıkışı olmuştur. Ege Üniversitesi’nden olan bağlantı 1994 başlarında, Bilkent Üniversite’nden 1995’te, İstanbul Teknik Üniversitesi’nden 1996’da gerçekleştirmiştir¹³⁷.

¹³² Şentürk/Korcuklu/Balay, **a.g.e.**, s. 299.

¹³³ Hasan Sınar, “İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı”, **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni (MHB)**, Yılmaz Altuğ’a Armağan Y:17-18, S. 1-2, 1997- 1998, s. 364.

¹³⁴ Akbulut, **a.g.e.**, s. 21; Kurt, **a.g.e.**, s. 45.

¹³⁵ Aşar/Öngören, **a.g.e.**, s. 13, 14, 15.

¹³⁶ Sınar, “İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı”, s. 364.

¹³⁷ Şentürk/Korcuklu/Balay, **a.g.e.**, s. 299; Orta, **a.g.e.**, s. 61.

Türkiye’de internet çalışmalarını yönlendiren önemli oluşum olarak İnternet Kurulu’nda da bahsetmek gerekir. Bu kurul ana işlevi Ulaştırma ve Alt Yapı Bakanlığı’na danışmanlık olmak üzere, Türkiye’de internetin altyapıdan başlayarak tüm boyutları ile hedeflerini belirlemek, bu hedeflere ulaşmak için gerekli kararların alınması ve uygulanması sürecine danışmanlık yapmak, uygulamada görülen aksaklıkları belirlemek ve giderilmesi için önerilerde bulunmak, uluslararası gelişmeleri yakından izlenmesi amaçları ile oluşturulmuştur. Bu kurumun sadece danışma organı olmaktan çıkarılarak kamusal bir örgütlenme işlevini üstlenmesi daha etkili bir işleyişin başlangıcı olacaktır¹³⁸.

II. BİLİŞİM SUÇU KAVRAMININ ORTAYA ÇIKIŞI VE GELİŞİMİ

A. Bilişim Suçu Kavramı

Bilginin ekonomik bir değer olması ile bilişim sistemi temelli cihazların gerçek hayat içerisinde çok önemli bir paya sahip olması gerçeği birleşince yeni dönem ekonomik, sosyal ve politik hayat bilişim teknolojilerine odaklanmıştır¹³⁹.

Bilişim suçları aslında bilişim teknolojisi olarak enformasyon ya da bilginin işlenmesi aracı olan bilgisayar sistemlerinin ve ayrıca iletişim aracı olarak karşımıza çıkan internetin ceza hukukuna etkisidir¹⁴⁰.

Bilişim sistemlerinde bilgi saklama ortamlarının, kapasitelerinin ve saklanan bilgiye erişim hızının çok yüksek olmasına karşılık bilginin muhafaza etme maliyetlerinin çok düşük olması ve veriler üzerinde genelde ilk bakışta anlaşılmayan iz, silinti ve kazıntı bırakmadan değişiklik yapılabilme imkânının varlığı suç işlenmesini kolaylaştıran etkenlerdendir¹⁴¹. Ayrıca bilgiler çeşitli veri taşıma araçlarına

¹³⁸ Sınar, **a.g.e.**, s. 114, 117.

¹³⁹ Okan Tanşu, “Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 144.

¹⁴⁰ Ketizmen, **a.g.e.**, s. 40-41.

¹⁴¹ Değirmenci, **a.g.t.**, s. 37.

kopyalanarak sistemlerin dışına da çıkarılabilmektedir. Tüm bunlar bilişim sistemlerinde suç nitelikli fiillerin icrasını kolaylaştıran etmenlerdendir¹⁴².

Klasik suçlarda suçun etki alanı sınırlı olup genelde bazı suçlar hariç suçun işlenmesiyle sonuçları dar bir alanda görülmektedir. Oysa bilişim suçlarında işlenen suçun sonuçları kimi zaman tahmin edilemez boyutlara ulaşmaktadır. Bazen ise bilişim suçu işlenip tamamlandıktan sonra suç başka suçlar doğurabilmektedir. Örneğin bir virüs saldırısında fail fiilini tamamladıktan sonra bunun doğurduğu sonuçlar bitmez, virüsler başka bilgisayarlara da hızlıca yayılabilme özelliğine sahiptir. Bu durum klasik suçlar ile bilişim suçlar arasındaki farkların en önemlisidir¹⁴³.

Bilgisayar suçları, bilişim suçları, internet suçları, siber suç, elektronik suç, dijital suç, ileri teknoloji suçları, siber uzay ortamında siber uzay aracılığıyla işlenen suçlar, bilişim sistemi aracılığıyla işlenen suçlar olmak üzere Türk hukukunda birçok kavram kullanılmaktadır¹⁴⁴.

Birçok farklı terimin kullanılması, “bilişim suçları” kavramı ile “bilgisayar suçları” kavramlarının birbirinin yerine kullanılmasından kaynaklanmaktadır. Bilişim, bilgisayara göre daha geniş bir kavramdır. Bu nedenle bilişim suçu bilgisayarı da kapsayan ancak daha geniş bir alanda bilişim sistemlerine karşı veya bilişim sistemleri ile işlenen suçları ifade etmek için kullanılmıştır. Bilgisayar programlara göre verileri otomatik işleme tabi tutan sistemlere verilen adken, bilişim ise bilgisayar da kullanılmak suretiyle bilginin saklanması, iletilmesi, işlenerek kullanılır hale gelmesini konu alan disipline verilen addır¹⁴⁵.

Günümüzde bilgisayar olarak nitelendirilemeyecek ancak bilişim aracı olarak kabul edilmesinde sakınca görülmeyen makineler hayatımıza girmeye başlamıştır. Örneğin üzerindeki web paneli sayesinde internete bağlanarak malzeme siparişi veren

¹⁴² Değirmenci, **a.g.t.**, s. 38; Karagülmez, **a.g.e.**, s. 60.

¹⁴³ Karagülmez, **a.g.e.**, s. 79.

¹⁴⁴ Akbulut, **a.g.e.**, s. 56.

¹⁴⁵ Yazıcıoğlu, **a.g.e.**, s. 131.

bir buzdolabı bilgisayar olarak kabul edilmediği halde geniş anlamda veri iletişimi yaptığından dolayı bilişim aracı olarak kabul edilir ve bilişim suçlarının konusunu oluşturmaktadır¹⁴⁶.

765 sayılı TCK’da yer alan “bilgileri otomatik işleme tabi tutan sistem” yerine 5237 sayılı TCK’da “bilişim sistemi” ifadesinin kullanılmış olması karşısında bu iki ifadenin birbirini karşılayıp karşılamadığını incelemek gerekir. Daha önce de belirttiğimiz gibi kanunun gerekçesinde bilişim sistemi “*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemlerdir*” şeklinde tanımlanmıştır. Bu tanımın 765 sayılı TCK’da bulunan tanımdan farkı, verilerin toplanıp yerleştirilmesi ve sistemin manyetik olması noktalarındadır. TDK’de manyetik kelimesi “*Yüzeyine manyetik kayıt yoluyla bilginin depolanabildiği mıknatıslanabilir kaplaması olan plak şekilli tabaka*”¹⁴⁷ olarak tanımlanmaktadır. Madde gerekçesindeki bu manyetik olma özelliği bilişim sistemi kavramını sınırlamaktadır. Böylece madde gerekçesi esas alındığında, manyetik olmayan fakat tanımda yer verilen diğer işlemleri yapabilen bir sistem bilişim sistemi kavramı kapsamında değerlendirilmemiş olacaktır¹⁴⁸.

Bu tanım yetersiz ve muğlak bir tanımdır. Tanımda bilişim sisteminin manyetik bir sistem olduğu belirtilse de manyetik olmayan bir sistemin bilişim sistemi olmasını imkânsızlaştırmıştır. Ayrıca tanımdaki bir başka sorun ise “verileri toplayıp yerleştirme” fiiline ilişkindir. Burada verileri kimin toplayacağı ve nereye yerleştireceği hususları muğlaktır. Gerekçe kanun metninden sayılmadığı için bağlayıcılığı olmasa da gerekçenin yorum aracı olduğu düşünüldüğünde bu tanımın yanlış uygulamalara sebebiyet vereceği açıktır¹⁴⁹. Bu nedenle gerekçede yer alan bilişim sistemini manyetik olma unsurunun ise zorunlu bir unsur olarak kabul edilmemesi gerekmektedir¹⁵⁰.

¹⁴⁶ Değirmenci, **a.g.t.**, s. 54.

¹⁴⁷ http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5cb9cb614006d3.66854511 (Çevrimiçi) 19.04.2019.

¹⁴⁸ Ketizmen, **a.g.e.**, s. 18.

¹⁴⁹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 968.

¹⁵⁰ Ketizmen, **a.g.e.**, s. 19.

Bütün bunlara rağmen bilişim araçlarının en yaygın olanının bilgisayar olması dolayısıyla yanlış da olsa bilgisayar suçları tabiri kullanılmaya devam edilmiştir. Bu tabirle bilgisayarın yer aldığı ve birimlerine karşı işlenen veya sistemlerin araç edinilmesi suretiyle gerçekleştirilen fiiller kast edilmiştir. Bilgisayar suçlarından bahsedebilmek için mutlaka bir bilgisayarın bulunması gerekmemektedir¹⁵¹. Bilgisayar suçu deyimini kullananlar, bilişim araçlarının en yaygın olanının bilgisayarlar olması ve diğer bilişim araçlarının da bilgisayar esasına dayanması sebebiyle bu kavramın kullanılması gerektiğini savunmaktadırlar¹⁵².

Bilgisayar suçu ile bilişim suçu tanımlarında birbiriyle benzerlikler bulunmaktadır. ABD’de bilgisayar suçları ile ilgili ilk düzenlemeler yapıldığı sırada internet ve iletişim yaygın olmadığından özellikle bu ülkenin mevzuatından etkilenen diğer ülke mevzuatlarında bu iki kavramın birbiri yerine kullandığı görülmektedir¹⁵³.

Bilişim suçu kavramı sanal ortamda meydana gelen hak ihlallerini anlatmak için türetilmiş bir kavramdır¹⁵⁴.

Bilişim suçu, bilgisayar kullanılarak işlenen klasik suçları da kapsamaktadır¹⁵⁵. Bilişim alanında bilgisayar suçlarının dışında da suçların işlenmesi mümkündür. Bilişim alanında bilgisayar suçu işlenebilecek suç kategorilerinden sadece biridir. Teknolojik gelişmeler karşısında daha farklı kategorilerin ortaya çıkması mümkündür. Bilişim alanının internet ayağı da bulunmaktadır. Bütün ağ suçları ya da internet suçları ya da siber suç özelliği gösteren fiillerin tamamı aynı zamanda bir bilgisayar suçu değildir. Bu kategorilerin tamamı aslında bilişim suçu üst başlığı altında toplanmaktadır¹⁵⁶.

¹⁵¹ Yazıcıoğlu, **a.g.e.**, s. 133.

¹⁵² Ersoy, **a.g.m.**, s. 151.

¹⁵³ Kurt, **a.g.e.**, s. 52.

¹⁵⁴ İnci Bıçkın, “Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları”, **Yargıtay Dergisi**, C. XXXII, S. 1-2, Ocak- Nisan 2006, s.150.

¹⁵⁵ Karagülmez, **a.g.e.**, s. 54.

¹⁵⁶ Kurt, **a.g.e.**, s. 52, 143; Erdoğan, **a.g.e.**, s. 45.

Bilişim suçları siber suçlar kavramına göre üst kavramdır, siber suçları da içine almaktadır¹⁵⁷. Dar anlamdan siber suçlar bilgisayar suçları olarak ifade edilmektedir. Bu suçlarla, bilgisayar sisteminin güvenliğine veya veri işlemine karşı işlenen fiiller kastedilmektedir. Bu kategoriye giren suçlar ikincil nitelikte olan ve belirtilen suçlara hazırlık niteliği taşıyan fiilleri içermektedir. Geniş anlamda siber suçlar ise, ceza kanunlarında var olan klasik suçların yeni teknolojilerle kolaylaştırılması ile bilgisayar bağlantılı suçlar olarak isimlendirilmektedir. Bilgisayar sistemi veya ağı aracılığıyla veya bunlarla ilgili olarak işlenen her türlü yasa dışı davranışları kapsar¹⁵⁸.

Siber uzay kavramı sadece interneti değil, benzer ağ sistemlerini de kapsadığı için internet suçu terimi yerine siber suç terimi de tercih edilebilir. Siber suç; kural olarak - en azından bugün itibarıyla - bilgisayarlar aracılığıyla işlenen ancak siber uzay ortamında yani sanal dünyada gerçekleştirilen suçları ifade etmektedir¹⁵⁹. Her internet suçu bir siber suçtur fakat her siber suç bir internet suçu olmayabilir¹⁶⁰.

Bilgisayar suçluluğu bilgisayar verilerine ilişkin tüm suçları içine alır. Bu kavram, elektronik verilerin işlenmesi ve naklinin söz konusu olduğu bilgisayar ve enformasyon tekniğinin karakteristiğini içermektedir. İnternet suçluluğu ise internette veya internet üzerinden işlenen bilgisayar suçlarıyla sınırlı bir kavramdır.¹⁶¹

Siber suçlar basitçe bilişim sistemleri aleyhine veya bilişim sistemleri aracılığıyla işlenen özellikle internet üzerinden gerçekleştirilen suçlar olarak tanımlanmaktadır¹⁶².

¹⁵⁷ Yenidünya/Değirmenci, **a.g.e.**, s. 33.

¹⁵⁸ Akbulut, **a.g.e.**, s.39-40; Koca, “AKSSS’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku”, s. 788-790; Ergün, **a.g.e.**, s. 16.

¹⁵⁹ Hasan Sınar, “İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı”, s. 356. Aynı görüşte Yener Ünver, “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısı’nın İnternet Açısından Değerlendirilmesi”, **İÜHFİ İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s.79.

¹⁶⁰ Sınar, **a.g.e.**, s. 69.

¹⁶¹ Ulrich Sieber, Bilgisayar Suçluluğu, Çev. Yener Ünver, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 16.

¹⁶² Murat Önok, “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof. Dr. Nur Centel’e Armağan, Özel Seri, C. XIX, S. 2, 2013, s. 1231; Orta, **a.g.e.**, s. 77.

Siber suç kavramının kullanımı son zamanlarda yaygınlaşsa da kelimenin yabancı kökenli olması ve aslında dilimizde bu kavramı karşılayan bilişim suçu kavramının bulunması nedeniyle bu terimin kullanılması gereksizdir¹⁶³.

İleri teknoloji kavramı, daha ileri teknolojilerin her zaman hayatımızda olabileceği ve klasik suçların bilişim araçlarıyla işlenmesini ifade etmekte yetersiz kalması noktalarında eleştirilmektedir. Elektronik suç ise elektronik cihazların yalnızca bilgisayarlar ve bilişim araçlarından ibaret olmaması nedeniyle tercih edilmemektedir¹⁶⁴.

Tüm verilen tanımların bu suçların belli bir özelliğini ortaya koyması açısından yerinde oldukları açıktır. Bilgisayarların ve bilişim araçlarının bu suçlar işlenirken herhangi bir safhada kullanıldıkları görülmektedir. Ancak yine de bilgisayarın suçun işlenmesinde kullanılması, bu suçun bilgisayar suçu olarak kabulüne yeterli olup olmaması tartışılması gereken husustur. Bu kavramın geniş yorumlanması hatalı sonuçlara sebebiyet verebilecek niteliktedir. Örneğin; bir kişinin vücuduna bilgisayarla vurulmak suretiyle zarar verilmesi durumunda da bu suçu bilişim suçu olarak kabul etmek yerinde bir sonuç değildir¹⁶⁵.

Kanımızca terim olarak “Bilişim Suçu” kavramının kullanılması isabetlidir. Suçların intranet gibi internet dışındaki ortamlarda işlenebilmesi ya da akıllı cep telefonu gibi bilgisayar dışındaki vasıtalar ile işlenebilmesi nedenleriyle bu suçlara internet ya da bilgisayar suçları olarak adlandırmak isabetli değildir¹⁶⁶. Diğer kavramlar ise ancak bu genel alanın daha özeldeki kısımlarının sınıflandırma işlev görebilirler¹⁶⁷. Genel olarak hem öğretide hem de yasal düzenlemelerde bilişim suçu kavramının kullanıldığını söyleyebiliriz¹⁶⁸.

¹⁶³ Dülger, **a.g.e.**, s. 74.

¹⁶⁴ Akbulut, **a.g.e.**, s. 59.

¹⁶⁵ Değirmenci, **a.g.t.**, s. 60.

¹⁶⁶ Erdoğan, **a.g.e.**, s. 47; Akbulut, **a.g.e.**, s. 58, 59.

¹⁶⁷ Umut Eker, “Türk Ceza Hukuku’nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 sayılı Yeni Türk Ceza Kanunu’nun İlgili Hükümlerinin Yorumu”, **TBB Dergisi**, 2006, s.105.

¹⁶⁸ Dülger, **a.g.e.**, s. 75.

B. Bilişim Suçlarının Tanımı ve Özellikleri

Doktrinde bilişim suçlarına ilişkin farklı tanımlamalar yer alsa da üzerinde anlaşılmış ortak bir tanım bulunmamaktadır. Suçların işlenmesinde bilişim teknolojisinin kullanılması ortak özellik olsa da bilişim suçlarını klasik suç tiplerinden ayırmak kolay değildir. Bunu yapabilmek için yazarlar çeşitli kriterleri esas almıştır. Yapılan tanımlamalarda ilk olarak bilgisayarla bağlantılı tüm fiiller bilişim suçu olarak değerlendirilmiştir. Ancak zaman içerisinde bilişim suçları konusunda çeşitli ayrımlara gidilmeye başlanmıştır¹⁶⁹.

Bilişim suçlarını klasik suçlardan ayıran temel özellik, bilişim suçlarının verilerle veya veri işlemle ilgisi olmasıdır. Bu suçlar temelde iki şekilde işlenir; ya fail bir bilişim sisteminde bulunan verileri veya ele geçirmeyi amaçladığı diğer bir unsuru hedef alacak ya da suçun işlenmesinde bilişim sistemini araç olarak kullanacaktır. İlk durumda suç bilişim sistemlerine karşı işlenmişken, ikinci durumda suç bilişim sistemleri aracılığıyla işlenmiş sayılır¹⁷⁰.

Bilişim suçlarının kendine has özellikleri bulunmaktadır. İlk olarak bu tip suçları işleyen faillerinin yakalanma riski klasik suçlara nazaran daha azdır. Çünkü çoğu zaman müdahalede bulunan ile müdahale konusu birbirinden farklı mekânlarda bulunduğundan müdahaledeki fiziksel mekânın getirdiği sınırlamalar ortadan kalkmaktadır. İkinci olarak bilişim suçları klasik suçlara nazaran daha az emek, masraf ve riskle işlenebilmesi dolayısıyla suçlar yaygınlaşma tehlikesini içinde barındırmaktadırlar¹⁷¹. Klasik suçlardan farklı olarak bilişim suçlarının sayıları, türleri ve işlenebilme olanakları çok çeşitlilik göstermektedir. Bu tip suçların en belirleyici özelliği, suçun etki alanının ve sonuçlarının hayal sınırlarını zorlayacak ölçüde olabilmesidir¹⁷².

¹⁶⁹ Akbulut, **a.g.e.**, s. 55.

¹⁷⁰ Değirmenci, **a.g.t.**, s. 61.

¹⁷¹ Erdoğan, **a.g.e.**, s. 87 vd.

¹⁷² Karagülmez, **a.g.e.**, s. 63.

Bu suçlar aynı zamanda devamlılık da arz etmektedir. Şöyle ki; sisteme girip yakalanmadan filleri gerçekleştiren fail, tesadüf ya da düzenli kontrollerde yakalanana kadar fiillerine devam etmektedir¹⁷³.

Bu suçların işlenebilmesi için, bilgisayar veya benzeri bir aygıt, enerji kaynağı, ağ bağlantısı ve bunu sağlayan telekomünikasyon hattı gerekmektedir. Bilişim suçlarında hedef, sistemdeki elektronik yapıdır¹⁷⁴.

Bu özellikler dikkate alındığında bilişim suçları geniş anlamda bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her türlü suç olarak tanımlanmaktadır. Dar anlamda ise verilere ve/veya bilişim sistemlerine veya sistemin/verilerin düzgün ve işlevsel işleyişine, güvenliğine ya da bütünlüğüne karşı işlenen suçlar olarak tanımlamak mümkündür¹⁷⁵.

O halde bilişim suçlarını, bilişim sisteminin kendisinin ya da sistemin içerisinde bulunan verilerin hedef alındığı ve bilişim teknolojilerinin kullanılması suretiyle ya da bilişim araçlarına müdahale yoluyla işlenen suçlar olarak tanımlamak mümkündür¹⁷⁶.

Bilişim suçlarını ekonomik suç olarak kabul eden görüş de bulunmaktadır. Bu görüş, bilişim suçlarını tanımlarken bunları malvarlığı suçlarıyla sınırlandırmaktadır. Ayrıca failin bu suçu işleyebilmesi için bilgisayar konusunda bilgi sahibi olması gerektiğini savunduklarından, bu suçları beyaz yaka suçları olarak kabul eden görüş de bulunmaktadır¹⁷⁷. Bu görüşe göre, büyük boyutlu bilişim suçlarının işlenebilmesinde hem teknik altyapıya hem de teknolojik bilgiye ihtiyaç olması ve bunların da faile belirli bir mali külfet gerektirmesi göz önüne alındığında bu suçların ancak belli bir düzeyin üstünde mali güce sahip kişilerce suçların işlenebilmesi

¹⁷³Klaus Tiedemann, “Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi”, Çev. Feridun Yenisey, **İÜHF**, C. XLI, S. 1-4, 1975, s. 324.

¹⁷⁴ Ali Karagülmez, “Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular”, **2. Polis Bilişim Sempozyumu Bildirileri**, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s. 31.

¹⁷⁵Kayihan İçel, “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri”, **İÜHF İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 2; Dülger, **a.g.e.**, s. 77-78; Akbulut, **a.g.e.**, s. 69.

¹⁷⁶ Eker, **a.g.m.**, s. 105; Erdoğan, **a.g.e.**, s. 52; Kurt, **a.g.e.**, s. 53.

¹⁷⁷ Ersoy, **a.g.m.**, s. 167.

gerekmektedir¹⁷⁸. Bu görüşün temelinde 765 sayılı TCK'da suçun oluşması için aranan “başkasına zarar vermek, kendisine veya başkasına yarar sağlama” şeklindeki amacın da bu suçlardaki ekonomik niteliği vurgulaması yatmaktadır. Suçların düzenlendiği yerin ise belirleyici olmamakla beraber, bir anlamının bulunmadığı görüşündedirler¹⁷⁹.

Ekonomik suç olarak kabul eden bu görüşe göre, bu suçlar internet ya da elektronik ortamlarda bilgisayar veri ile sistemlerinin gizlilik, bütünlük, elde edilebilirlik ve erişilebilirliğine karşı fiiller bireysel ya da finansal kazanç veya zarar verme amacıyla yürütülen bilgisayarlarla bağlantılı fiillerin icra edilmesi ile gerçekleşen suçlardır¹⁸⁰.

Beyaz yaka suçlarının güveni ihlal etmesi ve bu nedenle sosyal ahlakı düşüren ve geniş bir ölçekte sosyal düzensizliğe yol açan bir güvensizlik meydana getirmesi yanında bu suç faillerinin meslekleri süresince yüksek sosyal konuma sahip ve itibarlı durumda oldukları göz önüne alındığında¹⁸¹, bilişim suçlarının bu yapıda olmadığı görülecektir.

Bilişim sektörünün bugün geldiği aşamada bilgisayar kullanımı çok yaygınlaşmıştır. Ayrıca bilişim suçu işlemeyi düşünen kişilerin internetteki açıklayıcı bilgiler ve yardımcı yazılımlar sayesinde yeterli bilgi düzeyine kolaylıkla ulaşılacağı göz önüne alındığında bu suçun beyaz yaka suçlar kategorisinden ayrılmaya başladığını söyleyebiliriz¹⁸². Ayrıca bilişim suçu faillerinin amacı her zaman ekonomik nitelikte olmadığından bu açıdan da beyaz yaka suçlarından ayrılmaktadırlar¹⁸³.

¹⁷⁸ Karagülmez, **a.g.e.**, s. 62.

¹⁷⁹ Ersoy, **a.g.m.**, s. 166.

¹⁸⁰ Metin Turan, **Alman Bilişim Hukuku**, Ankara, Adalet Yayınevi, 2017, s. 25.

¹⁸¹ Edwin H. Sutherland, “Beyaz Yaka Suçluluğu”, Çev. Selman Dursun, **Suç Politikası, Karşılaştırması Güncel Ceza Hukuku Serisi**, Prof. Dr. Claus Roxin’e Armağan, Ankara, Seçkin Yayıncılık, 2006, s. 299.

¹⁸² Dülger, **a.g.e.**, s. 125.

¹⁸³ Yazıcıoğlu, **a.g.e.**, s. 231.

Haksız ekonomik çıkar sağlamak için yapılan ve özellikle finans kurumlarına veya bunlarla bağlantılı olarak bireylere yönelik olarak işlenen bilişim suçlarını ekonomik suç olarak nitelendiren görüş bulunmaktadır¹⁸⁴.

Bilişim suçlarının yalnızca malvarlığı suçlarıyla sınırlandırılması yönündeki bu görüş isabetli değildir. Sisteme yetkisiz girişler veya verilerdeki gerçekleştirilen sahtecilik fiilleri örneğinde bu durum gerçekleşmemektedir¹⁸⁵.

Bazı yazarlar ise bu suçları kesin olarak ekonomik suç kategorisi içerisinde değerlendirmemekle beraber söz konusu suçların ekonomik suç niteliği taşıyan fiillerle işlenebileceğini belirtmektedirler. Bu gruba ise haksız olarak kendi lehine başkası aleyhine çıkar temin etme amacıyla işlenen suçların girdiğini öne sürmektedir. Bilgisayarla işlenen güveni kötüye kullanma, dolandırıcılık, hırsızlık gibi suçlar ile bilişim sistemleri kullanılarak haksız çıkar sağlama suçu bu duruma örnek olarak gösterilebilir¹⁸⁶. Söz konusu suçlar kendilerine veya üçüncü kişilere çıkar sağlamak amacıyla başkalarının malvarlığı aleyhine işlenebileceği gibi başka bazı değerlerin ihlali şeklinde de işlenebilmektedir¹⁸⁷.

C. Bilişim Suçlarının İşlenme Şekilleri (Modus Operandi)

Modus operandi, Latince bir terim olup suç işleme metodu anlamına gelmektedir. Bu kavram, bir suçun başarıyla işlenebilme amacına yönelik hareketleri anlatmak için kullanılır¹⁸⁸.

Bu suçların klasik suçlardan ayrılan en büyük özelliği bu suçların işleniş biçiminin diğer suçlara göre farklı olmasıdır. Çok kısa zaman diliminde işlenen bu suçların sonucunda failin arkasında herhangi bir iz bırakmaması suçun işleyişini kolaylaştırmakta ve hareketin tespitini zorlaştırmaktadır¹⁸⁹.

¹⁸⁴ Dülger, **a.g.e.**, s. 134.

¹⁸⁵ Akbulut, **a.g.e.**, s. 70.

¹⁸⁶ Haluk İnanıcı, "Bilişim ve Yazılım Hukuku, Uygulamanın İçinden Görünüşü", **İBD**, C. LXX, S. 7-8-9, 1996, s. 515.

¹⁸⁷ Akbulut, **a.g.e.**, s. 72.

¹⁸⁸ Karagülmez, **a.g.e.**, s. 64.

¹⁸⁹ Değirmenci, **a.g.t.**, s. 75.

Suçlar bilişim sisteminde bulunan soyut unsurlara yönelik olarak işlendiğinden çoğu fiil internet veya diğer ağlar aracılığıyla amaçlanan işi yerine getirmeye yönelik olarak yapılmış programlar aracılığıyla gerçekleşmektedir¹⁹⁰.

İngilizce “malicious software” kelimelerinin kısaltması olan malware yani kötücül yazılım, bulaştığı sisteme zarar vermek veya kullanıcıları rahatsız etmek için tasarlanmıştır, hemen hemen her programlama dilinde yazıldığından birçok dosya içinde de taşınabilmektedir¹⁹¹. Birçok türü olan kötücül yazılımlarının bazılarını aşağıda anlatmaya çalışacağız.

Suçların işleniş şekilleri aşağıda tanımlanacaktır fakat bu tanımlama ve tespit işleminin sınırlayıcı değil örnekleyici şeklinde olduğunu belirtmek gerekir. Bu alan gelişmelerle beraber suçlarla paralel olarak yeni işleniş biçimlerine de açıktır. Bilişim dünyasındaki teknolojik ilerlemeler fiilin işleniş şekillerini değiştirmektedir. Örneğin virüsler 1996 yılı başlarında en çok disketlerle yayılmasına karşılık 1999 yılında en çok e-posta ile yayılmaya başlamıştır¹⁹².

1. Truva Atı (Trojan Horse)

Adını Yunan mitolojisindeki Akhalılar ile Troyalılar arasındaki Truva savaşında kullanılan tahta atın hediye olarak Truvalılara gönderilip, tahta at kalenin içine girdikten sonra atın içine gizlenen Akhalı askerlerinin kaleyi ele geçirmesi olayından alır. Çoğunlukla internet üzerinden ücretsiz indirilen yazılımlardaki sistem dosyaları içine Truva atı yazılımı eklenerek kullanıcılara ulaştırılmaktadır¹⁹³.

Görünüşte yararlı bir işleve sahip olduğu düşünülen ancak bünyesinde bilişim sistemine zarar verecek gizli kod içeren programlardır¹⁹⁴. Bu programların tümü

¹⁹⁰ Akbulut, **a.g.e.**, s. 73.

¹⁹¹ Cemal Aktürk, Tarık Talan, “Mobil Bilişim Suçları”, **Enformatik, Toplum ve Hukuk**, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016, s. 148.

¹⁹² Değirmenci, **a.g.t.**, s. 75.

¹⁹³ Avşar/Öngören, **a.g.e.**, s. 49; Dülger, **a.g.e.**, s. 104.

¹⁹⁴ Değirmenci, **a.g.t.**, s. 79.

zararlı değildir. Ancak yazılım hatası veya kullanıcının dikkat etmemesi durumlarda zararlı etkiler yapacağından kullanıcıların dikkatli olması gerekmektedir¹⁹⁵.

Bilişim sistemine iki şekilde erişim mümkündür. İlk olarak programın daha önceden bilgisayar sisteminde bulunup kullanıcının hiçbir şeyden şüphelenmeden sistemi kullandığı durumlarda söz konusu olabilir. İkinci olarak ise kullanıcı tarafından herkesin kullanımına açık sistemlerin ağlarından kopyalanarak sisteme girilmesi durumunda oluşur. Genelde diğer kullanıcıları cezbettirecek isimler altında bulunduklarından bu programlar kolaylıkla yayılabilmektedir¹⁹⁶.

Truva atı sisteme bulaştıktan sonra sistemin açılmasıyla kendisini belleğe yükler ve sistemin açıklarını kullanarak programı yerleştirenin komutlarını gerçekleştirmeye başlar. Truva atı iki kısımdan oluşur. İlk kısım hedef bilgisayarda çalışan sunumcudur. İkinci kısım ise müdahalede bulunan bilgisayarda çalışan istemci kısımdır. Müdahalede bulunulan hedef bilgisayara yerleştirilen sunumcu programı çok küçüktür. Boyutları küçük olduğundan tespit edilmesi güç olan bu kısım aktif olduğu anda müdahalede bulunan bilgisayarın komutlarını yerine getirmektedir¹⁹⁷.

Truva Atı görevini üstlenecek programın tıpkı efsanede olduğu gibi öncelikle sistemin içine isteyerek alınması gerekmektedir. Sistemin içinde bu görevi yapan programın çalışmasıyla süreç başlar. Fail, bilgisayarda kullanılan programın istediği çalışmayı gerçekleştirmesi için içine gizli bir başka programı yerleştirir. Böylece cihaz kendi işlemlerini yaptıktan sonra, fail tarafından programlandığı şekilde birkaç işlem daha gerçekleştirir. Öncelikle program sistem sahibinin amaçladığı şekilde çalışırken fail tarafından çağrıldığında veya önceden kodlanan direktifler doğrultusunda artık failin istediği şekilde çalışır hale gelmiştir¹⁹⁸.

Bu programlar en yaygın biçimde çok kullanıcıli bilişim sistemlerinin güvenlik önlemlerini aşmak için kullanılır. Kullanıldığı zaman başka bir kişinin sisteme girişine

¹⁹⁵ Akbulut, **a.g.e.**, s. 79.

¹⁹⁶ Değirmenci, **a.g.t.**, s. 79.

¹⁹⁷ **A.e.**

¹⁹⁸ Yazıcıoğlu, **a.g.e.**, s. 153; Kurt, **a.g.e.**, s. 63, 64.

izin verilen kodları müdahalede bulunan sisteme yükler. Mağdur olan sistem kullanıcısı ise uzun süre bunun farkında olmadan sisteme başkasının girişine izin veren bu programı kullanabilir¹⁹⁹.

Truva atı programlarının en önemlileri hedef bilgisayarı yeniden başlatmadan sisteme her türlü müdahale imkânını verip programın bulaştığı bilgisayar üzerindeki aktiviteleri takip eden ve aldığı bilgileri bir e-posta ile istemci bilgisayara gönderen programlardır. Özellikle giriş şifresi öğrenilebilmekte, kredi kartı şifresi gibi önemli bilgileri hedef bilgisayardan alınabilmektedir²⁰⁰.

Truva atının virüslerden farkı kendilerini kopyalayarak çoğaltmama noktasındadır²⁰¹. Truva atları bilgisayar kamerasını açarak kullanıcının görüntüsünü kaydetme, veriyi silme veya değiştirme, bilgisayara uzaktan erişime izin verme, casusluk, e-posta adreslerini toplayarak spam posta gönderme, bilgisayarın veya ağı performansını düşürme gibi zararlı fiilleri gerçekleştirebilirler²⁰².

2. Salam Tekniği

Bu teknik çok fazla sayıda kaynaktan çok az sayıda değerlerin transfer edilmesi şeklinde çalışmaktadır. Aslında tekniğin uygulanmasında Truva atı programı kullanılır. Birçok kaynaktan alınan dikkat çekmeyecek düzeyde değerlerin birleşerek failin hesabına geçirilmesi ile haksız kazanç sağlanması temelinde çalışır²⁰³.

Özellikle bankacılık alanında kullanılan bu yöntemde, bankacılık alanındaki değerlerin çok basamaklı olanlarının uygun basamağa kadar yuvarlanması ile yuvarlama sonucu ortaya çıkan rakamın belli bir hesaba gönderilmesi suretiyle işlenebilmektedir. Bu sayede hesaplara dikkatli şekilde bakılmadıkça ortaya çıkmayan bir azalma meydana gelmektedir. Bir hesap için değersiz görünen değerlerin alternatif

¹⁹⁹ Değirmenci, **a.g.t.**, s. 79.

²⁰⁰ **A.e.**, s. 80.

²⁰¹ Gürol Canberk, Şeref Sağiroğlu, “Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma”, **Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi**, C. 22, No. 1, 2007, s. 125.

²⁰² Aktürk/Talan, **a.g.m.**, s. 149.

²⁰³ Değirmenci, **a.g.t.**, s. 84.

hesaba aktarılması durumunda aslında büyük bir miktar oluşmaktadır²⁰⁴. Bankaların mevduat faizi değiştirmesi durumunda veya hesaplardaki çeşitli işlemlerde ortaya çıkan ondalık haneleri hesaba dâhil etmemesinden ya da edilse bile kişilerce fark edilmeyecek küçük miktarların başka bir hesapta toplanmasından faydalanan bu usulde küçük miktarlar büyük bir değer oluşturabilmektedir²⁰⁵.

3. Ağ Solucanları (Network Worms)

Bu programlar bilgisayarın hafızasına yerleşen ve hafıza kısmı yokmuş gibi davranarak sürekli olarak kendilerini buraya yazan programlardır²⁰⁶. Herhangi bir donanıma veya yazılıma zarar verme zorunluluğu olmaksızın bilgisayardan bilgisayara dolaşmaktadırlar. Yalnızca bu gezilerini sürdürmek için çoğalırlar²⁰⁷.

Herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve bir kopyası ağa bağlı olan diğer sisteme de kopyalanabilen programlardır. Bilgisayardan bilgisayara kayarak ilerler. Ağ üzerinden bir bilişim sistemine giren ağ solucanı yazılıma zarar verir ya da zarar vermek üzere sisteme Truva atı bırakır. Girdikleri ağ üzerinde her türlü veriyi toplar, gizemli mesajlar bırakır sonrasında ise yakalanmamak için kendilerinden kalan her türlü artığı silerler²⁰⁸.

Ağ solucanı kendini kopyalamadan önce sisteme bulaşıp bulaşmadığını saptar. Sistem içerisindeki varlığını operatörün dikkatini çekmeyecek şekilde kendisine sistemmiş izlenimi vererek de koruyabilir²⁰⁹.

Solucanlar tahmin edilmesi kolay şifreleri ve verileri kullanarak veya sistemde bulunan standart sözlükten yararlanarak veya yaygın şifrelerden oluşan kendi sözlüğünü deneyerek bilgisayarlara girerler ve sistemde karşılaştıkları veri ve programlara zarar verirler²¹⁰.

²⁰⁴ Değirmenci, **a.g.t.**, s. 84; Kurt, **a.g.e.**, s. 67; Aydın, **a.g.e.**, s. 47.

²⁰⁵ Yazıcıoğlu, **a.g.e.**, s. 155; Mungo/Clough, **a.g.e.**, s. 192.

²⁰⁶ Yazıcıoğlu, **a.g.e.**, s. 164; Akbulut, **a.g.e.**, s. 80.

²⁰⁷ Aydın, **a.g.e.**, s. 53.

²⁰⁸ Değirmenci, **a.g.t.**, s. 87; Mungo/Clough, **a.g.e.**, s. 125; Kurt, **a.g.e.**, s. 68.

²⁰⁹ Değirmenci, **a.g.t.**, s. 87.

²¹⁰ Akbulut, **a.g.e.**, s. 80.

Virüslerden farklı olarak bir başka çalıştırılabilir programın parçası olmazlar. Yayılmak için başka bir program ya da insan etkileşimine gerek duymadığı gibi sisteme zarar verme zorunluluğu olmaksızın da sistemin içinde hareket edebilirler²¹¹. Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında e-posta gibi alanlar bulunur. Solucanlar başka dosyaları değiştirmezler, bellekte dururlar²¹².

4. Bilişim Virüsleri

Virüsler en eski kötücül yazılım olarak kabul edilmektedir²¹³. Virüsleri diğer kötücül yazılımlardan ayıran en büyük özellik, etkin olması için insan etkileşimine ihtiyaç duyması noktasındadır. Yani yayılmaya başlaması için bir e-postanın açılması, bir sekmeye tıklanması ya da bir dosyanın çalıştırılması gerekir. Ekranda rahatsız edici mesajların çıkmasına neden olduğu gibi önemli dosyaları silmek veya sistemin tamamen çalışamaz hale getirmek gibi etkileri de bulunmaktadır. Ağ üzerinden yayılabildikleri gibi CD gibi ortamlardan da sisteme yayılabilmektedirler²¹⁴.

Kendisinin değiştirilmiş bir kopyasını eklemek için işletim sistemini ve programlarını değiştiren veya çalışamaz hale getiren programlardır. En önemli özelliği, programdan programa dosyadan dosyaya sistemden sisteme kopyalanabilmesidir. Bu kopyalanma sürecine virüsün bulaşması adı verilir. Yerleştikleri programın işletilmesiyle bilgisayarın hafızasına geçerler ve bilgisayar kapatılıncaya kadar orada kalıcı hale gelirler. Bazı virüsler ise programlar yerine diskin açılış sektörüne veya disk bölümlene kısmına bulaşılırlar. Bulaştıkları her dosyaya iz bırakarak yayılırlar ve sisteme hâkimiyet kurdukları an fiillerine başlarlar²¹⁵.

²¹¹ Akbulut, **a.g.e.**, s. 80; Dülger, **a.g.e.**, s. 109.

²¹² Canberk/Sağıroğlu, **a.g.m.**, s. 124.

²¹³ Virüs terimi 1985'te Güney Kaliforniya Üniversitesi'nde Fred Cohen adında bir yüksek lisans öğrencisinin kendi kendini kopyalayan programlar üzerindeki tezini tamamlamasıyla birlikte kullanılmaya başlandı. Belgelenen ilk bilgisayar virüsü saldırısı 22 Ekim 1987'de Delaware Üniversitesi'nde kaydedildi. Bu virüs yüzlerce dosyayı kullanılamaz hale getirmiştir. Mungo/Clough, **a.g.e.**, s. 100, 107, 116.

²¹⁴ Canberk/Sağıroğlu, **a.g.m.**, s. 123; Akbulut, **a.g.e.**, s. 77.

²¹⁵ Akbulut, **a.g.e.**, s. 77.

Virüsler, sistemdeki bilgilere zarar verebilmekte, sistemi çalışamaz hale getirebilmekte, sabit diski silebilmektedir. Son derece küçük ve kısa programlar olan virüsler, ana bellekte dahi çok az yer kapladığından tespitleri çok güç olmaktadır. Ancak özel yazılıma sahip programlar sayesinde bulunup zararsız hale getirilebilirler²¹⁶.

Virüs terimi aslında biyolojik virüsleri örnek alarak yaratılmıştır. Bilgisayar virüsleri, biyolojik virüsler gibi bilinçsizce yayılır ve kendi kopyalarını yaratırken değişime uğramaktadırlar²¹⁷.

Sonuç olarak virüsler sistemdeki verilere, yazılımlara hatta donanıma bile zarar verebilen bilgisayar programlarıdır. Donanıma zarar vermesine örnek olarak sabit diskin sürekli olarak dönmesine yol açan bir virüs diskin fazla ısınarak tahrip edilmesine neden olması ya da ekrana sürekli olarak sinyal göndermek suretiyle ekran kartına zarar verilmesi verilebilir. Bazı tip virüsler hareketleri gerçekleştirdikten sonra bütün izleri silerek geride hiçbir kanıt bırakmazlar ya da patlayarak sabit disk üzerindeki bütün verileri yok ederler²¹⁸.

Virüsler sırf bilgisayardaki varlıkları yüzünden kazara verilerin üzerine yazabilir ya da bir sistemin çökmesine neden olabilmektedir²¹⁹.

Özel bir yöntemle temizlenmedikleri takdirde virüslü dosyanın ortadan kaldırılması halinde dahi zararlarını devam ettirebilirler. Virüsü yazan kişiler başlangıçta maharet sergilemek için bu yola başvurmuşlardır. Virüslerin bulaşması disketlerin yaygınlaşmasıyla artmış, ardından ağ teknolojileri ve internetle beraber had

²¹⁶ Yazıcıoğlu, **a.g.e.**, s. 161.

²¹⁷ Virüsün kendini kopyalama süreci şu şekilde çalışır; ilk olarak virüs bulaşabileceği bir program arar. Programı bulduğunda söz konusu programın daha önce etkilenip etkilenmediğine bakar. Virüsler etkilenmiş bir programı tanıyabilmek için programa bir iz bırakır. İşaretlenmemiş dosya bulamadıklarında sistemin bütünüyle hâkimiyetleri altında olduğuna inanırlar. Sistem verileriyle oynamak da bu anda başlar. Bunun işaretin kötü yanı, virüs koruma programları tarafından tespit edilmesinin kolaylaşmasıdır. Uygun programı bulan virüs, bünyesindeki kodları bu programa yerleştirir. Programın komut akışına müdahale ederek programın her çalıştırılmasında gizli kodun da çalışmasını sağlar. Son olarak programın etkilenmiş olduğuna dair izi programa bırakır. Değirmenci, **a.g.t.**, s. 88, 90; Mungo/Clough, **a.g.e.**, s. 100.

²¹⁸ Yazıcıoğlu, **a.g.e.**, s. 163.

²¹⁹ Mungo/Clough, **a.g.e.**, s. 158.

safhaya ulaşmış, günümüzde ise e-postanın yaygınlaşmasıyla zaman ve mekân sınırını aşmıştır²²⁰.

Virüs bilincinin gelişmesi ve anti virüs uzmanlarının virüsleri tespit etmedeki becerilerinin artması ise virüs programcılarını daha iyi gizlenen, daha tehlikeli ve daha hızlı yayılan virüsler yazmaya yöneltmiştir. Böylece virüs evrimi de başlamış oldu. Uzmanlara göre gelecekteki virüsler bulaşmak için e-postayı açmanıza ihtiyaç duymadan e-posta programınızın yeni gelen mesajlarını kontrol etmesi faaliyete geçmeleri için yeterli olacaktır²²¹.

Bilişim suçlarının en yaygın işlenme biçimi virüsler olduğundan virüs çeşitlerini ayrıntılı olarak açıklamayı uygun görmekteyiz.

a. Boot Virüsleri

Belirleyici özelliği “boot sektörlerine” yerleşmeleridir. Bilgisayar açıldığında boot sektöründeki program otomatik olarak çalışır. Bu virüsler boot sektöründe yüklenecek programın komut akışına müdahale ederek, çalışmaları sayesinde komut akışını değiştirirler. Etkin hale gelen virüsler bilgisayar kapatılıncaya kadar bulaşmaya ve kendi kendilerini çoğaltmaya devam ederler²²². Bilgisayar çalışmaya başladığında virüsün ilk kısmı hafızaya sızar ve sonra kuyruğunu orijinal boot sektörünün peşinden getirir. Kuyruğunu ilştirirken bazı kısımların kazara üzerini yazabilir ya da ya da bu kısımdaki verileri silebilir. Varlığını özellikle tehlikeli veya bariz olan bir şey yapmaması ve bilgisayar kapatılana kadar bilgisayara takılan başka CD’leri hedef almasından kaynaklı olarak çok belli etmezler²²³.

Ping Pong virüsü ilk boot virüslerindendir. 1988 yılında keşfedilen bu virüs aktif hale geldiği zaman ekranda bir top çıkar ve bu top ekranın kenarlarına ve

²²⁰ Kurt, **a.g.e.**, s. 70.

²²¹ Hakan Altıntaş/Mehmet Tan, “Bilişim Suçları ve Güvenlik Önlemleri”, **2. Polis Bilişim Sempozyumu Bildirileri**, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, Ankara, s. 223- 224.

²²² Değirmenci, **a.g.t.**, s. 91; Yazıcıoğlu, **a.g.e.**, s. 164.

²²³ Mungo/Clough, **a.g.e.**,s. 108, 109.

karakterlerine çarpa çarpa hareket eder. Genelde bilgisayar işlemleri yoğunlaştığında ortaya çıkar²²⁴. Şair virüsü ve Çernobil virüsü bu virüs türüne verilebilecek örneklerdendir²²⁵.

b. File (Dosya) Virüsleri

Virüsün aktif hale gelebilmesi için boot virüslerindeki gibi sistemin yeniden çalıştırılmasına ihtiyaç duyulmadığından çok daha hızlı yayılırlar. Kendilerini EXE ya da COM gibi çalıştırılabilir dosyaların sonuna eklerler, bu dosyalara erişildiğinde devreye girerek RAM belleğe yerleşirler ve bilgisayar açık olduğu sürece orada kalmaktadır²²⁶.

Kendini bilgisayarın gerçekte en işe yarar programlarına ilişitirdikten sonra, enfekte olmuş programın bilgisayara yüklenmesiyle kendini bilgisayar hafızasına kaydeden Viyana virüsü de bu türün ilk örneklerindendir²²⁷.

c. Makro/Mail Virüsleri

Bu tip virüsler Microsoft Word ve Excel gibi güçlü makro desteği olan masaüstü programları kullanan ve bunlara ait belgelerin açılışında çalışan makrolar ile yayılırlar²²⁸.

Aslında birer dosya virüsü olan bu virüsler bir dosyanın sonuna yerleşerek dosya çalıştırıldığında aktif hale gelirler. Elektronik postanın yaygın olarak kullanılmasıyla en çok rastlanılan virüsleri oluştururlar. Kısa sürede birçok bilgisayara bulaşması dolayısıyla da en tehlikeli virüslerden kabul edilir²²⁹.

Doktrinde dördüncü virüs tipi olarak betik (script) virüslerini kabul eden yazarlar bulunmaktadır. Bu virüsler betik dil kullanılarak yazılırlar, Windows veya

²²⁴ Yazıcıoğlu, **a.g.e.**, s. 162; Mungo/Clough, **a.g.e.**, s. 157.

²²⁵ Yazıcıoğlu, **a.g.e.**, s. 162. Akbulut, **a.g.e.**, s. 84,85.

²²⁶ Değirmenci, **a.g.t.**, s. 91; Yazıcıoğlu, **a.g.e.**, s. 164

²²⁷ Mungo/Clough, **a.g.m.**, s. 105.

²²⁸ Canberk/Sağıroğlu, **a.g.m.**, s. 124.

²²⁹ Değirmenci, **a.g.t.**, s. 91, 92.

Linux komut ve hizmet dosyalarına bulaşır ya da çok bileşenli virüslerin parçası olarak çalışırlar²³⁰.

Günümüzde ise virüslerle mücadelede önemli mesafeler kat edilmiştir. Yaratılan bir virüsün arkasından hemen onu etkisiz hale getiren anti virüs programları ortaya çıkmaktadır²³¹.

5. İstem Dışı Alınan Elektronik İletiler (Spam)

Spam rahatsız edici ve istem dışı olarak atılan her türlü ileti ve eklerine denir²³². Spam genellikle bir ürünün reklamı, pazarlanması veya sosyal içerikli bir mesajın kitlelere ulaştırılması için kullanılır. Bu tür mesajlar bünyesinde elektronik posta adreslerinin veri tabanlarını tutan kuruluşların bu verileri çeşitli bedeller karşılığında satması sonucu artmıştır²³³.

Kullanıcıları üzerinde etkileri dikkate alınarak spamın iki grupta incelendiğini söyleyebiliriz. İlk grup, elektronik posta yoluyla direkt kullanıcıyı hedef alan spamlardır. Bu grup genellikle web adresinde adres aranması sonucu kendine uygun elektronik posta veri tabanı oluşturur. Gönderilen ileti muhatabı tarafından alınmadığında göndericiye geri dönmekte, spam göndericileri adres kısmında göstermelik bir adres gösterdiklerinde onlara da ulaşamayan ileteler postmaster hesabına dönmekte ve meydana gelen aşırı yığılma sistemi çalışmaz hale getirmektedir. İkinci grupta ise, tartışma listelerine gönderilmek suretiyle kişilere ulaştırılması amaçlanan spamlar bulunmaktadır²³⁴.

²³⁰ Canberk/Sağiroğlu, **a.g.m.**, s. 124.

²³¹ Buna örnek olarak Awast firmasının ürettiği Awast 32 programı verilebilir. Bu programlar kullanıcıları virüsün varlığı konusunda uyarırken aynı zamanda virüsleri temizlemekte veya başka dosyalara bulaşmasını önlemek için virüsleri karantina altına almaktadır. Değirmenci, **a.g.t.**, s. 95.

²³² Kurt, **a.g.e.**, s. 72.

²³³ Değirmenci, **a.g.t.**, s. 96, 97.

²³⁴ Değirmenci, **a.g.t.**, s. 96, 97; Kurt, **a.g.e.**, s. 72, 73.

İnternet üzerinden yapılan tüm işlemlerin sağlıklı olarak devamı için akıcı bir internet bağlantısı gereklidir. Spam internet ağını tıkamakta, e-posta iletimini yavaşlatmakta, bazen de sunucuları çökerterek işlem yapamaz hale getirmektedir²³⁵.

Spam e-postalarının kimden ve hangi elektronik posta adresinden gönderileceği önceden bilinmediği için verilen komutla e-postaların silinmesi sorunun çözümü olmamaktadır. Bu mesajlar sadece sisteme girmesiyle bile bazen bilgisayara virüs bulaştırma, kilitleme, kullanımı geçici engelleme gibi sonuçlara neden olabilmektedir²³⁶.

Bu tür mesajların sonunda yer alan ve mesaj listesinden çıkmak isteyen kişiler için sunulan listeden çıkma bağlantılarına da şüpheyile bakmak gerekir. Bu bağlantılar bilinen ve güvenilir kaynaklar dışında spam mesajını gönderen kişi veya gruba e-posta hesabının kullanılan gerçek bir hesap olduğunu göstermekte, bu bağlantıları gönderen kişiler gerçek bir kişiye ait olduklarını saptadıkları bu e-posta adreslerini üçüncü kişilere pazarlayarak hem kazanç elde etmekte hem de kişiye daha fazla spam gönderilmesine neden olmaktadır.²³⁷

Spam ile ilgili düzenlemeler yapan 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un ticari elektronik gönderme şartının belirtildiği 6. maddesinde ticari elektronik iletilerin gönderilmesi açıkça önceden onay şartına bağlanmıştır. Ayrıca alıcılara her zaman hiçbir gerekçe göstermeksizin ticari elektronik iletiyi reddetme hakkı bu kanun ile sağlanmıştır. Bu kanun ile beraber spamı doğrudan yasaklayan bir hüküm Türk Hukukunda ilk kez uygulanmaya başlanmış oldu²³⁸.

²³⁵ Kurt, **a.g.e.**, s. 72.

²³⁶ Ünver, **a.g.m.**, s. 108, 111.

²³⁷ Canberk/Sağiroğlu, **a.g.m.**, s. 126; Hüseyin Çakır/Mehmet Serkan Kılıç, **Güncel Tehdit: Siber Suçlar**, Ankara, Seçkin Yayıncılık, 2014, s. 31.

²³⁸ Dülger, **a.g.e.**, s. 115; Orta, **a.g.e.**, s. 100

6. Mantık Bombaları (Logic Bombs)

Mantık bombaları, daha önceden belirlenmiş özel durumların gerçekleşmesi durumunda zarar verici sonuçlar yaratan programlardır. Bir mantık bombası, belirlenmiş özel durum gerçekleşene kadar Truva atı programı gibi davranır. Söz konusu durum gerçekleşince sisteme zarar verir ve kendini gizli tutan Truva atı programından da bu özelliği dolayısıyla ayrılır²³⁹. Bu yöntemi kullananların amacı hırsızlık, istihbarat, şantaj, ızzar ya da sadece eğlence olabilir²⁴⁰. Örneğin bir mantık bombası kişinin maaş kayıtlarını izleyebilir ve kişinin maaşı belirli bir limitin altına düştüğünde yükseltmek, silmek ve herhangi bir işlem yapmak gibi işlemler yapacak şekilde programlanabilir²⁴¹.

Belirli şartlar gerçekleştiğinde bomba gibi patlamaya hazır hale getirilmişlerdir. Saatli bombalar, mantık bombaları, yazılım bombaları gibi değişik türleri vardır. Yazılım bombaları sisteme girer girmez herhangi bir uyarı söz konusu olmadan verilere çarparak yok ederler²⁴². Saatli bombalar ise Truva atı metoduyla bilgisayara yerleşir. Programlandıkları gibi belli bir zamanda çalışarak önceden belirlenen bilgileri veya yapılan işlemleri sistemden silip yok ederler²⁴³. Belirli bir sayıda çalıştırıldıktan sonra belirli bir tarihte veya günün belirli bir saatinde patlayacak şekilde programlanabilirler²⁴⁴.

Bu program sisteme zarar verebilmek için sürekli faaliyet gösteren bir yazılımdır ve bunu sistemde tespit edebilmek güçtür. Bilgisayar sistemini şaşırtmak veya bozmak için programlanmaktadır ve bunun için de bilgisayar sistemine sürekli mantık dışı ya da yapılan işlemin aksi yönünde işlem yapacak komutlar göndermektedir²⁴⁵.

²³⁹ Değirmenci, **a.g.t.**, s. 101.

²⁴⁰ Kurt, **a.g.e.**, s. 73.

²⁴¹ Aydın, **a.g.e.**, s. 52.

²⁴² Akbulut, **a.g.e.**, s. 83; Aydın, **a.g.e.**, s. 51.

²⁴³ Yazıcıoğlu, **a.g.e.**, s. 158; Kurt, **a.g.e.**, s. 74.

²⁴⁴ Aydın, **a.g.e.**, s. 52.

²⁴⁵ Yazıcıoğlu, **a.g.e.**, s. 157; Kurt, **a.g.e.**, s. 74.

Fail, mevcut programların bazılarını ya da tamamını yok etmek veya tahrip etmek için bilgisayarı programlayabilir. Eğer fail bilgisayarın şifresini çözebilirse bilgisayardaki tüm kayıtları ve programları silebilir ya da bir şirket bilgisayarına içindeki tüm bilgileri yok edecek veya kullanılmaz hale getirecek bir mantık bombası yerleştirebilir. Daha sonra programı çalıştırmadan sistem sahibinden para isteyebilir ve verilmediği takdirde de tüm giriş sistemini tahrip edebilir²⁴⁶.

7. Çöpe Dalma (Scavenging)

Çöplenme ya da artık toplama olarak da adlandırılan bu teknikte sistemde gerçekleştirilen işlem sonrası kalan bilgiler toplanmaktadır. Bu bilgiler ilk olarak çıktı alınan ve daha sonra çöpe atılan kâğıt gibi malzemeler üzerinde kalan bilgilerin toplanması suretiyle elde edilebilir. İkinci olarak da bilgisayarda işlem görüp silinmiş veya kayıtları yok edilmeye çalışılmış verilerin veya artık kullanılmayan silinmiş bilgilerin çeşitli tekniklerle elde edilmesiyle gerçekleştirilir²⁴⁷.

İlk yöntem fazla bir bilgiye ihtiyaç olmadan uygulanabilen bir yöntem olmasına karşılık diğer yöntem bilgisayarlarda bir dosyayı silerken gerçek bilginin silinmesinin ancak üzerine yeni bilginin yazılmasından sonra gerçekleşmesinden dolayı uzmanlık gerektiren bir yöntemdir²⁴⁸. Ayrıca yazıcı şeritlerinde ya da yazıcıların tonerleri üzerinde oluşan bilgilerin toplanılması ile de fiil gerçekleştirilebilir²⁴⁹.

Bu usulle askeri, ticari, toplumsal çok önemli sırlar öğrenilebilir, fail tarafından haksız menfaatler de elde edilebilir. Bu yöntem ile kişilerin özel hayatları ihlal edilmektedir²⁵⁰.

²⁴⁶ Halil İbrahim Dilek, “Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri”, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Diyarbakır, 2007, s. 32; Yazıcıoğlu, **a.g.e.**, s. 157.

²⁴⁷ Değirmenci, **a.g.t.**, s. 76; Yazıcıoğlu, **a.g.e.**, s. 159; Mungo/Clough, **a.g.e.**, s. 79; Dülger, **a.g.e.**, s. 119.

²⁴⁸ Değirmenci, **a.g.t.**, s. 76.

²⁴⁹ Orta, **a.g.e.**, s. 107.

²⁵⁰ Kurt, **a.g.e.**, s. 62.

8. Gizlice Dinleme (Eavesdropping) – Ağ Koklama (Sniffing)

Bilişim sistemlerinin veri naklinde kullandığı ağlara girilerek ya da az da olsa yaydığı elektromanyetik dalgaların yakalanarak verilerin tekrar elde edilmesini sağlayan tekniktir. Özellikle bilgisayar ekranlarının yaydığı elektromanyetik dalgaların yakalanması ve tekrar ekran görüntüsüne çevrilmesi yoluyla işlenebileceği gibi veri naklinde kullanılan ağlara yapılan müdahale sonucunda ağda nakledilen verinin elde edilmesi şeklinde de işlenebilir²⁵¹. Bu tür bir fiil hem başka suçlara da vasıta olarak hem de sadece dinleme amacıyla gerçekleştirilebilir. Hem araç hem de amaç olarak kullanılabilir²⁵².

9. Veri (Bilgi) Aldatmacası (Data Diddling)

Bu yöntem basit ve güvenilir olmasının yanında en zor açığa çıkan yöntemlerden biridir. Verinin bilgisayara kaydı sırasında değiştirilmesi yani bilgisayara yanlış veri girilmesi ya da verilerin kasten bırakılması ile gerçekleştirilir. Fail böylece bilgisayara girdiği veya orada bıraktığı verilerle değişiklik yapma ve cihazı istediği gibi kullanma imkânına sahip olur²⁵³. Bu yöntemde veriler sisteme girilirken ya yanlış veriler girilir ya da veriler girildikten sonra değiştirilir²⁵⁴.

10.Tarama (Scanning)

Bu sistem bilişim sistemlerine değeri her defasında değişen veriler girilmek suretiyle, sistemin olumlu cevap verdiği durumların tespitine yönelik bir tekniktir. Bilişim sistemlerinin telefon numaralarını veya internete bağlı sistemlerinin IP numaralarını bulmaya yönelik olabileceği gibi şifre ile korunan sistemlerin geçerli

²⁵¹ Değirmenci, **a.g.t.**, s. 77; Avşar/Öngören, **a.g.e.**, s. 52.

²⁵² Kurt, **a.g.e.**, s. 62.

²⁵³ Yazıcıoğlu, **a.g.e.**, s. 152; Kurt, **a.g.e.**, s. 62, 63.

²⁵⁴ Değirmenci, **a.g.t.**, s. 77.

şifresini bulmaya yönelik de olabilir. İlk duruma “port tarayıcı” ikinci duruma “password tarayıcı” denir²⁵⁵.

Bir password kırıcı program geçerli şifreyi bulmak için veri tabanında bulunan harf ve kelime dizilerini birer birer deneyerek şifreyi bulmak için değişen değerlere karşı sistemin cevaplarını da kontrol eder. Bu tür değişen verileri girerek sisteme giriş parolalarını elde eden programlara karşı alınacak önlemler teknik nitelikte olmalıdır. Örneğin cep telefonlarındaki gibi PIN numaralarının denemesi belli bir sayıyla sınırlandırılabilir²⁵⁶.

11. Süper Darbe (Super Zapping)

İsmi super zap kelimesinden gelmekte olan sistem programı olarak kullanılan oldukça yararlı bir programı ifade eder. Sistemin kilitlendiği durumlarda bu program en kısa zaman içinde sistemin yeniden çalışmasını sağlar. Bu programlar bir yandan sistemdeki emniyet tedbirlerini aşarken diğer yandan da sorunları çözer. Aslında faydalı olan bu program, kötüye kullanılma potansiyeline de sahiptir. Zira emniyet tedbirlerini aşabildiği gibi sisteme girip değişiklik de yapabilme özelliğine sahiptirler²⁵⁷.

CD’den CD’ye programın kopyalanmasını önleyen kopya programlarını atlatan bir program olarak ortaya çıkmıştır. Daha sonra ise bütün kontrolleri atlatarak sisteme müdahale eden programlar olarak işlevini genişletmiştir. Bilgisayarlar zaman zaman gerek programlardan kaynaklanan hatalardan zaman zaman da kullanıcının kendisinden kaynaklanan hatalardan dolayı istenen işlevi yapamaz duruma gelebilir. Bu durumlarda bu sistemler güvenli modda çalışırken olağanüstü durumlarda güvenlik kontrollerini aşarak sistemde değişiklik yapabilecek programlara ihtiyaç duyarlar. Bu tür işler için programlanmışken sonradan işlev değiştirmiştir²⁵⁸.

²⁵⁵ Değirmenci, **a.g.t.**, s. 82; Dülger, **a.g.e.**, s. 120.

²⁵⁶ Değirmenci, **a.g.t.**, s. 83; Dülger, **a.g.e.**, s. 120.

²⁵⁷ Yazıcıoğlu, **a.g.e.**, s. 156; Aydın, **a.g.e.**, s. 49.

²⁵⁸ Değirmenci, **a.g.t.**, s. 85.

12. Gizli Kapılar veya Hile Kapısı (Trap Doors)

Aslında meşru bir amaç için kullanılırken sonradan kötü amaçlar için kullanılmıştır. Programları hazırlayan programcılar bunları geliştirirken ileride ortaya çıkabilecek durumlara karşı programlara kod ekleyebilmek için programa istendiğinde durma mekanizması eklerler. İşte bu mekanizmalara “trap doors” adı verilir. Aslında değişikliğe kapalı olan şifreler üzerinde ortaya çıkan yeni şartlara göre ayarlama yapabilme olanağı yaratılmak istenmiştir, kapının programcı tarafından program bitip teslim edildiğinde kapatılması gerekir²⁵⁹. Bu mekanizmaların program veya işletim sistemi tamamlandığında ortadan kaldırılması gerekir ancak bazen bu mekanizmalar ortadan kaldırılmaz. Bu durumlarda bu kapılar hukuka aykırı faaliyetlere zemin sağlar²⁶⁰.

Bu yöntem, bilgisayar üzerinde normal kimlik kanıtlama süreçlerini atlatmayı ve kişinin sisteme uzaktan erişmeyi sağlaması üzerine kurulur. Sisteme giren saldırgan tek bir komut ile sistemin çökmesine neden olabilmektedir²⁶¹. Bir sisteme sızmak için çabalayan korsanlar daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklerler. En sık karşılaşılan arka kapı yöntemi hedef sistemde dinleme ajanı iştirilmiş bir kapıyı açık tutmaktır²⁶².

Truva atları gibi hedef sisteme sızmaya çalışan yazılım olsa da Truva Atından farklıdır. Truva Atı yararlı bir program gibi gözükürken arka kapı sadece sisteme erişimi sağlayan gizli yapılardır²⁶³.

13. Eş zamansız Saldırıları (Asynchronous Attacks)

İşletim sistemleri uygulanan değişik bilgisayar programlarının fonksiyonlarını ifa etmek için eş zamansız çalışır. Bu teknik de bu eş zamansız çalışmadan faydalanır.

²⁵⁹ Yazıcıoğlu, **a.g.e.**, s. 156-157; Çakır/Kılıç, **a.g.e.**, s. 32.

²⁶⁰ Değirmenci, **a.g.t.**, s. 85; Kurt, **a.g.e.**, s. 67.

²⁶¹ Akbulut, **a.g.e.**, s. 86, 87.

²⁶² Canberk/Sağıroğlu, **a.g.m.**, s. 126.

²⁶³ Aktürk/Talan, **a.g.m.**, s. 149.

Örneğin bir çıktı alınması işleminde işlem için çeşitli görevlerin sırasıyla çağırılması gerekir. İşletim sistemleri bu istekleri bekletir ve kaynaklar ulaşılabilir hale gelince isteğe uygun olarak öncelik düzenine göre yerine getirir. İşte birçok sistemin programları eş zamanlı aynı anda kullanılmamasından faydalanan failer, geliştirdikleri eş zamanlı saldırı teknikleri ile sistemde veya programda bulunan veriler üzerinde çeşitli filler gerçekleştirmektedir.²⁶⁴

Bu programlar bilgisayar kullanıcısına ara noktalarda yeniden başladığında bilgi kaybına neden olmadan programı elle durdurma olanağı verir. Kaybın önlenmesi için programın durduğu andaki durumunun belleğe kaydedilmesi gerekir. Kullanıcıların ya da dışarıdan programcıların bu mekanizmalarda bulunan kopya bilgilere ulaşma imkânları vardır. Ulaşma yetkisi olan kişiler yeniden başladığında programı daha yüksek bir güvenlik seviyesinde çalıştırıp sistem değerlerini değiştirebilirler²⁶⁵.

14.Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme

Bir web sayfasına ulaşmak isteyen kullanıcının ulaşmak istediği web sayfasına benzer şekilde hazırlanmış başka bir sayfaya yönlendirilmesi ve bu sayfada işlem yapmak isteyen kişinin kendiliğinden verdiği kullanıcı adı ve şifresine ulaşmak şeklinde işlenebilir. İkinci olarak da çok bilinen web sayfalarına ulaşmak için adresi küçük farklılıklarla yanlış yazanların adresin neresinde yanlış yapacağını tahmin ederek bunu yazabileceklerin ulaşabileceği yeni bir sayfa oluşturulması suretiyle gerçekleştirilebilir²⁶⁶.

Bu yöntem internet servis sağlayıcılarının herhangi bir şekilde internet başvurusuna ait bilgileri kötü niyetli üçüncü kişilere sızdırması suretiyle gerçekleştirilebileceği gibi servis sağlayıcısına bilgisayar korsanlarının erişmesiyle de gerçekleştirilmektedir²⁶⁷.

²⁶⁴ Yazıcıoğlu, **a.g.e.**, s. 158.

²⁶⁵ Değirmenci, **a.g.t.**, s. 86.

²⁶⁶ Kurt, **a.g.e.**, s. 73.

²⁶⁷ Değirmenci, **a.g.t.**, s. 99.

15. Sırtlama veya Yetki Dışı/ Gizlice Girme

Fiziksel veya elektronik yollarla bilişim sistemlerine yetkisiz olarak girme tekniğidir. Fiziksel sırtlama olarak anılan teknikte, girişe yetkili olan bir kimsenin giriş iznini kullanarak girmek ve mevcut verilere herhangi bir şekilde erişmek söz konusudur. Elektronik sırtlama ise, sisteme bağlı kullanıcıların herhangi birinin kullandığı hattan başka bir kullanıcının yetkisiz olarak bağlanması şeklinde gerçekleşir²⁶⁸. Fiziksel olan ilk yol elektronik yöntemlerle kontrol edilen yerlere giriş imkânı yaratmak amacıyla kullanılan bir usuldür. Örneğin, girişi kontrol altında bulunan bir alana giriş için bu yetkiye sahip birinin izlenmesi suretiyle girişin sağlanması gibi. Elektronik olan ikinci yol ise sistemin kullanıcıyı otomatik olarak tanıdığı sistemlerde söz konusudur. Görüldüğü üzere hem elektronik hem de fiziksel yolda amaç sisteme giriş için bir yetki ya da anahtar gereken durumlarda bunların gizlice sağlanarak sistem giriş fiilin gerçekleştirilmesidir. Bu anahtar kimi zaman kullanıcının göz bebeği ya da sesine özel kişisel özellikleri ya da manyetik bir kart ya da sayı veya rakam dizisi de olabilir. Bu teknik elinde sisteme girişi sağlayan veri ya da anahtar olmayan failin bunları veri hattına gizlenerek hattı kullanmaya yetkisi bulunan yasal kullanıcının yerine geçerek hattı kullanmasını sağlar²⁶⁹.

16. Yerine Geçme (Masquerading)

Temel olarak erişim imkânına sahip olmayan bir bilişim sistemi tarafından parola, erişim kodu veya belirlenmiş herhangi bir ayırıcı unsurun taklit edilerek erişim sağlanması fiilidir²⁷⁰.

Sistem işleyişindeki yetkiyi tanımlayabilmek için kişiden bir erişim kodu ya da parola ister. Sistemlerde yapılan ufak hilelerle erişim yetkisi olmayan ya da kısıtlı olan kişilere erişim hakkı ya da daha geniş erişim yetkisi verilebilmektedir. Eğer bu hile, erişim yetkisi olan bir kişinin sistemine parola ya da erişim kodu yazılması ya da

²⁶⁸ A.e., s. 101.

²⁶⁹ Yazıcıoğlu, a.g.e., s. 160.

²⁷⁰ Kurt, a.g.e., s. 74.

ona özgü göz retinası ya da parmak izin gibi niteliklerin taklit edilmesiyle yapılırsa bu hareket yerine geçme olarak adlandırılır²⁷¹.

17. Tavşanlar (Rabbits)

Adını aldıkları hayvan gibi hızlı üreyip kısa zamanda kolonileşip bilişim sisteminin işleme gücünü azaltmasına dair komut veren yazılım türüdür. Bir koloni yaratıldıktan sonra bu bir yavru koloni üretir ve yavru koloni yeterince gelişen yeni bir koloni doğurur böylelikle bu döngü sürekli devam eder. Öyle ki sistem en sonunda durma noktasına gelir²⁷².

Yerleştikleri bellekteki alanı koloni kurarak sürekli dolduran, sistemin bilgi işleme gücünü zayıflatan, bilgisayar veya sisteme sürekli gereksiz komutlar veren kendi kendilerine yetip virüsler gibi asalak olmayan programlardır²⁷³. Burada amaç özellikle çok kullanıcı sistemlerin iletişim ağ ortamlarında ana sistem bilgi işleme gücünü yitirinceye kadar sistemin kaynaklarını kurutmaktır²⁷⁴.

Tavşanların faaliyete geçebilmesi için dışarıdan müdahaleye ihtiyaç yoktur, kendi kendilerine çalışırlar²⁷⁵.

18. Bukalemun (Chameleon)

Aynı zamanda bir Truva atı olan bu program aslında suç işleme amacıyla üretilmemiş başka bir programın tüm hareketlerini taklit edebilen, girdiği sistemdeki verileri ve kullanıcı ad ve şifrelerini kopyalayıp gizli bir şekilde saklayabilen programlardır²⁷⁶. Sistem için normal çalışan, zararsız yazılım gibi davranan ve onun niteliklerine sahipmiş gibi görünen bu yazılımlar, sistemin içerisine girdikten sonra gerçek kimliklerini ortaya çıkarıp zarar verici fiillerde bulunmaya başlamaktadırlar²⁷⁷.

²⁷¹ Değirmenci, **a.g.t.**, s. 102; Mungo/Clough, **a.g.e.**, s. 53 vd.

²⁷² Değirmenci, **a.g.t.**, s. 102; Aydın, **a.g.e.**, s. 52; Mungo/Clough, **a.g.e.**, s. 67.

²⁷³ Kurt, **a.g.e.**, s. 75.

²⁷⁴ Aydın, **a.g.e.**, s. 53.

²⁷⁵ Değirmenci, **a.g.t.**, s. 103.

²⁷⁶ Kurt, **a.g.e.**, s. 75.

²⁷⁷ Dülger, **a.g.e.**, s. 111.

Sürekli kullanılan güvenilir programlar gibi davranmakla beraber gerçekte birtakım hile ve aldatmalar içerir. Bukalemunlar kullanıcı adı ve şifrelerini taklit etme özelliği nedeniyle gizli dosyalara ulaşır, şifreleri gizli bir dosyaya kaydetmektedirler. Daha sonra sistem bakım nedeniyle geçici bir süre kapatılacağına ilişkin mesaj verip bu programı kullanan kişilerin bu gizli dosyaya ulaşarak kullanıcı isim ve şifrelerinin ele geçirmesini sağlamaktadır²⁷⁸.

19. Casus Yazılımlar (Spyware)

Casus yazılım (spyware) sözcüğü, İngilizce spy ve software kelimelerinden oluşmuştur. Bu yazılım kullanıcılara ait önemli bilgilerin kullanıcıların bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesi üzerine kurulmuştur²⁷⁹.

Bazı kaynaklarda dar anlamda “snoopware (burun sokan yazılım)” olarak da adlandırılan bu yazılımlar, kullanıcılar tarafından sistemlere farkında olmadan bulaştırılmaktadırlar. Virüs ve solucanlardan farklı olarak sisteme bir kez bulaştıktan sonra kopyasını oluşturarak yayılmaya ihtiyaç duymazlar. Amacı seçilen sistem üzerinde gizli kalması istenen bilgileri toplamaktır. Bu bilgi kredi kartı numarası bile olabilir. Ticari firmalar internet üzerindeki kullanıcı alışkanlıklarını öğrenmek amacıyla casus yazılımları yayabilmektedirler²⁸⁰.

Özellikle iş yerindeki bilgisayar kullanıcıları, kullanılan bilgisayarların kendilerine ait olmadığını ve başkaları tarafından buradaki bilgilere erişimin olabileceği gerçeğini unutmamalıdır. Bir yere kaydedilen hiçbir şey özel değildir. Bu nedenle hangi verinin kaydedildiği büyük önem taşımaktadır²⁸¹.

²⁷⁸ Çakır/Kılıç, **a.g.e.**, s. 51.

²⁷⁹ Akbulut, **a.g.e.**, s. 84.

²⁸⁰ Canberk/Sağıroğlu, **a.g.m.**, s. 125.

²⁸¹ Leyle Keser Berber, **Adli Bilişim (Computer Forensic)**, Ankara, Yetkin Yayınları, 2004, s. 37.

20. Telefon Çeviriciler (Dialers)

Mağdurlara yüksek miktarda telefon ücreti ödetmek amacıyla kullanılan yazılımlardır. Genelde uluslararası uzak mesafe telefon numaralarını interneti kullanarak bağlantı numarası ile değiştirirler. İnternete bağlanan kişi farklı hattı kullandığının geç farkına vardığı için ödeyeceği miktar sürekli artmaktadır²⁸².

Bu yazılımın görevi bilgisayardaki mevcut dial-up bağlantısını keserek, bilgisayarın bağlı bulunduğu veya bağlanması gereken internet servis sağlayıcısı telefon numarası yerine program tarafından belirlenen başka bir telefon numarasına - ki bu genellikle yüksek ücreti nedeniyle 900'lü hatlar olmaktadır- internet bağlantısının yapılmasının sağlanmasıdır. Amacı gerçekte kullanıcının öngördüğü telefon bağlantısı yerine yazılımın öngördüğü uluslararası telefon hattı üzerinden internet bağlantısı yapılması ve bu suretle ödenecek ücretten komisyon alarak bağlantıyı yaptırtan kişinin bundan haksız menfaat temin etmesidir. Bu programlar temelde iki çeşittir. İlkinde hile ile bilgisayar kullanıcısının iradesi aldatılarak ona bu programı internetten indirtilerek bilgisayarına yükletilmeye çalışılır. Diğerinde ise buna gerek kalmadan kendisi bilgisayara girmekte ve kullanıcı internete bağlandığı anda bağlantıyı keserek telefonunu istediği numaraya bağlamaktadır²⁸³.

Son zamanlarda sıkça rastlanan bir türü de belirli siteye erişmek için kullanıcının hazırlanan bir telefon çeviricisini kullanması gerektiğinin belirtilmesidir, kullanıcının asla bunu indirip kurmaması gerekir²⁸⁴.

21. Sahte İleti (Fake/Fault Mail)

Sahte ileti adı üstünde muhatabınca gerçek olarak algılanabilmesi için gerçeğinden farksız olarak düzenlenmiş iletidir²⁸⁵.

²⁸² Akbulut, **a.g.e.**, s. 85.

²⁸³ Yılmaz Yazıcıoğlu, "Dialler, Key Logger Programları- İnternet Bankacılığı Dolandırıcılığı", **Bilişim Hukuku**, Der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 83.

²⁸⁴ Canberk/Sağiroğlu, **a.g.m.**, s. 127.

²⁸⁵ Kurt, **a.g.e.**, s. 76.

Aslında sahte elektronik postanın temelinde bilişim dünyasının sunduğu olanaklar ile orta ve düşük düzeydeki bilgisayar kullanıcılarının aldatılması yatmaktadır. Sahte e-posta ile internet kullanıcısının şifresi, kullanıcı adı veya internet servis numarasının o kişinin e-posta veya internet servis hesabından verilmiş izlenimini veren bir e-posta vasıtasıyla ele geçirilmesi söz konusu olmaktadır. Bilgileri elde eden kimse kullanıcının bilgisayarına girebilmekte, bilgisayarında değişiklik yapabilmekte ve verilerle oynayabilmektedir. Bilgisayarın IP numarası elde edilmiş olduğu için internet ya da bilgisayardaki herhangi bir işlem kullanıcı adına yapılmış gibi gözükmemektedir²⁸⁶.

Her türlü bilgi elde edilebilir. Genelde hesabınız tehlikede, lütfen kişisel bilgilerinizi teyit edin gibi içeriklere sahip e-postalar gönderilerek kişileri kimlik bilgilerini yazacakları bir internet sitesine yönlendirip, buraya yazılan bilgilerin kaydedilmesi ile olur²⁸⁷.

22. Sazan Avlama/Oltalama (Phishing)

İngilizce “password harvesting fishing” (şifre hasadı avcılığı) kelimelerinin kısaltmasından oluşur. 1980’de ilk kez psikolojik teknikler kullanarak kredi kartı bilgilerini elde eden Brien Phish’e atıfla bu şekilde adlandırılmıştır²⁸⁸.

İlk olarak e-postalar üzerinde gerçekleşen bu yöntem daha sonra sosyal ağların yayılmasıyla kişisel veriler, banka hesap numaraları, kredi kartı numaraları gibi kişisel bilgilerin elde edilmesinde kullanılmıştır. Sahte e-postaları alan kişi, istenilen gizli bilgileri göndererek bu bilgilerin kötü niyetli kişilerin ele geçmesine neden olmaktadır. Bu yöntemi kullanan kişi sistemdeki kullanıcıya bir link göndererek sonunda hediye ya da indirim vadetmekte daha sonra kullanıcı linke tıkladığında ise hesabının hacklenerek kişi listesine de aynı mesajların gönderilmesini sağlamaktadır²⁸⁹.

²⁸⁶ Yazıcıoğlu, “Dialler, Key Logger Programları- İnternet Bankacılığı Dolandırıcılığı”, s. 81.

²⁸⁷ Avşar/Öngören, **a.g.e.**, s. 54.

²⁸⁸ Canberk/Sağıroğlu, **a.g.m.**, s. 131.

²⁸⁹ Akbulut, **a.g.e.**, s. 86.

Bir diğerk örnek olarak “*bu elektronik posta bankanız tarafından gönderilmiş olup eksik bilgilerinizi tamamlamanız gerekmektedir.*” şeklinde kullanıcılara gönderilen e-postalar bilinçli olmayan kullanıcılar tarafından geçerli kabul edilerek yönlendirilen site üzerinden kişiye ait bilgiler elde edilerek kullanılmasıyla gerçekleşebilir²⁹⁰.

Arama motorlarında bazı bankaların dolandırıcılar tarafından hazırlanan sahte erişim adreslerinin bulunduğu gerçeğı karşısında tedbir olarak adreslerin adres çubuğuna elle yazılması doktrinde önerilmiştir²⁹¹.

23. Klavye Dinleme Sistemleri (Keyloggers)

Kullanıcıların klavye kullanarak girdiğı bilgileri yakalayıp, tutan ve bunları saldırganıa gönderen yazılımlardır²⁹².

İnternet kullanan banka müşterilerinin veya internet üzerinden ticaret yapan kullanıcıların online işlem şifrelerinin klavye tuş girdilerini kaydeden keylogger yazılımı ile elde edilmesi yöntemidir. Kullanıcıların bilgisayarlarına yerleştirilen bu yazılım, bilgisayarda yapılan her türlü işlemin kaydını tutar ve bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntülerini de içerebilir. Bu kayıtlar sistemde bir “txt (metin)” dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırganıa gönderilir²⁹³.

Screen logger programlar sanal klavyeden şifre girilirken kaydedilen ekran görüntülerini yazılımı hazırlayan kimselere istendiğı anda istendiğı oranda göndererek kullanıcının sanal klavyeyle işlemiş olduğı şifrelere ulaşabilme imkânını verir. Ekrandaki bilgisayar görüntüsünün kaydedilmesi, bilgilerin alınması şeklinde de ifade edilebilir²⁹⁴.

²⁹⁰ Orta, **a.g.e.**, s. 107.

²⁹¹ Dülger, **a.g.e.**, s. 117.

²⁹² Canberk/Sağıroğlu, **a.g.m.**, s. 126.

²⁹³ Dilek, **a.g.t.**, s. 41.

²⁹⁴ Yazıcıoğlu, “Dialler, Key Logger Programları- İnternet Bankacılığı Dolandırıcılığı”, s. 80.

Bu programların gerçek işlevi bilgisayar ekranındaki görüntünün kaydedilerek kullanıcının internet bankacılığındaki kişisel şifre ve bilgileri gibi verilere ulaşımın sağlanmasıdır. İster key logger isterse de screen logger programları kullanılsın yüklendikleri bilgisayardaki bilgileri programı kullanana ilettiklerinden hareket gerçekleşmiş olacaktır²⁹⁵.

Burada sadece bir kısmını anlatabildiğimiz bu tür yazılımlar teknolojinin gelişmesiyle her geçen gün çoğaltmaktadır. Takip edilmesi güç bir hızla ilerleyen dijital gelişmelere karşı her kullanıcının dikkatli olması gerekmektedir. Konuya gereken önemin verilmesi, bilgi birikimin artırılması ve gereken önlemlerin alınması gerekmektedir.

D. Bilişim Suçlarının Tarihi Gelişimi

Bilişim suçları ilk ortaya çıktığında, bilişim araçlarında kullanılan sistemlerin ve programların kendi kendilerini korumaya yeterli imkânlarla sahip olduğu ve dolayısıyla ayrı bir korumaya ihtiyaç duyulmayacağı düşünülmüştür. Programların satışında, program paketinin alıcı tarafından açılmasıyla başlayan lisans anlaşması hükümleri ve aksine davranış haline çeşitli yaptırımlar getiren düzenlemeleriyle bu alanın korunduğu fikri hâkim olmuştur. Daha sonraları virüs programları gibi önüne geçilemez suç işleme biçimleri olduğu fark edilmiş ve ayrı bir yasal korumanın gerekliliği önem kazanmıştır²⁹⁶.

1960'lı yılların sonuna kadar zaten bilişim suçları bilinmemekteydi, on kadar bilgisayarın bilgi işlem ile ilgili bütün sorunları çözeceği düşünülmekteydi. Bilgisayarın yayılma süreci bütün tahminleri boşa çıkarırken bilgisayar güvenliği ve kişisel gizlilik gibi konularla ilgili yeni sorunların ortaya çıkmasına neden olmuştur. Hızlı otomasyonun sonucu olarak bilişim suçları da artmıştır. Bilişim sistemine adapte

²⁹⁵ A.e., s. 80.

²⁹⁶ Ersoy, a.g.m., s. 156.

edilebilecek etkin kontrol yöntemlerinin olmaması kasıtlı fiillerin yapılması riskini de arttırmaktadır²⁹⁷.

Avrupa'nın bu suçlarla tanışması ise 1970'li yılları bulmuştur. Örneğin 1973 yılında Almanya'da bir şirkette çalışmakta olan iki kişi şirketin bilgisayarına sahte faturalar girmek suretiyle kendi banka hesaplarına 295.000 Mark aktarmışlardır. Faturaların aslına uygun düzenlenmesi için gereken şirket görevlilerinin imzası ise bir ressam tarafından taklit edilerek faturalar düzenlenmiştir. İmzaları taklit eden ressam 6 ay, şirkette çalışan iki kişi ise 18 ay hapis cezasına mahkûm olmuşlardır²⁹⁸.

1980'li yıllarda bilişim suçlarının o zamana kadar korunan değerlerin yanında maddi olmayan değerlere yani verilere zarar vermiş olması durumunu da korunması gerektiği düşüncesi ortaya çıkmıştır²⁹⁹.

1990'lara gelindiğinde ise birçok ülke ceza hukuku mevzuatında bu suçları düzenlemiştir³⁰⁰.

2000'li yıllarda da bilişim suçları önceki yıllara göre artarak işlenmeye devam etmiştir. İnternet aracılığıyla gönderilen virüsler, birçok bilgisayar sistemini çalışamaz hale getirmiştir. Birçok ülke de bu ilerlemeye kayıtsız kalmayarak bilişim suçlarının işlenmesinde kullanılan cihaz ya da programların üretilmesi, bunların ticaretinin yapılması, veri naklinin izlenmesi gibi fiilleri ceza kanununda yaptırım altına almıştır³⁰¹.

Bilişim suçlarının sayısı bildiklerimizle sınırlı değildir. Gündelik hayatta işlenen pek çok suç yetkili makamlara bildirilirken diğer kısmı ise bildirilmemektedir. Keza yetkili makamlara bildirilmesine rağmen suç failinin bulunması sırasında yaşanan zorluklar nedeniyle failin tespit edilemediği birçok suç da bulunmaktadır³⁰².

²⁹⁷ Aydın, **a.g.e.**, s. 13, 22.

²⁹⁸ Tiedemann, **a.g.m.**, s. 323.

²⁹⁹ Akbulut, **a.g.e.**, s. 26.

³⁰⁰ Değirmenci, **a.g.t.**, s. 147; Kurt, **a.g.e.**, s. 115.

³⁰¹ Akbulut, **a.g.e.**, s. 53.

³⁰² **A.e.**, s. 54.

Yaşanan gelişmeler göz önüne alındığında bilişim suçlarının ceza hukukunun gündemini daha uzun yıllar meşgul edeceğini söylemek mümkündür. Sanal gerçeklik, yapay zekâ, bio teknoloji, sürücüsüz araçlar gibi teknolojik alanda yaşanan gelişmeler ceza hukukunun konusu olacaktır. Yapay zekalı makinelerin suç işlemesi ya da bunların suç işlemede kullanılması söz konusu olacak ve sorumluluğun ne şekilde olacağı ceza hukukunu meşgul edecektir³⁰³.

E. Avrupa Konseyi Siber Suç Sözleşmesi

Bilinen suçların yeni teknolojiyle işlenir duruma gelmesiyle yeni bazı suç türlerinin de belirlenmesi gerekmiştir. İnternetin yaygınlaşmasıyla artık ulusal kanunlarla bu sorunu çözmek yetersiz kalmaya başlamıştır. Geleneksel ceza hukuku kuralları siber uzay olanaklarının kötüye kullanılmasını engellemeye yetmemekte, coğrafi sınırlar etkisiz kalmaktadır. Bu sorunun çözümü için uluslararası bir işbirliği gerektirmesinin sonucu olarak Siber Suç Sözleşmesi sınır tanımayan bilgi erişimine, sınır tanımayan bir ceza hukuku sistemi kurarak bunu sağlamaya çalışmıştır³⁰⁴.

Bilişim suçlarında bir ülkede serbest olan fiil diğer bir ülkede suç olarak kabul edilmiş olabilir. Bu nedenle ulusal kuralların yanında uluslararası bazı kurallara da ihtiyaç vardır. Bu sözleşme, genel ilkeleri ortaya koyan siber suçlar konusundaki ilk uluslararası belgedir³⁰⁵.

Uluslararası platformda işlenen suçların ortak bir tanım altında toplanıp, izlenmesi ve düzenlenmesi amacıyla Avrupa Konseyi Suç Sorunları Komitesi 1996 yılında siber suçlarla ilgili bir uzmanlar komitesi kurulmasına karar vermiştir³⁰⁶. Komitenin yaptığı son çalışmalar sonucunda Avrupa Konseyi Siber Suç Sözleşmesi 23 Kasım 2001 tarihinde Budapeşte’de imzalanmıştır. Sözleşme ilk olarak yirmi altısı

³⁰³ A.e.

³⁰⁴ Füsün Sokullu Akıncı, “Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi”, **İÜHFM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 12.

³⁰⁵ Özbek, “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları”, s. 105, 106.

³⁰⁶ Fatih Selami Mahmutoglu, “Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Sorumluluğu”, **İÜHFM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 39, 40.

Avrupa Konseyi üyesi, dördü üye olmayan (ABD, Japonya, Kanada ve Güney Afrika) toplamda 30 ülke tarafından imzalanmıştır³⁰⁷. Üye olmayan bu dört ülkenin gözlemci statüsü vardır³⁰⁸.

Sözleşme şu an itibariyle otuz biri Avrupa Konseyi üyesi toplamda 56 ülke için yürürlüktedir. Sözleşmenin etkisi yalnızca imza veya onay sayısı ile ölçülemeyecek denli önemlidir zira bu ülkelerin dışında Arjantin, Pakistan, Filipinler, Mısır ve Nijerya sözleşmeyi model hukuk olarak kullanan ve resmi olarak taraf olmadan ulusal mevzuatlarını buna uygun şekilde hazırlayan devletlerdir³⁰⁹.

Budapeşte’de 23/11/2011 tarihinde imzaya açılan ve 1/7/2004 tarihinde yürürlüğe giren “Sanal Ortamda İşlenen Suçlar Sözleşmesi”ni Türkiye 10/11/2010’da Strazburg’da imzalamıştır. Bu sözleşme TBMM tarafından 22/4/2014 tarih ve 6533 sayılı “Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun” ile onaylanması uygun bulunarak 2/5/2014 tarih ve 28988 sayılı Resmi Gazete ’de yayımlanarak iç hukukumuzun bir parçası haline gelmiştir³¹⁰.

Sözleşmenin önemli özelliği Avrupa Konseyi’ne üye olmamasına rağmen aralarında bilişim alanında çok gelişmiş ülkelerin de bulunduğu birçok ülke tarafından imzalanması ve kendi hukuk sistemleri açısından da geçerli olacağı yönünde irade beyanında bulunulmasıdır³¹¹.

Bu sözleşme internet ve bilgisayar ağları aracılığıyla işlenen telif haklarına tecavüz, dolandırıcılık, çocuk pornografisi ve şiddet gibi fiilleri içeren ilk sözleşme olma özelliği açısından önemlidir³¹².

³⁰⁷ Biçkin, **a.g.m.**, s. 147.

³⁰⁸ Erdoğan, **a.g.e.**, s. 67.

³⁰⁹ Marco Gerche, “Siber Suç Sözleşmesi ile 10 Yıl: Avrupa Konseyi’nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarıları ve Kusurları”, Çev. Kerem Öz, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 104, 105; Dülger, **a.g.e.**, s. 198.

³¹⁰ Orta, **a.g.e.**, s. 22, 82; Dülger, **a.g.e.**, s. 99.

³¹¹ Dülger, **a.g.e.**, s. 199.

³¹² Akıncı/Alıç/Er, **a.g.m.**, s. 217.

Sözleşme, kırk sekiz maddeden ve dört bölümden oluşmaktadır. İlk bölümde sözleşmeye ilişkin tanımlara yer verilmekte, ikinci bölümde ise siber suçlar konusunda ulusal düzlemdeki maddi ceza hukuku ve ceza muhakemesi hukukuna ilişkin düzenlemeleri uyumlaştırmayı amaçlayan hükümlere, üçüncü bölümde uluslararası iş birliği, son bölüm olan dördüncü bölümde ise sözleşmenin geçerliliği, uygulanması ve imzalanması ile sözleşmedeki hükümlerle çekince konulmasını düzenleyen nihai hükümlere yer vermektedir³¹³.

Sözleşmenin üç ana amacı bulunmaktadır. Bu amaçlar siber suç olarak ifade edilen bilişim suçları ile ilgili olarak ülkelerin düzenlemelerini sözleşmeye uygun hale getirmek, ülkeler açısından siber suçların ve bilgisayar sistemi kullanılarak işlenen soruşturulması ve kovuşturulması için gerekli olan ceza muhakemesi yetkilerini belirlemek ve son olarak da suçlarla etkin mücadele için sözleşmeye taraf ülkeler arasında iş birliği ağının oluşturulmasını sağlamaktır³¹⁴.

Bu üç amacın yanı sıra bilgisayar sistemlerinin, ağlarının ve bilgisayar verilerinin gizliliğine, doğruluğuna ve ulaşılabilirliğine zarar verici faaliyetlerin ayrıca bu sistemlerin, ağların ve verilerin kötü amaçlı kullanımının engellenmesi, bu tür faaliyetlerin cezai niteliklerini belirlemek ve söz konusu cezai suçlarla etkili biçimde mücadele edilmesi için gerekli yetkilerin temin edilmesini sağlamak da sözleşme ile hedeflenmiştir³¹⁵. Sözleşmeye taraf ülkeler siber uzay alanının suçların işlenmesi amacıyla kullanılması durumunda bu tür suçlara ilişkin delillerin bu ağlardan elde edilmesi ve bunların paylaşılması konusunda birbirlerine yardım etme yükümlülüğü altına girmektedirler³¹⁶.

³¹³ Hasan Sınar, “Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme”, Prof. Dr. Çetin Özek Armağanı, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s. 775; Kurt, **a.g.e.**, s. 90.

³¹⁴ Bayındır, **a.g.m.**, s. 58, 59; Biçkin, **a.g.m.**, s. 148.

³¹⁵ Feridun Nizam, “Avrupa Siber Suçlar Konvansiyonu ve Türk Ceza Kanunundaki Bilişim Suçlarının Karşılaştırılması”, **2. Polis Bilişim Sempozyumu Bildirileri**, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s. 217.

³¹⁶ Koca, “AKSSS’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku”, s. 786.

Sözleşme, iki ile onuncu madde arasında suç olarak tanımlanan fiilleri düzenlemiş olup, bunlar çoğunlukla verilere ve bilişim sistemine karşı hukuka aykırı amaçlarla gerçekleştirilen fillerdir³¹⁷. Bu fiillerin çoğu, taraf birçok ülke tarafından iç hukuklarında bilgisayar suçları veya bilişim alanında suçlar başlığı altında düzenlenmiştir. Sözleşmenin etkisiyle birçok ülkede internetin de yaygınlaşması sonucu ortaya çıkan hukuki sorunlara ilişkin ve özellikle de çocuk pornografisine ve şiddet içerikli yayınlara karşı yasal düzenlemelere gidilmiştir³¹⁸.

Avrupa Konseyi Siber Suç Sözleşmesi incelendiğinde internet ortamında ceza sorunluluğunun düzenlenmesi sırasından “*İnternet Ortamında Ceza Sorumluluğunun Avrupa Ana İlkeleri*” olarak dört ilke sayabilir, bunlardan ilki siber suçlarla ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce ve söz özgürlüğü ile iletişim özgürlüğü olmak üzere tüm temel hak ve özgürlüklerin gereklerine uyulmasıdır. İkinci ilke bilgisayarlarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak minimum standarda uyulması gerekliliğidir. Üçüncü ilke fiilin hukuka aykırı olması gerekmesidir. Son ilke ise fiilin kasten işlenmesi gerekmesidir³¹⁹.

Sözleşme incelendiğinde, bilişim suçlarının kapsamının sadece bilgisayar ve veriye yönelik fiilleri esas almadığı bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşmasıyla ortaya çıkan sorunları da kapsadığı görülecektir. Bu açıdan çocuk pornografisi, telif haklarına ilişkin ihlaller ve son olarak ek protokolle kapsama alınan yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükümler bu grubu oluşturur³²⁰.

Bazı bilişim suçlarının 5237 sayılı TCK’da düzenlenmediğini belirtmek gerekir. Örneğin; AKSSS m. 3’te düzenlenen bilgisayar sistemleri arasındaki iletişime müdahale suçunu yaptırım altına alan düzenleme bulunmamaktadır. Yine m. 6’da düzenlenen bilişim sistemlerine yasa dışı erişimi, müdahaleyi, sistemde yer alan verilere erişim ve müdahaleyi sağlayan cihazların, bilişim sistemine erişimi sağlayan

³¹⁷ Değirmenci, **a.g.t.**, s. 121.

³¹⁸ Kızıltan, **a.g.t.**, s. 39.

³¹⁹ İçel, **a.g.m.**, s. 6 vd.

³²⁰ Ketizmen, **a.g.e.**, s. 53; Erdoğan, **a.g.e.**, s. 70, 71.

eriřim kodlarının bulundurulması, üretimi, satışı, ithali veya dağıtımı gibi fiiller kanunumuzda suç olarak düzenlenmemiştir³²¹. Birtakım cihazların sözleşmede belirtilen suçların işlenmesi amacıyla elde edilmesi veya satılması gibi hareketlerin sözleşmeye taraf ülkelerle ortak bir ceza politikası belirlemek açısından kanunumuzda düzenlenmesi kovuşturma ve iade konularında uluslararası işbirliği konularında ülkemize kolaylık sağlayacaktır³²².

Siber Suç Sözleşmesi önemli bir adım olmakla beraber henüz sadece başlangıçtır. Sözleşme globalleşme amacıyla Avrupa Konseyi üyesi olmayan devletlere açık olsa da sözleşme bölgesel bir araç olup uzun vadede Rusya ve Çin gibi birçok siber saldırının gerçekleştiği ülkenin katılımıyla daha uygulanabilir nitelik kazanabileceği değerlendirilmektedir³²³.

Verilere müdahale başlıklı 4. maddenin amacı, bilgisayar verilerini ve bilgisayar programlarını da maddi varlığa sahip nesneler gibi kasıtlı olarak zarar verme fiillerine karşı korumaktır. Korunan hukuki yarar, depolanmış bilgisayar verileri ya da bilgisayar programlarının bütünlüğü ve uygun biçimde çalışmalarıdır³²⁴.

Sisteme müdahale başlıklı 5. madde ise bilgisayar sabotajı olarak adlandırılmaktadır. Bu hükmün amacı bilgisayar sistemlerinin hukuka uygun olarak kullanımının uluslararası düzeyde engellenmesinin fiilinin suç olarak belirlenmesidir. Korunan hukuki değer, bilgisayar sistemlerinin işletmecilerinin ve kullanıcılarının bu sistemleri uygun biçimde işletme haklarıdır. Her türlü işleyiş biçiminin koruma altına alınması amacıyla madde tarafsız bir dille yazılmıştır³²⁵. Sistemin işleyişinin engellenmesine ilişkin müdahaleler sisteme veri yoluyla müdahale edilmesi ya da sistem içerisindeki verilere müdahale edilmesi temel alınarak düzenlenmiştir. Bu açıdan fiziki müdahaleler sözleşmede sistemin işleyişine müdahale kapsamında

³²¹ Değirmenci, **a.g.m.**, s. 208.

³²² Koca, “AKSSS’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku”, s. 803.

³²³ Önok, **a.g.m.**, s. 1263, 1264.

³²⁴ Sokullu-Akıncı, **a.g.m.**, s. 18; Helvacıoğlu, **a.g.m.**, s. 284.

³²⁵ Sokullu-Akıncı, **a.g.m.**, s. 20; Koca, “AKSSS’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku”, s. 801.

değerlendirilmemiştir³²⁶. Engellemenin ise ciddi olması gerekir, ciddiyet tanımına taraf ülkelerin açıklık getirmesi öngörülmüştür³²⁷.

8. maddede düzenlenen bilgisayar aracılığıyla dolandırıcılık sistemin işleyişine ekonomik yarar sağlanması amacıyla müdahale edilmesi ve yarar sağlanması şeklinde tanımlanmış ve maddede sisteme yeni veri yerleştirilmesi, verinin değiştirilmesi, silinmesi veya erişilmez kılınması ya da işleyişe yönelik herhangi bir müdahale seçimlik hareketler olarak düzenlenmiştir³²⁸. Suça konu fiil bu fiile izin veren bir hakka sahip olmadan haksız gerçekleştirilmiş olmalı ve kazanılan ekonomik fayda da haksız kazanılmış olmalıdır. Diğer bir önemli ifade ise bilgisayar sisteminde ya da veride değişiklik yapan kişinin kendisinin ya da bir başkasının ekonomik fayda kazanmak niyeti ile kasıtlı olarak davranmış olması gerekmesidir³²⁹.

F. Türk Hukukunda Bilişim Sistemine Yönelik Düzenlemeler

Bilişim sistemlerinin tehdit ve risklere açık olması dolayısıyla bu alanların düzenlenmesi gerekliliği ortaya çıkmakta ve bu çerçevede bilgi ve belge iletişimi, finansal ve kurumsal işlemler ile teknolojik altyapı ve uluslararası standartlara yönelik düzenlemeler yanında ilgili kanunlarda bu hukuka aykırı fiilleri önleyici ve caydırıcı hükümlerin kurulması gerekmektedir³³⁰.

Dünyadaki gelişmelere paralel olarak Türkiye’de de 1987 tarihli Türk Ceza Kanunu Ön Tasarısı’nda bilişim suçları ile ilgili bir düzenleme yer almamasına karşın, 1989 Ön Tasarısı’nda 342 ile 346. maddeleri arasında bu suçlara taslak olarak yer verildi³³¹.

Bilişim suçlarının konusu olan veri, program ve diğer unsurlar klasik ceza hukuku anlayışı çerçevesinde cismi olan bir şey veya bir enerji olarak kabul

³²⁶ Ketizmen, **a.g.e.**, s. 51.

³²⁷ Helvacıoğlu, **a.g.m.**, s. 285.

³²⁸ Ketizmen, **a.g.e.**, s. 53.

³²⁹ Helvacıoğlu, **a.g.m.**, s. 287.

³³⁰ Metin Turan, **Bilişim Hukuku**, Ankara, Seçkin Yayıncılık, 2017, s. 34.

³³¹ Değirmenci, **a.g.t.**, s. 147.

edilemeyeceğinden taşınır mallar gibi mülkiyetin fiziki olarak bir kişiden diğerine geçirilmesi mümkün olmadığından bu unsurlara yönelik yapılan elde etme fiilleri hırsızlık suçu hakkındaki genel düzenleme ile korunamamaktadır. Kıyas yasağı ve kanunilik ilkeleri gereğince kanunda düzenlenmemiş bir hususun yorumla başka bir kanun maddesi kapsamında kaldığı söylenemeyecektir. Bu nedenle bilişim sahasının düzenlenmesi ve bu sahada ortaya çıkan ihlallerin ayrı müeyyideye bağlanması zorunluluk haline gelmiş ve bilişim suçları kavramı ilk kez 765 sayılı Türk Ceza Kanunu'nda değişiklik ve ekleme yapan 06.06.1991 tarih ve 3756 sayılı Kanunla Türk hukuk mevzuatına girmiştir. Bu düzenlemeler ise 765 sayılı Türk Ceza Kanunu'nu kaldıran ve 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı TCK'daki hükümler uygulanmaya başlayıncaya kadar yürürlükte kalmıştır³³².

Bilişim suçlarına ilişkin kanunlaştırma çabalarından ilki 1991 yılında TCK'da yapılan değişiklik, ikincisi ise 1995 yılında Fikir ve Sanat Eserleri Kanunu'nda yapılan değişikliktir. İlk olarak, 14.6.1991 tarih ve 3756 sayılı Kanunun 20. maddesi ile 765 sayılı Türk Ceza Kanunu'na "Bilişim Alanında Suçlar" başlığını taşıyan on birinci bap eklenmiştir. Bu suçlar, 1989 tarihli Türk Ceza Kanunu ön tasarısından birkaç fark dışında aynen alınarak kanunlaştırılmıştır. Bununla birlikte 765 sayılı Türk Ceza Kanunu'na 525. maddeden sonra gelmek üzere 525 a, 525 b, 525 c, 525 d olmak üzere dört madde eklenmiştir. Bu hükümler Fransız Ceza Kanunu Projesinden (madde 307)³³³ yararlanılarak meydana getirilen ön tasarının kanunlaştırılmasıyla oluşturulmuştur. Ancak bu suçlar Fransız Ceza Kanununda olduğu gibi "Mal Aleyhinde İşlenen Suçlar" bölümünde hüküm altına alınmamış, TCK'da "Cürümler" başlığını taşıyan ikinci kitabının "Bilişim Alanında Suçlar" adını taşıyan on birinci babında düzenlenmiştir³³⁴. 525/a-1 maddesinde verilerin hukuka aykırı olarak ele geçirilmesi, 525/a-2 maddesinde başkasına zarar vermek için verilerin kullanılması, nakledilmesi veya çoğaltılması, 525/b-1 maddesinde verilere ve sistemin işleyişine

³³² Kurt, **a.g.e.**, s. 115, 116.

³³³ Fransız Ceza Kanunu Projesinin 307. maddesi 5 Ocak 1988 tarihinde kanunlaşmış ve bu kanunun getirdiği hükümler, 1994 tarihli yeni Fransız Ceza Kanunun da esasını oluşturmuştur. Dönmezer, **a.g.e.**, s. 613; Yılmaz Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, C:II, S:2, 2005, s. 398.

³³⁴ Akbulut, **a.g.e.**, s. 96.

zarar verilmesi, 525/b-2 maddesinde bilişim sistemi aracılığıyla hukuka aykırı yarar sağlanması, 525/c maddesinde verilerde sahtekarlık suçu düzenlenmiştir. İkinci düzenleme ise 1995 yılında 4110 sayılı kanunla FSEK'e eklenen ve bilgisayar programlarını eser olarak kabul eden değişikliktir³³⁵.

1. 1989 Tarihli TCK Ön tasarısı

1989 TCK Ön tasarısı literatürümüzde bilişim suçlarının düzenlendiği ilk metindir. Özel Hükümler başlıklı ikinci kitabın “Topluma Karşı Suçlar” başlıklı ikinci kısmının “Bilişim Alanında Suçlar” başlıklı dokuzuncu bölümünde düzenlenmiştir³³⁶. Ön tasarının 342. maddesinde hile ile bilgi elde etme ve bunları haksız kullanma³³⁷, 343. maddesinde yarar sağlama ve zarar verme³³⁸, 344. maddesinde sahtecilik³³⁹, 345. maddesinde ferî cezalar³⁴⁰, 346. maddesinde³⁴¹ bu suçlardan dolayı tüzel kişilerin de

³³⁵ A.e., s. 37; Yazıcıoğlu, a.g.e., s. 205.

³³⁶ Yazıcıoğlu, a.g.e., s. 207.

³³⁷ Ön tasarının 342. maddesi şu şekildedir; “Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve bir milyon liradan on beş milyon liraya kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri ve diğer herhangi bir unsuru başkasına zarar vermek üzere, kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkra yazılı ceza verilir.” Değirmenci, a.g.t., s. 149.

³³⁸ Ön tasarının 343. maddesi şu şekildedir; “Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak amacıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemlerini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan elli milyon liraya kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyon liradan yirmi milyon liraya kadar ağır para cezası verilir.” Değirmenci, a.g.t., s. 150.

³³⁹ Ön tasarının 344. maddesi şu şekildedir; “Hukuk alanında delil olarak kullanılmak amacıyla, sahte bir belgeyi oluşturmak için bilgileri otomatik işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrip eden veya tahrip edilmiş olanları kullanan kimseye bir yıldan üç yıla kadar hapis cezası verilir.” Değirmenci, a.g.t., s. 150, 151.

³⁴⁰ Ön tasarının 345. maddesi şu şekildedir; “342 ve 343 üncü madde hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak aşağıdaki ferî cezalar da verilir: 1. İcrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma; 2. Suçun işlenmesinde kullanılan veya bu maksada tahsis edilmiş bulunan veya suçtan meydana gelen şeylerin müsadere; 3. Suç teşkil eden fillerin işlenmesinde kullanılan kurumların veya teşebbüse ait bir veya birden çok kurumun iki aydan bir yıla kadar kapatılması” Değirmenci, a.g.t., s. 151.

³⁴¹ Ön tasarının 346. maddesi şu şekildedir; “Bu bölüme giren suçlardan dolayı tüzel kişiler de sorumludur. Bu bölüme giren suçlara teşebbüs halinde tamamlanmış suçun cezası verilir.” Kurt, a.g.e., s. 120.

sorumlu olduđu ve teşebbüs halinde suçun tamamlanmış hali gibi cezalandıracağı hususları düzenlenmiştir³⁴².

Ön tasarının 342. maddesinin gerekçesinde, Türk ceza hukukunda ilk kez telaffuz edilen bilişim alanının tarifi, bilgileri toplayıp depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden oluşan alan şeklinde olmuştur. Bilgileri otomatik olarak işleme tabi tutan sistem ile bilgisayarın kastedildiği belirtilmiştir³⁴³.

Tasarıda geçen “bilgileri otomatik işleme tabi tutmuş sistemden” söz edilmek suretiyle ceza kurallarının uygulama alanının geniş tutulmak istendiği söylenebilir. Bu sistemlerin temelini teşkil eden bilgisayar kavramının esas alınmaması da bilgisayar kavramının dar olarak anlaşılması halinde aynı esasa dayalı sistemlerle ilgili olarak işlenebilecek aynı fiillerin cezasız kalmasının önüne geçilmesi bakımından isabetlidir³⁴⁴.

2. 3756 Sayılı Kanunla 765 Sayılı TCK’ya Eklenen Düzenleme

Yukarıda bahsedilen 1989 TCK Ön tasarısında yer alan maddeler birkaç değişiklik dışında, gerekçeleri de aynı olmak üzere, 14.6.1991 tarih ve 3756 sayılı kanunla TCK’ya dâhil edilmiştir. Tasarı ile kanunlaşan metin arasındaki ilk fark, sistem marifetiyle sahtecilik fiilindedir. Ön tasarının 344. maddesinde verileri veya diğer herhangi bir unsuru tahrif eden kişi ile tahrif edilen verileri kullanan kişiye aynı ceza hükmedilmişken, kanunlaşan metinde her iki failin cezası farklıdır. Başka bir söyleyişle, hem sahte veri oluşturmak ve hem de sahte olarak oluşturulmuş verileri kullanmak tasarıda da kanunda da suç olarak kabul edilmesine rağmen 525/c maddesinde ceza hususunda farklılık yaratılmıştır³⁴⁵.

³⁴² Kurt, **a.g.e.**, s. 117.

³⁴³ **A.e.**, s. 119.

³⁴⁴ Ersoy, **a.g.m.**, s. 165.

³⁴⁵ Akbulut, **a.g.e.**, s. 101.

İkinci fark ise Ön Tasarı m. 346/2’de yer alan “bu bölüme giren suçlara teşebbüs halinde tamamlanmış suçun cezası verilir.” kısmının çıkartılmasıdır³⁴⁶.

Üçüncü fark Ön Tasarı m. 346/1’de yer alan “*bu bölüme giren suçlardan tüzel kişiler de sorumludur.*” ibaresinin çıkarılmasıdır³⁴⁷.

Son fark ise, Ön Tasarı m. 345/2 ve m. 345/3’teki müsadereye ve kurumların kapatılmasına ilişkin hükümlerin kanunlaşan metnin kapsamına alınmayıp, sadece meslekten yasaklanmaya ilişkin ilk fıkranın kanunlaşmasıdır³⁴⁸.

Bu kanun TCK’ya On birinci Bap olarak “Bilişim Alanında Suçlar” başlığı altında 525/a³⁴⁹, 525/b³⁵⁰, 525/c³⁵¹ ve 525/d³⁵² maddelerini eklemiştir. İlk üç fıkra hukuki yarar ve konularını birbirinden farklı birden çok suçu düzenlerken, 525/d maddesi, 525/a ve 525/b maddelerinde yer alan hükümleri ihlal eden kişiler hakkında uygulanacak ferî cezaları düzenlemektedir³⁵³.

³⁴⁶ Değirmenci, **a.g.t.**, s. 152; Akbulut, **a.g.e.**, s. 102.

³⁴⁷ Değirmenci, **a.g.t.**, s. 152; Akbulut, **a.g.e.**, s. 102.

³⁴⁸ Değirmenci, **a.g.t.**, s. 152; Akbulut, **a.g.e.**, s. 102.

³⁴⁹ Ön tasarinın 525/a maddesi şu şekildedir; “*Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve bir milyon liradan on beş milyon liraya kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkra yazılı ceza verilir*” Değirmenci, **a.g.t.**, s. 162, 166.

³⁵⁰ Ön tasarinın 525/b maddesi şu şekildedir; “*Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan elli milyon liraya kadar ağır para cezası verilir. Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyon liradan yirmi milyon liraya kadar ağır para cezası verilir.*” Değirmenci, **a.g.t.**, s. 167.

³⁵¹ Ön tasarinın 525/c maddesi şu şekildedir; “*Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrip eden kimseye bir yıldan üç yıla kadar, tahrip edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir*” Değirmenci, **a.g.t.**, s. 167.

³⁵² Ön tasarinın 525/d maddesi şu şekildedir; “*525/a ve 525/b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak, meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma cezası da verilir.*” Akbulut, **a.g.e.**, s. 98.

³⁵³ Değirmenci, **a.g.t.**, s. 162.

Düzenlemeler suçla korunan hukuki değer kavramına göre değil bilgisayar ortak kavramına göre yapılmıştır. Kanundaki maddelerin hiçbirisinde bilişim kavramı kullanılmamasına rağmen maddelerin yer aldığı on birinci babın başlığı “Bilişim Alanında Suçlar” dır. Maddelerde ise bilişim kavramı yerine “bilgileri otomatik işleme tabi tutmuş sistem” kavramı kullanış ancak bu kavramın tanımı yapılmamıştır³⁵⁴.

3. 1997 Tarihli TCK Tasarısı

765 sayılı Türk Ceza Kanunu’na yöneltilen eleştiriler nazara alınarak Adalet Bakanlığınca oluşturulan komisyondan 1989 tarihli TCKÖT’yi gözden geçirmeleri istenilmiş, bir senelik çalışmanın sonucunda komisyon 1997 tarihinde bir metin ortaya çıkarmıştır³⁵⁵. Yeni hükümler ilave edilerek madde sayısı altıya çıkarılmıştır³⁵⁶.

1997 tarihli Türk Ceza Kanunu tasarısı, 1989 tarihli Türk Ceza Kanunu Ön tasarısında olduğu gibi bilişim suçlarını “Bilişim Alanında Suçlar” başlığı altında 347 ile 352. maddeleri arasında düzenlemiştir. Tasarının 3756 sayılı Kanundan ilk farkı “bilgileri otomatik olarak işleme tabi tutmuş sistem” kavramı yerine “bilişim sistemi” kavramının kullanmasıdır. Tasarının diğer farkı ise, sisteme girme fiillerinin ayrıca verilerin ele geçirilmesi koşulu gözetilmeden suç haline getirilmesidir³⁵⁷.

Bundan sonraki tasarıların da benimseyeceği gibi ilk defa bilgileri otomatik olarak işleme tabi tutan sistem yerine bilişim sistemi tabiri kullanılmış ayrıca bilişim sistemlerine yönelik girme fiili de suç olarak düzenlenmiştir. Tasarının 347. maddesinde bilişim sistemine girme, verileri tahrip ve bozma³⁵⁸, 348. maddesinde bilişim sisteminin işleyişini engelleme, bozma ve bilişim sistemlerinden haksız yarar

³⁵⁴ Erdoğan, **a.g.e.**, s. 76.

³⁵⁵ Kurt, **a.g.e.**, s. 123.

³⁵⁶ Erdoğan, **a.g.e.**, s. 78.

³⁵⁷ Değirmenci, **a.g.t.**, s. 152, 153.

³⁵⁸ Ön tasarının 347. maddesi şu şekildedir; “Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve yüz milyon liradan üç yüz milyon liraya kadar ağır para cezası verilir. Bu fiil nedeniyle sistemin içerdiği veriler yok edilir veya değişirse faile iki yıldan dört yıla kadar hapis ve iki yüz milyondan altı yüz milyon liraya kadar ağır para cezası verilir. Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir.” Değirmenci, **a.g.t.**, s. 153.

sağlama³⁵⁹, 349. maddesinde bilişim sistemleri marifetiyle sahtecilik³⁶⁰, 350. maddesinde ferî cezalar³⁶¹, 351. maddesinde tüzel kişilerin sorumluluğu³⁶², 352. maddesinde söz konusu suçları işlemek üzere örgütlenme³⁶³ hususları düzenlenmiştir³⁶⁴.

4. 2000 Tarihli TCK Tasarısı

Bilişim suçları, söz konusu tasarının ikinci kitabının ikinci kısmının dokuzuncu bölümünde “Bilişim Alanında Suçlar” başlığı altında 346 ile 352. maddeleri arasında düzenlenmiştir³⁶⁵. Burada en dikkat çeken husus, kanun koyucunun bu tür suçları artık mal aleyhine işlenen suçlar içinde değil, topluma karşı suçlar içerisinde düzenlemesidir³⁶⁶.

1997 tarihli Türk Ceza Kanunu Ön Tasarısı’nın 347, 348, 349, 350. maddeleri 2000 tarihli Türk Ceza Kanunu Ön Tasarısı’na gerekçeleriyle birlikte bazı kelime

³⁵⁹ Ön tasarının 348. maddesi şu şekildedir; “Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve yüz milyon liradan beş yüz milyon liraya kadar ağır para cezası verilir. Bilişim sistemine hukuka aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve üç yüz milyon liradan bir milyar liraya kadar ağır para cezası verilir. Yukarıdaki fıkralarda belirtilen eylemlerle fail, başkasının zararına ve kendisinin veya başkasının yararına haksız bir menfaat sağlarsa iki yıldan beş yıla kadar hapis ve iki yüz milyon liradan bir milyar liraya kadar ağır para cezasına hükmedilir. Bu suçlara teşebbüs halinde faille tamamlanmış suç cezası verilir.” Kurt, **a.g.e.**, s. 125, 126; Değirmenci, **a.g.t.**, s. 154.

³⁶⁰ Ön tasarının 349. maddesi şu şekildedir; “Hukuk alanında bir neticeye ulaşmak maksadıyla, sahte bir belgeyi oluşturmak için bilişim sistemine verileri yerleştiren veya var olan verileri tahrif eden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Birinci fıkrafta belirtilen sahte belgeyi kullananlara da aynı ceza verilir.” Değirmenci, **a.g.t.**, s. 155; Kurt, **a.g.e.**, s. 127.

³⁶¹ Ön tasarının 350. maddesi şu şekildedir; “347 ve 348 inci madde hükümlerini ihlal eden kişiler hakkında yukarıdaki maddelerde yazılı cezalara ek olarak aşağıda belirtilen fer’î cezalara da hükmolunur: 1. Meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma ve ayrıca suçta kullanılan araçların veya suçtan meydana gelen şeylerin müsaderesi.”

³⁶² Ön tasarının 351. maddesi şu şekildedir; “347 ve 348. Maddelerde gösterilen suçlardan dolayı tüzel kişiler de sorumludur” Değirmenci, **a.g.t.**, s. 155.

³⁶³ Ön tasarının 352. maddesi şu şekildedir; “Yukarıdaki maddelerde öngörülen suçları işlemek için oluşturulmuş ve varlığı bir veya birden çok maddi nitelikte hazırlıklardan anlaşılan bir teşekkülü kuran veya buna katılan kimselere işlemek istedikleri suçlardan en ağırının cezası verilir.” Değirmenci, **a.g.t.**, s. 156

³⁶⁴ Kurt, **a.g.e.**, s. 118.

³⁶⁵ Değirmenci, **a.g.m.**, s. 198.

³⁶⁶ Yazıcıoğlu, “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, s. 174.

farklarıyla ve para cezalarının güncellenmesi ile sırasıyla 346, 347, 348 ve 349. maddeleri olarak alınmış, yalnızca feri cezaların düzenlendiği 349. maddede fiillerin işlenmesinde kullanılan araçların müsaderesinin yanında “veya mülkiyetin devlete geçirilmesi” ifadesi eklenmiştir. Bu tasarının getirdiği en büyük yenilik ise hala da geçerliliğini koruyan banka ve kredi kartlarının kötüye kullanılması başlıklı 350. maddenin bilişim alanında suçlar arasında yer almasıdır.

Bu bölümde bulunan 346. maddede bilişim sistemlerine girme, verileri tahrip ve bozma³⁶⁷, 347. maddesinde sistemi engelleme, bozma, haksız yarar sağlama³⁶⁸, 348. maddesinde sahtecilik³⁶⁹, 349. maddesinde feri cezalar³⁷⁰, 350. maddesinde

³⁶⁷ Ön tasarının 346. maddesi şu şekildedir; “Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve bir milyar liradan üç milyar liraya kadar ağır para cezası verilir. Bu fiil nedeniyle sistemin içerdiği veriler yok edilir veya değişirse faile iki yıldan dört yıla kadar hapis ve iki milyar liradan altı milyar liraya kadar ağır para cezası verilir. Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir.” Değirmenci, **a.g.t.**, s. 157.

³⁶⁸ Ön tasarının 347. maddesi şu şekildedir; “Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve bir milyar liradan beş milyar liraya kadar ağır para cezası verilir. Bilişim sistemine hukuka aykırı olarak veriler sokan veya sistemin içerdiği verileri yok eden veya değiştiren kimseye üç yıldan altı yıla kadar hapis ve üç milyar liradan on milyar liraya kadar ağır para cezası verilir. Yukarıdaki fıkralarda belirtilen eylemlerle fail, başkasının zararına ve kendisinin veya başkasının yararına haksız bir çıkar sağlarsa iki yıldan altı yıla kadar hapis ve iki milyar liradan on milyar liraya kadar ağır para cezasına hükmedilir. Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir.” Değirmenci, **a.g.t.**, s. 157.

³⁶⁹ Ön tasarının 348. maddesi şu şekildedir; “Hukuk alanında bir neticeye ulaşmak maksadıyla, sahte bir belgeyi oluşturmak için bilişim sistemine verileri yerleştiren veya var olan verileri tahrif eden kimseye bir yıldan üç yıla kadar hapis cezası verilir. Birinci fıkrada belirtilen sahte belgeyi kullananlara da aynı ceza verilir.” Dönmezer, **a.g.e.**, s. 628.

³⁷⁰ Ön tasarının 349. maddesi şu şekildedir; “346 ve 347’nci madde hükümlerini ihlal eden kişiler hakkında yukarıdaki maddelerde yazılı cezalara ek olarak aşağıda belirtilen feri’i cezalara da hükümlenir: 1) Meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma ve ayrıca suç kullanılan kurumların iki yıldan bir yıla kadar kapatılması. 2) Fiillerin işlenmesinde kullanılan araçların veya suçtan meydana gelen şeylerin müsadere veya mülkiyetin Devlete geçirilmesi.” Değirmenci, **a.g.t.**, s. 158.

banka veya kredi kartının kötüye kullanılması³⁷¹, 351. maddesinde suç işlemek için örgütlenme³⁷², 352. maddesinde tüzel kişilerin sorumluluğu düzenlenmiştir³⁷³.

5. 2003 Tarihli TCK Tasarısı

2003 tarihli TCKÖT’da ise ikinci kitabın “ Topluma Karşı Suçlar” başlıklı ikinci kısmının “Bilişim Alanında Suçlar” başlıklı dokuzuncu bölümünde düzenlenmiştir. Bu bölümde bulunan 346. maddesinde bilişim sistemlerine girme, verileri tahrip ve bozma, 347. maddesinde sistemi engelleme, bozma, haksız yarar sağlama, 348. maddesinde sahtecilik, 349. maddesinde feri cezalar, 350. maddesinde banka veya kredi kartının kötüye kullanılması, 351. maddesinde suç işlemek için örgütlenme, 352. maddesinde tüzel kişilerin sorumluluğu düzenlenmiştir³⁷⁴.

2003 TCKÖT’nin Adalet Komisyonuna görüşülmek için gönderilmesi üzerine ön tasarının geneli üzerindeki görüşmeler sonucu Adalet Alt Komisyonunca düzenlenmiş bir metin ortaya çıkarılmıştır³⁷⁵. Adalet Komisyonunca kabul edilen maddeler şu şekildedir;

³⁷¹ Ön tasarının 350. maddesi şu şekildedir; “Başkasına ait veya diğer bir kişiye verilmesi gereken bir banka veya kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına haksız yarar sağlarsa üç yıldan altı yıla kadar hapis cezası ve iki milyar liradan az olmamak üzere ağır para cezası verilir. Aynı fiil bir banka veya kredi kartını tahrip ederek veya bunu sahtecilik suretiyle meydana getirerek işlendiğinde faile birinci fıkra gereğince verilecek ceza üçte bir oranında artırılır.” Kurt, **a.g.e.**, s. 129.

³⁷² Ön tasarının 351. maddesi şu şekildedir; “Yukarıdaki maddelerde öngörülen suçları işlemek için oluşturulmuş ve varlığı bir veya birden çok maddi nitelikte hazırlıklardan anlaşılan bir örgütü kuran veya buna katılan kimselere, işlemek istedikleri suçlardan en ağırının cezası verilir.” Yazıcıoğlu, “2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, s. 183.

³⁷³ Ön tasarının 352. maddesi şu şekildedir; “346, 347, 348, 350 ve 351 inci maddelerde gösterilen suçlardan dolayı tüzel kişiler de sorumludur.” Ünver, **a.g.m.**, s. 128.

³⁷⁴ Kurt, **a.g.e.**, s. 131.

³⁷⁵ **A.e.**, s. 133.

Bilişim sistemine girme 245. maddede³⁷⁶, sisteme yönelik fiiller 246. maddede³⁷⁷, banka veya kredi kartlarının kötüye kullanılması 247. maddede³⁷⁸, tüzel kişiler ile ilgili hükümler ise 248. maddede³⁷⁹ düzenlenmiştir.

6. 5237 Sayılı TCK

Adalet Alt Komisyonunca 12.05.2004 tarihinde tamamlanmış ve metin Meclis Genel Kurulu'na görüşülmek üzere sunulmuştur. Kanun 26.09.2004 tarih ve 5237 sayısıyla kabul edilmiştir. Kanun 12.10.2004 tarih ve 25611 Sayılı Resmi Gazetede yayımlanmış ve daha sonra 1 Haziran 2005 tarihinde yürürlüğe girmiştir³⁸⁰.

Bilişim alanında suçlar adını taşıyan bölüm başlığı daha sonra TBMM Adalet Komisyonu'nda "Bilişim Sistemlerine Karşı Suçlar" olarak kabul edilmiştir. Ancak TBMM Genel Kurulunda verilen bir önerge üzerine bölüm başlığı "Bilişim Alanında Suçlar" olarak tekrar değiştirilmiştir. Söz konusu değişiklik, bu alandaki tüm suçların bilişim sistemlerine karşı işlenmemesi yönünden isabetlidir. Zira bilişim suçları bilişim sistemlerine karşı ve/veya bilişim sistemleri vasıtasıyla işlenmektedir³⁸¹.

³⁷⁶ Tasarının 245. maddesi şu şekildedir; "Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve adli para cezası verilir. Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse iki yıldan dört yıla kadar hapis ve adli para cezasına hükmolunur. Bu suçlara teşebbüs halinde suç tamamlanmış gibi cezaya hükmolunur." Kurt, **a.g.e.**, s. 134.

³⁷⁷ Tasarının 246. maddesi şu şekildedir "Bir bilişim sisteminin işleyişini engelleyen veya bozan kimseye bir yıldan üç yıla kadar hapis ve adli para cezası verilir. 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. Bilişim sistemine hukuka aykırı olarak veriler yerleştiren, sistemin içerdiği verileri başka bir yere gönderen, bozan, değiştiren, erişilmez kılan veya yok eden kimseye üç yıldan altı yıla kadar hapis ve adli para cezası verilir. İkinci fıkradaki fiillerin bir yarar sağlamak ya da bir hak veya yetkinin elde edilmesi amacıyla işlenmesi halinde verilecek ceza yarı oranında artırılır. Bu suçlara teşebbüs halinde suç tamamlanmış gibi cezaya hükmolunur." Kurt, **a.g.e.**, s. 134.

³⁷⁸ Tasarının 247. maddesi şu şekildedir; "Başkasına ait bir banka veya kredi kartını her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır. Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır. Bu fıkra tanımlanan suça teşebbüs halinde suç tamamlanmış gibi cezaya hükmolunur." Kurt, **a.g.e.**, s. 135.

³⁷⁹ Tasarının 248. maddesi şu şekildedir; "Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur." Kurt, **a.g.e.**, s. 136.

³⁸⁰ Kurt, **a.g.e.**, s. 136.

³⁸¹ Akbulut, **a.g.e.**, s. 109.

Ayrıca bilişim sistemlerine karşı veya bunlar aracılığıyla işlenen suçların kişilerin hak ve menfaatlerini ihlal etme olasılığı mevcuttur. Örneğin bu suçların havalimanı uçuş kontrol bilgisayarlarında işlenmesi durumunda toplum hayatı felç olabilir. Bu nedenle bilişim alanında suçların düzenleme yeri olan topluma karşı suçlar bölümü de isabetlidir³⁸².

Bununla birlikte bilişim sistemlerine karşı suçlar başlığını isabetsiz bulan görüşler de bulunmaktadır. Bu görüşteki yazarlar başlığın suçların mağdurunun bizzat bilişim sistemi olduğunu çağrıştırdığını belirtmektedirler³⁸³.

3756 sayılı Kanunla getirilen düzenlemede bulunmayan bilişim sistemine girme ilk defa münhasıran düzenlenen bir suç haline gelmiştir. 1997, 2000 ve 2003 tarihli tasarı ve ön tasarılarında sürekli olarak öngörülen ancak bir türlü kanunlaşmayan bu suç Kanunun 243. maddesinde düzenlenmiştir. Tasarıda yer alan bu suça teşebbüs halinde tamamlanmış suçun cezasının verileceğine dair düzenleme kanunlaşmamıştır³⁸⁴. Maddeye 24/03/2016 tarihinde eklenen dördüncü fıkra ile bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlenmesi fiili suç olarak düzenlenmiştir.

244. maddede ise 2003 tarihli Türk Ceza Kanunu Ön Tasarısı'nda bu suça teşebbüsün de tamamlanmış suç gibi cezalandırılacağına dair düzenlemeye yer verilmemiştir³⁸⁵. Maddede hüküm altına alınan fiillerin bir kısmı 765 sayılı TCK m. 525/b-1'de düzenlenen verilere zarar verme fiillerini karşılarsa da daha ayrıntılı düzenlenmiştir. Eski düzenlemede bulunmayan sisteme veri yerleştirme ve var olan verileri başka yere gönderme fiili de bu düzenleme ile yaptırım altına alınmıştır. Tahrip eden ifadesi yeni düzenlemede yer almamaktadır. Diğer yandan 765 sayılı TCK

³⁸² Değirmenci, **a.g.m.**, s. 198.

³⁸³ Cevat Özel, "Bilişim Suçlarının Türk Ceza Kanunu ve Tasarıdaki Hükümler Yönünden Mukayeseli Olarak Değerlendirilmesi", **Bilişim Hukuku**, Der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 87.

³⁸⁴ Kurt, **a.g.e.**, s. 136, 145.

³⁸⁵ Kurt, **a.g.e.**, s. 146.

m.525/c’de yer alan hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturma ibaresine yer verilmemiş ancak genel olarak hukuka aykırı veri yerleştirme veya değiştirme şeklindeki seçimlik hareketler metne alınmıştır³⁸⁶.

TCK m. 245’te banka veya kredi kartlarının kötüye kullanılması düzenlenmiştir. Bu maddeye 8.7.2005 tarih ve 25869 sayılı Resmi Gazete’ de yayınlanarak yürürlüğe giren 29.6.2005 tarih ve 5377 sayılı Türk Ceza Kanununda Değişiklik Yapılmasına Dair Kanun ile iki fıkra daha ilave edilmiştir³⁸⁷. 5560 sayılı Çeşitli Kanunlarda Değişiklik Yapılmasına Dair Kanun’un 11. maddesi ile 6/12/2006 tarihinde maddeye beşinci fıkra olarak etkin pişmanlık hükmü eklenmiştir. 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 30. maddesi ile 24/03/2016 tarihinde fıkraya ek olarak 245/A eklenmiştir.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması başlıklı 246. maddede ise bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmedileceği ifade edilmiştir³⁸⁸.

Kanunda hırsızlık, dolandırıcılık, yağma suçları gibi suçlarda kişinin bir hukuki alacağını tahsil amacıyla hareket etmesi daha az ceza gerektiren nitelikli hal sayılırken bu durumun bilişim suçları açısından öngörülmemesi eleştirilmiştir. Kişinin sattığı bir bilgisayarın ücretinin ödenmemesi durumunda zorla alması durumunda bu durum indirim nedeni sayılırken böyle yapmayıp bilgisayar programını dışardan müdahale ile bilgisayar şebekesinden silmesi durumunda sistemi ve verileri bozma suçunun tam cezasıyla cezalandırılması söz konusu olacaktır³⁸⁹.

³⁸⁶ Esen, **a.g.e.**, s. 633.

³⁸⁷ Kurt, **a.g.e.**, s. 146.

³⁸⁸ **A.e.**, s. 137.

³⁸⁹ Yazıcıoğlu, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, s. 399-400.

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE SUÇLARI

I. BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE SUÇLARI

A. Kanuni Tanım

5237 sayılı Türk Ceza Kanunu’nda bilişim alanında suçlar, Kanunun ikinci kitabının, “*Topluma Karşı Suçlar*” başlıklı üçüncü kısmının, “*Bilişim Alanında İşlenen Suçlar*” başlıklı onuncu bölümünde düzenlenmiştir. Suç sistematigi içerisinde incelenecek olan 5237 sayılı Türk Ceza Kanunu’nun ilgili maddesi ve gerekçesi şu şekildedir:

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.
(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.
(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.
(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur¹.

¹ Madde gerekçesi madde 244- 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

TBMM Adalet Komisyonu tarafından kabul edilen Tasarı metninde, 244. maddenin 1 ve 2 numaralı fıkraları, “ (1) Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.” şeklindeydi daha sonra TBMM Genel Kurulu’nda bu fıkra şimdiki halini alarak iki farklı suç haline getirilerek cezaları farklılaştırılmıştır².

TBMM Genel Kurulu’ndaki önerenin gerekçesinde bu durum, suçun konusunun bilişim sistemi olmasıyla sistemdeki veri olması arasında fiilin ağırlığı bakımından kaynaklanan farklılık olmasıyla açıklanmıştır³.

Doktrinde her ne kadar bu suçlar topluma karşı suçlar arasında düzenlese de suçların tamamı kişilerin sahip olduğu veri ya da sistemlere karşı işlendiğinden suçların kişiye karşı suçlar arasından düzenlenmesinin daha isabetli olacağını belirten yazarlar bulunmaktadır⁴.

TCK’nın 244. maddesinde üç farklı suç tipi düzenlenmiştir. Birinci fıkroda “bilişim sistemine müdahale suçu” ikinci fıkroda ise “bilişim sistemindeki verilere müdahale suçu” fiilleri suç haline getirilmiştir⁵. Maddenin üçüncü fıkrasında ise ilk iki fıkroda düzenlenen suçların ortak nitelikli haline yer verilmiştir. Maddenin ilk iki fıkrasında düzenlenen suçlar, doğrudan bilişim sistemini ve bu sistemdeki verileri

diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkroda seçimlik hareketli bir suç meydana getirilmiştir. İkinci fıkroda, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde verilecek cezanın artırılması öngörülmüştür.

Üçüncü fıkroda ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir. Mustafa Artuç/Yıldırım Bayyurt, **Gerekçeli, Karşılaştırmalı, Tablolu, Eski ve Yeni Metinleriyle 5237 sayılı TCK**, Ankara, Seçkin Yayınları, 2008, s. 403.

² Karagülmez, **a.g.e.**, s. 235.

³ Mahmut Koca/İlhan Üzülmüş, **Türk Ceza Hukuku Özel Hükümler**, 5. bs., Ankara, Seçkin Yayıncılık, 2018, s. 866.

⁴ Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, Ankara, Yetkin Yayınları, 2010, s. 605.

⁵ Dülger, **a.g.e.**, s. 331; Ahmet Gül, **Doğrudan Dolaylı Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2016, s. 82.

korumaya yöneliktir. Dördüncü fıkra ise bilişim sistemi aracılığıyla haksız çıkar sağlanması suçu düzenlenmiştir. Maddenin başlığı ilk iki fıkra düzenlenen suçu yansıtmak nitelikte olduğundan ilk iki fıkra düzenlenen suçlar bazı konularda tekrara düşmemek ve birbirleriyle olan farklılıklarını daha belirgin bir şekilde belirtebilmek adına birlikte incelenecek, dördüncü fıkradaki suç ise ayrı bir başlıkta inceleme konusu yapılacaktır⁶.

B. Suçlarla Korunan Hukuki Değerler

765 sayılı Türk Ceza Kanunu'nun 525/b-1 maddesinde hem sisteme zarar vermeye hem soyut unsurlara hem de sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlamaya yönelik fiillere seçimlik olarak tek bir hükümde yer verildiğinden korunan hukuki değer konusunda birçok değişik görüş bulunmaktaydı. Bilgisayarın sadece elektromanyetik ortamına yönelen fiilleri değil, fiziksel kısımları da ilgilendiren fiilleri kapsayacak şekilde yorumlayan görüşe göre, genel olarak korunmak istenen menfaat kamu ekonomisi değil bireyin malvarlığıdır⁷. O dönemde düzenlenen suç, failin sistemin işleyişine müdahale ederek istenen sonucun ortaya çıkarmasını sağlayarak başkasının mülkiyetine zarar vermek ve kendisi veya başkası için yarar sağlamakla tamamlanmaktadır. Bu nedenle korunan hukuki değer mülkiyet hakkı olduğu ileri sürülmüştür⁸. Bireyin mal varlığının yanında kamunun güveni veya özel hayatın korunmasına yönelik bazı menfaatlerin de korunmaya alındığını bu kanun dönemindeki düzenleme bağlamında söyleyebiliriz⁹.

Bu kanun döneminde bilgisayarda yer alan bilgilerin doğruluğu ve sistemin usulüne uygun olarak çalışmasının sağlanması korunan hukuki değer olduğu kabul edilmektedir¹⁰. Kısaca tasarruf yetkilisinin verilerle meydana getirilmiş bulunan

⁶ Koca/Üzülmez, **a.g.e.**, s. 866.

⁷ Ersoy, **a.g.m.**, s. 166, 176.

⁸ Dönmezer, **a.g.e.**, s. 618. Mülkiyet hakkı olduğu yönünde Avşar/Öngören, **a.g.e.**, s. 135

⁹ Yazıcıoğlu, **a.g.e.**, s. 221.

¹⁰ Dönmezer, **a.g.e.**, s. 615.

bilgileri herhangi bir engel veya arıza olmadan kullanılmasındaki ve sistemin arızasız çalışmasındaki yararın korunduğu ifade edilmektedir¹¹.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 5. maddesinin dayanak raporuna göre bu suçla korunan hukuki değer, bilgisayar verilerine veya programlarına zarar verilmesini, veri ve programların bozulmasını, zarar görmesini engellemek ve böylece bunların doğru ve işlevsel olarak çalışmalarını sağlamaktır. Aynı sözleşmenin 4. maddesinin dayanak raporuna göre, bu suçla korunan hukuki değer ise temel olarak bilgisayar sabotajıyla ilgilidir ve sistemlerinin işletmeci ve kullanıcılarının sahip oldukları sistemleri uygun biçimde işletme haklarını korumaktadır ve buna yönelecek haksız davranışlara engel olmaktadır. Burada, sistem kullanıcılarının ve operatörlerinin fonksiyonlarına uygun şekilde bu sistemleri kullanma hakları korunmaktadır¹².

Avrupa Konseyi Siber Suç Sözleşmesi'nin açıklayıcı raporunda da belirttiği gibi, bu suçlar, bilgisayar sabotajı olarak nitelendirilen fiilleri önlemeyi amaçlamaktadır¹³.

5237 sayılı Kanun döneminde de tıpkı 765 sayılı TCK'da olduğu gibi korunan hukuki değer konusunda görüş birliği bulunmamaktadır.

Bir görüşe göre, bu madde ile hem bilişim sistemlerinin veri ve yazılımdan oluşan soyut kısmı hem de donanımdan oluşan somut kısmı koruma altına alınmıştır. Maddenin ilk fıkrasıyla temelde bilişim sisteminin işleyişi, özellikle sistemin kendisi yani donanımsal yanı koruma altına alınmışken maddenin ikinci fıkrası ile de sistemde yer alan veri ve veriyle ilgili unsurlar koruma altına alınmaya çalışılmıştır¹⁴.

¹¹ Akbulut, **a.g.e.**, s. 179.

¹² Ali Parlar/ Muzaffer Hatipoğlu, **Türk Ceza Kanunu Yorumu**, C. IV, Ankara, Seçkin Yayıncılık, 2008, s. 3475; Mehmet Emin Artuk/Ahmet Gökçen/Caner Yenidünya, **Türk Ceza Kanunu Şerhi**, 2. bs., C. V, Ankara, Adalet Yayınları, 2014, s. 6927.

¹³ Mehmet Emin Artuk, Ahmet Gökçen, Caner Yenidünya, **Ceza Hukuku Özel Hükümler**, 15. bs., Ankara, Adalet Yayınevi, 2015, s. 880.

¹⁴ Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", s. 409; Hayati Pallı, "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları", Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Kayseri, 2008, s. 164.

Bu görüşe göre, bu suçlarla korunan hukuki değer bilişim sistemi ve/veya bilişim sisteminin içerdiği veriler üzerinde tasarruf yetkisi bulunan kişinin, verilerle oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışma, bilgi vb. değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşması ve kullanmasındaki çıkarıdır. Kanun koyucu bu suç tipleriyle yalnızca veri ve yazılımlardan oluşan soyut unsurlarını koruma altına almamış aynı zamanda bilişim sistemlerinin somut unsuru olan donanım kısmını da suçun koruma alanında kabul etmiştir. Bu nedenle bu suçlarla korunan hukuki değerler karma bir nitelik göstermektedirler¹⁵. Sistemin hem donanım hem de yazılım unsurunun korunması kanun gerekçesinde “... sistemlere yöneltilen ızzar fiilleri özel bir suç haline getirilmiştir. Aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır...” denilmesi suretiyle temelini bulmuştur¹⁶. Gerekçede de görüleceği üzere, sistemlere yönelik ızzar fiilleri özel bir suç haline getirilmiştir. Bu fıkralarda düzenlenen suçların konusunu, bilişim sisteminin varlığını ve işlemlerini sağlayan bütün diğer unsurlar oluşturmaktadır. Aslında burada hem bilişim sisteminin hem de bu sistem içerisinde yer alan verilerin zarar görmemesinin amaçlandığı söylenebilir¹⁷.

Bu görüş sistemin yazılım unsurunu oluşturan veri ve programlar açısından genel olarak kişinin sistemin içerdiği veriye ulaşması ve kullanılmasındaki yararlarla birlikte sistemin veri ile birlikte işlevinin korunduğunu belirtir¹⁸.

Maddenin birinci fıkrasında bilişim sistemi sahibinin mülkiyet hakkı korunduğu gibi bilişim sistemi üzerinde sadece zilyetliğini sürdürmekte olanlara karşı ise bilişim sistemi dokunulmazlığı, iletişim kurma, teknolojik gelişim özgürlüğü engellenmiş olmaktadır¹⁹.

Maddenin ikinci fıkrasında ise sistemin ve sistem içerisinde yer alan verilerin dokunulmazlığı korunan hukuki değerdir. Maddede sayılı fiiller işlenmek suretiyle

¹⁵ Dölger, **a.g.e.**, s. 313, 314; Soyaslan, **a.g.e.**, s. 615.

¹⁶ Artuk/Gökcen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6927.

¹⁷ Karagölmez, **a.g.e.**, s. 237.

¹⁸ Ketizmen, **a.g.e.**, s. 128.

¹⁹ Kurt, **a.g.e.**, s. 162.

bazen mülkiyet hakkı bazen de eğer bu veriler özgün bir çalışmayı içeriyorsa fikri mülkiyet hakkı ihlal edilmiş bulunmaktadır. Örneğin bilgisayarıda çalışmasının bir kopyasını bulunduran akademisyenin ya da özgün müzik bestesini bilgisayarıda saklayan müzisyenin kayıtlarının yok edilmesi durumunda fikri mülkiyet hakkı ihlal edilmiş olmaktadır. Eser niteliği taşımayan ancak özel bilgiler içeren verilerin zarara uğraması veya başka bir yere gönderilmesi durumunda ise kişinin özel hayatının gizliliğine müdahale olduğu açıktır. Eğer bilgisayarda bulunan veri ticari sırlara ilişkin ise verilerin ele geçirilmesi halinde mülkiyet hakkı zarara uğramıştır. Veriler haberleşmeye ilişkin olduğundan haberleşme özgürlüğü ihlal edilmiş olacaktır. Verilen örneklerden de anlaşılacağı gibi tasarrufta bulunulan verinin içeriğine göre o veriye mahsus olarak farklı değerlerin ihlali söz konusu olduğundan doktrinde korunan hukuki değer konusunda pek çok görüş bulunmaktadır²⁰.

Haberleşme özgürlüğünün korunduğunu savunan görüşü eleştiren görüş ise haberleşme özgürlüğünün korunmasının maddenin düzenlendiği yer itibarıyla söylenemeyeceğini savunur²¹.

Yapılan düzenleme ile bilişim sistemi veya verileri üzerinde sahibi veya zilyedin zilyetlikten doğan hakları ve buna bağlı olarak toplum menfaati korunması amaçlanmıştır²². Bu suçları mala zarar vermenin elektronik türü olarak nitelendirirken görüşe göre korunan diğer hukuki yarar da bilgisayarın dokunulmaz olması ve sistemin istendiği şekilde hizmet görmesidir²³.

Diğer bir görüşe göre, burada temel olarak korunan iki hukuki değerden bahsetmek mümkündür. Bunların birincisi bütün olarak bilişim sisteminin ve verilerin güvenliğidir. Çünkü gerek birinci gerekse ikinci fıkrada düzenlenen fiillerle hem bilişim sisteminin işleyişi hem de veriler hedef alınmıştır. Fakat burada bir hususun altı çizilmelidir. TCK m. 244/2'deki fiillerin hedefi konumundaki veriler, bir bilişim

²⁰Kurt, **a.g.e.**, s. 162; Bayındır, **a.g.m.**, s. 71; Erdoğan, **a.g.e.**, s. 214. Aynı görüşte Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6927, 6933; Eker, **a.g.m.**, s. 125.

²¹ Akbulut, **a.g.e.**, s. 182.

²² Yılmaz, **a.g.m.**, s. 69.

²³ Erdağ, **a.g.m.**, s. 280.

sisteminin unsuru niteliğinde olmayan ve fakat bir bilişim sistemi içinde bulunan, sistemin işleyişine etkisi olmayan verilerdir. Diğer deyişle sistemin içinde yer alan ancak sistemin yapı taşı olmayan veriler korunmaktadır. Çünkü söz konusu veriler bir bilişim sisteminin işleyişi bakımından unsur niteliğindeyse, o halde verileri artık bilişim sisteminin içinde değerlendirilmesi gerekip TCK m. 244/1'in uygulanması gerekecektir²⁴. İkinci olarak korunan hukuki değer ise mülkiyet hakkıdır. Zira TCK m.244/1 ve TCK m. 244/2'de düzenlenen fiiller, sahibinin söz konusu bilişim sistemi ve veri üzerinde tasarrufta bulunma yetkisine açık bir müdahale niteliği taşımaktadır. Yine aynı şekilde TCK m. 244/4'te de anılan bu fiilleri gerçekleştirmek suretiyle haksız menfaat temin etme düzenlendiği için, TCK m. 244'ün aynı zamanda bir bütün olarak mülkiyet hakkını da koruduğunu söylemek mümkündür²⁵. Mülkiyet hakkının korunduğu görüşüne katılmayan görüş ise bu görüşü, hükümler yalnızca malik ya da tasarruf yetkilisinin veri ya da sistem üzerindeki yararlarını koruduğu gerekçesiyle eleştirmektedirler²⁶.

Diğer bir görüşe göre aynı maddede düzenlenen iki ayrı suç olduğundan ayrı ayrı belirleme yapılmalıdır. İlk fıkrada bilişim sistemleri sahipleri, işletmecileri ile kullanıcıların sistemin arızasız çalışmasındaki yararı korunmaktadır. Kanun koyucu sistemin işleyişinin engellemesi ve bozulması ifadeleriyle sistemin sorunsuz çalışmasındaki yararı korumak istemiştir. İkinci fıkrada ise, veriler üzerinde tasarruf yetkisine sahip olan kişilerin verilerin bozulmadan, engel çıkartılmadan, verilere herhangi bir müdahale olmadan kullanılmasındaki yararı korunmaktadır. Bu görüş sisteme veri yerleştirme hareketini ikinci fıkrada düzenlenmesini, bu hareketin verilerin kullanılmasındaki değeri etkilemeyen ve bu değeri koruyan diğer hareketlerle herhangi bir ilgisi bulunmadığından ikinci fıkrada düzenlenmesi kanunun sistematığe uygun olmadığını savunmaktadır²⁷.

²⁴ Erdoğan, **a.g.e.**, s. 215; Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 980.

²⁵ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 980. Aynı görüşte Durmuş Tezcan/Mustafa Ruhan Erdem/Murat Önok, **Teorik ve Pratik Ceza Özel Hukuku**, Ankara, Seçkin Yayıncılık, 2016, s. 954; Akıncı/Alıç/Er, **a.g.m.**, s. 237; Eker, **a.g.m.**, s. 115.

²⁶ Akbulut, **a.g.e.**, s. 182.

²⁷ **A.e.**, s. 181.

Diğer bir görüşe göre, ilk iki fıkra sistemin soyut unsurlarına zarar vermeye yönelik fiiller yaptırım altına alınmıştır. Bu fiiller aynı zamanda kişinin malvarlığı değerlerini de ihlal etmektedir. Kanun koyucunun, maddenin kanun sistematığındaki yeri de göz önüne alındığında kişinin malvarlığını korumaktan öteye geçerek bilişim sistemlerinin doğru şekilde işleyişini korumak istediği ifade edilebilmektedir²⁸.

Diğer bir görüşe göre, genel olarak da maddenin düzenlediği bölümün topluma karşı olduğu dikkate alındığında öncelikle sistemin toplum nazarında güvenilirliği ve toplumun tamamının menfaatleri korunmak istenmektedir. Bilişim sistemine yapılan her saldırı kişilerin sisteme olan güvenini etkileyecektir. Bilişim toplumuna geçiş için öncelikle toplumun bilişim sistemlerine güvenmesi gerektiğinden, bilişim sistemlerine yapılacak her haksız saldırı toplum içerisinde özellikle bilişim sistemlerini kullanmaya hâkim olmayan kişilerde bilişim sistemlerine güveni olumsuz etkileyecektir ve bu durum bilişim toplumuna geçişi geciktireceğinden burada bilişim sisteminin güvenilirliğinin korunduğu ifade edilmektedir. Ayrıca yazara göre korunmak istenen bir diğer değer de sistem sahibinin ve kullanıcısının maddi ve manevi çıkarlarıdır. Zira yapılacak her saldırı sistem sahibini maddi anlamda zarara uğratacağı gibi sistem güvenilirliğinin sorgulanması nedeniyle manevi zarara da uğratacaktır. Yine belirtmek gerekir ki sistemin güvenliği de ayrıca korunmak istenmektedir²⁹.

Bir kişi ya da kuruma ait veriler üzerinde başkası tarafından bir şekilde tasarrufta bulunulduğunda, o verilerin gizliliği ve dokunulmazlığı ihlal edildiğinden verilerin güvenliğinin de ihlal edildiğini söyleyebiliriz³⁰.

Ancak bazı durumlarda failin fiilin her iki fıkradaki suç tipine de girmesi halinde- örneğin değiştirilen verinin sistemi de bozması ya da engellemesi durumunda olduğu gibi- failin kastının belirlenebilmesi için bu suçlarla korunan hukuki değerlerin de ayrı ayrı ortaya konulması gerekir. Buradan hareketle ilk fıkra incelendiğinde, bu suç tipiyle bir bütün olarak bilişim sisteminin işleyişinin korunmak istendiğini

²⁸ Koca/Üzülmez, **a.g.e.**, s. 867. Sadece malvarlığının korunduğu yönünde Biçkin, **a.g.m.**, s. 157.

²⁹ Erdoğan, **a.g.e.**, s. 184, 216.

³⁰ **A.e.**, s. 215.

belirtmeliyiz. Bu fıkra da verilerden söz edilmeksizin doğrudan bilişim sisteminin kendisi suçun konusu yapılmaktadır, ayrıca bilişim sistemine zarar verilmesi sonucunda verilere de en azından ulaşılabilmesi gibi bir sonuç kendiliğinden doğacağı için ilk fıkradaki suç için ikinci fıkradaki suça nazaran daha ağır bir ceza öngörülmüştür³¹.

İlk fıkra ile bilişim sisteminin, sistemin güvenliği ve işleyişinin korunmak istendiği söyleyebiliriz. İkinci fıkra da ise sistemde bulunan verilerin bütünlüğü ve herhangi bir engel olmadan verilerin kullanılmasındaki yarar korunmaktadır. Veri ve sistem bir bütün olduğundan sistemin hem yazılım hem de donanım unsurunun birlikte korunduğunu görüşüne katılmaktayız.

Sadece mülkiyet hakkının korunduğunu kabul eden görüşe ise katılmıyoruz. Korunan hukuki değeri mülkiyet hakkı ile sınırlandırmak maddenin düzenleniş yeri itibarıyla da isabetli değildir. Bu madde ile veri veya sistem sahibinin mülkiyet hakları korunduğu gibi bunun yanında tasarruf yetkisine sahip olan kişilerin sistemi veya veriyi kullanmasındaki yarar da korunmaktadır.

Suçların topluma karşı suçlar bölümünde düzenlenmesi ise isabetlidir. Günümüz toplumunda hem kamusal hem de bireysel ilişkilerin çoğu artık bilişim sistemleri üzerinden gerçekleşmektedir. Bu madde ile toplumun bilişim sisteminin işleyişine güveni de korunmaktadır.

³¹ Dülger, **a.g.e.**, s. 314.

C. Suçların Temel Unsurları

1. Maddi Unsurlar

a. Suçların Konusu

(1) Genel olarak

244. maddenin 2. fıkrasında düzenlenen suç, 1. fıkra düzenlenenden suçtan ayıran en önemli husus suçun konusudur. 1. fıkra düzenlenenden suçun konusunu “*bilişim sistemi*”³² oluştururken, 2. fıkra yer alan suçun konusunu “*bilişim sisteminde yer alan veriler*” oluşturmaktadır³³. Bilişim sistemleri ve veri kavramları, sistemin çalışması için gerekli olan her türlü donanımı ifade ettiği gibi bilişim sistemi içinde yer alan her türden bilgi ile beraber yazılımı da içermektedir³⁴.

TCK m. 244/2’de açıkça sistem içerisinde yer alan veriden bahsedilmesi nedeniyle veri taşıma aygıtlarında bulunan verilere müdahale halinde bu fıkranın uygulanıp uygulanmayacağı doktrinde tartışmalıdır. Bir görüşe göre veri taşıma aygıtları yalnızca verinin saklanması için kullanılıyor ve üzerinde veri işleme ve veri iletişimi yapılamıyorsa, o cihazın bilişim sistemi olarak kabul edilmemesi gerekmektedir. Şayet verinin taşındığı aygıt veri işlemenin, veri saklamanın ve veri iletişiminin yapılabildiği bir aygıtsa (örneğin, internete açık bir cep telefonu) bu suça konu olarak kabul edilebileceğini aksi takdirde (örneğin; CD, USB/ flash bellek) konu olmayacağını kabul etmektedir. Yine aynı görüş USB belleğin bilgisayara takıldığında artık bilişim sisteminin bir unsuru haline gelip adeta bir sabit hard disk gibi çalıştığını ifade etmektedir. Bu nedenle bu taşıma aygıtlarının sisteme takılı oldukları zamanlarda onun bir parçası olduğunu ve dolayısıyla da bu suça konu olabileceğini kabul etmek

³² İlk fıkra düzenlenenden suçun konusunu “*bilişim sisteminin işleyişi*” olarak kabul eden görüş için bkz. Koca/Üzülmez, **a.g.e.**, s. 868.

³³ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 980; Tezcan/Erdem/Önok **a.g.e.** s. 955; Aynı görüşte Necati Meran, **Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar**, Ankara, Seçkin Yayınları, 2008, s. 571; Dülger, **a.g.e.**, s. 317.

³⁴ Kızıltan, **a.g.t.**, s. 77; Dülger, **a.g.e.**, s. 322; Taşkın, **a.g.e.**, s. 43.

gerektiğini savunmaktadırlar³⁵. Suçun konusunu oluşturan verinin mutlaka bilişim sisteminde yer alan veri olması gerektiğini kabul eden görüşe göre, CD ve USB bellek gibi yalnızca veri saklama işlevine sahip olan, tek başına bilişim sistemi olarak değerlendirilemeyecek nitelikteki veri taşıma ve saklama cihazlarında yer alan verilere müdahale bu suçu oluşturmaz³⁶. Aksi görüşte olan yazarlara göre donanım kavramının içine ana kart, ekran, yazıcı, ses sistemi, disket, modem kartı gibi maddi bünyeye sahip parçalar girmektedir. Sistemde yer alan veri kavramıyla bilgisayarın hafızasında kayıtlı bulunan veriler anlaşıldığı gibi ana kart üzerindeki veri yollarına takılmak suretiyle kullanılan USB bellek, CD-ROM gibi aygıtların içindeki veriler de bu kapsamdadır. Bu sebeple bu cihazlardaki verilere müdahale edilmesinin bu suçu oluşturabileceğini savunmaktadırlar³⁷.

Özbek/Doğan/Bacaksız/Tepe eserlerinde yazılım ile donanımın bir bütün olduğunu, yazılıma verilecek bir zararın donanımın da işlevselliğini olumsuz yönde etkileyeceğini belirtip durumu bir örnekle açıklamışlardır; yüksek kapasiteli ve yüksek hızlı, bilgisayara monte edilmiş, teknik müdahale haricinde çıkarılamayan, manyetik usullere göre bilgi okuyup yazan hard disk bir donanım unsurudur. Hard disk tek başına maddi varlığı ile bu işlemleri gerçekleştiremez. Bu işlevleri gerçekleştirebilmesi için hard diske BIOS adı verilen programın yüklü olması gerekmektedir. Bu anlamda bir bilgi işlem faaliyeti için yazılım-donanım uyumluluğunun zorunlu olduğunu savunmaktadırlar. Dolayısıyla suçun konusunu bilişim sisteminin işleyişi bakımından unsur niteliği taşımak koşuluyla hem donanım hem de yazılım unsurlarının oluşturduğunu belirtmektedirler³⁸.

İçerisinde veri bulunmayan bir bilişim sisteminin ya da veri taşıma aracının suçun konusunu oluşturmayacağı açıktır. Zira maddenin düzenlenme amacı sadece somut unsuru olan donanım unsuruna verilen zararları korumak değil soyut unsurları olan veriler ve bilişim sisteminin işleyişini korumaktır³⁹. Suçun TCK m. 244'ün

³⁵ Erdoğan, **a.g.e.**, s. 211.

³⁶ Ketizmen, **a.g.e.**, s. 413.

³⁷ Akbulut, **a.g.e.**, s. 189; Akıncı/Alıç/Er, **a.g.m.**, s. 238.

³⁸ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 981. Aynı görüşte Kızıltan, **a.g.t.**, s. 77.

³⁹ Soyaslan, **a.g.e.**, s. 616.

gerekçesinde “böylece sistemlere yöneltilen ızzar fiilleri özel bir suç haline getirilmiştir, aracın fizik varlığı ve işlemlerini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır.” denilmekteyse de gerekçe yalnızca maddelerin daha iyi açıklanmasını ve kanun koyucunun görüşünü yansıtmaları için konulduğundan bağlayıcı değildir. Çalışmayan ve işlemlerinin engellenmesi veya bozulması mümkün olmayan bilişim sistemi suçun konusunu oluşturmayacağı gibi içerisinde veri bulunmayan donanım unsuru da suça konu olamaz⁴⁰. Aksi görüşe göre, veriler ikinci fıkra ile koruma altına alınmışken ilk fıkra bakımından bilişim sistemleri korunmaktadır. Bu nedenle içinde veri bulunmasa bile bilişim sisteminin temel özellikleri olan veri alma, depolama ve gönderme özelliklerine sahip bilişim sistemleri ilk fıkra kapsamında korunmalıdır. Bu görüş, her an veri alabilecek, depolayabilecek ve aldığı veriyi başka bir yere gönderebilecek bir bilişim sisteminin o an için içinde veri yok diye sistemi korumamak, sistemi hukuki güvenceden yoksun bırakmak olduğunu savunmaktadır⁴¹.

Kanaatimizce ilk fıkra ile bilişim sistemlerinin işleyişi de korunduğundan henüz içerisine veri yüklenmemiş haldeki bilişim sistemi de suçun konusunu oluşturacaktır.

Bilişim sistemleri yazılım ve donanım unsuru ile bütündür. CD veya USB bellekte bulunan verinin suça konu olacağı açıktır. Bu tür aygıtlarda bulunan veriler sisteme tanımlandığında sistem kullanıcısının üzerinde tasarruf edeceği durumda olacaktır. Burada bulunan verilerin silinmesi, başka bir taşıyıcı cihaza aktarılması mümkün olduğundan suça konu verilerin mutlaka sistemde bulunması şartının aranmaması gerekmektedir.

⁴⁰ Taşkın, **a.g.e.**, s. 43, 44.

⁴¹ Erdoğan, **a.g.e.**, s. 196.

(2) İnternet Oyunlarındaki Özne ve Nesnelerin Durumu

“Avatar” denilen oyunlardaki öznelerin ya da oyunlarda kullanılan dijital malzemelerin, kullanıcısı olmayan kişilerce şifrenin kırılması veya hukuka aykırı bir şekilde ele geçirilmesi durumunda fiilin suç oluşturup oluşturmayacağı ve eğer suç oluşturuyorsa hangi madde kapsamında inceleneceği hususu bu başlık altında incelenecektir⁴².

Hint mitolojisi kökenli “Avatar”⁴³ kavramı, genel olarak dijital oyunlar ile çok katılımcılı online rol yapma oyunlarının ve özel olarak da sanal gerçeklik çalışmalarının gelişim evresinde, bilgisayar ortamı ile kullanıcısı insan arasındaki etkileşimi temellendirmek ve açıklamak ihtiyacının doruğa çıktığı bir zamanda tekrar keşfedilmiştir. Avatar, insan kullanıcısının sanal alemde yeniden ve farklı bir formla doğuşunu sembolize etmektedir⁴⁴.

Sanal dünya ise (*virtual world*) program kodu çerçevesinde katılımcı ile şirketin ortak çalışmasının ürünüdür. İnternet ve ağ temelli uygulamalar kapsamında internet alan adları (*domain names*), URLs (*uniform resource locators*), web siteleri, email hesapları, Facebook profili, chat/sohbet odaları, internet üzerinde eş zamanlı oynanan çok katılımcılı online oyunlarının siber ve sanal mülkiyet özelliklerini bir arada taşıdığı söylenebilir⁴⁵.

Bu oyunlara girişte oyuncu tarafından kabul edilen ve geçerliliği tartışmalı olan sözleşmelerde söz konusu avatarların ve malzemelerin mülkiyetinin oyunun sahibi

⁴² Dülger, **a.g.e.**, s. 318.

⁴³ Avatar, Hindu mitolojisinden kaynaklanan bir terimdir. Gerçekten avatar (avatara) kelime olarak türeyiş/köken anlamına gelmekte ve Hindu mitolojisinde cennetten dünyaya inen tanrıyı ifade etmektedir. Bu yönüyle somut olarak Tanrı Vishnu’nun cismani şekilde yeniden doğumunu müjdelemektedir. Hindu dinine göre, tanrı insanlarla iletişime geçebilmek için kutsal varlığını temsili bir araçla yansıtmak durumundadır. Dolayısıyla, Tanrı insanlarla iletişime geçerken “avatarı” kullanmaktadır.

⁴⁴ H. Burak Gemalmaz, **Sanal Dünyalarda İktidar ve Özgürlük**, İstanbul, Beta Yayıncılık, 2011, s. 49.

⁴⁵ Gemalmaz, **a.g.e.**, s. 104 vd.

olan (lisans sahibi) şirkete ait olduğu belirtilmektedir. Sözleşmenin ve sanal mülkiyet konusunun hala netleşmemiş olması nedeniyle, tek başına şirketin bu hususu belirtmesi mülkiyetin şirkete ait olduğu anlamına gelmemektedir. Zira artık oyuncunun emeğiyle ve oyundaki çeşitli aşamalardan geçtikçe oyuncunun hususiyetini kazanan bir sanal mülkiyet konusu ortaya çıkmıştır⁴⁶.

Özel hukuk açısından ne olacağı şimdilik belirsizliğini korumasına rağmen, ceza hukuku açısından bunlar veridir ve suçun mağduru olmak için aşağıda izah edileceği üzere verinin sahibi olunması gerekmemektedir, ilgilisi olmak yeterlidir. Ayrıca hukuka aykırı bir yarar elde edilsin ya da edilmesin bizatihi bu avatarların ya da malzemelerin yani suç kapsamındaki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması suçtur. Bu durumda TCK m. 244/2'nin uygulanması gerekir. Özel hukuk açısından eğer bunlar satış sözleşmesinin konusu olursa TCK m. 244/4'ün uygulanması gündeme gelmektedir⁴⁷.

Malın ekonomik değerinin objektif kriterlere göre belirlenebilmesi gerektiğini savunan görüşe göre mağdurun beyanıyla eşyaya ekonomik değer atfedilmesi doğru olmayacaktır. Ancak kişinin bunu bir delille (banka dekontu gibi) ispatlarsa hırsızlık suçu oluşabileceğini ileri sürmektedirler. Doktrinde bir görüş suçun konusunun ekonomik değeri varsa TCK 142/2-e maddesinden düzenlenen bilişim sistemi ile yolu işlenen hırsızlık suçunu oluşturacağını ileri sürmektedir⁴⁸.

Oyun karakterleri de aslında bir veri olduğundan incelediğimiz suç tiplerine konu olabilecektir. Biz bu bölümde sadece buna benzer veri birikimlerinin incelediğimiz suçlara konu edilebileceğini söylemekle yetiniyoruz. Bu hareketlerin hangi suç tipini oluşturacağı konusundaki tartışmayı üçüncü bölümde sonlandırmayı suç sistematığı açısından uygun bulmaktayız.

⁴⁶ Dülger, **a.g.e.**, s. 319.

⁴⁷ **A.e.**

⁴⁸ Gül, **a.g.e.**, s. 90.

b. Fiil

Bu suçların seçimlik hareketli olup olmadığı hususu tartışmalıdır. Bir görüş, TCK m. 244/1'deki engelleme ve bozmanın seçimlik hareketler olduğu⁴⁹ ve suçun oluşması için engelleme ve bozma fiillerinden herhangi birinin gerçekleştirilmesinin yeterli olduğunu, ikisinin birden gerçekleşmesinin suçun tekliğini etkilemeyeceğini belirtirken; diğer görüş engelleme ve bozmanın eylemin neticesi olduğunu⁵⁰ suçun serbest hareketli suç olduğunu belirtmektedir. Diğer deyişle ikinci görüş, buradaki engelleme ve bozmanın suçun hareketi değil, hareketin neticesi olduğunu kabul etmektedir⁵¹.

Suçu seçimlik hareketli olarak kabul eden ilk görüşe göre hareketin yapılması halinde tek suç oluşur fakat TCK m. 61 gereğince hâkim alt sınırdan uzaklaşarak ceza verebilir⁵². Bu görüşe göre, suçun oluşması için seçimlik hareketlerden birinin yapılması yeterlidir. Suçun tamamlandığını kabul bakımından bir zararın meydana gelmesi aranmamaktadır. Öte yandan suç bağlı hareketli bir suç olduğundan ancak tipte yer alan hareketlerin gerçekleşmesi suretiyle suç işlenebileceğini savunmaktadırlar⁵³.

Suçun serbest hareketli olduğunu savunan ikinci görüşe göre bu suç herhangi bir şekilde işlenebilir. Sistemin işleyişinin engellenmesi veya bozulması bu suçun netice unsurunu oluşturur, bu neticeleri meydana getiren her hareketle suç işlenebilir⁵⁴. Bu husus maddede “*engelleyen, bozan, yerleştiren, gönderen, erişilmez kılan, değiştiren ve yok eden*” şeklinde gösterilmiş, yani hareketin meydana getirilmesi ve bir sonucun ortaya çıkması aranmış ancak bu hareketlerin nasıl yapılacağı

⁴⁹ Kızıltan, **a.g.t.**, s. 78; Karagülmez, **a.g.e.**, s.187. Eker, **a.g.m.**, s. 124, 125; Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 985; Gül, **a.g.e.**, s. 83; Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6928; Meran, **a.g.e.**, s. 572; Kurt, **a.g.e.**, s. 164.

⁵⁰ Erdoğan s. 186; Berrin Akbulut, “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C. XXIV, S. 2, 2016, s. 27; Akbulut, **a.g.e.**, s. 190.

⁵¹ Erdoğan, **a.g.e.**, s. 186; Yılmaz, **a.g.m.**, s. 77.

⁵² Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6933.

⁵³ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 985.

⁵⁴ Koca/Üzülmez, **a.g.e.**, s. 869.

belirtilmemiştir⁵⁵. Önemli olan husus yapılan hareket sonucunda neticelerden birinin gerçekleşmesidir. Failin suçu işlemek için Truva atı, virüsler, solucanlar gibi yazılımlar kullanmasıyla sistemin başına geçip fiziken kullanması bakımından bir fark bulunmadığı bu görüşçe savunulmaktadır. Bir verinin bulunduğu yerden alınıp başka bir sisteme kaydedildiği durumlarda veriyi yok etmek, erişilmez kılmak ve başka yere göndermek neticelerinin tamamı oluşmaktadır. Bu gibi birden fazla neticenin meydana geldiği hallerde ortada yine tek suç vardır. Zira neticenin çokluğu suçun tekliğini etkilemez⁵⁶.

Doktrinde bu suçun zarar suçu mu yoksa tehlike suçu mu olduğu hususu da tartışmalıdır. Bir görüşe göre, failin yaptığı hareketlerin neticesinde bir zararın meydana gelmesi gerekmektedir. Fiil konuya zarar verdiğinden zarar suçu söz konusudur⁵⁷. Bozma ve engellemeyi hareket olarak değil de netice olarak kabul eden görüş bu suçu zarar suçu olarak kabul etmektedir. Zira engelleme ve bozma halinde sistem eski haline getirilinceye kadar istenildiği gibi kullanılamayacaktır. Diğer deyişle, hareketin neticesinde bozma ya da engellenmenin gerçekleşmesi sistemin zarar görmesi anlamına geleceğinden burada zarar suçu söz konusu olmaktadır. Zararın maddi olmasının gerekmediği kabul edildiğinde, hak sahibi tarafından sisteme girilemediği ya da sistem istenildiği gibi kullanılmadığı sürece zararın da olduğunu kabul etmektedirler. Sisteme güvenin sarsılması nedeniyle, kişi miktarı net olarak tespit edilemese de pek çok kişi o sistemi kullanmaktan vazgeçecek ya da hiç kullanmaya başlamayacaktır. Bu durumun ise, özellikle ticari sistemlerde miktarı tespit edilemeyen maddi kayıplara neden olduğunu savunmaktadırlar⁵⁸. Bu görüşe göre madde metninde suçun oluşması için bir zararın meydana gelmesi aranmamakla birlikte seçimlik hareketlerin gerçekleşmesi sonucunda mağdura ait bilişim sisteminin işleyişini engelleme veya bozma, bir bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka yere gönderme fiilleri zaten bünyesinde zarar ögesini barındıran fiillerdir. Söz konusu bu

⁵⁵ Dülger, **a.g.e.**, s. 332-333.

⁵⁶ Erdoğan, **a.g.e.**, s. 219.

⁵⁷ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 888; Esen, **a.g.e.**, s. 635.

⁵⁸ Erdoğan, **a.g.e.**, s. 187.

durum maddede açıkça belirtilmemiş ise de madde gerekçesinde vurgulandığını belirtmektedirler⁵⁹.

Diğer görüş ise bozma fiilleri sonucunda bilişim sisteminde bir zararın meydana gelebileceği kabul edilebilir görmekte ise de, sistemin işleyişinin engellenmesi sonucunda bir zararın doğmamasının mümkün olduğunu, bu suçun oluşması için mutlaka bir zararın doğmasını aramanın, suçun kapsamını daraltacağını, ayrıca zararın ne olduğunun tespitinin de başlı başına sorun oluşturduğu, AKSSS'de de bu suçun karşılığı olan sistem engellemeleri düzenlenmesinde sistemin sekteye uğratılmasından bahsedilmiş olup herhangi bir zararın meydana gelmesinin aranmadığını, bu nedenlerle bu suçun zarar suçu olmayıp tehlike suçu olduğunu belirtilmektedir⁶⁰. Özellikle verilerin değiştirilmesi ve başka yere gönderilmesi suçu bakımından zarar doğması şartı aranmamaktadır⁶¹. Bu görüşe göre fiillerin gerçekleştirilmesi sonucunda sistemde ve/veya verilerde bir zarar meydana gelebileceği gibi suçun oluşumu açısından mağdurun zarara uğraması ya da suçun konusunda ayrıca bir zararın oluşması aranmaz⁶². Bizim de katıldığımız görüşe göre seçimlik neticeler sonucunda zarar oluşabileceği gibi zararın oluşması suçun tamamlanması için şart değildir. Suçun düzenlendiği yer de göz önüne alındığında suçun tehlike suçu olduğunu söyleyebiliriz.

Bu suçun ihmali hareketle de işlenebileceğini savunan görüşe göre teknik destek sorumlusunun kasıtlı olarak bir virüs saldırısını önlemek için gerekli yazılımları sisteme yüklememesi ya da sistemi dışarıdan saldırıya karşı savunmasız bırakması halinde olduğu durumlarda suçun ihmali suretle işlenmesi de mümkün olabilir⁶³. Yine örnek olarak bir şirketin bilişim sistemi sorumlusunun bir saldırı karşısında anti virüs programını çalıştırması gerekirken kasıtlı olarak zamanında çalıştırmaması sonucunda

⁵⁹ Meran, **a.g.e.**, s. 572-573.

⁶⁰ Erdoğan, **a.g.e.**, s. 186-187.

⁶¹ Taşkın, **a.g.e.**, s. 50.

⁶² Dülger, **a.g.e.**, s. 332-333.

⁶³ Dülger, **a.g.e.**, s. 321.

sistemdeki verilerin zarar görmesi halinde ikinci fıkradaki suç ihmali hareketle gerçekleşebileceğini savunmaktadırlar⁶⁴.

Biz suçların ihmali suretle işlenebileceğini savunan bu görüşe katılmıyoruz. Görünüşte ihmali suçlardan bahsedebilmek için suçları önlemek konusunda özel bir yükümlülüğün bulunması gerekmektedir. Teknik destek sorumlusunun suçun gerçekleşmesini önlemek konusunda özel bir yükümlülüğü öngörülmediğinden bu örnekte de görünüşte ihmali suçun oluşmadığını söyleyebiliriz.

Suçun mütemadi şekilde işlenmesi mümkündür. Bu durumda suç, kesintinin gerçekleştiği zaman işlenmiş kabul edilecek ve zamanaşımı da bu andan itibaren işlemeye başlayacaktır. Örneğin elektriğin kesilmesi ya da veri taşıma araçlarının saklanması fiillerinden olduğu gibi suçu oluşturan fiillerin devamlılık kazandığı hallerde bu durum gerçekleşebilecektir⁶⁵.

c. Netice

Bize göre de tezimizin konusunu oluşturan suç tipleri neticeli suç olma özelliği taşımaktadır. Sistemin engellenmesi, bozulması ile verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, yerleştirilmesi ya da gönderilmesi suçların neticesini oluşturur. Kanunda sayılan bu neticeler herhangi bir şekilde gerçekleşebileceğinden suçlar serbest hareketli olma özelliğini taşımaktadır.

(1) Bilişim Sistemine Müdahale Suçu

i. Bilişim Sisteminin İşleyişini Engellemek

Doktrinde ortak bir engelleme tanımı bulunmamaktadır. Sistemin engellenmesi teriminden gerektiği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da kilitlenme noktasına

⁶⁴ Erdoğan, **a.g.e.**, s. 219.

⁶⁵ Dülger, **a.g.e.**, s. 338.

getirilmesi anlaşılmalıdır⁶⁶. Sistemin hızı ve hatasız çalışabilme özelliğinin olumsuz etkilenmesi söz konusudur. Bunun gerçekleşmesi sistemin maddi unsuru olan araçlarla bozulması ile olacağı gibi teknik müdahalelerle de gerçekleşebilir⁶⁷.

Genel olarak engelleme, bilişim sisteminin olağan işleyişini durdurmak, fonksiyonların doğru biçimde işlenmesini engellemek veya benzeri sonuç doğuran hareket anlamına gelir⁶⁸. Bilişim sisteminin işleyişinin engellenmesi sistem aracılığıyla veri işleme faaliyetinin gerçekleştirilmesinin engellenmesidir⁶⁹.

Bir görüşe göre, bilişim sisteminin işleyişini engellemek; veri işlem yapılmasını yani verilerin kullanılmasını, kaydedilmesini, depolanmasını, işlenmesini veri aktarımını önlemeye yönelik her tür fiili kapsar. Kanun koyucu bazı hareketlerin cezasız kalmasının önüne geçmek için sistemin işleyişini engelleme kavramını geniş tanımlamıştır. Sisteme yapılan müdahale veri işlem yapılmasını kesintiye uğratmışsa veya önlemişse sistemin işlenmesine engel olduğu kabul edilir. Sisteme ve unsurlara zarar veren veya sistemin işlevde bulunmasını önleyen fiiller yine bu kavram içine girer. Sistemin teknik fonksiyonuna zarar vermek, veri akışının kesilmesi, program verilerinin silinmesi veya değiştirilmesi suretiyle gerçekleştirilebilir. Engellenmesi halinde sistemin bozulması söz konusu olmayıp normalde yerine getirdiği fonksiyonlarını ifa etmesinin önüne geçilmiş olunmaktadır. Örneğin; sistem eskisi kadar hızlı çalışmamakta, veri işleme hızı düşmekte, istenilen performansta çalışmamakta, kısacası normal şartlarda rahatlıkla yerine getirebildiği işlevlerini hiç ya da gereği gibi yerine getirememektedir. Buna rağmen sistem bozulmuş değildir. Fail bir kısım fiillerle işleyişi engellemektedir⁷⁰. Engellenme çok değişik bilişim suçu işlenme şekilleriyle gerçekleştirilebilir. Mesela elektronik posta bombardımanı (spam)

⁶⁶ Kurt, **a.g.e.**, s. 161.

⁶⁷ İsmail Malkoç, **Açıklamalı- İctihath 5237 sayılı Yeni Türk Ceza Kanunu**, C. II, Ankara, Malkoç Kitapevi, 2007, s. 1677.

⁶⁸ Eker, **a.g.m.**, s. 125.

⁶⁹ Ketizmen, **a.g.e.**, s. 129.

⁷⁰ Akbulut, **a.g.e.**, s. 191; Kurt, **a.g.e.**, s. 164.

yoluyla sistem kilitlenebilir, zararlı virüsler vasıtasıyla sistem yavaşlatılabilir, komutları algılamaz hale getirilebilir⁷¹.

Bilişim sisteminin veya veri işlem taşıyıcısının yetkili kişinin tasarruf alanından uzaklaştırılması, şifrenin değiştirilmesi veya şifre ilavesiyle sistemin kullanılmasına engel konulması, var olan programın bozulması, sistemin kilitlenmesi hareketleri bu neticeye örnek olarak verilebilir. Sistemin işlemesine engel olma, sisteme fiziki etki şeklinde olabileceği gibi soyut unsurlara yapılan müdahalelerle de söz konusu olabilir. Verilerin bozulması, yok edilmesi, erişilmez kılınması, verilerin değiştirilmesi, sisteme veri yerleştirilmesi suretiyle de sistemin işlemesine engel olunabilir. Sistemin engellenmesine yönelik hareketler sınırlı sayıda değildir, engelleme neticesini oluşturan her türlü hareketle bu suç işlenebilir⁷².

Yargıtay 11. Ceza Dairesi'nin 13.01.2013 tarihli, 2011/2816 Esas 2013/4065 Karar numaralı kararında engellemeyi *“Sistemin işleyişinin ‘engellenmesi’ ibaresi ile bilişim sisteminin verimli çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi”* olarak tanımlanmıştır⁷³.

Bilişim sisteminin işlemesini engelleme, sistemin çalışmasının herhangi bir şekilde kesintiye uğratılmasıdır. Burada, sistemin işleyişi bozulmamakta fakat işlemesi bir şekilde engellenmektedir. Engellemeyi sağlayacak her türlü müdahale bu suçu oluşturabilir⁷⁴. Buna göre, işleyen sisteme yöneltilecek yoğun elektro manyetik dalgalarla sistem merkezinin etkilenmesini sağlama ya da sisteme yapılacak müdahaleyle işletim sisteminin geçici süre devre dışı bırakılması konuya örnek olarak verilebilir⁷⁵. Yerine göre, sistemin elektriğini kesmek bile bu suçu oluşturabilir⁷⁶.

⁷¹ Erdoğan, **a.g.e.**, s. 189.

⁷² Akbulut, **a.g.e.**, s. 191.

⁷³ Gül, **a.g.e.**, s. 83.

⁷⁴ Karagülmez, **a.g.e.**, s. 237. Aynı yönde Erdoğan, **a.g.e.**, s. 189.

⁷⁵ Değirmenci, **a.g.m.**, s. 205; Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 881.

⁷⁶ Yazıcıoğlu, **a.g.e.**, s. 263.

Engelleme bakımından bilişim sistemini kesintiye uğratmanın geçici mi yoksa sürekli mi olması gerektiği doktrinde tartışma yaratmıştır. Bu doğrultuda birinci görüş sistemin işleyişini geçici olarak kesintiye uğratılması gerektiğini savunmuştur⁷⁷. Engellenmenin geçici olması gerektiğini savunan görüşe göre, engelleme süreklilik taşırsa artık sistem gerektiği gibi faaliyet yapamadığından engellenmenin ötesine geçilmiş bulunulmakta ve bu durum da artık fiilin engelleme değil bozulma olarak nitelendirilmesini zorunlu tutmaktadır⁷⁸. Diğer görüş ise suçun oluşması bakımından engellenmenin geçici ya da sürekli olması arasından bir fark olmadığını savunmuştur⁷⁹.

Bizce de sistemi engellenmenin geçici ya da sürekli olması arasında fark olmadığını savunan ikinci görüş isabetlidir. Sürekli engellenme durumunda erişilmek istenen bir sistem varlığını sürdürmekteyken kullanıcının sisteme ulaşamaması durumu bulunmaktadır. İki görüşün de ortak kabulüne göre sistemin işleyişi geçici olarak engellendiğinde de suç oluşacaktır zira nükleer reaktörleri kontrol eden bir sistemin geçici de olsa devre dışı bırakılması, bir ev bilgisayarının sürekli işlevsiz hale getirilmesinden çok daha vahim sonuçlar doğurabilecektir⁸⁰.

Doktrinde sistemin işleyişinin geçici olarak engellenmesi durumunda suçun oluşacağının kabul edilmesi ile birlikte her türlü engellenmenin cezalandırılmaması gerektiğini savunan görüş de bulunmaktadır. Kanunda böyle bir sınırlandırma bulunmamakla beraber sistemin işlemlerini önemsiz ölçüde engelleyen veya birtakım değişikliklerle meydana getirilen durumun ortadan kalkmasına neden olan hallerin haksızlık içeriğinin azlığı sebebiyle ceza verilmemesi yoluna gidilmesi gerektiğini savunan görüş de bulunmaktadır⁸¹. Kanaatimizce eğer failde sistemi engelleme kastı varsa çok kısa süre de olsa sistemin engellenmesi suçu oluşturur. Nitekim bu suçla

⁷⁷ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 881.

⁷⁸ Erdoğan, **a.g.e.**, s. 190.

⁷⁹ Fatih Selami Mahmutoglu, "Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Prof. Dr. Füsün Sokullu-Akinci'ya Armağan, C. LXXI, S. 1, 2013, s. 866; Meran s. 571; Karagülmez, **a.g.e.**, s. 237; Yazıcıoğlu, **a.g.e.**, s. 263; Gül, **a.g.e.**, s. 83; Akbulut, **a.g.e.**, s. 193; Yılmaz, **a.g.m.**, s. 72.

⁸⁰ Pallı, **a.g.t.**, s. 168.

⁸¹ Akbulut, **a.g.e.**, s. 193.

korunan hukuki değerlerden biri de sistemin düzgün çalışmasıdır, bu nedenle her türlü engelleme suçu oluşturmaktadır.

Doktrinde sistemin olağan işleyişini yavaşlatmanın engelleme kapsamında olup olmayacağı tartışmalıdır. Bir görüş yavaşlatmayı engelleme olarak kabul etmektedir⁸². Örneğin bilişim sistemine herhangi bir suretle sokulan ve sistemin işleyişini zayıflatan “tavşan-rabbits” programlarının kullanımı da bu anlamda sistemin işleyişini engellemektedir⁸³. Diğer görüş ise örneğin hatalı program teslimiyle bir firmanın işlemlerinin yavaş işlemesine neden olunmasında olduğu gibi, sistemin yavaş işlemesini sistem engellenmesi olarak kabul edilmeyeceğini ileri sürmektedir⁸⁴.

Kanaatimizce yavaşlatma hareketi de engelleme kapsamındadır. Sistemin yavaşlatılması sistemin istenildiği hızda kullanılmasının engellemesidir. Bazı yavaşlatma hareketleri sistemi durma noktasına getirdiğinden yavaşlamayı da engellenme kapsamında kabul etmekteyiz.

765 sayılı TCK’da bulunan “sistemin yanlış biçimde işlemesini sağlama” seçimlik hareketinden yeni düzenlemede vazgeçildiği görülmektedir. Bunun sebebi ise, sistemin işleyişini engelleme neticesinin, “sistemin yanlış biçimde işlemesini sağlama” durumunu da kapsamasıdır. Ayrıca sistem gerektiği gibi işlemiyorsa sistemin işleyişinin engellendiği sonucuna varmak da mümkündür⁸⁵.

765 sayılı TCK’nın 525/b-1 maddesinde sistemin tahrip edilmesi ayrıca seçimlik olarak sayılmıştı. Ancak o dönemde de sistemde oluşan zararın suç oluşturabilmesi için sistemin içinde bulunan soyut unsurlara (verilere) zarar vermesi gerektiği kabul ediliyordu. Verilere zarar vermeyen hareketlerin 525/b-1 bakımından tahrip etmek değil sistemin işlemesine engel olma niteliği taşıdığını söyleyebiliriz. Yeni kanunda tahrip edilmenin ayrıca hareket olarak düzenlenmemesinin sebebi, eğer tahrip ile verilerde bir zarar oluşmuşsa bunun zaten verileri bozma kavramı içine

⁸² Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 881.

⁸³ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6928

⁸⁴ Akbulut, **a.g.e.**, s. 191.

⁸⁵ Pallı, **a.g.t.**, s. 168.

gireceğini, eğer verilere bir zararın verilmesi söz konusu olmayıp sistemin işleyişine engel olunması söz konusu ise zaten ilk fıkrada düzenlenen sistemin işleyişine engel olmak kavramı içinde değerlendirilebilmesidir⁸⁶.

Sisteme yapılan müdahale, veri işlem yapılmasını kesintiye uğratmışsa sistemin işlemesine engel olunmuştur. Bu anlamda sisteme ve unsurlarına zarar veren veya sistemin işlevde bulunmasını önleyen hareketler, sistemin işlemesine engel olmak kavramı içindedir. Bilişim sisteminin teknik fonksiyonuna zarar vermek, veri akışının kesilmesi, program verilerinin silinmesi veya değiştirilmesi suretiyle gerçekleştirilebilir. Yine DoS, DDoS (distributed denial of service) saldırıları⁸⁷ da sistemin işlemesine engel olmaktadır. Keza bilişim sisteminin veya veri işlem taşıyıcısının kişinin tasarruf alanından uzaklaştırılması (gizlemek veya çalmak gibi) şifrenin değiştirilmesi veya şifre ilavesiyle sistemin kullanılmasına engel konulması, programın bozulması, sistemin kilitlenmesi hareketleri de sistemin işlemesine engel olma niteliği taşımaktadır. Görüldüğü üzere sistemin işlemesine engel olma, sisteme fiziki etki şeklinde gerçekleştirilebileceği gibi, soyut unsurlara yapılan müdahalelerle de söz konusu olabilir⁸⁸.

Suçun konusunu sadece yazılım unsuru olarak kabul eden görüşe göre, bir bilgisayarın ya da ünitelerinin bir eşya olarak tahrip edilmesi veya çalınması bu suç oluşturmaz. Sadece bilgilerin kaydedildiği disket ya da USB belleğin tahrip edilmesinin de bu suç oluşturmayacağı savunulmaktadır. Bu görüşe göre bunlar sistemin birer elemanı olsa da bunların zarar görmesi bilişim sisteminin işleyişini ne engeller ne de bozar. Bu görüş, sistemin işleyişinin engellenmesini veya bozulmasını sistemin donanım unsuruna verilen zararlar yazılımın etkisiz kılınması halinde değil, yazılım unsuruna yönelik müdahale sonucu donanımın bir işe yaramaması halinde gerçekleştirilebileceğini ileri sürmektedir. Sistemin işleyişini sağlayan bir soyut unsura, sistemin bir bütün olarak kendisinden beklenen fonksiyonu yerine getirmesine

⁸⁶ Akbulut, **a.g.e.**, s. 192, 193.

⁸⁷ Bu saldırılar, bir kişinin bir sisteme düzenli veya arka arkaya yaptığı saldırılar sonucunda hedef sistemin kimseye hizmet veremez hale gelmesi veya o sisteme ait tüm kaynakların tüketimini amaçlar. Dülger, **a.g.e.**, s. 117.

⁸⁸ Akbulut **a.g.e.**, s. 27. Aynı görüşte Dülger, **a.g.e.**, s. 321.

engel olabilecek şekilde müdahalede bulunmakla bu suçun oluşacağını ifade etmektedirler⁸⁹.

Biz yukarıda ayrıntılı olarak açıkladığımız gibi hem donanım hem de yazılım unsuruna yapılan müdahalenin bu suçu oluşturacağını kabul etmemiz nedeniyle bu görüşe katılmıyoruz. Somut veya soyut unsura müdahale ile sistemin işleyişi engelleniyorsa neticenin gerçekleştiğini söyleyebiliriz.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 5. maddesi engel olma fiilini sisteme bilişim verilerinin girilmesi, nakledilmesi, bozulması, silinmesi, tahrip edilmesi, ortadan kaldırılması suretiyle gerçekleştirilebileceğini belirterek fiilin seçimlik hareketlerini göstermiştir⁹⁰. Bunun aksine TCK'daki düzenlemede engellemenin hangi hareketlerle gerçekleştirilmesi gerektiği belirtilmemiştir. Bu nedenle bilişim sisteminin işleyişini engelleme neticesi her türlü hareketle gerçekleştirilebilmektedir. Sistemin işleyişi, sistemin tümüne yöneltilen herhangi bir hareketle bozulabileceği gibi sistemde yer alan verilere yapılacak müdahaleler ile de bozulabilir. Sistemde yer alan verilere yapılan müdahaleler yönünden, müdahalenin sistemin işleyişini engellememesi veya bozmaması halinde TCK m. 244/2'de yer alan suç, müdahalenin sistemin işleyişini engellemesi veya bozması halinde ise TCK m. 244/1'de yer alan suç oluşur⁹¹. TCK m. 244/2'de düzenlenen suçun oluşması için verilere yönelik bu tür müdahalelerin bilişim sistemini engelleme boyutuna gelmemesi gerekir⁹².

ii. Bilişim Sisteminin İşleyişini Bozmak

Öncelikle ifade edilmelidir ki doktrinde bir görüşe göre, kanun metninde kullanılan bozma kavramı gereksiz yere kullanılmıştır. Ne şekilde olursa olsun bilişim sisteminin işleyişi bozulduğunda sistem engellenmiş de olacaktır. Zira engellemenin kısmen olması da yeterlidir. Sistemin işleyişinin bozulması, en azından sistemin işleyişinin kısmen engellenmesi sonucunu doğurur. Her engelleme bozma niteliğinde

⁸⁹ Koca/Üzülmez, **a.g.e.**, s. 871.

⁹⁰ Karagülmez, **a.g.e.**, s. 238; Parlar/Hatipoğlu, **a.g.e.**, s. 3476

⁹¹ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 882.

⁹² Koca/Üzülmez, **a.g.e.**, s. 871.

olmamasına rağmen her bozmanın engelleme olduğu açıktır. AKSSS ‘nin 5. maddesinde “... bilgisayar verilerini başka yerlere iletme, tahrip etme, silme, bozma, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilinin...” denilerek engelleme fiilini bozmayı da kapsayan bir şekilde açıklandığı görülmektedir⁹³. Bu görüşe göre ilk fıkrada sadece “sistemin işleyişinin engellenmesi” kavramıyla yetinilmesi gerekmektedir. Zira bilişim sisteminin kısmen veya tamamen işleyişinin bozulması, sistemin kısmen veya tamamen işleyişine engel olunması fiilidir. Bu görüş, madde gerekçesinde bozmanın da engelleme olduğu açıklanmasıyla birlikte madde metninden bozmanın çıkarılması gerektiğini ileri sürmektedir⁹⁴.

Aksi görüş ise sistemin işleyişinin bozulması durumunda engellenmesinin de söz konusu olacağını belirtmekle beraber her engellenme durumunda sistemin bozulması gerçekleşmediğinden kanun koyucu tarafından ayrı bir belirme yapıldığını savunmaktadır⁹⁵.

Kanaatimizce sistemi engellemenin her zaman bozma anlamına gelmeyeceğini savunan ikinci görüş isabetlidir. Zira engellenen bir sistem bozulmamış durumda olabilmektedir.

Engelleme fiilinde olduğu gibi bozma fiilinin tanımında da doktrinde görüş birliği bulunmamaktadır.

Bozma teriminden ise sistemin engellenmesi halinin en üst noktası olan durma noktasından da ileri gidilerek sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi hatta bazı görüşlere göre fiziki olarak dahi zarar verilmesi anlaşılmalıdır⁹⁶.

Sistemin bozulması durumunda ise sistemin tamamıyla çalışamaz hale gelmesi söz konusudur. Çalışamaz hale getirilmesi sistemin çökertilmesi, program akışının

⁹³ Erdoğan, **a.g.e.**, s. 194. Aynı yönde Karagülmez, **a.g.e.**, s. 238.

⁹⁴ Karagülmez, **a.g.e.**, s. 238.

⁹⁵ Koca/Üzülmez, **a.g.e.**, s. 869.

⁹⁶ Kurt, **a.g.e.**, s. 161.

değiştirilmesi, bozulması, yazılımlarının virüsler aracılığıyla işlemez hale getirilmesi şekillerinde gerçekleştirilebilir. Sistemin engellenmesi durumunda ise sistem sağlam olmasına rağmen engelleme durumundan dolayı çalışmamaktadır. Bozulmada ise tamamıyla devre dışı bırakılma söz konusudur. Bozulmadan kast edilen bilişim sistemin işleyişinin bozulmasıdır. Bu suç bilişim suçlarının işleme şekillerinden birisiyle yani bizzat sistemin başına oturarak ya da bir ağ üzerinden ulaştığı sisteminin işletimini sağlayan programlara zarar vermek ya da sistemin işletim yazılımını çökertmek suretiyle işleyişini bozmak suretiyle işlenebilir⁹⁷.

Sistemin çalışma şeklinin bozulması, sistemin yapması gerekenden farklı şeyleri yapmasını ifade etmektedir. Bilişim sisteminin veri işlem yapmasının, verileri aktarmasının sistemden beklenildiği gibi gerçekleştirilememesi ve sistemin eskisi gibi işlemleri yapamaması olarak tanımlanabilir⁹⁸.

Bozma ise sistemin çalışma düzenini aksatmak, işlemlerini engellemekten öte ayrıca bir sonucu doğuracak nitelikteki yani sistemin artık işlemlerinin olanaksız olduğu, hiçbir fonksiyonunu yerine getiremediği bir çalışmama neticesini ve buna neden olan hareketleri kapsar⁹⁹.

Diğer bir görüş TDK tanımı ile kanun metnini birleştirerek bilişim sisteminin işleyişinin bozulmasını bilişim sisteminin veri işleme faaliyeti yapamayacak hale getirilmesi ya da doğru sonuçlara ulaşmasına engel olacak şekilde müdahalede bulunulması olarak tanımlamıştır¹⁰⁰.

Yargıtay 11. Ceza Dairesi'nin 13.01.2013 tarih 2011/2816 Esas 2013/4065 Karar numaralı kararında sistemin bozulmasını tabiri ile *“bilişim sistemine dâhil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara*

⁹⁷ Kurt, **a.g.e.**, s. 164.

⁹⁸ Akbulut, **a.g.e.**, s. 194.

⁹⁹ Eker, **a.g.m.**, s. 125.

¹⁰⁰ Erdoğan, **a.g.e.**, s. 193.

uğratılması, işlemez hale getirilmesi veya fiziki olarak dahi zarar verilmesi anlaşılmaktadır...” anlaşılması gerektiğini belirtmektedir¹⁰¹.

Bilişim sisteminin işleyişinin bozulması, bilişim sisteminin olağan ve normal koşullarda yapması gereken işlevlerinin değişikliğe uğratılmasıdır¹⁰². Sistemin çalışma şeklinin bozulması, sistemin yapması gerekenden farklı şeyleri yapmasının sağlanmasını ifade etmektedir. Kısaca bilişim sisteminin veri işlem yapmasının, verileri aktarmasının sistemden beklenildiği şekilde gerçekleştiremeyecek, sistemin performansının düşürülmesi ve yavaşlatılması söz konusu olacaktır¹⁰³.

Bir görüş, bilişim sisteminin işleyişini bozma neticesini kalıcı surette sistemden istifadenin engellenmesi¹⁰⁴ olarak tanımlarken; diğer görüş, haksız müdahale ile sistemin sağlıklı işleyişinin geçici ya da sürekli şekilde ortadan kaldırılması olarak neticeyi tanımlamıştır¹⁰⁵.

İlk görüşe göre, sisteme yüklenen yazılım ile sistemin işleyişine müdahalede bulunulması durumunda eğer bilişim sisteminin işleyişinin geçici olarak kesintiye uğramışsa engelleme, sistemin işleyişi o andan itibaren kalıcı olarak sonlandırılmışsa bozma gerçekleşmiş olur¹⁰⁶.

Verilerin bilginin sayısal koda dönüştürülmüş hali olduğundan, bu kodlardan birinin dahi olmaması verinin kullanılmasını engeller veya verilerden oluşan bütünü bozmaya yetebilir. Bu nedenle bunların kısmen ya da tamamen bozulması açısından bir fark bulunmaz. Örneğin bilişim sisteminin işlemcisine ya da güç dağıtıcısına etkide bulunulmadan sabit diskinin kırılması durumunda her ne kadar bilişim sisteminin bir kısmının bozulması söz konusu olsa da sistemin içerdiği veriler sabit diskin üzerinde bulunduğu ve bunun bozulmasıyla verilere ulaşamayacağı ve dolayısıyla bilişim

¹⁰¹ Aktaran Gül, **a.g.e.**, s. 84.

¹⁰² Yazıcıoğlu, **a.g.e.**, s. 263.

¹⁰³ Akbulut, **a.g.e.**, s. 30; Gül, **a.g.e.**, s. 84.

¹⁰⁴ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s.882.

¹⁰⁵ Karagülmez, **a.g.e.**, s. 238. Aynı görüşte Parlar/Hatipoğlu, **a.g.e.**, s. 3477.

¹⁰⁶ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 984.

sisteminden beklenen işi yapamayacak duruma geleceğinden suç gerçekleşmiş olur¹⁰⁷.

Bozma ağ üzerinden, bilişim sistemine fiziki temasla ve hatta bilişim sistemine hiç dokunmaksızın elektrik kesilmesi ya da virüs gönderilmesi gibi hareketlerle yapılabilecektir¹⁰⁸. Örneğin sistemin parçalarının değiştirilmesi veya verilerin değiştirilmesi veya bazı verilerin silinmesi veya hatalı program teslimi veya basit virüsler göndermek suretiyle bilişim sisteminin işleyişinin bozulması söz konusu olabilir. Sistemin başka şekilde işleminin veya yanlış işleminin sağlanması da bozulma kavramının içine girer. Sistemin içine kurulan programlar sistemin işleyişini bozabilir. Bu programlar bağlantıyı kopararak uluslararası olan kendi serverlarına bağlamakta, bu şekilde kullanıcının 900'lü hatlara bağlanıyormuş gibi ücret ödenmesine neden olmaktadır. Bu şekilde ödenen ücretler oldukça yüksek miktarlara ulaşmaktadır. Bu yazılımlara genelde erişimi yasak olarak girilen sitelerde rastlanılmaktadır¹⁰⁹.

Burada dikkat edilmesi gereken husus fiziki zararın sistemin işleyişine verilmesi gerektiğidir. Bu husus madde metninde de vurgulanmıştır. Bilişim sisteminin işleyişinin engellenmesi neticesinden bilişim sistemine bilişim suçunun işlenme şekillerinden birisiyle ya da fiziki saldırılar sonucu sistemin tamamıyla çökertilmesi, bozulması, işlemez hale getirilmesi anlaşılmalıdır. Bilişim sisteminin işleyişinin engellenmesinin bilgisayar ortamına ilişkin hareketler ya da fiziki saldırılarla gerçekleşiyor olması suçun oluşumu açısından bu sebeple önemli değildir. Bilişim sisteminin üzerine su dökmek, bir cisimle vurmak ya da yüksek voltaj akım vermek suretiyle de bilişim sisteminin işleyişi bozulabilir¹¹⁰.

Bilişim sisteminin işleyişinin bozulmasının ne şekilde gerçekleştiği suç açısından önem arz etmez. Fail ister verilerin düzeninin bozsun, ister verilerin bulunduğu bilişim sistemine virüs göndererek verileri tahrip etsin isterse de tahrip

¹⁰⁷ Dülger, **a.g.e.**, s. 322

¹⁰⁸ Erdoğan, **a.g.e.**, s. 193.

¹⁰⁹ Akbulut, **a.g.e.**, s. 194.

¹¹⁰ Kurt, **a.g.e.**, s. 165, 166.

edilmek istenilen verilerin bulunduğu sistemi baltayla parçalasın suç gerçekleşmiş olacaktır¹¹¹.

Fiziksel müdahalelerin bu suçu oluşturmayacağını kabul eden görüşe göre, maddede ayrıca bilişim sisteminin işleyişinin bozulmasına yer verilmesi, bu madde ile fiziksel müdahalelerden çok yazılım ve veriye müdahale yoluyla sistemin bozulmasına ilişkin bir düzenleme yapılması amacını taşımaktadır. Bu fıkra ile sadece sistemin yazılım yönüne yönelik fiillerin yaptırım altına alındığını belirtilmektedir. Bu nedenle donanıma ait unsurlara zarar verilmesi durumunda mala zarar verme suçunun oluştuğunu savunmaktadırlar¹¹².

Kanaatimizce bilişim sistemin işleyişinin bozulması sistemin kendinden beklenen işleyiş ve veri işlem faaliyetinin yerine getirilemeyecek şekilde sistemin zarar görmesi olarak tanımlandığından bunun fiziksel müdahale ya da soyut unsurlarına müdahale ile gerçekleşmesi arasında bir fark bulunmamaktadır. Her iki unsura müdahale bu suçu oluşturmaktadır.

(2) Bilişim Sistemindeki Verilere Müdahale Suçu

Bu fıkroda bir bilişim sistemi içerisindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi fiilleri suç olarak düzenlenmiştir. Verilere karşı gerçekleştirilecek erişilmez kılmadan yok etmeye kadar tüm fiiller sayılarak bunlarla beraber iki fiilin arasında kalan bozma ve değiştirme de kapsam içine alınmıştır. Bunlardan ayrı olarak verilerin bir başka yere gönderilmesi de verilere karşı işlenebilecek bir fiil olarak düzenlenmiştir¹¹³. Ancak düzenlenen bu fiillerin sistemi engellememesi veya bozmaması gerekmektedir. Aksi halde TCK m. 244/1’de düzenlenen suç oluşur¹¹⁴.

¹¹¹ Dülger, **a.g.e.**, s. 322. Aynı görüşte Akbulut **a.g.e.**, s. 31; Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 881; Yazıcıoğlu **a.g.e.**, s. 263.

¹¹² Ketizmen, **a.g.e.**, s. 136.

¹¹³ Kurt, **a.g.e.**, s. 161.

¹¹⁴ Koca/Üzülmez, **a.g.e.**, s. 871.

765 sayılı TCK'nın 525/b-1 maddesinden farklı olarak bilişim sistemi içerisindeki veriye müdahale TCK m. 244/2'de ayrıca düzenlenmiş ve sisteme müdahaleye göre daha az ceza öngörülmüştür¹¹⁵.

TCK m. 244/2'nin Avrupa Konseyi Siber Suç Sözleşmesi'nin 4. maddesi ile paralel olarak düzenlendiğinden yukarıda bahsetmiştik. Sözleşmedeki “zarar verme” neticesi TCK'da bulunmasa da aşağıda ayrıntılı olarak açıklanacak olan neticelerin kapsamının geniş olmasından dolayı bunu bir eksiklik olarak görmek mümkün değildir. Aynı şekilde “silme” kavramına TCK'da yer verilmemiş olsa da 2. fıkradaki “yok etme” ve “erişilmez kılma” neticelerinin içerisinde değerlendirilebileceğinden bu konuda da bir eksiklik bulunmamaktadır. 2. fıkra düzenlenirken başta “erişilmez kılma”, “sisteme veri yerleştirme”, “var olan verileri başka bir yere gönderme” şeklindeki neticelerin Sözleşme'nin “Bilgisayar Bağlantılı Sahtecilik” başlıklı 7. ve “Bilgisayar Bağlantılı Dolandırıcılık” başlıklı 8. maddelerindeki bilgisayar sisteminin çalışmasına yönelik her türlü müdahalenin yasaklanmasına ilişkin düzenlemelerin gereğinin yerine getirilmesine yönelik olduğu söylenebilir¹¹⁶.

i. Verileri Bozmak

Verileri bozmak, verilerden elde edilmek istenen faydanın elde edilememesi durumudur. Bu hareket mevcut verilerin niteliğinin değiştirilmesi şeklinde gerçekleşebileceği gibi verilerin tamamen ya da kısmen tahribi ile de gerçekleşebilir. Örneğin bilişim sistemlerine sızan yazılımlar yoluyla sistemde yer alan veriler tahrip edilebilir. Ancak sistemin fiziki varlığına yapılacak müdahaleler yönünden ancak içindeki verilerin zarar görmesi halinde verilerin bozulmasından bahsedilebilecektir¹¹⁷. Bu durumda veriler varlıklarını devam ettirmektedir fakat varlık sebebini, işlevini, kısmen ya da tamamen programlandıklarına uygun şekilde yerine getirememektedirler¹¹⁸.

¹¹⁵ Ketizmen, **a.g.e.**, s. 137.

¹¹⁶ Karagülmez, **a.g.e.**, s. 240.

¹¹⁷ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6933.

¹¹⁸ Erdoğan, **a.g.e.**, s. 220.

Verileri bozma, sistemdeki verilerin yok edilmeden kullanılamayacak oranda zarar görmesini, işlevini yitirecek şekilde şeklinin değiştirilmesini ifade eder¹¹⁹. Bozma, verilerin kullanılabilirliğine zarar verilmesidir¹²⁰. Verinin içeriğine müdahalenin var olan verinin içerdiği bilgiye olumsuz müdahaleyi kapsadığını belirtmek gerekir. Verinin yok edilmesinden farklı olarak burada verinin tasarruf alanından çıkartılmaması söz konusudur¹²¹.

Bilişim sisteminin işleyişini bozmak neticesi bakımından bahsedilen hareketler verileri bozmak neticesi açısından da geçerlidir¹²².

Veri içeren bir dosyanın (ses, müzik, metin vb.) bozularak ya tamamıyla faydalanamayacak ya da kısmen hasarlı hale getirilmesidir. Bozulmanın ya içeriden gelen bilişim temelli bir hareketle ya da dışarıdan gelen bir hareket sonucunda gerçekleşmesi gerekir¹²³.

Sistem içerisindeki veri grubunu oluşturan programa virüs gibi kötü amaçlı kodların eklenmesi, bu anlamda veriyi bozma değil, verinin değiştirilmesi olarak anlamak gerekir. Bu halde virüs gibi kötü amaçlı kodların öngörülen şekilde çalışmasından önceki bir aşamada var olan veriye eklenmesi söz konusu olup, veri tamamen ya da kısmen kullanılamaz hale gelmemiştir¹²⁴.

Veriye virüs bulaştırılması, mantık bombası, kurtçuk gibi yazılımlar yoluyla kullanılmaz hale getirilmesi verilerin bozulmasına örnek olarak gösterilir. Bunun dışında verileri içeren sabit diskin ya da veri taşıma aracının fiziken kırılması ya da SD diskin ezilmesi yoluyla da bu fiilin gerçekleştirilmesi mümkündür¹²⁵.

Verinin bozulmasıyla yok edilmesi arasındaki farktan da bahsetmek gerekir. Bozulmada veri sahibinin veriye ulaşması imkânına son verilmezken, verinin yok

¹¹⁹ Meran, **a.g.e.**, s. 571.

¹²⁰ Akbulut, **a.g.e.**, s. 196.

¹²¹ Ketizmen, **a.g.e.**, s. 139.

¹²² Dülger, **a.g.e.**, s. 322

¹²³ Kurt, **a.g.e.**, s. 167.

¹²⁴ Ketizmen, **a.g.e.**, s. 140.

¹²⁵ Koca/Üzülmez, **a.g.e.**, s. 871; Dülger, **a.g.e.**, s. 322.

edilmesi durumunda bu imkân da kaybedilmektedir. Bozmada bozulmuş da olsa bir veri bulunmaktadır sadece veri kısmen ya da tamamen işlevini yerine getirememektedir. Diğer bir fark ise bozulma sonrası bozulan veri teknik destekle eski haline getirilebilirken, yok edilmede çoğunlukla verinin eski hale getirilmesi mümkün değildir¹²⁶.

ii. Verileri Yok Etmek

Verinin yok edilmesi, verinin varlığına son verilmesi, ortadan kaldırılması, hak sahibinin tekrar elde edemeyeceği ya da çeşitli programları kullanarak elde edebileceği şekilde tasarrufundan çıkarılması olarak tanımlanabilir¹²⁷.

Burada mevcut kayıtların, bulundukları yerlerden silinmesi kast edilmektedir. Ancak burada anlaşılması gereken husus maddi anlamda bir yok etme değil, sadece silinen unsura ulaşabilmek bakımından gereken normal bağın ortadan kaldırılması, bilgilerin tanınmaz hale getirilmesidir. Burada silmek kelimesini şeklen anlamak gerekmektedir. Zira maddi anlamda verilerin silinmesi genelde imkânsızdır. Çünkü bir kere hard diske kaydolunan veriler, teknik olarak bu disk üzerinde çeşitli suretlerde yer almaya devam ederler. Bazen silinen bir kaydı basit komutlarla, bazen de çok karışık çalışmalar neticesinde geri kazanmak mümkündür. Bu bakımdan verinin silinmesinden anlaşılması gereken, mevcut bilgilere normal ulaşım bağlarının koparılması veya mutlak ulaşım yollarının engellenmesidir¹²⁸. Verileri yok etmek ile kast olunan bu bilgilere normal ve olağan yoldan ulaşım bağlantılarının kesilmesidir¹²⁹.

Verileri yok etmek için sisteme uzaktan muamele iki yöntemle gerçekleştirilebilir. Bunlardan ilki çeşitli hile yöntemleri ile tahrip özelliği bulunan veya uzaktan tahribi sağlayabilecek yazılımların bilişim alanına sokulması ile olur. İkincisi ise hedef cihaza virüs ya da Truva Atı gibi herhangi bir yazılım kaydetmeksizin sistemin eksikliğinden

¹²⁶ Erdoğan, **a.g.e.**, s. 220.

¹²⁷ Ketizmen, **a.g.e.**, s. 138.

¹²⁸ Yazıcıoğlu, **a.g.e.**, s. 263.

¹²⁹ Meran, **a.g.e.**, s. 572.

faydalananarak yani yazılımların açık olarak tabir edilen kusurlarından yararlanılarak tahribatta bulunmaktır¹³⁰.

Doktrinde birçok yazarın katıldığı görüşe göre bilişim sistemindeki veriler açısından, sözlükteki gerçek anlamıyla onları tamamen ortadan kaldırmak mümkün değildir. Kanun koyucunun bu ifadeyle somut anlamda yok etmek fiilini değil, bilişim alanında geçerli olan soyut anlamda yok etmek fiilini kastettiğini kabul etmekteyiz¹³¹.

Silmek, bilişim ortamındaki verilerin veya programların üzerine başka veri veya programlar yerleştirilmesi veya verilerin bellek üzerinde bulunduğu noktaya ulaşılmasını sağlayan bağların koparılması suretiyle verilerin kullanılmaz hale getirilmesini ifade etmektedir¹³².

TCK m. 244/2’de 765 sayılı TCK m. 525/b’de olduğu gibi verinin silinmesinden bahsedilmemiş, verinin yok edilmesi esas alınmıştır. Verinin silinmesini yok etme kapsamında olup olmadığının tartışılması gerekmektedir. Zira verinin silinmesi, teknik olarak silinen veriye her zaman için ulaşılabilmesi anlamına gelmemekte, sadece olağan yollardan o veriye ulaşılması imkânının olmamasını ifade etmektedir¹³³.

Bilişim sisteminde herhangi bir veriyi yok etmek amacı ile sil komutu verildiğinde o veriler tamamen yok olmamakta yalnızca dosyalama sistemine göre o verilere ulaşımı sağlayan anahtar veriler değiştirilmekte ve bilişim sisteminin dosyalama sistemi sayesinde bir daha normal yollarla söz konusu veriye ulaşılması engellenmektedir. Ancak çoğu zaman gösterilen çabalar sayesinde verilerin tekrar elde edilmesi mümkün olmaktadır. Örneğin genel olarak verilerin yok edilme yöntemi olarak bilinen “bilgisayara format atma” işleminde, aslında veriler silinmemekte ancak bilgisayarın sabit diskinde verilerin nerede bulunduğunu gösteren fihristteki kayıtlar silinmekte, böylelikle fihristte bu verilerin bulunduğu sektörler, yeni verilerin

¹³⁰ Akıncı/Alıç/Er, **a.g.m.**, s. 175, 176.

¹³¹ Erdoğan, **a.g.e.**, s. 222; Kızıltan, **a.g.t.**, s. 81.

¹³² Kızıltan, **a.g.t.**, s. 47.

¹³³ Ketizmen, **a.g.e.**, s. 138; Yazıcıoğlu, **a.g.e.**, s. 263.

yazılabilmesi için boş gösterilmektedir. Dolayısıyla bu sektörlerin üzerine yeni veriler yazılmadıkça, veri kurtarma programlarıyla bu verilerin geri getirilmesi mümkün olmaktadır. Verilerin gerçek anlamda silinmesi ise “wipe” denilen işlemle sabit diske elektromanyetik şok verilmesi ve sabit diskin katmanları üzerinde bulunan ve okuyucu kafanın izlediği çizgilerin yok edilmesiyle gerçekleşmektedir¹³⁴. Dolayısıyla silme hareketi yok etme hareketinin kapsamında olmakla birlikte yok etme kavramının daha geniş olduğunu söyleyebiliriz.

Yok etme verilerin ortadan kaldırılarak silinmesi ya da mevcut olduğu sistemin biçimlendirilmesi şeklinde gerçekleştirilebilir. Yok etme sisteme fiziksel müdahale yoluyla yapılabileceği gibi sisteme bir bilişim ağı vasıtasıyla etki etmek suretiyle de yapılabilir¹³⁵.

Verilerin geri dönüşüm kutusuna gönderilmesiyle verinin yok edilmiş sayılıp sayılmayacağı doktrinde tartışma konusu olmuştur. Bir görüş¹³⁶ dosyanın geri dönüşüm kutusuna taşınmasıyla sırf yerinin değiştirildiğinden bahisle suçun oluşmayacağını, geri dönüşüm kutusundaki verilerin tek bir tıkla yeniden eskisi gibi oluşturabildiğini, bu nedenle buradaki verilerin yok olduğunun kabul edilmeyeceğini belirtirler. Diğer görüş¹³⁷ ise bilişim sistemlerinde gerçek anlamda bir silme işlemi değil mantiki bir silmenin söz konusu olduğunu, bunun da o verilere ulaşılmasının bir şekilde engellenmesiyle gerçekleştiğini, mağdur açısından verilerin yok edilmiş anlamına geldiğinden suçun oluştuğunu kabul eder. Bu görüşe göre geri dönüşüm kutusundaki veriler bulundukları yerde olduğu sürece kullanılamaz. Verinin bulunduğu geri dönüşüm kutusundan çıkartılıp sisteme geri alınması gerekir. Sistem içine alma basit bir işlem olarak gözüксе de veri sahibin bu külfete katlanması beklenemez. Silinmesinin üzerinden geçen gün sayısı ya da silindiği bilişim sisteminin gelişmişliği ya da karışıklığı gibi nedenlerle bu basit işlem çoğu zaman daha karışık bir hal almaktadır¹³⁸. Dolayısıyla bu görüşe göre veri sahibinin verisini bıraktığı yerde

¹³⁴ Dülger, **a.g.e.**, s. 323, 324.

¹³⁵ Akıncı/Alıç/Er, **a.g.m.**, s. 176; Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6933.

¹³⁶ Koca/Üzülmez, **a.g.e.**, s. 872.

¹³⁷ Dülger, **a.g.e.**, s. 324.

¹³⁸ Erdoğan, **a.g.e.**, s. 222.

bulamaması halinde veriye tekrar ulaşabilme imkânının olması suçun oluşmasına engel değildir¹³⁹.

Bu görüşe karşı çıkan görüşe göre verinin silinmesi yani o mağdurun o veriye ulaşımının engellenmesi halinde “verilerin yok edilmesi” değil “verilerin erişilmez kılınması” söz konusudur. Verilere ulaşmayı son derece zorlaştıran silme programları olduğu gibi ne olursa olsun bu bağı kurmayı mümkün hale getirecek çok işlevli programlar da bulunmaktadır. Verilerin silinmesinin değil verilerin erişilmez kılınması neticesinin bu gibi durumlarda gerçekleştiğini savunmaktadırlar¹⁴⁰.

Kanaatimizce verilerin geri dönüşüm kutusuna gönderilerek silinmesi hareketi verilerin yok edilmesi kapsamındadır. Burada failin kastı verileri silerek veri kullanıcısının bu verileri kullanmasının önüne geçmektedir. Verilerin erişilmez kılınması durumunda veri kullanıcısı verilerin sistemde olduğunu bilmesine ya da simgesel olarak verileri görmesine rağmen bu verilerin içeriğine ulaşamamaktadır. Verilerin geri dönüşüm kutusuna gönderilmesi ve hatta buradan da silinmesi durumunda sistem kullanıcısı verileri sistemde bulamamaktadır, bu nedenle geri dönüşüm kutusuna gönderilen verilerin durumu yok edilme anlamındadır.

Verilerin yok edilmesi bozmadan farklıdır. Bozmada verilerin sonuç olarak işlevsiz ve kullanılamaz hale getirilmesi söz konusudur ancak yine de bazı durumlarda düzeltilmeleri mümkündür. Ancak yok edilmede ortada düzeltilecek bir unsur da kalmamıştır¹⁴¹.

TCK m. 244/2’deki yeni düzenlemede verilerin silinmesi ifadesine yer verilmemesi isabetlidir. Bilişim sistemindeki verilerin silinmesi durumunda veri yok edilmiş olmakta, yine yukarıda açıkladığımız üzere veri sahibinin verisine ulaşması

¹³⁹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 987.

¹⁴⁰ Kurt, **a.g.e.**, s. 168.

¹⁴¹ Kurt, **a.g.e.**, s. 168.

imkânı normal yollarla ortadan kalkmaktadır. Dolayısıyla yok etmek, silmek fiilini de kapsadığından yeni düzenlemede bu fiile yer verilmemesi isabetlidir¹⁴².

Başkasına ait e-posta hesabına (facebook, twitter, instagram gibi sosyal paylaşım siteleri) şifresini ele geçirerek girmek, bu hesapta bulunan e-postaları (verileri) silmek bu suçun işleniş şekline örnek olarak verilebilir¹⁴³.

Verilerin disk, CD, USB cihazı gibi bir taşıma aracında bulunması durumunda bu cihazların kırılması verilerin silinmesine örnek olarak verilebilir¹⁴⁴. Taşıma aracındaki verilerin veri kurtarma yazılımları sayesinde kısmen veya tamamen kurtarılabilir olmasının suçun tamamlanmasında bir önemi yoktur¹⁴⁵.

iii. Verileri Değiştirmek

Var olan verinin kullanılmasını engellemeyen fakat verinin içeriğinin ya da kendisinin orijinalliğini ortadan kaldıran her türlü değişiklik olarak tanımlanabilir. Bu nedenle kötü amaçlı kodların veriye yerleştirilmesi bu kapsamdadır¹⁴⁶. Örnek olarak kullanıcının sisteme koyduğu şifrenin yerine başka bir şifrenin konulması hali verilebilir¹⁴⁷.

Verilerdeki yeni bir bilginin oluşmasını sağlayan her türlü hareket değiştirme kavramı içinde kabul edilmektedir. Yine aynı şekilde kaydedilmiş verilerin içerik değiştirilmesinin her formu verilerin değiştirilmesidir. Verilerin içeriğinin tamamen değiştirilmesi veya veri sonuçlarının değiştirilmesi veya program dilinin değiştirilmesi veya verilere ek şeylerin katılması yeni bir bilginin oluşmasını sağlayan hareketlerdir¹⁴⁸. Verilerin silinmesi verilerin yok edilmesi kapsamı içinde yer alsada

¹⁴² Erdoğan, **a.g.e.**, s. 223.

¹⁴³ Gül, **a.g.e.**, s. 85.

¹⁴⁴ Kurt, **a.g.e.**, s. 168; Soyaslan, **a.g.e.**, s. 619.

¹⁴⁵ Dülger, **a.g.e.**, s. 324.

¹⁴⁶ Ketizmen, **a.g.e.**, s. 140; Eker, **a.g.m.**, s. 126.

¹⁴⁷ Dülger, **a.g.e.**, s. 324.

¹⁴⁸ Akbulut, **a.g.e.**, s. 198.

eğer silinen veriler yeni bir şey ifade ediyorsa bu da değiştirmek kavramı içinde değerlendirilebilir¹⁴⁹.

Verinin içeriğinin değiştirilmesi, bir veri yerine başka bir verinin yerleştirilmesi, verinin başka bir görünüme getirilmesini ifade eder¹⁵⁰. Değiştirmenin kısmen olması mümkün olduğu gibi tamamen olması da mümkündür. Amacın bir önemi olmadığı gibi fail bu fiili menfaat temin etmek ya da herhangi bir amaç gütmeksizin yapabilir¹⁵¹. Veriyi değiştirmekte amaç veriyi yok etmek ya da erişilmez kılmak değildir, veri değiştirildiğinde sistem işlemeye devam eder. Amaç veriye ulaşıldığında yanlış bilgilere erişilmesini sağlamaktır¹⁵². Ancak verilerin menfaat temin edilmesi amacıyla değiştirilmesi söz konusu olursa fiil başka bir suç oluşturmadığı takdirde TCK m. 244/4'te düzenlenen bilişim sistemi kullanılarak haksız çıkar sağlama suçunun olduğu kabul edilmektedir¹⁵³.

Verilerin izinsiz şekilde kopyalanması verilerin değiştirilmesi kapsamında değerlendirilemez. Ancak mevcut verilerde değişiklik yapmak suretiyle başkasına ait WLAN (wireless local area network – kablosuz yerel alan ağı) ağının kullanılması söz konusu olmuşsa şifre değişikliğinden dolayı verilerde de değişiklik meydana geldiğini kabul etmek gerekir¹⁵⁴.

Verileri değiştirmek hareketi, veriler üzerinde yapılan manipülasyonları içermektedir. Bunlar verilerin başka biçimlere sokulması, verilere yeni içerik kazandırılması, verilerin eski niteliklerinin değiştirilmesi şeklinde olabilir¹⁵⁵.

Doktrinde verilerin değiştirilmesi, silinmesini ve erişilmez kılınması fiillerini aynı fiil olarak kabul eden görüş de bulunmaktadır. Bu görüş, verilerdeki her değişiklikte bellek yerinin yeniden yazılmasına yani orada daha önce bulunan verilerin

¹⁴⁹ Manfred Möhrenschlager, **Das neue Computerstrafrecht**, wistra, 1986, Heft 4, s. 141. Akbulut, **a.g.e.**, s. 198'den naklen.

¹⁵⁰ Koca/Üzülmez, **a.g.e.**, s. 872..

¹⁵¹ Kurt, **a.g.e.**, s. 168, 169.

¹⁵² Kızıltan, **a.g.t.**, s. 82.

¹⁵³ Parlar/Hatipoğlu, **a.g.e.**, s. 3478.

¹⁵⁴ Akbulut, **a.g.e.**, s. 198.

¹⁵⁵ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6933.

silinmesine dayanmaktadır¹⁵⁶. Verilerin değiştirilmesi hareketinde, veri ortadan kaldırılmadığından halen değiştirilmiş de olsa veriye ulaşım mümkün olduğundan biz bu görüşe katılmıyoruz.

iv. Verileri Erişilmez Kılmak

Verileri erişilmez kılmak, verilere erişim sağlayan yolların erişmek isteyen kişinin erişemeyeceği şekilde değiştirmesi veya bu yolların silinmesi şeklinde gerçekleştirilebilir. Mağdurun sisteminde bulunan verilere ulaşması imkânsızdır¹⁵⁷. Bu durumda aslında veriler mağdurun sisteminde olduğu halde fail, yaptığı işlemlerle mağdurun kendi verilerine ulaşmasını imkânsız hale getirmektedir¹⁵⁸. Söz konusu veriye erişimin engellenmesi o verinin yok edildiği anlamına gelmez. Erişilmez kılınması verinin içerdiği bilgiye müdahale edilmeden veriye olağan şekilde erişimin engellenmesi olup veri burada içerik olarak bütünlüğünü korumaktadır. Veri ne yok edilmekte ne de bozulmakta fakat ulaşılması için gereken işlem bağı koparılmaktadır¹⁵⁹.

Genel olarak verinin içerdiği bilgiye müdahale edilmeden veriye olağan şekilde erişimin engellenmesi, verilere ulaşım için gereken işlem bağına ortadan kaldırılmasıdır¹⁶⁰. Bu durumda veri içerik bakımından bütünlüğünü korumaktadır¹⁶¹.

Verilerin erişilmez kılınması herhangi bir şekilde gerçekleştirilebilir. Şifre koymak veya dosya isimlerini değiştirmek, dosyaları gizlemek, veri taşıyıcısına el koymak, elektronik postaları gizlemek gibi yollarla verilerin erişilmez kılınması gerçekleştirilebilir¹⁶².

¹⁵⁶ Jan C. Schuhr, “Bilgisayar Ceza Hukukunda Kıyas ve Davranış Normu: Verilerin Değiştirilmesi Örneği (Alman Ceza Kanunu madde 303a ve Siber Suç Sözleşmesi madde 4)”, Çev. Ahmet Mert Duygun, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 322.

¹⁵⁷ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6934.

¹⁵⁸ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 867.

¹⁵⁹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 987.

¹⁶⁰ Meran, **a.g.e.**, s. 572.

¹⁶¹ Ketizmen, **a.g.e.**, s. 140.

¹⁶² Akbulut, **a.g.e.**, s. 199.

Veriler üzerinde tanımlı bulunan yetki ayarlarının değiştirilerek verilere erişimin engellenmesi veya verilere erişimi sağlayan anahtar verilerin değiştirilmesi hareketlerinden birisiyle gerçekleştirilebilir¹⁶³.

Yargıtay 8. Ceza Dairesi'nin 2012/33557 Esas 2013/25987 Karar sayılı 01.11.2013 tarihli kararı şu şekildedir; *“katılana ait elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabında yazışmalar yapan ve şifreyi değiştirmek suretiyle katılanın anılan hesaplara erişimini engelleyen sanığın, eylemine uyan TCK.nun 244/2. maddesi uyarınca cezalandırılmasına karar verilmesi gerekir.”*¹⁶⁴

Verileri erişilmez kılma verilere ulaşmak istenildiği anda sistemin elektriğinin kesilmesi gibi çeşitli şekillerde gerçekleştirilebilir. Verilerin silinmesine yönelik de olsa verilerin bulunduğu bilişim sisteminin bozulması ya da çalışmasının engellenmesi durumunda ilk fıkradaki hükmün uygulanması gerekir. Ancak ilk fıkra da 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 ikinci fıkranın uygulanması gerekmektedir¹⁶⁵.

Verilerden faydalanmasına engel olan hareketlerin ne kadar süre için olması gerektiği konusunda farklı görüşler mevcuttur. Verinin içeriğinin bütünlüğü bozulmamasına rağmen veriye geçici ya da sürekli olarak kullanımının engellenmesi bu fıkra kapsamında düzenlenmiştir¹⁶⁶. Genel görüş olarak geçici sürede de olsa suçun oluştuğu kabul edilmekle beraber, bu süreden ne anlaşılması gerektiği belirli değildir. Geçiciliği, önemsiz olmayan bir süre için verilere erişimin imkânsız olması şeklinde kabul etmek en doğru seçenek olacaktır¹⁶⁷.

¹⁶³ Kızıltan, **a.g.t.**, s. 83; Bayındır, **a.g.m.**, s. 74.

¹⁶⁴ www.corpus.com.tr (Çevrimiçi) 17.03.2019.

¹⁶⁵ Dülger, **a.g.e.**, s. 325.

¹⁶⁶ Ketizmen, **a.g.e.**, s. 142; Taşkın, **a.g.e.**, s. 48; Dülger, **a.g.e.**, s. 325.

¹⁶⁷ Akbulut, **a.g.e.**, s. 201.

v. Veri Yerleřtirmek

Fail tarafından biliřim sistemine ya da veri taşıma aracına dıřarıdan ve sistem maliki ya da ilgisinden izin almaksızın çeřitli verilerin sisteme kaydedilmesi, yüklenmesi ya da eklenmesi neticesini oluřturan hareketler kast edilmektedir¹⁶⁸.

Sistem üzerinde hak sahibi olan kiřinin rızasına aykırı olarak herhangi bir verinin sisteme girilmesi halinde sisteme veri yerleřtirme neticesi söz konusu olur. Veri yerleřtirmek izinli ya da izinsiz olarak girilen sisteme doğrudan veri giriři yapılarak ya da dıřarıdan veri aktarımı řeklinde olabilir¹⁶⁹.

Veri yerleřtirmek sistemde bulunmayan dıř verilerin biliřim sistemine girilmesidir. Örneėin; flash bellek ya da CD gibi veri taşıyıcılar aracılıėıyla veriler sisteme girilmiře sisteme veri yerleřtirilmiřtir. Yine aynı řekilde internet ortamından sisteme veri yerleřtirilmiře suç tamamlanmıř sayılır¹⁷⁰. Yerleřtirilen veri bakımından suçun oluřması için failin amacı önemli deėildir, fiil neticesinde bir zarar doğmuř olması ya da failin kendisine menfaat saėlaması da gerekli deėildir¹⁷¹.

Veri yükleme neticesi aėısından sisteme hukuka uygun ya da hukuka aykırı olarak girmiř olmanın bir önemi yoktur. Zira hukuka uygun olarak girilen sisteme hukuka aykırı veri yerleřtirmek mümkündür¹⁷². Örneėin bedeli karřılıėında hizmet veren bir internet sitesine bedel ödenerek ve gerekli řifreler alınarak girilmesi kiřiye bu siteye veri yükleme hakkını çoėunlukla verse de her somut olayda sisteme giren kiřinin veri yükleme hakkının olup olmadığını arařtırmak gerekir¹⁷³.

¹⁶⁸ Dölger, **a.g.e.**, s. 328.

¹⁶⁹ Koca/Üzölmez, **a.g.e.**, s. 872.

¹⁷⁰ Akbulut, **a.g.e.**, s. 202.

¹⁷¹ Bayındır, **a.g.m.**, s. 74.

¹⁷² Kızıltan, **a.g.t.**, s. 83.

¹⁷³ Dölger, **a.g.e.**, s. 328.

Sisteme veri yerleřtirmek, sistemde yer alan verilere zarar vermeden sistemde mevcut olmayan ek bir takım verilerin sistemin ieriğine eklenmesidir. Netice sonucunda sarsılan verilerin güvenilirliėidir¹⁷⁴.

vi. Verileri Bařka Bir Yere Gndermek

Verilerin bařka bir yere gnderilmesi ibaresi, TBMM'ye 15.05.2003 tarihinde sunulan Tasarının sistem ve veriye mdahaleyi dzenleyen 347. maddesinde yer almamaktadır. TBMM Adalet Komisyonu tarafından bu madde deėiřtirilmiř ve sz konusu ibare maddeye eklenmiřtir¹⁷⁵.

Verilerin gnderilmesi, verilerin transfer edilmesidir. Bu netice, bir biliřim sistemindeki verilerin kopyalanması anlamına gelir. Bununla birlikte verilerin nereye kopyalandıėının bir nemi yoktur. Bir bařka biliřim sistemine ya da veri tařıma aracına aktarılması, kaydedilmesi ya da kopyalanmasıyla hareket gerekleřmiř olacaktır. Sistemden casusluk amacıyla askeri bilgilerin alınması ya da bir ėrencinin sınav sorularını alması durumunda bu hareket gerekleřmiř olmaktadır. Verilerin transferi sonucunda bařka bir sonu doėmuyorsa sadece bu netice nedeniyle fail cezalandırılacaktır¹⁷⁶.

Verinin bařka bir yere gnderilmesi verinin kopyalanması olarak kabul edilmiřtir. Kopyalamak ise oėaltmak anlamına gelir. Verinin oėaltılması ise verinin kendisine, verinin kullanımı aısından herhangi bir etkide bulunacak bir hareket deėildir¹⁷⁷.

Telekomnikasyon yolları zerinden veya mevcut aė ierisinde bir sistemdeki verilerin bařka bir sisteme gnderilmesidir¹⁷⁸. Verilerin gnderilmesi fiili genellikle internet zerinden sisteme yerleřtirilen Truva Atı, key logger ve virsler gibi programlarla gerekleřebileceėi gibi veri tařıma cihazına gnderilmesi de bu hareket

¹⁷⁴ Artuk/Gken/Yenidnya, **Trk Ceza Kanunu řerhi**, s. 6934.

¹⁷⁵ Ketizmen, **a.g.e.**, s. 141.

¹⁷⁶ Kurt, **a.g.e.**, s. 170; Dlger, **a.g.e.**, s. 328.

¹⁷⁷ Ketizmen, **a.g.e.**, s. 141.

¹⁷⁸ Akbulut, **a.g.e.**, s. 202.

kapsamında kabul edilir. Bunlar aracılığıyla faile çeşitli kullanıcı adları ve parolalar veya sisteme ilişkin veriler gönderilmekte ve sistem hakkında failin bilgilendirilmesi sağlanmaktadır¹⁷⁹. Bu neticenin oluşması açısından verilerin kopyasının mı orijinalinin mi gönderilmesi gerektiği madde metninden anlaşılamamaktadır. Her ikisinin de gönderilmesi durumunda suçun oluşacağını kabul etmek gerekmektedir. Suçun oluşması bakımından önemli olan verinin bulunduğu sistemden başka bir sisteme aktarılması, aktarılan sistemin kullanıcısının da o veriye ulaşabilmesidir¹⁸⁰.

Var olan verileri başka yere göndermek, sistem kullanıcısına ait verilerin yine aynı bilişim sisteminde farklı bir dosyaya ya da farklı bir bilişim sistemine gönderilmesi anlamını taşır¹⁸¹. Program, veri veya diğer unsurları uzak veya yakın başka bir bilgisayara nakletmek anlamındadır¹⁸².

Başkasına ait e-posta hesabına (facebook, twitter, instagram gibi sosyal paylaşım siteleri) şifresini ele geçirerek girmek, bu hesapta bulunan e-postaları (verileri) başka yere göndermek bu suçun işleniş şekline örnek olarak verilebilir¹⁸³. Dolayısıyla söz konusu netice serbest hareketle işlenebilir¹⁸⁴.

Verinin başka yere gönderilmesi, verinin aslının ortadan kaldırılması olarak anlamak da bu madde açısından uygun düşmez. Verinin aslının ortadan kaldırılması ikinci fıkrada düzenlenen neticeler arasından verinin yok edilmesi kapsamında kabul etmek gerekmektedir¹⁸⁵.

Burada hak sahibinin verilere ulaşıp ulaşamadığına bakılmaksızın verinin kopyalanması dâhil bulunduğu yerden başka bir yere gönderilmesi bu suçu oluşturur.

¹⁷⁹ Yılmaz, **a.g.m.**, s. 74.

¹⁸⁰ Orijinal verinin gönderilmesi durumunda suçun oluşacağı yönünde, Akbulut, **a.g.e.**, s. 202, 203.

¹⁸¹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6934; Erdoğan, **a.g.e.**, s. 227.

¹⁸² Dönmezer, **a.g.e.**, s. 621.

¹⁸³ Gül, **a.g.e.**, s. 85.

¹⁸⁴ Dülger, **a.g.e.**, s. 329.

¹⁸⁵ Ketizmen, **a.g.e.**, s. 141.

Örneğin fotoğraf ya da belge gibi verilerin sadece yazıcı gibi cihazlardan çıktısının alınması dahi bu kapsamdadır¹⁸⁶.

Bu fiil bakımından verinin ortadan kaldırılması veya bütünlüğünün bozulması söz konusu değildir. Bu fiil bakımından verinin erişilmez olup olmadığına bakılmaksızın, bulunduğu sistemin dışına transfer edilmesinin yeterli olduğu sonucuna varmak gerekecektir¹⁸⁷.

Kanun koyucu tarafından bu hareket çok muğlak şekilde düzenlenmiştir. Çünkü bir bilişim sisteminde gerçekleşecek her türlü işlem için mutlak suretle bir veri iletimi zorunludur. Bilişim sistemlerindeki her türlü faaliyetin veri iletimini gerektirmesi nedeniyle muğlaklık eleştirisi yerindedir¹⁸⁸.

d. Fail

Bilişim sistemleri ve internetin hızla gelişmesiyle bilişim suçları da yaygınlık kazanmıştır. Bilişim suçu failleri klasik suçlara nazaran özellik gösterdiğinden genel olarak açıklama yaptıktan sonra suç tipi açısından fail başlığını incelemeyi uygun gördük.

(1) Genel Olarak Bilişim Suçları Bağlamında Fail

“Hacker”, “elektronik korsan”, “siber terörist”, “cyber punks”, “elektronik korsan”, “sisteme saldıranlar”, “bilgi hırsızları”, “bilgi korsanları”, “müdahalede bulunanlar”, “bilgisayar kurtları”, “veri gezginleri” gibi çok çeşitli isimlerle anılan bu kişiler bilişim suçlarının faillerini oluştururlar¹⁸⁹.

Bilişim suçlarının işlenmesinde kullanılan yöntemlerin bazıları basit ve biraz bilgisayar bilgisine sahip olanlar tarafından gerçekleştirilebilirken diğer bazı yöntemler ise ancak bilgisayar konusunda uzman kişiler tarafından

¹⁸⁶ Erdoğan, **a.g.e.**, s. 228.

¹⁸⁷ Koca/Üzülmez, **a.g.e.**, s. 873.

¹⁸⁸ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 988; Erdoğan, **a.g.e.**, s. 228.

¹⁸⁹ Değirmenci, **a.g.t.**, s. 69; Yazıcıoğlu, **a.g.e.**, s. 46, 113; Mungo/Clough, **a.g.e.**, s. 102, 234.

gerçekleştirilebilmektedir. Örneğin kötücül yazılım yazarak sistem zarar verme fiilini ancak uzman kişiler gerçekleştirebilir¹⁹⁰.

Bilgisayarların ilk ortaya çıktığı zamanlarda bilişim suç failleri bu sistemlerle yakından ilgilenen sistemleri kullanabilen kişilerden oluşmaktaydı. Daha sonra teknolojinin gelişmesiyle ve bilgisayar kullanımının basitleşmesi sonucunda uzman olmayan birçok insan da bilişim suçlarının faili olabilmektedir¹⁹¹.

İlk bilişim suç failleri “phreaker”¹⁹² olarak adlandırılırdı¹⁹³.

Hacker kavramı ise günümüzde bilgisayar sistemlerine erişim yetkisi olmadığı halde sisteme erişmenin bir yolunu bulan ve sistemden bazı bilgiler alan, sistemin işleyişini değiştiren veya sonlandıran kişileri tanımlamaktadır¹⁹⁴.

Hacker denildiğinde ilk olarak akla bilgisayar kullanmaya hevesli, sektör ile yakından alakalı, konuyla ilgili merak ve arzuları son derece büyük ve bilgi sahibi genelde öğrenci ve amatör ruhlu gençler akla gelmektedir. Bunlar bazen çılgınlığa varan ölçülerde bilgisayar üzerinde uğraşarak uzman koruma mekanizmalarını bertaraf etmek suretiyle sistemlere girmeye ve müdahale etmeye çalışmaktadırlar¹⁹⁵. Hacking 1960’larda bugünkü anlamından uzak olarak en iyi, en hızlı ve en akıllı bilgisayar programlarını yazmak anlamına geliyordu. İlk hackerlar o sıralarda henüz geliştirilmekte olan yeni bilgisayar sistemleri için program yazmak üzere birlikte çalışan Massachusetts Institute of Technology (MIT) laboratuvarında çalışan

¹⁹⁰ Akbulut, **a.g.e.**, s. 73.

¹⁹¹ Değirmenci, **a.g.t.**, s. 69.

¹⁹² Phreaking; freak, phone ve free kelimeleriyle bir kelime oyunu olarak ünlendi. İlk başlarda amaçları sadece telefon santralleri üzerinden ücretsiz olarak görüşmek olan bu grup teknolojiyi özgürleştirdiklerini düşünmekteydiler. İlk başlarda phreakerların çoğu görme engelli gençlerdi. Yaptıkları iş için görmeye ihtiyaç yoktu, yalnızca duymak ve elektroniğe karşı bir yetenek yetiyordu. 1970’lerdeki ilk phreakerlar aileleriyle uzun mesafe konuşmalarını ekonomik olarak yapmak isteyen kişilerdir. Ancak kısa sürede kendilerini geliştirerek telefon santralinden fazlasını keşfettiler. Bu sistem bağlantıları ve çağrılarıyla Kuzey Amerika’dan Avrupa’ya kaydıran mekanizmaları ve uydu sistemleri ile büyük bir alandı. Bu grup, eylemlerini meşrulaştırmak için bilginin güç olduğunu ve bilgisayar ağlarında bulunan verilere herkesin ulaşabilmesi gerektiğini savunmuştur. Değirmenci, **a.g.t.**, s. 71.

¹⁹³ Değirmenci, **a.g.t.**, s. 71.

¹⁹⁴ Gökşin Akdeniz, “Hacker Etiği”, **Hack Kültürü ve Haktivizm: Yeni Bir Siyaset Biçimi**, Mustafa Akgül’e Armağan, Der. Ali Rıza Keleş, Yetkin Sal, İstanbul, Alternatif Bilişim, 2013, s. 8.

¹⁹⁵ Yazıcıoğlu, **a.g.e.**, s. 114.

teknolojiye meraklı gençlerden oluşmaktaydı¹⁹⁶. MIT öğrencilerinin kendi aralarında yaptığı şakalara “hack” ismi veriliyordu. Hack kısa sürede ilk anlamını kaybetmiş ve günümüzdeki anlamıyla anılmaya başlanmıştır¹⁹⁷.

Hackerlar genellikle bu fiillerini gerçekleştirirken şu aşamaları kullanırlar; keşif yapma, tarama yapma, sisteme sızma, sistemde kalıcılığı sağlama ve son olarak sistemdeki izleri yok etmek¹⁹⁸.

Bilgisayara yapılan bu saldırılar sadece içeriden değil dışarıdan da kaynaklanabilmektedir. Basit bir modem sayesinde yasal olmayan yollardan özel ya da kamusal bilgisayar ağına girmek mümkündür. Bunun için sadece bilgi merkezinin internet servis sağlayıcısının numarasının bilinmesi ve programlara giriş şifresinin bulunması yeterlidir¹⁹⁹.

Bilişim suçu failleri yakalanma olasılıklarının az olduğuna inandıklarından haklarında nadir olarak dava açılabilindiğini, dava açılrsa bile çoğunlukla mahkûmiyete yeterli delil elde edilemeyeceğini veya ceza verilse bile fazla ceza almayacağını düşünmektedir. Bilişim failleri şirket yetkililerinin de böyle bir durumda özellikle şirketin güvenilirliğini zedelememek için bilgi vermekte isteksiz davranacaklarının farkındadırlar. Bu tip suçlular bu durumlardan güç almaktadırlar²⁰⁰.

Bilişim suçu faillerinin birçok şekilde adlandırılabilindiğinden bahsetmiştik. Bunlardan bazılarını aşağıda açıklamaya çalıştık.

¹⁹⁶ Mungo/Clough, **a.g.e.**, s. 47; Çakır/Kılıç, **a.g.e.**, s. 33.

¹⁹⁷ Akdeniz, **a.g.m.**, s. 9. Hackerlar birbirleri ile iletişimlerini amatör olarak çıkarılan dergiler ve BBS (Bulletin Board System – Bülten Panosu Sistemi) aracılığıyla devam ettirmektedirler. BBS yazılım yüklenmiş ve modeme bağlanmış olan bilgisayarları ifade etmek için kullanılır. Dergilerin ise büyük kısmı bilgisayarlar aracılığıyla dağıtımı yapıp hackinge dair çeşitli makaleleri içermektedirler. Elektronik gazete niteliğindeki bu yazılımlar, politik propagandadan bilişim suçunun ne şekilde işlenebileceğine kadar çeşitli konulardaki haberleri hiçbir kontrol mekanizmasına takılmadan hackerlar arasında yayılmasını sağlamaktadırlar. Değirmenci, **a.g.t.**, s. 74; Mungo/Clough, **a.g.e.**, s. 75; Yazıcıoğlu, **a.g.e.**, s. 118.

¹⁹⁸ Karagülmez, **a.g.e.**, s. 89, 90.

¹⁹⁹ Yazıcıoğlu, **a.g.e.**, s. 46.

²⁰⁰ Karagülmez, **a.g.e.**, s. 63.

Rodents tabiriyle sisteme müdahale edenler arasında en alt düzeyde olanlar ifade edilmiştir. Konuya merak duyan, yeni ilgilenen kişileri tanımlamak için kullanılır²⁰¹.

Swappers ile kast edilen, oyun amaçlı olarak sisteme girmeye çalışanlar kastedilmektedir. Bu grup, en çok hoşgörü ile karşılanan grubu temsil etmektedir²⁰².

Elektronik Vandallar ise sisteme girmek konusunda oldukça deneyimli olan kişileri ifade eder. Bu kişiler girdikleri sisteme ironik veya tahkir edici mesajlar bırakır ve yaptıkları tahribat uyarınca zarar vericidirler²⁰³.

Burada son olarak Ethical Hacker kavramına da değinmek gerekir. Bilişim suçlarındaki artışa paralel olarak bilişim sistemini kullanan kurum ve kuruluşlar da yeni güvenlik önlemleri kullanma arayışına girmiştir. Bu arayışlar da bilişim sistem güvenliğinin test edilmesi işleminin yapılarak güvenlik durumunun belirlenmesini gündeme getirmiştir. Buna bağlı olarak da bu kavram ortaya çıkmıştır²⁰⁴.

Burada sistem kontrol edilirken genelde daha önce bilişim korsanlığı yapmış kişilerden faydalanılır. Önemli olanın bilişim sisteminin gerçek bir hacker saldırısında güvenli olarak kalması olarak düşünüldüğünde, suça hiç karışmamış bilişim uzmanının sistemi kontrol etmesinden daha fazla bir faydanın sağlanacağı söylenebilir²⁰⁵.

Ethical Hackerlar görevlerine başlayıp belirli araştırma işlemlerini yaptıktan sonra müşterisinin bilişim sistemine söz konusu sistemin zarar görmesi pahasına da olsa tıpkı suç işleyen hackerlar gibi saldırılar yapmaktadır. Dışarıdan bakıldığında bunun suç olarak nitelendirileceği düşünülse de bu fiilleri gerçekleştirirken suç işleme

²⁰¹ Yazıcıoğlu, **a.g.e.**, s. 121.

²⁰² **A.e.**

²⁰³ Yazıcıoğlu, **a.g.e.**, s. 122.

²⁰⁴ Karagülmez, **a.g.e.**, s. 91.

²⁰⁵ **A.e.**, s. 92.

kastı olmadığından ve sistem sahibi ile arasındaki anlaşma gibi nedenlerle bu fiiller suç oluşturmaz²⁰⁶.

(2) Suçların Faili

Sistemin işleyişini bozan, engelleyen, verileri yok eden, değiştiren, veri yerleştiren, başka yere veri gönderen herkes bu suçun faili olabilir²⁰⁷. İncelediğimiz suçlar, özgü suç değildir.

Bilişim suçları ilk zamanlarda beyaz yaka suçlarının (white- collar crime) bir türü olarak ele alınmaktaydı. Çünkü henüz bilişim sistemlerinin yaygınlaşmadığı bir dünyada, bu suçlar ancak bilgisayarın olduğu ve bilgisayarla çalışan kimselerin işleyebileceği suçlardandı. Ancak günümüzün küreselleşen toplumunda bu suç faillerini sadece bir kesimle sınırlamak pek mümkün değildir²⁰⁸.

Kanun metninde bu açıdan herhangi bir özellik gösterilmemiş olsa da suçun uzmanlık gerektirdiği göz önüne alındığında incelediğimiz suçların genelde “*hacker*” ya da “*cracker(sistem kırıcılar)*” denilen kişilerce işlendiğini söyleyebiliriz.

Bilişim sisteminin güvenliğinin kırılıp sisteme girilmesi fiilini diğer suç işleme şekillerinden ayıran en önemli özellik genellikle sisteme giriş sırasında yardımcı yazılımlar kullanılmasından ziyade fiilin bizzat bilişim korsanının becerisine dayanmasıdır. Kimi hallerde güvenlik kodlarının çözülmesi için olasılık ve kombinasyon hesaplarını hızla yapan yardımcı yazılımlar kullanılsa da sistem içinde gezinme ve verileri ele geçirme fiilleri bilişim korsanının kendisi tarafından yapılmaktadır²⁰⁹.

Söz konusu suç gerçek kişilerin yanı sıra, bir tüzel kişi yararına da işlenebilir. Tüzel kişilerin TCK m. 20 gereği suç faili olamayacağı ve cezai sorumluluklarının bulunmadığı, dolayısıyla bilişim suçlarının faillerinin tüzel kişi olamayacağı ve şirket

²⁰⁶ A.e., s. 93.

²⁰⁷ Gül, a.g.e., s. 83.

²⁰⁸ Artuk/Gökçen/Yenidünya, *Ceza Hukuku Özel Hükümler*, s.866.

²⁰⁹ Dülger, a.g.e., s. 125.

yararına suç işlense dahi bundan dolayı tüzel kişiye ceza verilemeyeceği açıktır²¹⁰. Bu durumda tüzel kişiler suç faili olamayacağından cezalandırılmasa da TCK m.246 atfıyla, TCK m. 60 uygulama alanı bularak tüzel kişi hakkında güvenlik tedbirine hükmolunacaktır²¹¹.

e. Mağdur

(1) Genel Olarak Bilişim Suçları Bağlamında Mağdur

Bilişim suçlarında suç fillerinin adli makamlara bildirilmemesi nedeniyle suçlar iş dünyası içinde gizli kalmakta ve toplumun orta ve üst seviyesinde yer alan bazı failler fiillerini gizleyebilmektedirler. Bundan dolayı bu suçlar hakkında çoğu zaman net rakamlara ulaşmak mümkün değildir²¹².

Özellikle şirket seviyesinde gerçekleşen bilişim suçları kimseye duyurulmadan gizlenmeye çalışılmaktadır. Şirket yöneticileri, polisin işlenen suç dolayısıyla şirketin iç işlerine karışılmasını ve böylece detaylı bilgi edinmelerini istememektedirler. Böyle bir araştırmanın şirketin prestij ve müşteri kaybına neden olacağı açıktır²¹³. Bu anlamda bilişim suçu faillerinin en önemli yardımcılarının suç mağdurlarının kendileri olduğunu söylemek mümkündür²¹⁴.

Mağdurların suçları bildirmemesi dolayısıyla toplum da zarar görmektedir. Suç failleri yargı denetiminden kaçmakta ve bunlara karşı gerekli denetim mekanizmaları geliştirme imkânı sağlanamamaktadır²¹⁵.

Bilişim mağdurlarının suçları bildirmemekteki farklı kaygılarının temelinde bilişim alanına devletin hâkim olmadığı düşüncesinin etkili olduğu doktrinde ifade

²¹⁰ Dülger, **a.g.e.**, s. 252.

²¹¹ Mahmutoglu, "TCK'da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", s. 866. Aynı görüşte Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6929.

²¹² Yazıcıoğlu, **a.g.e.**, s. 110; Karagülmez, **a.g.e.**, s. 73.

²¹³ Yazıcıoğlu, **a.g.e.**, s. 109.

²¹⁴ Kurt, **a.g.e.**, s. 58.

²¹⁵ Yazıcıoğlu, **a.g.e.**, s. 110, 111.

edilmektedir. Mağdurlar tarafından tam olarak denetlenemediği düşünülen bu alandaki faillerinin tespit edilip gerekli cezaya çarptırılacaklarına dair güven duygusu topluma verilebilirse mağdurların suçları resmi makamlara bildirme konusundaki çekinceleri de azaltılmış olacaktır²¹⁶.

Bilişim suçları ile mücadelede mağdurların bilgisayar kullanırken dikkatli davranmaları bu suçların engellenmesinde büyük bir etkiye sahip olabilir. Bilgisayar kullanıcılarında teknolojiye güven duygusu öne çıksa da bilgisayarların her an saldırıya uğrayıp sisteme ve kullanıcıya zarar verme özelliği karşısında her kullanıcının dikkatli olması gerekmektedir²¹⁷.

Mağdurların bilişim suçlarına karşı bilgilendirilmelerinde, bilgisayarların üzerinde uyarı yazıları bulundurmak, bilgisayar ve program satıcılarına sorumluluk yüklemek, basın ve medya kuruluşlarına sorumluluk yüklemek, kanunlarda mağdurları güvenlik önlemleri almaya zorlayacak düzenlemeler yapmak gibi değişik yöntemler kullanılabileceği doktrinde belirtilmektedir²¹⁸.

Bilişim sistemlerinin dışarıdan gelecek saldırılar her gün gelişebilecek niteliktedir. Sistemi koruyan programların da buna bağlı olarak gelişme göstermesi gerekmektedir beraber sistem ya da veri kullanıcılarını gelecekte mağdur olmalarının önüne geçmek amacıyla bu kişilere temel bilgisayar eğitim verilmesi yerinde olacaktır.

Bilişim suçlarını düzenleyen kanunlarda mağdurun duyarlılığına göre işlenen suçun ve cezasının niteliğinin değiştiği düzenlemeler yapılabilir. Örneğin TCK m. 141’de kilitlenmemiş otomobilden hırsızlığın cezası bir yıl haptiden başlarken, TCK m 142’de kilitlenmek suretiyle muhafaza altına alınmış eşyanın çalınması daha ağır nitelikte görülerek cezası artırılmıştır. Aynı uygulama bilgisayarda güvenlik önlemi alan bir mağdurun durumu için de düzenlenebilir²¹⁹.

²¹⁶ Karagülmez, **a.g.e.**, s. 74.

²¹⁷ **A.e.**, s. 76.

²¹⁸ **A.e.**, s. 75, 76.

²¹⁹ Karagülmez, **a.g.e.**, s. 77.

(2) Suçların Mağduru

Suçların mağduru TCK m. 244/1’de düzenlenen sisteme müdahale suçu açısından sistem kullanıcısı veya işleticisi olabilir²²⁰.

Bilişim sistemi ile verilerin sahibinin birbirinden farklı olması durumunda mağdurun belirlenmesi sorun teşkil edebilir. Fiil bilişim sistemine yönelik olarak gerçekleştirilmişse sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelikse bu verilerin, hem bilişim sistemine hem de verilere karşılık gerçekleştirilmişse her ikisinin de ayrı ayrı mülkiyet, kullanım ve tasarruf haklarının kime ait olduğunu ve zararı kimin meydana getirdiğini açıkça ortaya koymak gerekir²²¹.

Bilişim sistemi üzerinde hak sahibi olan kişi o sisteme karşı işlenen suçların da mağduru konumundadır. Hak sahibi olma, mülkiyet hakkı sahibi olmakla ya da başka bir kısım sözleşmelerle (kira, ariyet, finansal kiralama gibi) hak sahipliğini elinde bulundurmak suretiyle kazanılabilir. Örneğin finansal kiralama yoluyla almış olduğu bilgisayarları ticari bir üretimde kullanan kiracının bilgisayarlar üzerinde mülkiyet hakkı bulunmamakta ise de zilyetlik hakkı gereğince suçun mağduru olduğu kabul edilecektir. Bu örnekte finansal kiralama şirketinin sistemler üzerinde mülkiyet hakkı bulursa da suçtan zarar gören olarak kabul edilemeyecektir. Verilerin gizliliği ve özel hayatın gizliliği ihlal edilen bilişim sistemi üzerinde zilyetliğini sürdüren finansal kiralayandır²²². Bu görüşe katılmayan görüş ise korunan değer mülkiyet hakkı olmadığına katılmakla beraber, sistemin güvenilirliği korunan bir değer olduğundan kiralaan şirket olay nedeniyle yeni kiracı bulmakta zorlanacağından şirketin de suçtan zarar gören değil suçun mağduru olduğunu savunmaktadır. Kiralaan kiracının sistemine zarar verirse sistemin maliki olmasına rağmen fail de olabilecektir²²³.

²²⁰ Akbulut, **a.g.e.**, s. 185.

²²¹ Soyaslan, **a.g.e.**, s. 615; Yazıcıoğlu, **a.g.e.**, s. 241.

²²² Kurt, **a.g.e.**, s. 163.

²²³ Yavuz Erdoğan, “Bilişim Sistemine Girme ve Kalma Suçu”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. XII, Özel Sayı, 2010 (Basım yılı:2012), s. 1395.

Bu suçları oluşturan hareketlerin gerçekleştirilmesi sonucunda bilişim sistemine ve/veya verilerle oluşturulan yazılım, ekonomik/finansal bilgi, bilimsel çalışma, istatistiki veri gibi değerlere herhangi bir engel, arıza ya da gecikme olmadan ulaşılmasında ve kullanılmasında çıkarı bulunan ve bilişim sistemi ve/veya veriler üzerinde tasarruf yetkisi bulunan kişi mağdur olur²²⁴.

Suçun mağduru TCK m. 224/2’de düzenlenen verilere müdahale suçu açısından veriler üzerinde tasarruf yetkisine sahip olan kişileridir. Tasarruf yetkisine sahip olmayan verilerin kullanıcısı ise suçun mağduru olmamakla birlikte suçtan zarar gören olabilir²²⁵.

Bu suç tipi mağduru bakımından herhangi bir özellik göstermemektedir. İşleyişi engellenen, bozulan, yok edilen veya değiştirilen sistem üzerinde hak sahibi olan kişiler suçun mağdurudur. Failin fiilinin birden fazla kimsenin hakkını ihlal ettiği durumlarda, bu kişilerin hepsi mağdur sıfatını kazanır²²⁶.

Fiiller nedeniyle bilişim sistemindeki verilere ulaşamayan, geç ulaşan ya da sistemi kullanamayan ve sistem üzerinde tasarruf yetkisi bulunan kişinin çıkarları zedelendiğinden suçun mağduru olacaktır²²⁷.

Verilerin bulunduğu ya da müdahalede bulunulan bilişim sistemi üzerinde hak sahibi olan kişinin farklı kişiler olması ihtimalinde her ikisinin de suçun mağduru olduğunu kabul etmek isabetli olacaktır²²⁸. Örneğin başkasının bilgisayarına kendi hazırladığı verileri içeren dosyaları yükleyen kimsenin durumu böyledir²²⁹.

Tüzel kişi suçun mağduru değil suçtan zarar gören olabilir. Bu durumda suçun mağduru olarak tüzel kişiyi oluşturan gerçek kişilerin suçun mağduru olduğu kabul

²²⁴ Dülger, **a.g.e.**, s. 317.

²²⁵ Akbulut, **a.g.e.**, s. 185.

²²⁶ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s.866. Aynı görüşte Gül, **a.g.e.**, s. 83.

²²⁷ Yılmaz, **a.g.m.**, s.77.

²²⁸ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6935.

²²⁹ Yenidünya/Değirmenci, **a.g.e.**, s. 95.

edilmelidir. Dolayısıyla kamu kurum ve kuruluşlarının bilişim sistemlerine karşı fiillerin işlenmesi halinde o toplumu oluşturan herkes suçun mağdurudur²³⁰.

Bilişim sisteminin işleyişinin engellenmesi veya bozulması ile içerisinde bulunan verilerin bozulması ya da yok edilmesi durumunda eğer birden fazla kimsenin hukuken korunan hakları ihlal ediliyorsa bunların hepsi mağdur sıfatını kazanır. Örneğin; bir bankanın bilişim sisteminin işleyişini engelleyerek banka müşterilerinin verilerinin değiştirilmesi durumunda verileri değişen her bir müşteri suçun mağduru konumundadır. Tüzel kişiliğe sahip banka da bu suçtan zarar gören olarak karşımıza çıkmaktadır²³¹.

Aynı şekilde birden fazla kimsenin kişisel dosyasının tek bir bilgisayarda olduğunu düşündüğümüzde, failin veri sahiplerinin verilerini ayrı ayrı bozması, yok etmesi, değiştirmesi ya da başka yere göndermesi durumunda her veri sahibinin mağdur olduğunu söyleyebiliriz²³².

Veriler üzerinde tasarruf yetkisinin kime ait olduğu konusunda doktrinde görüş birliği bulunmamaktadır. Veriler gibi soyut unsurlar medeni hukuk anlamında mal olmadıklarından mülkiyet ile ilgili kurallar ceza hukukuna birebir uygulanamamakta ve veriler üzerinde tasarruf yetkisine sahip kişi mülkiyet ilişkisiyle belirlenememektedir. Somut olayda mülkiyet ilişkisi ile belirlenemeyen verilerin sahibini belirlemek için değişik kriterler ileri sürülmüştür;

- 1- Verilerin kazanılması; bu görüşe göre veriler üzerinde tasarruf yetkisine sahip kişi verileri hukuka uygun olarak kazanan kişidir.
- 2- Verilerin içeriği ile ilgili olmak; verilerin hakkında bir şeyler söylediği kişi tasarruf yetkisine sahiptir.
- 3- Veri taşıyıcısında mülkiyet; veri taşıyıcısının mülkiyetine sahip olan kişi verilerin tasarruf yetkisine de sahiptir. Örnek olarak bir bilgisayara sahip olan kimse içindeki verilerinde tasarruf yetkisine sahiptir.

²³⁰ Akbulut, **a.g.e.**, s. 185. Aynı görüşte Koca/Üzülmez, **a.g.e.**, s. 868.

²³¹ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s.867.

²³² **A.e.**, s.888.

- 4- Verilerin fikri hak sahibi; verilerin üreticisi veriler üzerinde tasarruf yetkisine sahiptir görüşünü benimser.
- 5- Verilerin kaydedilmesi; verilerin kaydedilmesini veya nakledilmesini doğrudan gerçekleştiren kişinin verilerin sahibi olduğu görüşünü savunur²³³.

Belirtilen beş kriterden hiçbirisi tek başına veriler üzerinde tasarruf yetkisine sahip kişinin belirlenmesinde yeterli ölçüt değildir. Bir kişi hem bilişim sisteminin maliki olabilir hem de veriler üzerinde tasarruf yetkisine sahip kişi olabilir. Bununla birlikte bilişim sisteminin mülkiyetine sahip olmamakla beraber veriler üzerinde tasarruf yetkisine sahip olabilir. Örneğin birinden kiraladığı bilgisayara verilerini kaydeden kişi bilgisayarın maliki olmamakla beraber veriler üzerinde tasarruf yetkisine sahip olan kişidir. Aynı şekilde veri taşıyıcısının maliki başkası tarafından hukuka uygun olarak kaydedilen verilere zarar verirse TCK m. 244/2'deki suçu işlemiş olur. Örneğin kendi veri taşıyıcısına bir başkası tarafından yetkisiz olarak kaydedilen verilerin silinmesi durumunda verileri kaydeden kişi tasarruf yetkisine sahip olmadığından, başkasının kendi sistemine yüklediği verileri silen kişinin fiili suç teşkil etmez²³⁴.

E-mail gönderiminde gönderenin tasarruf yetkisi, mailin alıcının servis sağlayıcısının serverına ulaştığı ana kadar geçen sürenin sonunda sona erer. Bu andan sonra artık tasarruf yetkisi alıcıya aittir. Alıcının veriler üzerinde değişiklik yapması tasarruf yetkisi kendisinde olduğundan suç oluşturmaz. Bir başkasının değişiklik yapması durumunda ise alıcı suçun mağduru olacaktır²³⁵

2. Manevi Unsur

İncelenen suçlar kasten işlenebilir. Fail fiilin bilişim sisteminin işleyişini engellediğini veya sistemi bozduğunu bilişim sistemindeki verileri bozduğunu, yok ettiğini, değiştirdiğini, erişilmez kıldığını veya sisteme veri yerleştirdiğini ya da var

²³³ Akbulut, **a.g.e.**, s. 186.

²³⁴ **A.e.**, s. 187.

²³⁵ Akbulut, **a.g.e.**, s. 187.

olan verileri başka bir yere gönderdiğini bilecek ve bunu isteyecektir. Suç tipinde doğrudan kasta işaret eden herhangi bir ibare yer almadığından fiil, olası kastla da gerçekleştirilebilir. TCK m. 244/1'in 765 sayılı TCK'da karşılığını oluşturan 525b/1 maddesinde "başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak" amacı aranmaktayken yeni düzenlemede bu düzenlemeden vazgeçilmiştir²³⁶. 1997 ve 2003 Tasarılarında bu suçun karşılığını oluşturan 348. ve 347. maddelerin birinci ve ikinci fıkralarında bu şekilde amaca yer verilmemiştir. Ancak daha önce de bahsettiğimiz gibi 348. ve 347. maddelerin verilere müdahaleyi düzenleyen ikinci fıkralarında hukuka aykırı olma şartı aranmıştı²³⁷.

Bilişim sistemine su dökmek ya da vurarak sistemi bozmaya yönelik hareketleri yapan failin doğrudan kastı belirlenemese bile fiziki saldırı sonucunda sistemin çalışmasının aksayacağını veya bozulacağını öngörmesi kaçınılmazdır. Bu nedenle faili sorumlu tutmak gerekecektir²³⁸.

Kanunda herhangi bir saike yer verilmediği için suçun manevi unsurlarında saik aranmasına gerek yoktur. Failin suçu işleyiş amacının sistemin güvenliğini denemek, eğlenmek, merak veya oyun olması arasında bir fark yoktur²³⁹.

Bu suçun taksirli şekline kanunda yer verilmemiştir. Ancak verilere ya da sisteme zarar vermek taksirli şekilde işlenebilir. Örneğin, fail ücret ödeyerek girdiği sistemdeki verilere dikkatsizlikle zarar verebilir. Taksirli şekli düzenlenmediğinden bu fiilin cezalandırılması söz konusu değildir²⁴⁰. Doktrinde bu suçların taksirli halinin düzenlenmesine yönelik görüş de bulunmaktadır. Bu görüşe göre, bilişim sistemlerinin hayatımızdaki artan önemi ve çağımızın bilişim çağı olduğu dikkate alınması ve bu fiillerin taksirle gerçekleşmesi halinin de cezalandırılması gerekmektedir²⁴¹. Teknik serviste görevli kişinin sistemdeki arızayı gidermesi için çağırılması ve sistemdeki

²³⁶ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6930.

²³⁷ Akbulut, **a.g.e.**, s. 203.

²³⁸ Malkoç, **a.g.e.**, s. 1678.

²³⁹ Mahmutoğlu, "TCK'da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", s. 862.

²⁴⁰ Akbulut, **a.g.e.**, s. 204.

²⁴¹ Erdoğan, **a.g.e.**, s. 230.

verilerin kaybolması durumunda sorumlu tutulması gerektiğini savunmaktadırlar²⁴². Bu suçlarla bilişim sistemine ve verilere yönelik olarak kasten müdahale edilmesi düzenlendiğinden ve suçlarla korunan hukuki değer de göz önüne alındığında suçların taksirli halinin kanunda düzenlenmesi gerektiğini savunan bu görüşe katılmıyoruz. Bu suçların taksirle işlenebileceğinin kabulü suçların kapsamının öngörülemez biçimde artmasına neden olacaktır. Bu kapsamda tazminat gibi özel hukuk yaptırımları yeterli olup ayrıca hapis cezasının öngörülmesi ağır olacaktır.

3. Hukuka Aykırılık Unsuru

Bilindiği üzere bir fiilin tipikliği onun aynı zamanda hukuka aykırılığı açısından karine oluşturmaktadır. İstisna olarak somut olayda tipik fiilin hukuka aykırılığını kaldıran bir neden yoksa tipik fiil aynı zamanda hukuka aykırıdır. Burada artık bir hukuka uygunluk nedeniyle örtülen bir haksızlıktan değil, cezalandırılabilir bir haksızlıktan bahsedilecektir. Buna karşılık, somut olayda bir hukuka uygunluk nedeni bulunduğu bu hukuka aykırılık karinesi çürümüş olacaktır. Çünkü hukuka uygunluk nedenleri, fiilin haksızlığını örtmekte, onun hukuka aykırı olarak doğmasını engellemektedir²⁴³.

Hukuka uygunluk sebeplerinden ilgilinin rızasının incelediğimiz suç tipleri bakımından gerçekleşmesi mümkündür. Yetkili kişi verilerin yok edilmesine, değiştirilmesine veya maddede sayılı diğer fiillere rıza göstermişse suç oluşmayacaktır. Rızanın bilişim sistemi üzerinde hak sahibi olan kimse tarafından verilmesi, rızanın sınırlarının aşılmamış olması ve bu kişinin yaptığı fiillerin rızanın kapsamının dışına çıkmaması gerekmektedir²⁴⁴. Bilişim sistemi için teknik destek alınması sırasında bu durum ortaya çıkabilir. Bu kişilere bilişim sisteminin teslim edilmesi ve içindeki verilere müdahale etme yetkisinin verilmesi kişilere sistemin içindeki verileri yok etme ya da zarar verme yetkisini vermemektedir. Bu nedenle söz

²⁴² Taşkın, **a.g.e.**, s. 53.

²⁴³ Kayıhan İçel/Füsün Sokulu-Akinci/ İzzet Özgenç/ Adem Sözüer/Fatih Selami Mahmutoğlu/Yener Ünver, **Suç Teorisi**, 3. bs. , İstanbul, Beta Yayıncılık, 2004, s. 92, 93.

²⁴⁴ Erdoğan **a.g.e.**, s. 201.

konusu kişilerin sistemde bulunan verilere kasten zarar vermesi durumunda bilişim sisteminde yer alan verilerin yok edilmesi veya değiştirilmesi suçu oluşur. Burada artık kullanım hakkının devredildiği kişiye baştan verilen rızanın sınırları aşılmış ve bu kişinin yaptığı fiil hukuka aykırı hale gelmiştir²⁴⁵.

Bu suçlar ile hem bir bütün olarak bilişim sistemine hem de verilere zarar verilmesi suç olarak düzenlenmektedir. Bu nedenle kişinin, başkasına zarar vermeksizin herhangi bir bilişim sisteminde bulunan kendisine ait verilere zarar vermesi suç oluşturmaz. Yine aynı şekilde başkalarının haklarını ihlal etmediği sürece failin kendi sisteminin işleyişini engellemesi veya bozması suç kapsamında değildir²⁴⁶. Ancak failin kendisine ait olmayan bir bilişim sisteminde bulunan kendisine ait olan verileri yok etmek ya da erişilmez kılmak için sistemin işleyişini bozması ya da engel olması halinde ise her ne kadar 244. maddenin ikinci fıkrasındaki suç gerçekleşmeyecek olsa da birinci fıkrasındaki suç gerçekleşmiş olacaktır²⁴⁷.

Yetkisiz olarak başkasının veri taşıyıcısına kaydedilen verilere, veri taşıyıcısının hukuka uygun sahibinin zarar vermesi TCK m. 244/2 kapsamına girmez. Örneğin; dizüstü bilgisayar ya da akıllı telefon gibi bir veri taşıyıcısının bir hırsız tarafından çalınması durumunda veri taşıyıcısının sahibinin verileri silmesi bu niteliktedir. Birinin bilgisayarına yetkisiz olarak kurulan virüs, cookie gibi dosyaların silinmesi TCK m. 244/2 kapsamında belirlenen suçu oluşturmaz²⁴⁸.

Fail hareketlerini bilişim sistemine yönelik olarak gerçekleştirmişse sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelik gerçekleştirmişse bu verilerin, hem bilişim sistemine hem de verilere karşı gerçekleştirilmişse her ikisinin ayrı ayrı mülkiyet, kullanım ve tasarruf haklarının kime ait olduğu açıkça ortaya

²⁴⁵ Dülger, **a.g.e.**, s. 335; Erdoğan, **a.g.e.**, s. 201; Akbulut, **a.g.e.**, s. 204; Yılmaz, **a.g.m.**, s. 78.

²⁴⁶ Akbulut, **a.g.e.**, s. 183.

²⁴⁷ Dülger, **a.g.e.**, s. 316.

²⁴⁸ Akbulut, **a.g.e.**, s. 184, 185.

konulmalıdır²⁴⁹. Zira mülkiyet sahibinin kiracıya ya da kiracının mülkiyet sahibinin yetki alanına müdahalesi gibi durumlar söz konusu olacaktır²⁵⁰.

Verilere veya sistemin işleyişine zarar vermek suçunun işlenip işlenmediğinin tespitinde bilgisayarın kullanım hakkıyla ilgili bir değerlendirme yapılmalıdır. Kişi veri taşıyıcısının sahibi olmakla beraber verilerin kullanımını üçüncü kişiye bırakmış olabilir. Örnek olarak programla birlikte bilgisayarın kullanılması için kiralanması durumunda kullanan kişi bilgisayar malikinin sistem programına kasten zarar verirse, hareket TCK m. 244/2 kapsamında cezalandırılabilir bir hareket niteliği taşır²⁵¹. Bilgisayarı kullanmak üzere alan kişi, bilgisayarın malikine ya da kullanıcısına ait içindeki işletim veya uygulama yazılımına zarar vermesi durumunda da TCK m.244'te düzenlenen suçlar gerçekleşmiş olacaktır²⁵².

Veri taşıyıcısının mülkiyeti ile kullanım hakkının birbirinden ayrıldığı durumlarda tasarruf yetkisi, ilgililerin arasındaki hukuki ilişkiye yani sözleşmeye göre belirlenmelidir. Sözleşmeye göre kullanım yetkilisi, devredilen veriler üzerinde tasarruf yetkisine sahip olmuşsa verilere müdahale etmesi suç oluşturmaz. Tasarruf yetkisi verilmemişse yalnızca verileri sisteme girme yetkisi verilmişse kullanan kişinin verilere kasten zarar vermesi TCK m. 244/2'de düzenlenen verilere zarar verme suçu kapsamına girecektir²⁵³.

5651 sayılı Kanun'un 8. maddesinde erişimin engellenmesine dair usul düzenlenmiştir. Bu karar ancak intihara yönlendirme (TCK m. 84), çocukların cinsel istismarı (TCK m. 103/1), uyuşturucu veya uyarıcı madde kullanımını kolaylaştırma (TCK m. 190), sağlık için tehlikeli madde temini (TCK m. 194), müstehcenlik (TCK m. 226), fuhuş (TCK m. 227), kumar oynanması için yer ve imkân sağlama (TCK m. 228) suçlarıyla 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun'da yer alan suçlar için uygulanabilir. Bunların yanında bu suçların işlendiğine dair yeterli

²⁴⁹ A.e., s. 316.

²⁵⁰ Erdoğan, a.g.e., s. 194.

²⁵¹ A.e.

²⁵² Dülger, a.g.e., s. 335.

²⁵³ Akbulut, a.g.e., s. 184.

şüphenin oluşması da aranacaktır²⁵⁴. 5651 sayılı Kanun'un 8. maddesi temel alınarak karar verilen erişimin engellenmesi hareketlerinin kanun hükmünü icra kapsamına girdiğini ve fiillerin hukuka uygun hale getireceğini söyleyebiliriz.

Görevin ifası da fiili hukuka uygun hale getirecektir. 5271 sayılı Ceza Muhakemesi Kanunu'nda bilişim sistemleriyle ilgili olarak bazı koruma tedbirleri düzenlenmiştir. Buna göre CMK m. 134'te düzenlenen "Bilgisayarlar, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El koyma", m.135'te düzenlenen "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" ve m. 140'ta düzenlenen "Teknik Araçla İzleme" koruma tedbirlerinin koşullarına uygun olarak uygulanması halinde kanun hükmünü icra hukuka uygunluk nedeninden söz edilecektir²⁵⁵. Burada emri veren açısından kanun hükmünü icra, emri uygulayan bakımından ise emrin ifası söz konusu olacaktır²⁵⁶. Hukuka uygunluk sebeplerinden emrin ifasına örnek olarak belirli döneme ait veya bazı şartların gerçekleşmesi şartıyla, vergi borçlarının silinmesi yolunda karar alınması ve buna dayanılarak yapılan düzenleme çerçevesinde vergi borçlarının silinmesi durumundan verileri silen kişi verileri yok etmekten sorumlu tutulamaması verilebilir²⁵⁷.

Doktrinde bu suçlar bakımından meşru savunmanın mümkün olup olmadığı konusundan bir görüş birliği yoktur. Bir görüşe göre, hukuka uygun görülen bir meşru savunma niteliğindeki karşı saldırı durumunda, bir bilişim korsanının bilgisayarına zarar vermek, sistemin işleyişini engellemek de hukuka uygun olacağından herhangi bir suçun işlendiğinden bahsedilemeyecektir²⁵⁸. Diğer görüşe göre ise saldırının niteliğine bakılarak karar verilmesi gerekir. Eğer saldırı ağ üzerinden yapılıyorsa,

²⁵⁴ Taşkın, **a.g.e.**, s. 155.

²⁵⁵ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s.877; Aynı görüşte, Mahmutoglu, "TCK'da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", s. 862; Koca/Üzülmüş, **a.g.e.**, s. 873; Soyaslan, **a.g.e.**, s. 611; Dülger, **a.g.e.**, s. 335.

²⁵⁶ Selman Dursun, "Türk Ceza Hukuku'nda Emrin İfasının Hukuki Niteliğinin Alman ve İtalyan Ceza Hukuku'yla Karşılaştırmalı Olarak İncelenmesi", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XVIII, Y. 2014, S.2, s.235.

²⁵⁷ Akbulut, **a.g.e.**, s. 198.

²⁵⁸ Pallı, **a.g.t.**, s. 171.

yapılan saldırı devam ederken saldırının mağdur tarafından anlaşılması halinde bilişim sistemi kapatıldığında ya da en azından ağ bağlantısı kesildiğinde otomatik olarak saldırı da engellenmiş olunacağından meşru savunma mümkün olmayacaktır. Zira savunma yaparken karşı saldırı için zorunluluk bulunmamaktadır. Tekrar eden bir tehdit yoksa failin sistemine zarar verilemez. Ancak sisteme fiilen temasla saldırı yapılıyorsa artık diğer şartların da bulunması halinde meşru savunma mümkündür²⁵⁹.

Meşru savunmanın gerçekleşebilmesi için savunma hareketinin zorunlu olması yani tecavüzü başka şekilde defetme imkânının bulunmaması gerekmektedir. Kişinin yasal yollardan ya da 5651 sayılı Kanun vasıtasıyla yayına müdahale imkânının bulunması nedeniyle meşru savunmayı kabul etmek mümkün değildir²⁶⁰.

Kişilerin kendileri hakkında hakaret içeren web sitelerine karşı harekete geçerek kendileri hakkındaki verileri bozarlarsa ya da değiştirirlerse suçun oluşmayacağını savunan bir görüş de bulunmaktadır. Bu durum açısından meşru savunma halinin suça uygulanabileceği savunulmaktadır²⁶¹.

Böyle bir suça maruz kalan kişi karşısındaki kişinin sistemine zarar vermeden önce kendi sistemini güvenlik altına almalı ve eğer mümkünse kendisine saldırıda bulunan kişinin kimlik bilgilerine ulaşabilmek için gerekli işlemleri yapmalıdır. Ancak bilişim suçuna maruz kalan kişi açısından TCK m. 25/1’de yer alan “*o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu*” koşulunun gerçekleştiğinden söz edebilmek mümkün değildir. Zira teknik açıdan bilişim sistemine yapılan saldırının kapsamını saldırı anında belirleyebilmek her zaman mümkün değildir. Meşru savunmanın orantısını ve ölçüsünü ortaya koymak bu suç tipi açısından öngörülebilir değildir²⁶². Örneğin, banka hesabından bilişim yoluyla para aktarılması olayında mağdurun sanığın hesabından aynı miktarda parayı alması durumunda burada meşru savunmanın varlığından söz edilemez. Bir an için bilişim suçlarında meşru savunma hakkının varlığı kabul edilse bile bunun koşulları ve

²⁵⁹ Erdoğan, **a.g.e.**, s. 201.

²⁶⁰ **A.e.**, s. 231.

²⁶¹ Avşar/Öngören, **a.g.e.**, s. 138.

²⁶² Dülger, **a.g.e.**, s. 286.

ölçüsünü koymanın imkânsızlığı gerçeği karşısında bu sadece bir düşünceden ibaret olacaktır²⁶³.

D. Suçların Nitelikli Unsuru

765 sayılı TCK'da düzenlenen benzer suç tipinde bilişim sisteminin şahsa veya özel kuruluşa veya kamu kuruluşuna ait olması arasındaki ayrımın yapılmaması eleştiriliyordu. İşte 244. maddenin 3. fıkrasında yer alan bu düzenlenmeyle eleştirilere karşılık verilmiş ve bilişim suçları açısından var olan bir eksiklik giderilmiş, zarar verilen sistemin bankaya, kredi kurumuna ya da bir kurum ve kuruluşa ait bilişim sistemi olması suçun nitelikli hali sayılmıştır²⁶⁴.

Ülkemizde kamusal hizmetlerin ve alt yapı hizmetlerinin büyük bir kısmının yerine getirilmesini kamu kurum ve kuruluşları sağlamaktadır, benzer şekilde banka ve finans kurumları da tüm ekonomik sistemin işleyişini ilişkili oldukları kamu kurumları ve kamu bankalarıyla birlikte gerçekleştirmektedirler. Bu kuruluşların bilişim sistemlerinde meydana gelecek bir sorun, kesinti veya bozukluk ya da bunların bilişim sistemlerinde yer alan verilerin bozulması, erişilmez kılınması veya değiştirilmesi yalnızca bu kurumlar ya da bankaların kendisi açısından değil, hizmet verdikleri kesimler ve dolayısıyla toplumun büyük bir kısmı açısından da büyük sorunların ortaya çıkmasına neden olacaktır. Bu nedenle 765 sayılı TCK'daki bu suçun karşılığı olan 525b/1'deki önemli eksikliğin 3. fıkranın eklenmesiyle giderilmesi isabetli olmuştur²⁶⁵.

TCK'nın 244. maddesinin 3. fıkrasında, birinci ve ikinci fıkradaki tanımlanan fiillerin “(özel ya da kamuya ait) bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi” suçların nitelikli hali olarak

²⁶³ Karagülmez, **a.g.e.**, s. 75.

²⁶⁴ Dülger, **a.g.e.**, s. 333; Demircan, **a.g.e.**, s. 93.

²⁶⁵ Dülger, **a.g.e.**, s. 334.

öngörülmüştür. Buna göre nitelikli halin gerçekleşmesi durumunda faile verilecek ceza yarı oranında artırılacaktır²⁶⁶.

Bu suçların malvarlığına karşı suçlar arasında düzenlenmesi gerektiğini savunan görüşe göre, bilişim suçlarının tarihsel gelişimi bakımından bu suçların ilgili bölümlerde düzenlenmemesi ve diğer suçlar ile bağlantısının tam olarak kurulamaması bu tür eklemelerin yapılmasına yol açmaktadır. Bu suçlar malvarlığına karşı suçlar arasında mala zarar verme suçu ile beraber ya da mala zarar verme suçunun özel şekli olarak düzenlenmiş olsaydı, mala zarar verme suçlarına ilişkin daha fazla cezayı gerektiren nitelikli hal ile bağlantısının kurulmasını kolaylaştıracağını ve böylece bu tür ek düzenlemelere gidilmesine gerek olmayacağını savunmaktadırlar²⁶⁷.

Böyle bir nitelikli halin kabul edilmesinin sebebi, fiilin maddede sayılı kurumların sistemleri aracılığıyla yerine getirdiği kamu hizmetlerini aksatması nedeniyle toplumu oluşturan bireyleri mağdur etmesidir. Örneğin, Adalet Bakanlığı'na ait olan UYAP sisteminin etkilenmesi, nüfus müdürlüğüne ait bilgisayar sisteminin ya da bir bankanın bilgisayar sisteminin bozulmasıyla bu sistemde işi olan herkes mağdur olacaktır²⁶⁸.

Kamu kurum ve kuruluşları tabirinden, devletin yasama, yürütme ve yargı faaliyetlerinin yapıldığı il, belediye ve köylerin içine girdiği mahalli idarelerle kamu iktisadi teşebbüsleri kapsayacak şekilde tüm idari kuruluşların anlaşılması gerekir. Tüzel kişiliğinin olup olmamasına bakılmaksızın tüm idari kuruluşlar için geçerli bir kavramdır²⁶⁹. Banka veya kredi kurumu niteliğinde olmayan özel kurum ve şirketler, dernek ve vakıflara ait bilişim sistemine karşı bu suçun işlenmesi halinde, anılan nitelikli hal uygulanmaz²⁷⁰.

²⁶⁶ Dülger, **a.g.e.**, s. 333; Kurt, **a.g.e.**, s. 161.

²⁶⁷ Ketizmen, **a.g.e.**, s. 144.

²⁶⁸ Koca/Üzülmez, **a.g.e.**, s. 874.

²⁶⁹ Akbulut, **a.g.e.**, s. 207.

²⁷⁰ Erdoğan, **a.g.e.**, s. 197.

Buradaki banka veya kredi kurumunun kamuya ait olması gerekmemektedir. Özel bir bankanın bilişim sistemine yönelik zarar verici fiiller bakımından da bu nitelikli hal uygulanır. Ancak diğer kurum veya kuruluşların kamu kurum ve kuruluşu olması gerekir²⁷¹. Nitekim özel kurumlardan banka ve kredi kurumları bilişim suçlarında mali çıkar sağlamak amacıyla en çok hedef alınan kesimdir²⁷².

Çok çeşitli amaçlarla kurulan kamuya yararlı derneklere çeşitli imkân ve ayrıcalıklar sağlanmış olsa da bu derneklerin kamu tüzel kişilikleri bulunmadığından kamu kurumu ya da kuruluşu olarak sayılmayacağı açıktır. Bu nedenle söz konusu nitelikli hal bu derneklerin bilişim sistemine karşı işlendiğinde uygulama alanı bulamayacaktır.

5411 sayılı Bankacılık Kanunu'nun "Sistemi engelleme, bozma, verileri yok etme veya değiştirme" başlıklı 157. maddesinde 5411 sayılı Bankacılık Kanunu'na tabi kuruluşların, 5237 sayılı TCK'nın 244. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu açısından "banka veya kredi kurumu" olarak kabul edileceği belirtilirken, Bankacılık Kanunu'na tabi kuruluşlar ise 2. maddede açıkça sayılmıştır²⁷³.

Banka kavramı ise 5411 sayılı Bankacılık Kanunu'nun 3. maddesine göre; mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını ifade eder. Kredi kurumu kavramı ise, yine aynı kanunun 3. maddesine göre, mevduat bankalarını ve katılım bankalarını belirtmek için kullanılır. Bu kavramları tanımlarken kullanılan bankaların ne anlama geldiği de yine Bankacılık Kanunu'nda belirtilmiştir. 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"* ifade eder. Katılım bankası ise Bankacılık Kanunu m. 3'e göre; *"bu kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren"*

²⁷¹ Koca/Üzülmez, **a.g.e.**, s. 874.

²⁷² Parlar/Hatipoğlu, **a.g.e.**, s. 3480.

²⁷³ Erdoğan, **a.g.e.**, s. 198, 199.

kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini” ifade eder. Kalkınma ve yatırım bankası kavramı ise yine aynı maddede “Bu Kanuna göre mevduat veya katılım fonu kabul etme dışında; kredi kullandırmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini” şeklinde tanımlanmaktadır²⁷⁴.

Doktrinde yukarıda sayılanları isabetli bulmakla beraber burada kamu görevlisinin ya da banka ve kredi kurumunun görevlisinin bu suçu işlemesi halinin ayrıca nitelikli hal olarak düzenlenmesini savunan görüş de bulunmaktadır. Zira bu kişiler söz konusu kurumların içerisinde görev yapmakta olup bilişim sistem ağına ihtiyaç olmaksızın ve hatta bir bilişim güvenlik duvarını aşması gerekmeksizin dışarıdan müdahalede bulunmak isteyen kişiye nazaran çok kolaylıkla bu suçu işleyebilmektedirler²⁷⁵.

Doktrinde nitelikli halin uygulanmasını yalnızca banka veya kredi kurumu ya da kamu kurum ve kuruluşlarıyla sınırlandırılmasının yerinde olmadığını savunan görüş de bulunmaktadır. Zira bir şirket ya da işletme açısından da sistemin işleyişinin engellenmesi çok fazla önem taşıyabilir. Dolayısıyla kanun hükmünün sadece kanunda belirtilen kurum ve kuruluşlarla sınırlandırılması yerinde olmadığını belirtirler. İkinci olarak sabit artırım sistemin kabul edilmesi de yerinde olmadığını savunmaktadırlar. Artırım miktarının alt ve üst sınırının kabul edilmesi gerektiğini belirtirler. Nitekim sistemin işleyişinin engellenmesi ile verilere müdahale niteliği taşıyan fiiller aynı ölçüde zarar verici değildir²⁷⁶.

Açıklanan nitelikli hale dair gerekçede yalnızca “İkinci fıkrada, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür” denilmekle yetinilmiştir. Yukarıda da açıklandığı üzere bu şekilde bir nitelikli halin

²⁷⁴ Akbulut, **a.g.e.**, s. 208.

²⁷⁵ Erdoğan, **a.g.e.**, s. 197. Aynı görüşte Dülger, **a.g.e.**, s. 334.

²⁷⁶ Akbulut, **a.g.e.**, s. 206.

düzenlenmesinin sebebi bu kurumlara yapılacak engelleme, bozma ve tahribatların özel sistemlere karşı yapılacak saldırılara nazaran çok daha ağır sonuçlar vermesidir. Bu sistemlerin doğru çalışmasında tüm toplumun menfaati bulunmaktadır. Düzgün çalışmayan sistemde hizmet alamayan tüm toplum mağdur olmaktadır. Örneğin; bir bankanın bilişim sistemi engellendiğinde o bankayı kullanan belki milyonlarca kişi işini yapamaz hale gelecektir²⁷⁷.

Bu fıkranın uygulanmasına, eczacının SGK tarafından verilen online şifresini yetkisiz kullanarak SGK'nın internet sitesine girip şirket adına işlem yapması, öğrenim gördüğü okulun bilişim sistemine girerek ders notlarını değiştiren failin durumu, başkası adına ÖSYM sitesine girerek sınav başvuru belgelerinde değişiklik yapan kişinin durumu örnek olarak gösterilebilir²⁷⁸.

Diğer bir nitelikli hal de Terörle Mücadele Kanunu'nda yer almaktadır. TMK'nın 4. maddesinde TCK'nın 244. maddesinde yer alan suçun TMK'nın 1. maddesinde belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde terör suçu olarak kabul edileceği belirtilmektedir. TMK m. 5'e göre ise; *"3 ve 4 üncü maddelerde yazılı suçları işleyenler hakkında ilgili kanunlara göre tayin edilecek hapis cezaları veya adli para cezaları yarı oranında artırılarak hükmolunur. Bu suretle tayin olunacak cezalarda, gerek o fiil için, gerek her nevi ceza için muayyen olan cezanın yukarı sınırı aşılabılır. Ancak, müebbet hapis cezası yerine, ağırlaştırılmış müebbet hapis cezasına hükmolunur."* şeklinde. Dolayısıyla TCK m. 244/1-2'de yer alan suçlar terör örgütünün faaliyeti çerçevesinde işlendiği takdirde TMK m. 5'e göre hüküm kurulacaktır²⁷⁹.

²⁷⁷ Erdoğan, **a.g.e.**, s. 198. Aynı görüşte Akbulut, **a.g.e.**, s. 206.

²⁷⁸ Gül, **a.g.e.**, s. 87. Yargıtay 8. Ceza Dairesi 2013/9180 Esas 2014/9692 Karar 15.04.2014 tarihli kararı; *"Sanığın; SGK.nun bilişim sistemine girerek katılanın eczanesi adına kayıtlı reçeteleri sistemden silmek şeklindeki eylemi nedeniyle hükmolunan cezanın SGK.nun kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden..."* www.corpus.com.tr (Çevrimiçi) 17.03.2019.

²⁷⁹ Akbulut, **a.g.e.**, s. 208; Dülger, **a.g.e.**, s. 274.

Doktrinde bir görüş, birinci ve ikinci fıkralarda düzenlenen fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlamasını nitelikli hal olarak kabul etmektedir²⁸⁰.

Söz konusu hükmü müstakil bir suç olarak değil de maddenin ilk iki fıkrasında yer alan suçların nitelikli hali olarak kabul eden görüş, bu görüşünü kanun yapma tekniğine dayandırır. Bu tekniğin bir sonucu olarak önce bir suçun temel şekli oluşturulur, buna suçun basit şekli denilmektedir. Daha sonra suçun ağır ya da hafif biçimlerine yer verilmektedir. Dikkat edilmesi gereken husus suçun nitelikli hali düzenlenirken temel suç tipine bağlılığın devam etmesidir. TCK m. 244/4 incelendiğinde ilk iki fıkraya bağlılığın “yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle” ifadesi ile gerçekleştiği görülür. Bu durum karşısında söz konusu fiiller işlenerek haksız bir çıkar sağlanması suçun temel şekline bağlı nitelikli hal olarak kabul etmektedirler. Düzenlemenin nitelikli hal olup olmaması iki açıdan önem taşımaktadır. İlki eğer nitelikli hal ise temel suç tipi oluşmadığı sürece bu nitelikli hal uygulanmaz. İkincisi ise nitelikli halin gerçekleşmemesi durumunda teşebbüsten söz edilemez, sadece bu fıkra uygulanmaz ancak suçun basit şeklinden ceza verilebilir²⁸¹.

Biz TCK m. 244/4’ü ayrı bir suç olarak kabul ettiğimiz için bu görüşe katılmıyoruz. Buna ilişkin tartışma bilişim sistemleri kullanılmak suretiyle haksız çıkar sağlama suçunu incelediğimiz üçüncü bölümde yapılmıştır.

E.Suçların Özel Görünüş Biçimleri

1. Teşebbüs

Bilişim sistemine müdahale suçu ile bilişim sistemindeki verilere müdahale suçlarının suçlarının teşebbüs aşamasında kalması mümkündür. İcra hareketlerinin failin elinde olmayan nedenlerle yarıda kalması ve bu nedenle sisteme etki edememesi

²⁸⁰ Esen, **a.g.e.**, s. 636; Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 989.

²⁸¹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 989.

durumunda teşebbüs gündeme gelecektir²⁸². Örneğin, failin bilişim sistemine ve/veya içerdiği verilere zarar verilmesi amacıyla sisteme bir bilişim virüsünün veya mantık bombası yüklenmesi ve bunların harekete geçmeden sistem ve/veya veri sahibi tarafından fark edilerek etkisiz duruma getirilmesi durumunda suça teşebbüs gerçekleşmiş olacaktır²⁸³. Yine aynı şekilde virüs programları aracılığıyla sisteme girilen virüsün yok edilmesi durumunda ve DoS saldırısının fark edilip failin sistemin işleyişini engelleyememesi halinde de teşebbüs aşamasında kalmış suç söz konusudur²⁸⁴.

Doktrinde suçun neticeli suç olup olmadığı konusunda iki farklı görüşün varlığından yukarıda bahsetmiştik. Bu çerçevede ve suçu neticeli olarak kabul eden görüşe göre; teşebbüs icra hareketlerine başladıktan sonra bu hareketlerin yarıda kalması şeklinde olabileceği gibi suçun icrasına ilişkin fiiller tamamlandıktan sonra suçun oluşumu için aranan netice meydana gelmeden failin elinde olmayan nedenlerle suçun gerçekleşmemesi şeklinde de olabilir²⁸⁵.

Engelleme ve bozmayı hareket değil, hareketin neticesi kabul eden görüşe göre, bu suça teşebbüs mümkündür. Failin, bilişim sisteminin işleyişini bozmak veya engellemek için icra hareketlerine başlayıp elinde olmayan nedenlerle, engelleme ve bozma sonucunu gerçekleştiremezse suçun teşebbüs aşamasında kalmış sayılacağını kabul etmektedirler²⁸⁶. Örneğin; failin amaca elverişli bir virüsü sisteme sokup faal hale getirmesine karşın, anti virüs programı sayesinde sistemin işleyişini engelleyememiş veya bozamamışsa bu suça teşebbüsten cezalandırılması gerektiğini savunmaktadırlar²⁸⁷.

Bu bölümde incelediğimiz suç tiplerini neticeli suç olarak kabul ettiğimiz için icra hareketlerine başlanılmasına rağmen yarım kalması ya da neticenin

²⁸² Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 868.

²⁸³ Dülger, **a.g.e.**, s. 336.

²⁸⁴ Akbulut, **a.g.e.**, s. 208.

²⁸⁵ Dülger, **a.g.e.**, s. 336; Erdoğan **a.g.e.**, s. 202, 232; Koca/Üzülmez, **a.g.e.**, s. 874.

²⁸⁶ Pallı **a.g.t.**, s. 171; Erdoğan, **a.g.e.**, s. 202, 232; Kurt, **a.g.e.**, s. 265.

²⁸⁷ Pallı **a.g.t.**, s. 171, 172.

gerçekleşmemesi durumunda suçların teşebbüs aşamasında kaldığını kabul eden görüşe katılmaktayız. Maddede sayılan bazı hareketlerin tamamlanması bazılarının ise teşebbüs aşamasında kalması durumunda diğer neticeler teşebbüs aşamasında kalmış olsalar da suç tamamlanmış sayılacak ve faile tamamlanmış suçtan ceza verilecektir²⁸⁸. Örnek olarak fail verilerin tamamını silmek isterken kısmi silmeyi gerçekleştirmişse verilerin yok edilmesi neticesi gerçekleşmiş olacaktır²⁸⁹.

TCK m. 36’da düzenlenen gönüllü vazgeçme kurumunun burada uygulama imkânının olup olmayacağı tartışma konusu yapılabilir. Bilindiği üzere gönüllü vazgeçme, suçu tamamlama imkânına sahip olan failin kendi iradesiyle icra hareketlerinin tamamlanmasından vazgeçmesidir. Bu durumda faile işlemek istediği suça teşebbüsten ceza verilmez ancak vazgeçinceye kadar yaptığı hareketler başka bir suçu oluşturuyorsa o suçun cezası verilir. Örneğin fail sisteme girdikten sonra vazgeçip sistemden çıkarsa o ana kadarki fiili TCK m. 243’teki bilişim sistemine girme ve kalma suçunu oluşturacağından bu durumda faile TCK m. 244’teki suça teşebbüsten değil tamamlanmış olan m. 243’ten ceza verilmelidir²⁹⁰.

Failin sisteme girdiği fakat TCK m. 244’te sayılan fiillerden birini gerçekleştirmedeği durumlarda fail yalnızca TCK m. 243’ten sorumlu olacağı kabul edilmektedir. Sanığın banka hesaplarına internet üzerinden giriş yapması fakat hesapta herhangi bir oynama yapmaması durumunda sadece TCK m. 243 uygulama alanı bulacaktır²⁹¹. Yargıtay 8. Ceza Dairesi 2014/607 Esas 2014/15426 Karar sayılı 18.06.2014 tarihli kararı; “*Sanığın, giriş yaptığı katılana ait mail adresinden onun arkadaşlarına pek çok sayıda hakaret ve uygunsuz görüntüler içeren mesajlar gönderdiğinden bahisle bilişim suçundan açılan davada; TCK.nun 244. maddesinin 2.*

²⁸⁸ Dülger, **a.g.e.**, s. 336; Aynı görüşte Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6931; Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 868.

²⁸⁹ Akbulut, **a.g.e.**, s. 209.

²⁹⁰ Erdoğan, **a.g.e.**, s. 202; Aynı görüşte Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6936; Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 868; Kurt, **a.g.e.**, s. 266; Taşkın, **a.g.e.**, s. 54.

²⁹¹ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 865.

fıkrasında yazılı seçimlik hareketlerin yapıldığına ilişkin bir tespit bulunmaması karşısında, eyleminin TCK.nun 243/1. maddesine uygun bulunduğu gözetilmeden yazılı şekilde karar verilmesi, Yasaya aykırı,”²⁹² şeklindedir.

2. İştirak

Bu suç iştirak açısından bir özellik göstermez, genel hükümler uygulanır²⁹³. TCK’nın 37, 38, 39 ve 40. maddelerinde suça iştirake ilişkin genel hükümler düzenlenmiş olup, bu çerçevede ortaya çıkan durumlar bu suç tipi için de uygulanacaktır²⁹⁴.

Bu suç bakımında söz konusu olabilecek iştirak şekilleri daha ziyade suçun işlenmesinde kullanılan araçları sağlamak ve suç işlemeye teşvik biçimindedir. Örneğin; suçun işlenmesi için bir kimseye ihtiyacı olan bilgisayar ve unsurlarını, programlarını sağlayan ya da kişiyi suç işlemeye teşvik eden kişi suça iştirak iradesinin de olması şartıyla iştirak hükümlerince yardım eden olarak (TCK m. 39) cezalandırılabilir²⁹⁵.

Bir bilişim sistemini bozma amacıyla birden fazla bilgisayar korsanının topluca bilişim sistemine girmeleri ve bunlardan birisinin fiili ile bir kısım verilerin zarar görmesi halinde ortak bir suç işleme kararı ile fiili gerçekleştirdiklerinden ve her biri fiil üzerinde hâkimiyet kurduklarından bilişim sistemine zarar verme suçu nedeniyle bütün bilgisayar korsanları müşterek fail olarak cezalandırılacaktır²⁹⁶.

3. İçtima

Türk Ceza Kanunu sisteminde gerçek içtima kural olup her bir suçtan ayrı ayrı cezaya hükmedilmesi gerekmektedir. Suçların içtimaı ise bu kuralın istinasını

²⁹² www.corpus.com.tr (Çevrimiçi) 27.03.2019.

²⁹³ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6931.

²⁹⁴ Esra Yayıcı, “Bilişim Suçları”, Gazi Üniversitesi SBE Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Ankara, 2007, s. 96.

²⁹⁵ Koray Doğan, “Bilişim Suçları ve Yeni Türk Ceza Kanunu”, **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y. 2, S. 6-7, Ekim 2005, s. 300.

²⁹⁶ Kurt, **a.g.e.**, s. 267.

oluşturmaktadır. Aşağıda karışıklığa yer vermemek için ayrı başlıkta incelediğimiz suç tiplerinin içtima ilişkisini açıklamaya çalıştık.

a. Görünüşte İçtima

İlk tartışılması gereken husus TCK m. 243'ün incelediğimiz suç tipleri açısından geçit suç olarak kabul edilip edilmeyeceği hususudur. Doktrinde bu konuda görüş birliği bulunmamaktadır.

İlk görüş TCK m. 243'ü geçit suç olarak kabul eden görüştür²⁹⁷. Bu görüşe göre, sisteme müdahale suçunun işlenmesi için fail genellikle hukuka aykırı olarak bilişim sistemine girmek veya sistemde kalmak durumundadır. Örneğin TCK'nın 244. maddesindeki bilişim sisteminde var olan verileri başka bir yere göndermek veya bir bilişim sistemindeki verileri değiştirmek ya da bozmak için sisteme girmek de gerekmektedir²⁹⁸.

Diğer görüş ise geçit suç olarak kabul edilmeyeceğini savunur. Bu görüş, 244. maddenin 1. ve 2. fıkralarındaki suçların mutlaka 243. maddedeki fiiller gerçekleştirmek suretiyle işlenmesi gerekmediğini belirtmektedirler.

Bu suçlar arasında gerçek içtima kurallarının uygulanmasını kabul eden görüşe göre fiiller arasında zamansal açıdan yakınlık olmayıp farklı kastlarla hareket edildiği durumlarda faile her iki suçtan ayrı ayrı ceza verilmesi gerekir, geçit suç koşulları oluşmaz. Eğer sisteme girilmeksizin diğer fiilin gerçekleştirilmesi mümkün değilse bu takdirde geçit suçun varlığı kabul edilerek yalnızca sonraki fiilden ceza verilmesi yoluna gidilebileceğini belirtmektedirler. Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçundaki her fiil için ve her somut olayda mutlaka sistem girme veya orada kalmaya devam etme suçunun işlenmesi gerekmediğinden geçit suç ilişkisi bulunup bulunmadığı her somut olayda ayrı ayrı değerlendirilmesini gerektiğini kabul etmektedirler²⁹⁹. Gerçekten de bilişim

²⁹⁷ Parlar/Hatipoğlu, **a.g.e.**, s. 3479; Taşkın, **a.g.e.**, s. 34, 55; Ketizmen, **a.g.e.**, s. 137.

²⁹⁸ Erdoğan, **a.g.e.**, s. 170.

²⁹⁹ Dülger, **a.g.e.**, s. 300.

sistemine girmeden verilerin bozulması durumunda zaten TCK m. 243'ten bahsedilemez³⁰⁰.

Suçların arasındaki ilişkiyi gerçek içtima olarak kabul eden görüşe göre, TCK m. 243 ve m. 244 farklı hukuki değerleri koruduğundan geçit suç olarak sayılmaz. Bu sebeple ihlal edilen her hukuki değer açısından fiiller ayrı suç oluşturacak ve gerçek içtima uygulanacaktır³⁰¹.

Artuk/Gökçen/Yenidünya, 243. maddede yer alan suç için daha sonra işlenen suçlar bakımından bir geçit olma özelliği taşıdığını ve failin sadece amaç suçtan cezalandırılması gerektiğini savunur. Örneğin, bir bilişim sisteminin işleyişini engellemek amacıyla bilişim sistemine giren fail, hem 243. maddeyi hem de 244. maddeyi ihlal etmiş olsa da amaç suç olan 244. maddeden cezalandırılması gerektiğini ileri sürmektedirler³⁰².

Bu suçlar arasında fikri içtima ilişkisi olduğunu ileri süren görüşe göre tek fiille iki ayrı suç olduğundan farklı neviden fikri içtima gereği fail daha ağır ceza içeren fıkradan ceza alması gerekmektedir³⁰³.

Suçlar arasında görünüşte içtima olduğunu kabul eden görüşe göre, TCK m. 244'ün oluşabilmesi için TCK m. 243'ün gerçekleştirilmiş olması gerektiğinden, m. 244'ün m. 243 açısından tüketen norm niteliğinde olduğunu savunmaktadır. Tüketen-tüketilen norm ilişkisi gereği de TCK m. 244'ün uygulanması gerektiğini belirtmektedirler³⁰⁴.

Fail TCK m. 244/2'de sayılan neticelerden birini gerçekleştirmek kastıyla değil de sadece sisteme girip kalmak amacıyla girmiş fakat sonradan bu neticelerden birini

³⁰⁰ Mahmutoglu, "TCK'da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", s. 869.

³⁰¹ Orta, **a.g.e.**, s. 119.

³⁰² Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6931; Kurt, **a.g.e.**, s. 270; Ali Parlar, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Bilge Yayınevi, 2011, s. 28.

³⁰³ Erdoğan, **a.g.e.**, s. 202; Soyaslan, **a.g.e.**, s. 612; Koca/Üzülmez, **a.g.e.**, s. 875

³⁰⁴ Mahmutoglu, "TCK'da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", s. 869.

gerçekleştirmişse (mesela başkasının e-posta hesabına girerek e-postalarına bakmak istemiş sonradan kastını değiştirerek şifreyi değiştirmiş ve bunu yaparak asıl hesap sahibinin erişimini engellemiş ise) bu durumda fail TCK m. 244/2 maddesinden cezalandırılacaktır³⁰⁵.

b. Zincirleme Suç

Bu suçların zincirleme suç şeklinde işlenmesi mümkündür (TCK m. 43/1). Aynı kişiye karşı tek suç işleme kararıyla değişik zamanlarda fiilin gerçekleştirilmesi durumunda zincirleme suçun varlığından söz edebiliriz³⁰⁶. Örneğin, sistemin çalışmasının engellenmesi ya da hukuka aykırı veri yerleştirilmesi için kısa zaman aralıklarıyla ve aynı suç işleme kastıyla bilişim sistemine birçok kez etkiye bulunulması halinde zincirleme suç gerçekleşir³⁰⁷.

Yargıtay 8. Ceza Dairesi'nin 2012/33044 Esas 2014/236 Karar sayılı 08.01.2014 tarihli kararı; *“Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması, Sanığın değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması gerektiğinin gözetilmemesi... Yasaya aykırı”*³⁰⁸ şeklindedir.

Farklı bilişim sistemlerinin engellenmesi veya farklı bilişim sistemlerindeki verilerin yok edilmesi veya değiştirilmesi durumunda ise ayrı mağdurlara ait bilişim sistemine yönelik hareketler bağımsız suç oluşturduğundan burada zincirleme suç söz konusu olmaz³⁰⁹.

³⁰⁵ Gül, **a.g.e.**, s. 87; Soyaslan s. 612.

³⁰⁶ Akbulut, **a.g.e.**, s. 209.

³⁰⁷ Dülger, **a.g.e.**, s. 336.

³⁰⁸ www.corpus.com.tr. (Çevrimiçi) 17.03.2019

³⁰⁹ Esen, **a.g.e.**, s. 636.

Yargıtay 12. Ceza Dairesi'nin 2016/10818 Esas 2017/7390 Karar sayılı 11.10.2017 tarihli kararı şu şekildedir; “Sanık ...'un, mağdurlar ... ve ...'ya ait MSN adreslerinin ve facebook hesaplarının internet şifrelerini, onların rızası dışında değiştirerek, mağdurların bilişim sistemindeki hesaplarına erişimlerini engellemesi şeklinde sübutu kabul edilen eylemlerinden dolayı TCK'nın 244/2. madde ve fıkrasında tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan mağdur sayısınca iki ayrı mahkumiyet hükmü kurulması ve MSN ile facebook hesaplarının iki farklı bilişim sistemi olmasından dolayı bir suç işleme kararının icrası kapsamında değişik zamanlarda her bir mağdura karşı aynı eylemi birden fazla işleyen sanık hakkında TCK'nın 43/1. madde ve fıkrasında düzenlenen zincirleme suç hükmünün uygulanması gerektiği gözetilmeden, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan tek bir mahkumiyet hükmü kurulup, zincirleme suç hükümlerinin uygulanmaması ve olayda uygulama alanı bulunmayan TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme suçundan da ayrıca mahkumiyet hükmü kurulması, kanuna aykırı.”³¹⁰

Ancak zincirleme suç bakımından varlığı gerekli olan aynı suçun işlenmesiyle kast edilen, kanunun aynı maddesinin birden çok kez ihlal edilmesi değildir. TCK'nın birçok maddesinde birbirinden bağımsız suç tiplerine aynı maddede ver vermiştir. Dolayısıyla işlenen fiiller kanunun aynı maddesini ihlal etmesine rağmen, aynı suç oluşturmayabilir. Bu bağlamda failin ilk önce mağdurun bilişim sistemini bozması (TCK m. 244/1), sonrasında ise bu bilişim sistemini kullanarak haksız yarar elde etmesi halinde (TCK m. 244/4) bu fiiller aynı suç işleme kararı kapsamında gerçekleşeler de farklı suçlar oluşturdukları, farklı hukuki değerleri korudukları için zincirleme suç oluşturmaz³¹¹. Aynı durumu TCK m. 244/1 ve TCK m. 244/2'deki suç tipleri arasındaki ilişki için de söyleyebiliriz³¹².

Doktrinde bir diğer görüş ise; TCK'nın 244. maddesinin birinci ve ikinci fıkralarındaki suçların, dördüncü fıkradaki bilişim sistemleri aracılığıyla hukuka aykırı

³¹⁰ www.kazanci.com (Çevrimiçi) 04.03.2019

³¹¹ Koca/Üzülmez, **a.g.e.**, s. 874.

³¹² Dülger, **a.g.e.**, s. 337.

çıkar sağlamak suçu arasındaki ilişkiyi fiil tekliği ilişkisi olarak nitelendirmektedirler. Bu durumda birden fazla fiil ve birden fazla suç bulunmayıp tek fiil ve tek suç bulunmaktadır. Bu görüşteki yazarlara göre, birinci ve ikinci fıkrada yer verilen fiiller dördüncü fıkradaki suçun unsuru niteliğindedir. Dolayısıyla verilere müdahale ederek veya sistemin işleyişini bozarak veya engelleyerek çıkar sağlayan kişi sadece TCK m. 244/4'ten cezalandırılacaktır³¹³. Bu görüşe göre, maddenin ilk iki fıkrasında yaptırım altına alınan fiiller dördüncü fıkradaki suçun unsuru olduğu için bileşik suç söz konusudur ve ortada tek fiil bulunmaktadır. Verileri başka yere göndererek, verileri değiştirerek, bozarak haksız bir yarar sağlayan fail yalnızca TCK m. 244/4'te düzenlenen suçu işlemiş olur³¹⁴.

c. Fikri İçtima

Fail eğer tek bir hareketle aynı suçu birden fazla kişiye karşı gerçekleştirmişse TCK m. 43/2 gereği aynı neviden fikri içtima gündeme gelecektir. İki kişinin ortak kullandığının açıkça belli olduğu bir hesabın şifresinin değiştirilmesi ya da tek bir hareketle birden fazla kişiye virüs yollanması durumu örnek olarak verilebilir.

Fail eğer tek bir hareketle her iki suçu da gerçekleştirmişse yani bilişim sistemindeki verilere zarar verilmesi, sistemin işleyişini engellemiş ya da bozmuş ise failin farklı neviden fikri içtima kuralları gereğince cezası daha ağır olan TCK m. 244/1'den cezalandırılması gerekir³¹⁵.

TCK m. 244/1'de düzenlenen bilişim sistemine karşı fiillerin sistemdeki veriler aracılığıyla gerçekleştirilmesi halinde her iki fıkradaki suçlar da ihlal edilmiş olacaksa da ikinci fıkradaki suç, birinci fıkradaki suç tarafından yutulur ve fail sadece birinci fıkradaki suç nedeniyle cezalandırılır³¹⁶.

³¹³ Akbulut, **a.g.e.**, s. 210.

³¹⁴ Koca/Üzülmez, **a.g.e.**, s. 875.

³¹⁵ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 886; Avşar/Öngören, **a.g.e.**, s. 137; Erdağ, **a.g.m.**, s. 290; Değirmenci, **a.g.m.**, s. 205; Erdoğan, **a.g.e.**, s. 236.

³¹⁶ Yılmaz, **a.g.m.**, s. 83.

Bilişim sisteminin bozulması sonucunu doğuran fiil verilerin değiştirilmesi suretiyle gerçekleştirilmiş ise bu durumda TCK m. 244/1’de düzenlenen suç mu yoksa verilerin bozulmasını düzenleyen TCK m. 244/2’de düzenlenen suç mu oluşur sorusunu failin kastının ne olduğunu belirlemek suretiyle de aşabilmesi mümkündür. Sistemin işletim yazılımındaki sistem dosyalarını silmiş olan sanığın kastının sadece verileri bozmak değil bunu aşarak sistemin işleyişini bozmak olduğunu söyleyebiliriz. Zira sıradan verileri değil, sistemin işleyişini sağlayan verilerin silinmesi yoluna gidilmiştir³¹⁷.

Bilişim sisteminin işleyişinin bozulması fiili verilerin bozulması fiiliyle de gerçekleştirilebilir; ancak görüldüğü üzere verilerin bozulması fiili TCK m. 244/2’de ayrıca düzenlenmiştir. Bunun nedeni yukarıda da değindiğimiz gibi faildeki farklı kasıtlarla gerçekleştirilen fiillerin olmasıdır; ancak bu kasıt, suç tipleri açısından bir unsur oluşturmamakta, yalnızca hangi fıkranın uygulanacağını belirlenmesi açısından bir yorum aracı olmaktadır. Bilişim sisteminin işleyişinin engellenmesi için verilerin bozulması halinde failin kastı sistemde bulunan verilere zarar vermek değil bir şekilde bilişim sisteminin işleyişini bozmaktır. Maddenin ikinci fıkrasında yer alan verileri bozmak hareketinde fail bilişim sisteminin içerdiği bir kısım verileri örneğin bir uygulama yazılımını ya da depolanmış bazı bilgileri kullanılamaz hale getirmek istemektedir. Faildeki bu kast somut fiile hangi fıkranın uygulanacağı hususunda yol göstericidir³¹⁸. Eğer fiil sıradan verilere değil de işletim yazılımındaki sistem dosyalarının silinmesi biçiminde sistemin işleyişini sağlayan dosyalara yönelik ise bu durumda TCK m. 244’ün ikinci fıkrası değil birinci fıkrası olaya uygulanır³¹⁹.

Sisteme dışarıdan gönderilen dosya, TCK m. 244/2’de sayılan suçu oluşturur. Eğer sisteme dışarıdan gönderilen bu dosyanın içinde yer alan programlar vasıtasıyla bilişim sistemine girmek mümkün ise bu durumda bilişim sistemine girme suçundan

³¹⁷ Kurt, **a.g.e.**, s. 167.

³¹⁸ Dülger, **a.g.e.**, s. 322, 323.

³¹⁹ Parlar/Hatipoğlu, **a.g.e.**, s. 3477.

bahsedilir. Bu durumda mail yoluyla gönderilen dosyayı alan kişinin bu dosyayı açamaması halinde ise teşebbüs tartışması TCK m. 243 için yapılabilir³²⁰.

Sistemin işleyişi, sistemin tümüne yöneltilen herhangi bir hareketle bozulabileceği gibi, sistemde yer alan verilere veya sistemin diğer unsurlarına yapılacak müdahaleler ile de bozulabilir. Eğer sistemde bulunan verilere yapılan müdahaleler yönünden, müdahalenin sistemin işleyişini engellememesi veya bozmaması durumunda TCK m. 244/2’de yer alan suç, müdahalenin sistemin işleyişini engellemesi veya bozması durumunda TCK m. 244/1’de yer alan suç oluşur³²¹.

Failin bilişim sistemine yerleştirdiği veri sistemine veri yerleştirilen kişinin bir suçu işlediğini ispata yarayacak delil niteliğinde olursa bu durumda verilere zarar verme suçu ve suç uydurma suçları birlikte işlenmiş olacaktır. Bu durumda tek fiille kanunun birden fazla normu ihlal edilmiş olacağından farklı neviden fikri içtima kuralı uygulanarak cezası daha ağır olan suçtan ceza verilir³²².

TCK m. 244/2’deki “var olan verileri başka yere gönderme” suçu eğer kişisel bilgiler içeren belgeler ve e-postalar fikir ve sanat eserleri hakkında ortaya çıkmış olursa, Fikir ve Sanat Eserleri Kanunu’nda düzenlenen suçların oluşabilme ihtimali bulunmaktadır. Fikri içtima kuralları gereğince hangi madde daha ağır ceza içeriyorsa o suçtan ceza verilmelidir³²³.

Bilişim sistemine veri eklenmesi ya da var olan verilerin değiştirilmesi durumunda söz konusu veriler bir belgenin düzenlenmesine esas teşkil edecek nitelikteyse fail ayrıca belgenin niteliğine göre diğer şartları taşıması halinde TCK m. 204’te düzenlenen “resmi belgede sahtecilik” ve TCK m. 207’de düzenlenen “özel belgede sahtecilik” suçunu oluşturabilir³²⁴.

³²⁰ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 861.

³²¹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6929.

³²² Dülger, **a.g.e.**, s. 338.

³²³ Avşar/Öngören, **a.g.e.**, s. 138.

³²⁴ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6936.

Belgede sahtecilik suçlarında şu hususa dikkat etmek gerekir; veri eğer bilişim sisteminde kalıyorsa TCK m. 244'ün ilgili fıkrasından, sistemde kalmayıp örneğin kağıda basılması suretiyle somut bir belge haline geliyorsa duruma göre TCK m. 204 veya TCK m. 207'den failin sorumluluğu doğabilir. Yargıtay 11. Ceza Dairesi'nin 2017/17411 Esas 2018/2663 Karar sayılı 27.03.2018 tarihli kararı şu şekildedir; *“İşyerinde çalışmadıkları halde çalışıyorlarmış gibi gösterilerek işe giriş bildirgelerinin verildiğinin anlaşılması halinde suça konu edilen işe giriş bildirgelerinin yazılı olarak mı yoksa e-bildirge şeklinde mi verildiğinin araştırılması, yazılı olarak verilmişse asıllarının getirtilerek aldaticılık niteliğinin olup olmadığının değerlendirilmesi ve bu durumda yüklenen eylemlerin sübutu halinde TCK 207. maddesinde düzenlenen “özel belgede sahtecilik” suçunun oluşacağı; bildirimlerin yalnızca elektronik ortamda verilmiş olması halinde ise TCK'nın 244/2. maddesinde düzenlenen sisteme veri yerleştirme suçunu oluşturacağı gözetilmeden ve tartışılmadan yazılı şekilde hüküm kurulması yasaya aykırıdır.”*³²⁵

Yargıtay 21. Ceza Dairesi'nin 2015/8042 Esas 2016/6504 Karar sayılı 01.11.2016 tarihli kararı ise şu şekildedir; *“Olay tarihinde ... İlçe Tarım Müdürlüğünde işçi olarak çalışan sanık ... ile ziraat teknisyeni olarak görev yapan ..., ... Bankası Akkaya şubesinde servis görevlisi olarak çalışan sanık ... , 'nın babası olan sanık ... ve amcası olan sanık ... 'nın, iştirak halinde birlikte hareket ederek, ..., isimli kişilerin herhangi bir başvurusu olmaksızın, Akkaya ilçesinde kendilerine ait taşınmazları varmış gibi çiftçi kayıt sistemine arazi girişlerinin yapılmasını, sanıklar ... ve ... 'nın, 23.07.2004 tarihinde doğrudan gelir desteği almak amacıyla ibraz ettikleri belgelerde yer almayan taşınmazların sisteme kaydı yapılarak, ... adına 23.000 m2, ... adına 258.823 m2 fazladan arazi girişinin yapılmasını sağladıkları iddiasıyla kamu görevlisinin resmi belgede sahteciliği suçundan cezalandırılmaları talebiyle açılan kamu davasında; sanıkların üzerine atılı çiftçi kayıt sistemine gerçeğe aykırı olarak arazi girişi yapılmasına iştirak etmekten ibaret eylemlerinin, ortada belgede sahtecilik suçlarına konu olabilecek bir belgenin bulunmaması nedeniyle,*

³²⁵ www.corpus.com.tr (Çevrimiçi) 17.03.2019.

*resmi belgede sahtecilik suçunu oluşturmayacağı ancak sübutunun ve unsurlarının varlığı halinde TCK'nın 244/3. maddesinde düzenlenen “sistemi engelleme, bozma, verileri yok etme veya değiştirme” suçunu oluşturabileceği*³²⁶. Kararda belgede sahtecilik suçunun ortada suça konu somut bir belgenin olmadığından bahisle oluşmayacağı belirtilerek, kamu kurumu hesaplarının değişmesinden dolayı TCK m. 244/3'ün uygulanacağı belirtilmiştir. Yargıtay'ın aynı doğrultuda bilgisayar gibi ortamlarda hazırlanan dosyalarda yapılan değişiklikleri TCK m. 244'de belirtilen suçların oluştuğunu belirten birçok kararı bulunmaktadır³²⁷.

Kişiler arasındaki internet ortamındaki haberleşmenin veya basın ve yayın faaliyetinin engellenmesi halinde TCK m. 124 maddesinde düzenlenen haberleşmenin engellenmesi suçunun mu yoksa TCK m. 244 maddesindeki suçlardan birinin mi oluştuğunu tartışmamız gerekirse, tek fiile birden fazla suçun işlenmesi söz konusu olduğundan, bilişim sistemleri vasıtasıyla işlenen bu suçlarda TCK 44. madde gereğince daha ağır ceza içeren TCK m. 244 uygulanıp tek bir ceza verilmelidir³²⁸. Aynı şekilde TCK m. 136'da düzenlenen “Kişisel Verileri Verme, Yayma, Ele Geçirme Suçu” ile TCK m. 244 arasında da fikri içtima söz konusu olabilir³²⁹. Failin mağdurun bilişim sistemleri üzerinden yaptığı haberleşmeleri takip etmesi halinde TCK m. 132'de düzenlenen haberleşmenin gizliliğini ihlal suçu oluşacaktır. Bu durumda farklı neviden fikri içtima gereği hangi suç daha ağır ceza içeriyorsa onun uygulanması gerekecektir³³⁰.

Örneğin bir kişinin başka bir kişiyle internet üzerinden gerçekleştirdiği haberleşme esnasında üçüncü bir kişi tarafından haberleşmenin gerçekleştiği bilgisayara virüs atağı gerçekleştirilse ve bilgisayar devre dışı kalması durumunda kast

³²⁶ www.corpus.com.tr (Çevrimiçi) 22.03.2019.

³²⁷ Yargıtay 23. Ceza Dairesi'nin 2016/1076 Esas 2016/7401 Karar sayılı 08.06.2016 tarihli kararı; “e-bildirge, imza ve şifre ile bilgisayar ortamında işe giriş bildirgelerini verdiği somut olayda, sahte oluşturulmuş maddi varlığa sahip somut bir belge bulunmadığından, muhasebeci sanığın resmi belgede sahtecilik suçundan değil, TCK'nın 244/2. fıkrasında düzenlenen sisteme veri yerleştirme suçundan cezalandırılması gerektiği gözetilmelidir.”

³²⁸ Erdoğan, **a.g.e.**, s. 203.

³²⁹ Akbulut, **a.g.e.**, s. 212.

³³⁰ Erdoğan, **a.g.e.**, s. 241.

da varsa TCK m. 244/1 ile TCK m. 124'te düzenlenen haberleşmenin engellenmesi suçları arasında fikri içtima kuralları uygulanacaktır³³¹.

Kamu kurumlarının internet ortamında haberleşmesini engellemek için bilişim virüsleri, kurtçuklar, Truva atları gibi zarar verici yazılımları kamu kurumunun sistemine yollayan kişi aynı zamanda bilişim sistemine zarar vereceğini öngörebilmesine rağmen fiili gerçekleştiriyorsa, TCK m. 124/2 ve kastına göre TCK m. 244/1-2 suçları arasında fikri içtima ilişkisi gereğince sorumlu olur³³².

F. Kusurluluk ve Cezalandırılabilirliğin Diğer Koşulları

Kanun sistematigi bakımından suçla korunan hukuki değer m. 244 m. 167'de yazılı şahsi cezasızlık sebepleri ile TCK m. 168'deki etkin pişmanlık hükümlerinden yararlanma olanakları bulunmaktadır. Mala zarar verme ile aynı hukuki değeri koruduğunu kabul ettikleri TCK m. 244 kanun sistematiginde mala zarar verme suçu gibi ikinci kısım onuncu bölümde yer alsaydı, TCK m. 244'deki yazılı suçu işleyenler de şahsi cezasızlık ve etkin pişmanlık hükümlerinden faydalanabileceğini ileri sürmektedirler. Buna örnek olarak, benzer eleştirinin TCK m. 245 için de geçerliken 5377 sayılı Kanun'un 27. maddesi ve 5360 sayılı Kanun'un 11. maddesi ile bu eksiklikler giderilerek faile etkin pişmanlık ve şahsi cezasızlık sebeplerinden yararlanma olanağının getirilmesini vermektedirler. Benzer bir düzenlemenin TCK m. 244 için de getirilmesi uygun olacağını belirtmektedirler³³³.

Biz yukarıda ayrıntılı olarak açıkladığımız gibi bu suçun mala zarar verme suçu ile aynı hukuki değeri koruduğu görüşüne katılmadığımızdan, bu suçlarla toplumun bilişim sisteminin işleyişine güveninin de korunduğundan söz konusu eleştiriye katılmamaktayız.

³³¹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 996.

³³² Handan Yokuş Sevik, **Türk Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018, s. 213.

³³³ Yılmaz, **a.g.m.**, s. 69

Kusurluluğu etkileyen hallerden zorunluluk hali inceleme konusu yaptığımız suçlar için gündeme geleceği düşünülebilir. Zorunluluk halinin uygulanması için kişinin kendisinin veya başkasının hakkına yönelik olarak ağır ve muhakkak bir tehlikeden başka suretle korunmak olağanının bulunmaması gerekmektedir. Bilişim suçları bakımından sistemine ya da verisine müdahalede bulunan kişinin ilgili mercilere başvurarak korunma olanağı bulunduğundan inceleme konusu yaptığımız suçlar bakımından zorunluluk halinin uygulanma olanağının olmadığını söyleyebiliriz.

G. Yaptırım

TCK m. 244/1’de düzenlenen suçu işleyen failin bir yıldan beş yıla kadar hapis cezalandırılması kabul edilmiştir³³⁴. TCK m. 244/2’de düzenlenen suçu işleyen failin ise altı aydan üç yıla kadar hapis cezası ile cezalandırılması gerekmektedir³³⁵.

TCK m. 244/3’e göre bu fiillerin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinden işlenmesi halinde, verilecek ceza yarı oranında artırılacaktır. Bu noktada hâkimin takdir yetkisi bulunmayıp, cezanın 1/2 oranında artırılması gerekmektedir. Bu artırım yapılırken TCK m. 61 gereğince hâkim önce temel cezayı belirleyecek daha sonra ise artırımı yapacaktır³³⁶.

Doktrinde bu fiillerin işlenme sıklığı ve kişi ve toplum bakımından ortaya çıkardığı zararın ağırlığı göz önüne alındığında bu suçlar için öngörülen hapis cezasının alt sınırının az olduğunu ileri süren bir görüş bulunmaktadır. Bu nedenle yapılacak bir değişiklikle hapis cezasının alt sınırının yükseltilmesi isabetli olacağını savunmaktadırlar³³⁷.

³³⁴ Erdoğan, **a.g.e.**, s. 207.

³³⁵ Akbulut, **a.g.e.**, s. 213.

³³⁶ Erdoğan, **a.g.e.**, s. 207.

³³⁷ Koca/Üzülmez, **a.g.e.**, s. 875.

Doktrinde tıpkı dördüncü fıkra gibi hapis cezası ile adli para cezasının birlikte öngörülmesinin suçların niteliği açısından daha isabetli olacağını savunan görüş de bulunmaktadır³³⁸.

Maddede sistemin ister veri yoluyla olsun isterse hareketle olsun işleyişinin engellenmesine yönelik hareketlerin farklı yaptırımlar altında düzenlenmesi doktrinde eleştirilmiştir. Bilişim sisteminin fiziki yanının işleyişinin engellenmesine yönelik ızzar fiilleri için öngörülen ceza miktarı ile bilişim sisteminin yazılımsal yanına yönelik ızzar fiilleri için öngörülen ceza miktarının farklı olması uygulamada sorun çıkarabilir. Bir bilişim sisteminin işleyişini engellemek için bazen sistemi elektrik prizinden çekmek yeterken bu harekete sisteme girerek oradaki verileri özel bilgi gerektiren usullerle yok etmeye oranla daha fazla ceza öngörülmesinin suç siyaseti ile bağdaşmadığını öne sürülmektedir³³⁹.

Öngörülen cezaların türü ve miktarı ne olursa olsun suçların önlenmesi açısından yeterli olduğunu söylemek güçtür. Suçların çoğunlukla uzman kişiler tarafından gerçekleştirilmesi ve tespitinin zor olması, farklı ülkelerde bulunan kullanıcılar tarafından işlenebilmesi kişilerin suç işlemesini engelleneceği beklenirken işlenen suçları artırmaktadır. Ayrıca Bilişim suçlarının sayısı ve ortaya çıkardıkları zarar her geçen gün artmakla beraber, bunların çok az bir kısmı kovuşturma makamlarına intikal etmektedir. Bankalar ve ünlü şirketler bu tür olayları müşterilerinin yanında güvenilmez olarak gözükmek için saklamakta ve sorunu kendi bünyelerinde halletmek yolunu tercih etmektedirler³⁴⁰.

Kanaatimizce günümüzde kişilerin hem toplumsal ilişkilerinde hem de kamusal ilişkilerinde sıkça kullanılan bilişim sistemine ve verilere karşı suçlar için öngörülen hapis cezasının alt sınırının artırılması gerekmektedir.

Faile bu maddeye göre 2 yıldan az hapis cezası verilirse, CMK m. 231'e göre hâkim hükmün açıklanmasının geri bırakılması kararı verebilir. Hükmün açıklanması

³³⁸ Akbulut, **a.g.e.**, s. 213.

³³⁹ Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", s. 409.

³⁴⁰ Akbulut, **a.g.e.**, s. 213.

geri bırakılma kararı verilemezse ve TCK m. 51'deki diğer şartlar varsa erteleme kararı verilebilecektir. Hükmün açıklanması geri bırakılma kararı verilmez ve hükmolunan cezada indirim nedeniyle 1 yılın altına düşerse bu takdirde hâkim yine erteleme yapabileceği gibi TCK m. 50 gereğince ceza seçenek yaptırımlara çevrilebilecektir³⁴¹.

TCK m. 246 gereğince suçun bir tüzel kişinin faaliyeti çerçevesinde ya da temsilci sıfatını taşıyan gerçek kişiler tarafından tüzel kişi yararına işlenmesi halinde tüzel kişi hakkında bunlara özgü güvenlik tedbirleri uygulanır³⁴².

Öngörülen ilk güvenlik tedbiri faaliyet izninin iptalidir. Bunun için ilk koşul özel hukuk tüzel kişisine belirli bir faaliyette bulunabilmesine ilişkin bir kamu kurumunca verilen bir iznin varlığı, ikinci koşul ise bu iznin sağladığı yetkinin kötüye kullanılması suretiyle tüzel kişi yararına kasıtlı bir suç işlenilmesi son koşul ise orantılı olmasıdır. Öngörülen ikinci güvenlik tedbiri ise müsadere'dir. Müsadere hükümlerinin koşulları gerçekleşmiş ise o suçla bağlantılı olan eşya ve maddi çıkarların müsaderesine hükmedilmesi gerekir³⁴³.

H. Soruşturma ve Kovuşturma

İncelenen suçun ceza miktarı ile 5235 s. Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10, 11 ve 12. maddeleri hep birlikte değerlendirildiğinde görevli mahkemenin asliye ceza mahkemesi olduğu görülmektedir³⁴⁴.

Suç şikâyeteye bağlı olmadığından, mağdurun rızası fiil öncesinde elde edilmiş olmalıdır. Fiil sonrası fiili onaylama, fiilden şikayetçi olmama oluşan suçu ortadan kaldırmaz ve suçun soruşturması ve kovuşturmasını engellemez³⁴⁵.

³⁴¹ Erdoğan, **a.g.e.**, s. 207.

³⁴² Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6939.

³⁴³ Kurt, **a.g.e.**, s. 239, 240.

³⁴⁴ Erdoğan, **a.g.e.**, s. 208.

³⁴⁵ Malkoç, **a.g.e.**, s. 1667.

TCK m. 244 1. ve 2. fıkralarında yer alan suçlar re'sen soruşturulur ve kovuşturulur. Bu suçların davasına suçtan zarar gören kişilerin katılması mümkündür. Mağdur, suçtan zarar gören gerçek veya tüzel kişiler kamu davasına CMK m. 237'ye göre katılabilirler³⁴⁶.

Bilişim suçlarının bazen şikâyet üzerine kovuşturulması gündeme gelmektedir. Örneğin, yabancı ülkede bilişim suçu işleyen Türk vatandaşı failin daha sonra Türkiye'ye gelmesi durumunda, suçun takibi şikâyet üzerine yapılır. Vatandaş iade edilemeyeceğinden, yargılanmasının Türkiye'de yapılması gerekmektedir. TCK m. 11'e göre; Türk vatandaşı, 13. maddede yazılı suçlar dışında, Türk kanunlarına göre aşağı sınırı bir yıldan az olmayan hapis cezasını gerektiren bir suçu yabancı ülkede işlediği ve kendisi Türkiye'de bulunduğu takdirde Türk kanunlarına göre cezalandırılması gerekmektedir. Bu halde ise suç hakkında soruşturma ve kovuşturma yapılması şikâyete bağlı değildir. Ancak suç, bir yıldan az hapis cezasını gerektirdiğinde resen soruşturma ve kovuşturma yapılamamakta suçtan zarar gören veya yabancı ülkenin şikâyeti gerekmektedir. Bu halde şikâyet vatandaşın Türkiye'ye girdiği tarihten itibaren altı ay içinde yapılmalıdır. Dolayısıyla incelediğimiz suçlardan 244/2'de düzenlenen suçun cezası da altı aydan başladığından bir yıldan az olduğundan yukarıdaki halde resen soruşturma ve kovuşturma yapılamayacaktır. Dolayısıyla yabancı ülkede suç işleyip Türkiye'ye gelen Türk vatandaşı fail hakkında ancak şikâyet gerçekleşirse soruşturma ve kovuşturma yapılması mümkün olacaktır. Eğer yabancı ülkede işlenen suç 244/1'de düzenlenen bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu ise bu suçun cezasının alt sınırı bir yıldan fazla olduğundan resen soruşturma ve kovuşturma yapılacaktır³⁴⁷.

Yetkili mahkeme ise CMK m. 12'ye göre suçun işlendiği yer mahkemesidir. Suçun işlendiği yerin belirlenmesi ise TCK m 8'e göre yapılır. Bu maddeye göre hareketin kısmen veya tamamen Türkiye'de işlenmesi durumunda suç Türkiye'de işlenmiş sayılır. Örneğin bilişim sisteminin işleyişinin engellenmesi veya bozulması

³⁴⁶ Akbulut, **a.g.e.**, s. 215.

³⁴⁷ Akbulut, **a.g.e.**, s. 215.

veya sistemdeki verilerin yok edilmesi veya bozulması veya deęiřtirilmesi neticeleri kapsamında hareketlerden birinin Trkiye’de gerekleřmiř olması suun iřlendięi yerin Trkiye olmasını ve bylece Trk mahkemelerinin yetkili olması sonucunu doęurur. Verilerin bařka yere gnderilmesi suunda suun iřlendięi yer ve yetkili mahkeme hareket unsuruna gre belirlenecektir. Hareketin gerekleřtirildięi yer, kiřinin fiziki olarak bulunduęu yeri ifade eder. Ancak biliřim sularında kiřinin beden olarak bulunduęu yer ile hareketin aıęa ıktıęı yerler genelde farklı yerlerdir. Bu nedenle her iki yerin de hareket yeri olarak kabul edilmesi gerekmektedir. Bilgisayar aracılıęıyla interneti kullanan kiřinin bu sırada fiziki olarak bulunduęu yer ile zerinde su teřkil eden hareketin gerekleřtirildięi ama aracın bulunduęu yer birbirinden farklı olduęundan her iki yer de hareket yeri olarak kabul edilir. Almanya’dan Trkiye’ye veri gnderilmesi rneęinde veri gnderme hareketi Trkiye’de gerekleřtięinden yetkili mahkemenin Trk mahkemesi olduęu kabul edilir³⁴⁸.

³⁴⁸ Akbulut, **a.g.e.**, s. 216, 217.

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU VE İNCELENEN SUÇLARIN BENZER SUÇLARLA KARŞILAŞTIRILMASI

I. BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU

A. Kanuni Tanım

Sistemi engelleme, bozma, verileri yok etme veya değiştirme
“(4)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.”¹

Doktrinde bazı yazarlar bunun TCK m. 244/1-2 fıkralarında yer alan suçların nitelikli hali olarak kabul etse² de biz bu görüşe katılmıyoruz.

Bilişim sistemlerinin yaygın olarak kullanılması, ekonomik değerin bilgisayar sistemleri içerisinde veri olarak temsil edilmesi olanağı sonucunda bu tür veriler üzerinde bilgisayar sistemleri aracılığıyla işlem yapılması suretiyle ekonomik değerin değişimini olanaklı kılmıştır. Bu tür temsili değişim olanağı, aynı zamanda ekonomik değerin temsil edildiği verilere ya da bu verileri barındıran sistemlerine müdahale aracılığıyla hukuka aykırı olarak ekonomik değerin elde edilmesi olanağını beraberinde getirmiştir³.

¹ Madde gerekçesi TCK m. 244/3 “Üçüncü fıkroda ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.” Tasarıdaki fıkranın iki fıkra haline getirilmesi sonucu meydana gelen teselsül sonucu burada kast edilen 4. fıkradır. Artuç/Bayyurt, **a.g.e.**, s. 403.

² Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 989.

³ Ketizmen, **a.g.e.**, s. 144.

Bilişim sistemleri aracılığıyla çıkar sağlama suçunun hırsızlık, dolandırıcılık gibi suçlardan ayrı olarak düzenlenmesinin temelde iki gerekçesi vardır. Bunlardan ilki hileli ya da aldatıcı hareketlerin gerçek kişiye karşı yapılmaması; ikincisi ise klasik suçlarda maddi varlığı olan şeylerin elde edilmesine karşılık bilişim sistemlerinde sadece verinin ele geçmesi ve verinin de somut bir varlığının olmamasıdır⁴.

Bu gerekçelerle bilgisayar aracılığıyla para ya da diğer ekonomik değerlerin elde edilmesine yönelik bu tür fiillerin etkin olarak cezalandırılabilmesi amacıyla bu fiillere özgü düzenlemeler yapılmıştır. Bilişim sistemleri aracılığıyla yarar sağlama suçu genel olarak malvarlığı kapsamında değerlendirilebilecek bir değer, bilişim ya da bilgisayar sistemlerine müdahale edilmesi yoluyla hukuka aykırı olarak ele geçirilmesi fiillerini kapsayan bir terim olarak karşımıza çıkmaktadır⁵.

TCK m. 244/4'te düzenlenen haksız çıkar sağlama suçunun ilk iki fıkrada düzenlenen suçlarla birlikte aynı madde içinde düzenlenmesi, suçun koruduğu hukuki değerlerin ilk iki fıkralarda düzenlenen suçlardan farklı olması nedeniyle yerinde değildir⁶.

Kanun metni ile gerekçe arasında çelişki bulunmaktadır. Madde metninde “başka bir suç” ifadesi kullanılırken gerekçede “fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması” ifadesine yer verilmiştir⁷. Her ne kadar madde metni ile gerekçesi arasında bir çelişki bulunmakta ise de madde metninin açık olması ve madde gerekçelerinin sadece yol gösterici olması karşısında bir başka suçun ağır veya hafif cezayı gerektirmesine bakılmaksızın esas olan madde metni dikkate alınmalıdır⁸.

TCK m. 244/4 düzenlemesi, 1997 tarihli Türk Ceza Kanunu Tasarısı'nın (m. 348/3) ve cezalar dışında aynı hükümlere yer veren 2003 tarihli Türk Ceza Kanunu

⁴ Erdoğan, **a.g.e.**, s. 266.

⁵ Ketizmen, **a.g.e.**, s. 145.

⁶ Yazıcıoğlu, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, s. 410.

⁷ Bayındır, **a.g.m.**, s. 79; İlker Tepe, “İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku'ndaki Yeni Gelişmeler”, **Alman-Türk Karşılaştırmalı Ceza Hukuku**, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi, İstanbul, 2010, C. I, s. 284.

⁸ Mermut/Alpaslan, **a.g.m.**, s. 134; Taşkın, **a.g.e.**, s. 57; Ketizmen, **a.g.e.**, s. 177; Yılmaz, **a.g.m.**, s. 87; Dülger, **a.g.e.**, s. 340.

Tasarısının (m. 347/3) bazı değişikliklerle değiştirilerek kanunlaştırılmış halini oluşturmaktadır⁹.

765 sayılı TCK m. 525b/2’de “*Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyon liradan yirmi milyon liraya kadar ağır para cezası verilir...*” denilmek suretiyle söz konusu suç düzenlenmiştir¹⁰.

525/b-2’nin geniş yorumu açık olması sebebiyle 1997 ve 2003 tarihli Türk Ceza Kanunu Tasarılarını hazırlayan komisyon, bilişim sisteminin işlemlerini etkileyen hareketleri ayrı bir suç haline getirerek ve bunları haksız çıkar sağlama suçunun unsuru kapsamına alarak ve ayrıca ikinci fıkrada verilere müdahale teşkil eden ve suç oluşturan fiilleri haksız çıkar sağlamanın unsuru niteliğine sokarak sınırlandırma yoluna gitmiştir. 765 sayılı TCK döneminde de kanunilik ilkesine aykırılık niteliği taşıması dolayısıyla ve hangi hallerde fiilin suç oluşturacağı açıklanmayan böyle bir düzenlemenin belirlilik ilkesine aykırılık taşıdığı belirtiliyordu. Yapılan bu yeni düzenleme ile kanun koyucu bu hususları aşmaya çalışmış, fiiller açıkça gösterilerek suçun sınırları çizilmiştir¹¹. 765 sayılı TCK’nın 525/b-2 maddesi aslında 5237 sayılı TCK ile dörde bölünmüştür. 525/b-2 maddesinin içerdiği bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlamak, banka ve kredi kartlarını kötüye kullanmak, bilişim sistemleri aracılığıyla dolandırıcılık ve hırsızlık fiilleri farklı suç tipleri olarak düzenlenmiştir¹².

Avrupa Konseyi Siber Suç Sözleşmesi’nin “bilgisayarla bağlantılı dolandırıcılık” başlıklı 8. maddesinde bu suçun karşılığı düzenlenmiştir. İlgili maddeye göre; “*şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekarlık niyetiyle bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme, engelleme veya bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunmak kasten ve haksız gerçekleştirildiğinde ve başka bir şahsın*

⁹ Akbulut, **a.g.e.**, s. 218.

¹⁰ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6937.

¹¹ Akbulut, **a.g.e.**, s. 219.

¹² Erdoğan, **a.g.e.**, s. 247.

mal kaybına sebebiyet verdiğinde cezalandırılacaktır.” Sözleşmede yer alan sisteme veri girişi yapma, verileri değiştirme, silme veya engelleme TCK m. 244/4 kapsamında değerlendirilir. Sistemin işleyişine herhangi bir müdahalede bulunmak suretiyle fiilin gerçekleştirilmesi ise geniş bir ifadedir. Sisteme yapılacak müdahale ile sistemin işleyişi engellenmese veya bozulmasa bile yarar sağlanması ve mal kaybına neden olunması halinde suç gerçekleşmiş olacaktır. 5237 sayılı TCK m.244/4’te sözleşmede yer alan suçun maddi menfaat sağlamak amacıyla gerçekleştirilmesi aranmamış onun yerine haksız çıkar sağlanması aranmıştır. Çıkarın maddi nitelikte olup olmamasının bir önemi yoktur. Yine sözleşmede yer alan mal kaybı yani zarara neden olunması ise TCK m. 244/4’te yer almamıştır. Sözleşmede yer alan hile ve sahtekârlık saiki de TCK m. 244/4’te yer bulmamıştır. Haksız çıkar sağlama ve kasten fiilin gerçekleştirilmesi ise hem sözleşmede hem de TCK m. 244/4’te ortak olan kısımdır¹³.

Avrupa Siber Suç Sözleşmesi’nin 8. maddesinde kendisine veya bir başkasına haksız menfaat sağlamak amacıyla veriler üzerinde etkide bulunan ya da bilişim sisteminin işleyişini engelleyen kişilerin fiillerinin cezalandırılması istenmektedir. Kanun koyucu TCK m. 244/4 hükmüyle Sözleşme ile ulusal mevzuat arasında paralellik sağlamaya çalışmıştır¹⁴.

B. Korunan Hukuki Değerler

Doktrinde bir görüşe göre, bu suç verilere ve bilişim sisteminin işleyişine müdahale ederek haksız çıkar sağlamak suretiyle işlendiğinden malvarlığına karşı işlenen suçlar kapsamındadır. Bu nedenle korunan hukuki değer malvarlığı olduğunu savunmaktadır¹⁵. Zira bilişim sistemi malvarlığı değerine yönelik olarak saldırıda bir araç olarak kullanılmaktadır. Bu suçla malvarlığı değerinin yanı sıra 244. maddenin 1. ve 2. fıkralarının koruduğu hukuki değerlerin de birlikte korunduğunu belirtilmektedir¹⁶.

¹³ Akbulut, **a.g.e.**, s. 220.

¹⁴ Artuk/Gökcen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6937.

¹⁵ Akbulut, **a.g.e.**, s. 230.

¹⁶ Koca/Üzülmez, **a.g.e.**, s. 881.

Korunan hukuki değer kişilerin özel hayatlarının gizliliğinden malvarlığı haklarının korunmasına kadar genişleyebilecek niteliktedir. Genel olarak söylemek gerekirse bilişim sistemlerine haksız müdahalede bulunarak kişilerin maddi ve manevi haklarına yapılan saldırılar önlenmek istenmiştir¹⁷.

765 sayılı TCK m. 525/b-2’de düzenlenen “*“bilişim sistemi aracılığıyla hukuka aykırı yarar sağlamak suçu”* ile korunan hukuki değer konusunda öğretide çeşitli tartışmalar bulunmaktaydı çünkü bu suç tipi ile birden fazla suç tipi düzenlenmekteydi. Yeni kanun ile “*“bilişim sistemleri aracılığıyla hukuka aykırı yarar sağlamak suçu”* bakımından benzer tartışmaların olması mümkün değildir, zira bu suç tipi diğer suç tiplerinden ayrılmış ve maddi unsurunu oluşturan fiiller tek tek gösterilmiştir. Bu suç tipinin yeni düzenlemesi karşısında suçla korunan hukuki değer de mağdurun hem manevi hem de maddi hakkıdır¹⁸.

Bu suçla suçun işleniş biçimlerine göre zilyetlik, üçüncü kişilerin iyi niyetleri ve maddi ya da manevi haklarının korunduğu belirtilmektedir¹⁹. Bilişim sistemleri veya verilerin zarar görmesi kişinin malvarlığında bir azalma meydana getireceği gibi toplumun, bilişim sistemlerinin işleyişine olan güvenleri ve ekonomik düzenin sağlıklı işleyişi etkilendiği bilişim sistemlerinin zarar görmeden işler durumda bulunmasında toplumsal yarar olduğu için bu suç topluma karşı suçlar kısmında düzenlenmiştir²⁰.

Bilişim sistemi ya da verilere müdahale ile çıkar sağlanması verilerin kişi ya da mal olarak kabul edilemeyecek olunması nedeniyle dolandırıcılık gibi hükümlerin uygulama alanı bulamamasından kanun koyucu bu düzenlemeyi yapmış ve boşluk olmaması için bu hükmü yardımcı norm olarak değerlendirerek fiilin başka bir suça sebebiyet vermesi halinde bu hükmün uygulanmayacağını belirtmiştir. Bu nedenle bu fıkra ile gerçek ya da tüzel kişi, maddi ya da manevi menfaat ayrımı yapmaksızın her türlü değer koruma altına alındığını söyleyebiliriz²¹.

¹⁷ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6938; Dönmezer, **a.g.e.**, s. 622.

¹⁸ Dülger, **a.g.e.**, s. 342, 343.

¹⁹ Parlar/Hatipoğlu, **a.g.e.**, s. 3476.

²⁰ Parlar, **a.g.e.**, s. 25.

²¹ Erdoğan, **a.g.e.**, s. 251.

Bu suç bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemdeki verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi, erişilmez kılınması, değiştirilmesi ve yok edilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlamasıyla işlenebilir. Haksız çıkarın ise yalnızca maddi olması gerektiğini ileri süren görüşe katılmadığımızdan bu suçla korunan hukuki değerın mağdurun hem maddi hem de manevi haklarını olduđu görüşüne katılmaktayız.

C. Suçun Unsurları

1. Maddi Unsurlar

a. Suçun Konusu

Doktrinde bir görüş suçun konusunu bilişim sistemi veya bu sistemde bulunan veriler olarak kabul etmektedir. Fail bu sistem veya veriler üzerinde gerçekleştirdiği fiil sonucunda haksız menfaat elde eder. Suçun bu nedenle zarar suçu olduğunu kabul etmektedirler²².

Suçun konusunu malvarlığına ilişkin herhangi bir değer olarak açıklayan görüş de bulunmaktadır. Bu görüşteki yazarlar konuyu, suçun malvarlığına karşı işlenen suçlardan olması ve suçun oluşması için çıkar sağlanması gerektiğinden suçun konusunun da çıkarı oluşturan ve malvarlığı kapsamına giren her türlü değer olarak belirtmektedirler²³.

Doktrinde bir görüş de bu suçun konusunu “*haksız şekilde sağlanan çıkar*” olduğunu belirtir. Çıkar TDK’da “dolaylı bir biçimde elde edilen kazanç, menfaat, yarar” olarak tanımlanmıştır. Çıkarın mutlaka para, eşya gibi maddi varlığı olan bir kazanç şeklinde olması gerekmez. Kişilerin ekonomik durumunda doğrudan ya da dolaylı olarak iyileşme oluşturacak herhangi bir menfaat ya da yarar suçun konusunu

²² Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s. 893.

²³ Akbulut, **a.g.e.**, s. 234.

oluşturabilir. Failin kendisinin ya da başkasının malvarlığında artışa veya borçlarında azalmaya neden olan her türlü kazanç bu suça konu olabilir. Örneğin bilişim sistemine yaptığı haksız müdahale sebebiyle işe alınması, işinde terfi etmesi, bir ihaleyi kazanması gibi hallerde çıkar sağlandığını söyleyebiliriz. Ekonomik olarak ölçülmeyip yalnızca kişilerde manevi tatmin duygusu meydana getiren haz veya manevi yararın da bu suça konu olamayacağını savunmaktadırlar²⁴. Diğer görüş ise maddi ve manevi her türlü çıkarın madde kapsamında olduğunu kabul etmektedir²⁵. Bu görüşe göre, yarar ekonomik değeri olan mali bir yarar olabileceği gibi ekonomik bir getirisi ve değeri olmayan tamamen duyguları tatmine yönelik manevi bir yarar da olabilir²⁶.

Haksız çıkarın ise daha önce de belirttiğimiz gibi mutlaka maddi nitelikte olması şart değildir. Örneğin bir öğrencinin okulunun sistemine girerek sınav sorularını çalması ya da notlarını düzeltmesi durumunda fail maddi olarak bir şey kazanmamakta ancak bu fiilleri haksız manevi çıkar yerine geçmektedir²⁷.

Kanaatimizce suçun konusu suçun üzerinde gerçekleştiği şey olan bilişim sistemi ve verilerdir. Failin çıkara yönelik gerçekleştirdiği hareketler sonucunda haksız çıkar elde etmesi ile suç tamamlanmış olmaktadır.

Failin kendisine veya başkasına çıkar sağlaması suçun oluşması açısından yeterlidir. Mağdurun ayrıca bu fiil nedeniyle zarara uğraması aranmasa da failin kendisinin veya başkasının yararına çıkar sağlaması suretiyle suç işlendiğinden bu suçun zarar suçu olduğu kabul edilmektedir²⁸.

Suçun oluşması için mağdurun zarara uğraması gerektiğini savunan görüş de bulunmaktadır. Failin sağladığı yarar maddi ya da manevi olduğu gibi mağdurun uğradığı zarar da maddi veya manevi olabilir. Bu madde kapsamında yapılan her

²⁴ Koca/Üzülmez, **a.g.e.**, s. 881.

²⁵ Yazıcıoğlu, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, s. 410; Parlar/Hatipoğlu, **a.g.e.**, s. 3479; Dülger, **a.g.e.**, s. 341; Malkoç, **a.g.e.**, s. 1682; Erdoğan, **a.g.e.**, s. 255.

²⁶ Dülger, **a.g.e.**, s. 343; Meran, **a.g.e.**, s. 573.

²⁷ Kurt, **a.g.e.**, s. 175; Mahmut Koca, “Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları”, **Prof. Dr. Ali Güzel’e Armağan**, C. II, İstanbul, Beta Yayıncılık, 2010, s. 1659; Eker, **a.g.m.**, s. 127; Meran, **a.g.e.**, s. 573.

²⁸ Koca/Üzülmez, **a.g.e.**, s. 876; Akbulut, **a.g.e.**, s. 235; Erdoğan, **a.g.e.**, s. 260.

saldırının otomatik olarak toplum nazarında güvenirliliğin sarsılmasından dolayı zarar sonucu doğuracağını kabul etmektedir²⁹.

Suçu tehlike suçu olarak kabul eden görüşe göre, kanun maddesinde fail tarafından gerçekleştirilen fiil sonucunda hukuka aykırı bir yararın elde edilmesinin gerekliliği belirtilmişken fiil sonucunda bir zararın ortaya çıkmasının gerektiğinden bahsedilmemiştir. Fiil neticesinde bir zararın oluşması kaçınılmazdır ancak maddenin ilk iki fıkrasında düzenlenen suçlardan farklı olarak failin kastı burada sisteme ya da verilere zarar vermek değil hukuka aykırı yarar sağlamaktır. Dolayısıyla netice açısından incelenen zarar kavramı bu hukuka aykırı yarar elde edildikten sonra mağdurda bir zararın meydana gelip gelmediğidir yoksa bilişim sistemi ya da veriler üzerinde bir zararın oluşup oluşmadığı tartışma konusu değildir. Suç tipi aynı fiilleri içermesine rağmen ilk iki fıkrada düzenlenen suçlardan farklı olarak hukuka aykırı yarar sonucunda mağdurda bir zararın oluşup oluşmadığına bakılmamasından dolayı zarar suçu değil tehlike suçu olarak kabul edilmektedir. Suçun oluşması bakımından failin hukuka aykırı yarar elde etmiş olması aranacak, ancak bunun sonucunda bir zararın ortaya çıkıp çıkmadığı konusu dikkate alınmayacağını belirtilmiştir³⁰.

Kanaatimizce her ne kadar kanun metninde açık olarak mağdurun zarara uğranması aramasa da failin kendisine veya başkasına haksız çıkar sağlamasıyla suç oluşacağından bu suç zarar suçudur. Haksız çıkar sağlanması ile en azından toplumun bilişim sistemlerine duyduğu güven azalmaktadır. Haksız çıkar sağlanması ile sistem veya veri sahibinin zarara uğrayacağı ise açıktır.

b. Fiil

Bu suçun gerçekleşmesi için ilk olarak TCK m. 244/1 veya m. 244/2’de tanımlanan bilişim sisteminin işleyişinin engellenmesi veya bozulması ya da verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi,

²⁹ Erdoğan, **a.g.e.**, s. 254.

³⁰ Dülger, **a.g.e.**, s. 349; Gül, **a.g.e.**, s. 89.

erişilmez kılınması, değiştirilmesi ve yok edilmesi fiillerinden en az birini gerçekleştirilmesi gerekmektedir.

TCK m. 244/4 bağlı hareketli bir suçtur. Haksız çıkarın maddenin ilk iki fıkrasındaki fiillerin işlenmesi suretiyle yani bilişim sistemlerinin engellenmesi veya sistemdeki verilerin bozulması, değiştirilmesi veya başka yere gönderilmesi suretiyle sağlanması gerekir³¹.

Bilişim sistemi aracılığıyla yarar sağlama suçunu oluşturabilecek fiiller iki başlık altında toplanabilir. Bunları verilere veya programlara müdahale aracılığıyla işlenen yarar sağlama halleri olarak belirlemek mümkündür. Verilere müdahale yoluyla yarar sağlama, bilgisayar sistemi içerisinde yer alan verilerin değiştirilmesi, erişilmez kılınması, silinmesi veya sisteme yeni veriler eklenmesi şeklinde olabilmektedir. Programlara müdahale yoluyla yarar sağlama ise, bilgisayar sistemleri içerisinde var olan programa müdahale edilmesi ya da daha önce olmayan bir program eklenmesi yoluyla olabilmektedir³².

Verilerin değiştirilmesi suretiyle hukuka aykırı yarar sağlamak fiiline örnek olarak manyetik telefon kartlarının üzerindeki verilerin değiştirilmesi suretiyle ücret ödemeksizin telefon görüşmesi yapılması gösterilebilir. Burada bilişim sistemleri kavramını dar yorumlayarak telefon kartlarını işleten sistemin buna dâhil olmadığı düşünülebilirse de bu isabetli değildir. Nitekim bilişim sistemlerini ya da bilgisayarları dar tanımlamak günümüz teknolojisinin eriştiği aşama itibariyle bu aygıtları sınırlamak anlamına gelmektedir. Günümüzde belli bir işi yapmaya özgülenmiş çok gelişmiş bilgisayarlar bulunmaktadır. Bunların TCK açısından bilişim sistemi sayılmaması ve bu aygıtlar aracılığıyla ya da bunlara karşı işlenen suçlara uygulanmaması pek çok hukuka aykırı fiilin yaptırımsız kalması anlamına gelmektedir. Aslında telefonları işleten sistem de belli bir alana özgülenmiş gelişmiş bir bilişim sistemidir³³.

³¹ Koca/Üzülmez, **a.g.e.**, 876; Akbulut, **a.g.e.**, s. 234.

³² Ketizmen, **a.g.e.**, s. 146.

³³ Dülger, **a.g.e.**, s. 344, 347.

Fiil ya doğrudan ya da dolaylı bir çıkarın sağlanmasına yöneliktir. Doğrudan çıkar sağlanmasına bir banka hesabından başka bir hesaba hukuka aykırı olarak para transferini, dolaylı çıkar sağlanmasına da ücreti karşılığında yararlanabilen bir hizmetten başkasına ait şifreleri ele geçirerek yararlanılması ve hizmet bedelinin üçüncü kişiye ödettirilmesi örnek olarak verilebilir³⁴.

c. Netice

TCK m. 244/1 ve m. 244/2’de yer alan fiillerin icrasıyla birlikte “haksız çıkar sağlama” neticesinin elde edilmesi halinde suç tamamlanır³⁵. Bu nedenle suç neticeli suç olma özelliği taşır³⁶.

Failin bu fiilleri işlemek suretiyle kendisine ya da başkasına haksız bir çıkar sağlama gerekmektedir. Ayrıca bilişim sistemine veya verilere yönelik fiillerle kazanılan çıkar arasında bir bağlantının olması gerekir. İlk iki fıkradaki fiiller kendisine ya da başkasına haksız çıkar sağlama amacıyla işlenmelidir³⁷.

Sağlamak, haksız çıkarın failin veya başkasının tasarruf alanına sokulması ya da söz konusu haksız çıkar üzerinde tasarruf edebileceği imkâna kavuşmasıyla gerçekleşir. Örneğin suçun konusunu paraysa, bu paranın failin veya başkasının hesabına ya da cüzdanına geçmesiyle haksız çıkar sağlama unsuru gerçekleşir. Bir başka örnek olarak 244. maddenin ilk iki fıkrasındaki fiiller ile iş imkânına kavuşmasıyla çıkar sağlama unsurunun gerçekleştiğini söyleyebiliriz³⁸.

Kanun metninden de açıkça görüleceği üzere çıkar kendi yararına sağlanabileceği gibi başkasının yararına da sağlanabilir. Çıkarın maddi yararları mı içerdiği yoksa bunun dışından elde edilen yararları da kapsayıp kapsamadığı tartışmalıdır.

³⁴ Ketizmen, **a.g.e.**, s. 146.

³⁵ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6938; Erdoğan, **a.g.e.**, s. 252.

³⁶ Yılmaz, **a.g.m.**, s. 88.

³⁷ Koca/Üzülmez, **a.g.e.**, 876; Akbulut, **a.g.e.**, s. 234, 235.

³⁸ Koca/Üzülmez, **a.g.e.**, 876; Akbulut, **a.g.e.**, s. 234.

Doktrinde bilişim sistemi aracılığıyla haksız çıkar sağlama suçunu malvarlığı aleyhine bir suç olarak kabul eden görüş, suçun konusunu malvarlığını oluşturan herhangi bir değer olduğundan bahisle çıkarın da ekonomik nitelikte olması gerektiğini savunmaktadır. Ekonomik nitelikte olmayan çıkarın bilişim sistemi aracılığıyla haksız çıkar sağlama suçunun oluşmayacağını, unsurları varsa TCK m. 244/1 veya m. 244/2'in gerçekleştirilebileceğini, diğer suçların kapsamına giren fiillerin olması durumunda ise ilgili suçların işlenebileceğini kabul etmektedirler³⁹.

Hukuka aykırı her türlü menfaat haksız çıkardır⁴⁰. Nitekim bu yönde Yargıtay 6. Ceza Dairesi'nin 1.4.2002 tarihli 2002/3301 Esas 2002/4105 Karar sayılı kararında Tedaş'ta görevli olan sanığın kendisine ve 30 kişiye ait elektrik faturalarına bilgisayardaki kayıtları silmek veya ödenmediği halde ödendi şeklinde değiştirmek suretiyle gerçekleşen fiilin fatura borcunu sildiği için her kişi için ayrı ayrı TCK m. 525/b-2'de düzenlenen suçu oluşturduğunu kabul etmiştir⁴¹.

Yargıtay ise çıkarın mutlak surette maddi nitelikte olmasını aramamıştır. Verdiği bir kararda, alkol muayenesine yapılan itiraz üzerine hastaneye götürülen kişinin ceza almasını ve ehliyetine el konulmasını engellemek amacıyla hastane otomasyonuna müdahale etmesini ve verilerle oynama yapmasını TCK m. 244/4 kapsamında değerlendirmiştir⁴².

Çıkarın sağlanmış olması için çıkarın fiilen elde edilmesine gerek yoktur. Fail çıkar üzerinde hakimiyet kurmuş, yani onun üzerinde tasarruf edebilir duruma gelmişse suç tamamlanmış demektir⁴³.

Çoğunlukla büyük ekonomik değeri olan ve kullanıcısı tarafından uzun sürede ve büyük bir emekle geliştirilen oyun karakterlerinin başka kişi tarafından asıl

³⁹ Akbulut, **a.g.e.**, s. 254.

⁴⁰ Meran, **a.g.e.**, s. 573.

⁴¹ İsmail Ergün, "Yeni Türk Ceza Kanunu'nda Bilişim Suçları", **2. Polis Bilişim Sempozyumu Bildirileri**, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s. 27.

⁴² Akbulut, **a.g.e.**, s. 253. (Yargıtay 11. Ceza Dairesi'nin 15.01.2013 tarih 2010/12162 Esas 2013/658 Karar numaralı kararı)

⁴³ Akbulut, **a.g.e.**, s. 255.

kullanıcısının şifre değişimi gibi yollarla sisteme girişinin engellenerek geliştirilen karakterin failin kendisinin kullanması da bu suçu oluşturur. Yargıtay 13. Ceza Dairesi'nin 2014/25309 Esas 2015/10302 Karar sayılı 03.06.2015 tarihli kararı bu görüşümüzü destekler niteliktedir; *“sanığın öncesinden tanıştığı müşterinin askere gitmesini fırsat bilerek şifresini kırarak oyun sitesine girmesi, sonrasında müşterinin ablası tanık Sevgi'nin telefonunu öğrenerek tanığa sanki kardeşi müşteriki imiş gibi mesaj atıp oyundaki carlarını sattığını, bir arkadaşının telefonundan mesaj çekmekte olduğunu, e-postadan carlarının satışına onay vermesini istemesi, ablası tanığın da mesaj atanın kardeşi müşteriki olduğunu sanarak gelen e-posta mesajını onaylaması ile müşterinin oyundaki 2000-TL değerindeki carlarının sanığın hâkimiyet alanına geçmesi şeklinde tarif edilen eylemin küll halinde TCK'nın 244/2-4'üncü maddesine uyduğu halde...”*⁴⁴

Yargıtay birçok kararında aynı şekilde oyun karakterinin bağlı olduğu e-posta hesabına girişin engellenmesi suretiyle karakterin ele geçirilmesi fiilini TCK m. 244/4'e uygun olduğunu kabul etmiştir⁴⁵.

Ancak bunun aksine kararlar da bulunmaktadır. Yargıtay 8. Ceza Dairesi'nin 17.02.2016 gün 2015/14257 Esas 2016/1702 Karar sayılı kararında; *“...oyun sitesine girerek katılanın gerek ücreti karşılığında gerekse level atlama şeklinde kazandığı oyun karakterlerini ele geçirmek şeklindeki eylemin, sübutu halinde bilişim suretiyle hırsızlık suçunu oluşturacağı...”* şeklinde karar vermiştir⁴⁶.

Kanaatimizce her ne kadar ekonomik değeri olsa da oyuncuların kendi emekleriyle geliştikleri oyun karakterlerinin hukuka aykırı olarak ele geçilerek bundan haksız kazanç sağlaması olaylarında bilişim sistemleri kullanılarak haksız çıkar

⁴⁴ www.corpus.com.tr (Çevrimiçi) 22.02.2019.

⁴⁵ Yargıtay 13. Ceza Dairesi'nin 2016/2155 Esas 2017/10403 Karar sayılı 10.10.2017 tarihli kararı; *“Katılanın 23.10.2011 tarihinde internette Knight Online isimli oyunu oynarken bilgi ve rızası dışında eposta adresine girilerek şifresinin ve e-posta adresinin değiştirildiğini ve oyun karakterlerinin çalındığını...Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği, bu itibarla; suçun sübutu halinde eylemin, 5237 sayılı TCK'nın 244/4. maddesindeki suçu oluşturacağı gözetilmeksizin suç vasfında yanılığa düşülerek yazılı şekilde hüküm kurulması,”*

⁴⁶ Gül, a.g.e., s. 90.

sağlama suçu oluşmaktadır. Her ne kadar büyük maddi değerleri olsa da bu karakterler sonuç olarak halen veri yığını niteliklerini korumaktadırlar.

d. Fail

Herhangi bir özellik göstermediğinden sistemin işleyişini bozan, engelleyen, verileri yok eden, değiştiren, veri yerleştiren, başka yere veri gönderen ya da bu yolla haksız çıkar sağlayan herkes bu suçun faili olabilir⁴⁷.

Suçun faili, veriler üzerinde tasarruf yetkisine sahip olmayan kişi, sistemin sahibi olmayan kişi ya da kullananın dışındaki herhangi bir kişi olabilir. Eğer veriler üzerinde tasarruf yetkisine sahip kişi ile sistemin sahibi farklı kişi ise sistem sahibi de haksız çıkar sağlaması koşuluyla bu suçun faili olabilir. Tasarruf yetkisine sahip olmayıp sadece kullanım yetkisine sahip kişi de bu suçun faili olabilir. Sistemin sahibi ile sistem kullanıcısının farklı olması durumunda sistemi kullanma yetkisine sahip kişi de bu suçu işleyebilir⁴⁸.

TCK m. 246 gereğince suçun bir tüzel kişinin faaliyeti çerçevesinde ya da temsilci sıfatını taşıyan gerçek kişiler tarafından tüzel kişi yararına işlenmesi halinde tüzel kişi hakkında bunlara özgü güvenlik tedbirleri uygulanır⁴⁹.

TCK m. 246 ile Avrupa Konseyi Siber Suç Sözleşmesi'nde öngörülen kurumsal yükümlülükler önerisine somut bir düzenleme ile uygulanabilirlik kazandırılmıştır. Güvenlik tedbirlerinin uygulanabilmesi için suç teşkil eden fiillerin ilgili tüzel kişiye haksız menfaat sağlaması, fiil ile tüzel kişi arasında nedensellik bağının olması gerekmektedir. Avrupa Konseyi Siber Suç Sözleşmesi'nde olan suçun tüzel kişinin yetkili bir yöneticisi veya çalışanı tarafından yetkilerinin kullanılması sırasında işlenmesi şartları da TCK m. 60 ile tutarlılık arz etmektedir⁵⁰.

⁴⁷ Gül, **a.g.e.**, s. 83

⁴⁸ Akbulut, **a.g.e.**, s. 231.

⁴⁹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6939.

⁵⁰ Eker, **a.g.m.**, s. 132.

e. Mağdur

Failin müdahale ederek haksız menfaat sağladığı bilişim sistemi ya da verinin sahibi suçun mağdurudur⁵¹.

Sağlanan çıkar sonucunda maddi veya manevi hakları zarara uğrayan kişi suçun mağdurudur. Bilişim sistemi aracılığıyla haksız çıkar sağlama suçunun, TCK m. 244/1 ve m. 244/2’de yer verilen fiillerin işlenmesi suretiyle gerçekleşmesi gerektiğinden buna göre belirleme yapılması gerekmektedir. Hakları zarara uğrayan kişi ile işlemlerin yapılmasını sağlayan bilişim sisteminin sahibi veya verilerin tasarruf yetkilisi farklı kişiler olabilir. Her iki kişinin de aynı kişi olması durumunda herhangi bir sorun olmayıp söz konusu kişi suçun mağdurudur. Ancak ayrı kişi olmaları durumunda bilişim sisteminin işleyişi engellenen veya sistemdeki verileri zarar gören kişiler de suçun mağduru konumundadırlar⁵². Örneğin bilişim sisteminde yer alan programda manipülasyon yapılarak haksız çıkar sağlanmışsa ve program sahibiyle maddi haklarında azalma olan kişi farklı kişilerse her ikisi de suçun mağduru olacaktır⁵³.

Bu suçun mağdurunu bilişim sisteminin maliki ya da zilyediyle sınırlamak mümkün değildir, çünkü özellikle verilere zarar verilerek hukuka aykırı yarar sağlanması durumunda zarara uğratılan verilerin maliki ile verilerin üzerinde kayıtlı olduğu bilişim sisteminin ya da veri taşıma aracının maliki aynı kişiler olmayabilir. Hatta mağdur olmak için zarara uğratılan verilerin maliki olunması bile şart değildir, bir şekilde verinin ilgilisi olmak suçun mağduru olmak için yeterlidir⁵⁴.

Doktrinde bir görüşe göre, internet üzerinden bankadaki hesaptan başka bir hesaba havale yapılması durumunda bankadaki hesabından havale yapılan kişi, suçun mağdurudur. Banka ise suçtan zarar gören konumundadır⁵⁵.

⁵¹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6939.

⁵² Koca/Üzülmez, **a.g.e.**, s. 881.

⁵³ Akbulut, **a.g.e.**, s. 233.

⁵⁴ Dülger, **a.g.e.**, s. 342.

⁵⁵ Akbulut, **a.g.e.**, s. 233.

Aynı şekilde internette yayınlanan bir sanal ekonomi gazetesindeki sistemdeki veriler değiştirilerek bir ticari şirket hakkındaki olumlu haberlerin olumsuz haberlere dönüştürülmesi sonucu şirketin hisse senetlerinin menkul değerler borsasında aniden değer kaybetmesi ya da bu haber yüzünden şirketin bir krediyi alamaması durumunda da şirketin hissedarları mağdur konumunda olduğu gibi şirketin kendisi de suçtan zarar gören konumunda olur⁵⁶.

2. Manevi Unsurlar

Suçun işlenmesi için kast yeterlidir. Fail ilk iki fıkrada belirtilen sonuçlarla birlikte çıkar sağlayacak hareketleri bilerek ve isteyerek gerçekleştirmesi gerekir⁵⁷.

Doktrinde bir görüşe göre, 244. maddenin dördüncü fıkrasında “*Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde*” denilerek, failin bu fiilleri kendisinin veya başkasının yararın haksız bir çıkar sağlamak maksadıyla işlemesinde amaç söz konusudur⁵⁸. Bu görüşe göre failin sağladığı çıkarın haksız olduğunu bilmesi gerekmektedir. Çıkarın haksızlığına ilişkin bilgi kastın kapsamında değerlendirilmesi gerekmektedir⁵⁹. Bu görüşe göre, suçun oluşabilmesi için failin maddi unsurların hepsine ilişkin bilgisinin bulunması gerekir. Fail başkasının bilişim sistemini engellediğini, bozduğunu veya sistemdeki verilere bozmak, değiştirmek veya başka yere göndermek suretiyle zarar verdiğini, bu fiilleri işlemek suretiyle kendisine veya başkasına çıkar sağladığını ve zaten bu fiilleri de kendisine çıkar sağlamak maksadıyla icra ettiğini ve çıkarın da haksız olduğunu bilmelidir⁶⁰.

Diğer görüşe göre, kast unsurunun dışında ayrıca bir amaç unsuru aranmamaktadır. Bu görüşe göre suç tipinde yer alan “ *kişinin kendisinin veya*

⁵⁶ Dülger, **a.g.e.**, s. 343.

⁵⁷ Erdoğan, **a.g.e.**, s. 257.

⁵⁸ Karagülmez, **a.g.e.**, s. 240; Gül, **a.g.e.**, s. 88.

⁵⁹ Koca/Üzülmez, **a.g.e.**, s. 883.

⁶⁰ **A.e.**

başkasının yararına haksız çıkar sağlama” ifadesi suçun maddi unsurunda yer alan neticeye yöneliktir. Kanun koyucu failin gerçekleştirdiği fiilin dışında ayrıca kendisinin veya başkasının yararına haksız çıkar sağlama neticesinin gerçekleştirmesini aramış failin hangi amaçla hareket ettiğini önemsemediğini belirtmiştir. Failin böyle bir amacı olmaksızın örneğin sırf mağdurun bilişim sistemine zarar vermek amacıyla hareket etmesi ancak bu zararın sonucunda müşterilerin çökertilen siteye giremeyip failin sahibi olduğu siteye yönelip buradan alışveriş yapması durumunda failin bundan bir yarar elde etmesi halinde TCK m. 244/4 uygulanması gerektiğini savunmaktadır. Buna gerekçe olarak da suç tipinde failin amacı değil, fiil sonucunda gerçekleşen neticenin suçun oluşması için arandığını belirtmektedir⁶¹.

Kanaatimizce suçun oluşması için ayrıca amaç unsuru aramayan ikinci görüş isabetlidir. Faildeki suç işlemeye yönelik kast suçun manevi unsurunu oluşturmaktadır. Haksız çıkar sağlanması neticeyi ifade etmektedir. Netice olduğu için failin bilgisi kast kapsamındadır, ayrıca amaç unsuru suçun oluşması bakımından aranmamaktadır.

Hukuka aykırı hukuken tasvip edilmeyen her türlü menfaat haksız çıkar kapsamındadır. İlk görüş çıkarın haksızlığına ilişkin bilgi kastın kapsamında incelendiğinden suçun olası kastla işlenemeyeceğini savunmaktadır⁶².

Bizim de katıldığımız kast dışında ayrıca bir amaç unsurunun aranmadığını savunan görüşe göre, olası kastın uygulanma imkânı bu suçta bulunmakta ve öğretmenin bilişim sistemine giren bir kişinin pekâlâ öğrencilik statüsünü etkileyecek verileri de görebileceğini öngörmesine rağmen hareketine devam etmesi nedeniyle faile dördüncü fıkra olası kast hükümleri çerçevesinde uygulanabileceğini savunmaktadırlar⁶³.

⁶¹ Dülger, **a.g.e.**, s. 351.

⁶² Koca/Üzülmez, **a.g.e.**, s. 883.

⁶³ Erdoğan, **a.g.e.**, s. 258.

3. Hukuka Aykırılık Unsuru

Suçun kanuni tanımındaki unsurların gerçekleşmesiyle hukuka aykırılık unsuru da karine olarak gerçekleştirmiş sayılır. Fiilin işlenmesini hukuka uygun hale getiren bir sebebin bulunduğu hallerde suçun oluştuğundan söz edilemez. Kanun hükmünün icrası ve ilgilinin rızası bu suç için uygulanabilecek hukuka uygunluk sebeplerindendir⁶⁴. Her somut olayda rızayı verenin rıza vermeye yetkisi olup olmadığı araştırılmalıdır⁶⁵.

Failin yarar sağladığı hareketleri bir rızaya dayanarak gerçekleştirdiği hallerde suç oluşmaz, çünkü kanunda suçun oluşması için failin elde ettiği yararın haksız olması aranmıştır, rızanın varlığı halinde bu hukuka aykırılık ortadan kalkar. Fiili hukuka uygun hale getirecek rızanın yalnızca bilişim sisteminin maliki tarafından verilmesi her zaman suçun oluşmasını engellenmez. Zira üzerinde işlem yapılan bilişim sistemiyle bu sistemin içerdiği verilerin maliki her zaman aynı kişi olmayabilir. Örneğin akademisyenlere host ve depolama hizmeti sağlayan bir üniversitenin sistemine giren failin düşmanlık beslediği bir akademisyenin sistemde yüklü bulunan doktora tezi çalışmasını yok ederek manevi bir yarar sağlaması durumunda üniversitenin failin fiiline rıza vermiş olmasının suçun oluşup oluşmadığı hususunda bir önemi yoktur. Çünkü bu fiilde fail bilişim sistemi aracılığıyla bir başka kişinin ürününe yani verilerine zarar vermektedir. Bu nedenle rızanın bulunduğu her olayda rıza sahibinin durumu önem taşımaktadır⁶⁶.

⁶⁴ Koca/Üzülmez, **a.g.e.**, s. 883.

⁶⁵ Taşkın, **a.g.e.**, s. 59.

⁶⁶ Dülger, **a.g.e.**, s. 351.

D. Suçun Nitelikli Unsuru

Maddenin 3. fıkrasında yalnızca ilk iki fıkrada düzenlenen suçların ortak nitelikli haline yer verildiğinden bu fıkra TCK m. 244/4'te düzenlenen suç için nitelikli unsur değildir⁶⁷.

Üçüncü fıkradaki nitelikli halin dördüncü fıkrayı da kapsayacak şekilde her üç suç için düzenlenmesi yerinde olurdu. Zira kamu kurumuna ait bilişim sistemi üzerinde gerçekleştirilen fiiller sonucunda haksız çıkar sağlanması durumlarında da nitelikli halin uygulanması gerekir. Örneğin e-okul sistemine girerek devamsızlık ve ders notlarını değiştiren öğrencilerin durumunda her iki fıkra da ihlal edilmiş durumdadır. Bu tür fiillerin toplumun bilişim sistemine olan güvenini daha fazla etkilemesi nedeniyle nitelikli halin bu suçu da kapsayacak şekilde düzenlemesi gerekmektedir.

E. Suçun Özel Görünüş Biçimleri

1. Teşebbüs

Bu suç maddenin ilk iki fıkrasında sayılan fiillerin işlenmesi suretiyle failin kendisine veya başkasına haksız çıkar sağlamasıyla tamamlanmış sayılır⁶⁸. Failin suç tipinde düzenlenen fiili gerçekleştirdikten sonra haksız çıkar elde edememesi halinde suçun teşebbüs aşamasında kaldığı söylenebilir. Ancak bu durumda sisteme yönelik müdahalenin hangi kastla yapıldığı büyük önem arz eder. Haksız çıkar sağlamak kastıyla sisteme müdahale durumunda TCK m. 244/4'e teşebbüs ancak failin kastının

⁶⁷ Koca/Üzülmez, **a.g.e.**, s. 874; Erdoğan, **a.g.e.**, s. 255.

⁶⁸ Koca/Üzülmez, **a.g.e.**, s. 883. Yargıtay 11. Ceza Dairesi'nin 2010/12162 Esas 2013/658 Karar sayılı 15.01.2013 tarihli kararı; "5237 sayılı TCK.'nun 244/4. maddesinde tanımlanan bilişim suçunun hukuka aykırı yararın elde edilmesiyle tamamlanacağı, sanığın henüz amaçladığı sonuca ulaşmadan yakalandığının anlaşılması karşısında, eylemin teşebbüs aşamasında kaldığı gözetilmeden yazılı şekilde suçun tamamlanmış hali üzerinden fazla ceza tayini, Yasaya aykırı," www.corpus.com.tr (Çevrimiçi) 17.03.2019

sadece sisteme veya verilere zarar vermek olduğu durumlarda TCK m. 244/1 ve m. 244/2 kapsamında suçun değerlendirilmesi gerekecektir⁶⁹.

TCK m. 244/4'te düzenlenen suçun icra hareketlerine ilk iki fıkrada düzenlenen fiillerin gerçekleştirilmesiyle başlanacaktır. Eğer bilişim sistemine giren fail, ilk iki fıkradaki fiilleri işlemeyen sistemden çıkmışsa, dördüncü fıkradaki suçun icra hareketlerine başlamış olmadığından, bu suça teşebbüsten bahsedilemeyecektir. Bu durumda fail yalnızca sisteme girmek ve sistemde kalmak fiilini içeren TCK m. 243'ten dolayı cezalandırılmalıdır⁷⁰.

Suçun tamamlanabilmesi için haksız çıkarın sağlanması şarttır. Fail bilişim sistemi üzerinde gerekli hareketleri yapmasına rağmen menfaati elde edememişse suçun teşebbüs aşamasında kaldığını söyleyebiliriz. Bu durumda failin bilişim sistemindeki verilere yönelik müdahaleyi hangi kastla yaptığının tespit edilmesi önem taşır. Haksız çıkar sağlama kastıyla bu fiilleri gerçekleştirmiş ancak menfaati sağlayamamışsa TCK m. 244/4'e teşebbüsten, kastı yalnızca verilere veya sisteme zarar vermekse TCK m. 244/1-2'den cezalandırılması gerekir⁷¹.

2. İştirak

Fail verileri bizzat bilgisayara girmeyip, üçüncü kişileri kullanarak suçu işlemiş olabilir. Aracı kişinin, fiili gerçekleştirmesinde kastının olmaması gerekir. Aracı kişiyi kullanan kişi ise dolaylı fail konumundadır. Ancak söz konusu kişi verilerin içeriğini kontrol etme yükümlülüğüne sahip birisi ise TCK m. 244/4'ün oluşup oluşmadığı doktrinde tartışmalıdır. Bazı yazarlar bu durumda hukuku aykırı yararın bilgisayarın kullanılmasıyla değil bir insanın aldatılmasıyla elde edildiğini, dolayısıyla da bilişim sistemi aracılığıyla haksız çıkar sağlama suçunun değil dolandırıcılık suçunun oluştuğunu kabul ederler⁷². Diğer yazarlar ise kontrol etmekle görevli kişinin

⁶⁹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6940; Dülger, **a.g.e.**, s. 352.

⁷⁰ Koca/Üzülmez, **a.g.e.**, s. 884.

⁷¹ Koca, "Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları", s. 1660.

⁷² Theodor Lenckner/ Winkelbauer Wolfgang, Computerkriminalität- Möglichkeiten und Grenzen des 2. WiKG, CR, 1986, Heft 10, s. 656. (Aktaran; Akbulut, **a.g.e.**, s. 231.)

yanıtılması durumunda da kast olmaması şartıyla dolaylı fail durumunun ve TCK m. 244/4'te düzenlenen suçun oluştuğunu kabul ederler. Bu yazarlara göre olayda aynı zamanda dolandırıcılık suçu oluşmuştur ve olay içtima kurallarına göre çözümlenmelidir. Türk hukukunda yaygın olan görüş ise, verilerin içeriğini kontrol yetkisine sahip kişinin aldatılması durumunda, haksız çıkar bir insan davranışıyla sağlandığından dolandırıcılık suçunun oluştuğu yönündedir⁷³.

3. İçtima

Doktrinde bu suçun TCK m. 42 anlamında bileşik suç olduğuna dair görüşler bulunmaktadır. Bu görüşe göre maddenin ilk iki fıkrasında yer alan fiiller dördüncü fıkradaki suçun unsuru olduğundan bileşik suç söz konusudur ve ortada tek fiil bulunmaktadır. Yani bu suçun oluşabilmesi için failin bir bilişim sisteminin işleyişini engelleyerek veya bozarak ya da bir bilişim sistemindeki verileri bozarak, yok ederek, değiştirerek, erişilmez kılarak, veri yerleştirerek ya da mevcut verileri başka yere göndererek kendisinin ya da başkasının yararına haksız çıkar sağlaması gerekmektedir. Dolayısıyla failin öncelikle maddenin ilk iki fıkrasından tanımlanan fiilleri işlemesi daha sonra ise bu fiillerle nedensellik bağı içerisinde haksız yarar sağlaması gerekmektedir. Bütün bu fiiller işlenirken hukuki anlamda ortada tek fiil ve tek suç vardır. Bu nedenle bilişim sistemini engelleyen veya bozan ya da sistemdeki verileri başka yere göndererek, verileri değiştiren bozarak haksız yarar sağlayan fail sadece TCK m. 244/4'ten sorumlu olur⁷⁴.

TCK m. 42'de düzenlenen bileşik suç “*Biri diğerinin unsuru veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suçta bileşik suç denir*” şeklinde tanımlanırken devamında “*Bu tür suçlarda içtima hükümleri uygulanmaz*” denilmiştir. Dolayısıyla bu görüş, TCK m. 244'ün ilk iki fıkrasıyla dördüncü fıkranın bileşik suç olduğunu ve aralarında içtima hükümlerinin uygulanmayacağını savunmaktadır. Diğer bir deyişle TCK m. 244/1-2 ve TCK m. 244/4'ün birlikte

⁷³ Akbulut, **a.g.e.**, s. 232.

⁷⁴ Koca/Üzülmez, **a.g.e.**, s. 876-884; Gül, **a.g.e.**, s. 86-96.

gerçekleştiği durumlarda artık ilk iki fıkra hükmü değil yalnızca dördüncü fıkra hükmünün içtima hükümleri uygulanmaksızın doğrudan uygulanacağını ileri sürülmektedir⁷⁵.

Bir diğer görüşe göre, burada fiilin başka bir suçu oluşturması halinde bu hükmün uygulanmayacağının düzenlenmesi kanun koyucunun bağımsız bir suç yaratmak istediğinin kabulü anlamındadır. Zira mukayese eşitler arasında yapılabilir, kanun koyucunun daha fazla cezayı gerektiren nitelikli hal ile bir suçu karşılaştırması kabul edilemez. Dördüncü fıkra bir suçta bulunması gereken tüm unsurlara yer verilmiştir. Kanun koyucu bu fıkra ile artırım oranı belirlemek yerine doğrudan ceza belirlemiş ve ayrı bir suç olarak düzenlemiştir⁷⁶.

Kanun koyucu 4. fıkra düzenleneni bilişim sistemleri aracılığıyla haksız çıkar sağlama suçunu tali norm olarak düzenlemiştir⁷⁷. Madde metninde suçun bu özelliğini belirtmek için fiilin “başka bir suçu oluşturmaması” gerektiğinden bahsedilmiştir. Bilişim sistemleri aracılığıyla haksız çıkar sağlama şeklinde bir olayla karşılaşıldığında ilk olarak bu fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma gibi başkaca suçları oluşturup oluşturmadığı araştırılmalıdır. Olayın gerçekleştiriliş şekli bu suçlardan birisine uygunsa bu suç aksi halde TCK m. 244/4 oluşacaktır. “Asli normun önceliği ilkesi” gereğince bir fiil hakkında asli ve tali norm olmak üzere iki hüküm bulunuyorsa asli norm fiile öncelikle uygulanır. Özetle TCK m. 244/4 hükmü bilişim sistemleri aracılığıyla menfaat sağlama olaylarına uygulanacak asıl hüküm değildir ve olaya uygulanacak başka bir hüküm varsa öncelikle o hüküm uygulanmalıdır zira tali normlar bir boşluk bırakmamak için konulan hükümlerdir⁷⁸.

Fıkra düzenleneni hüküm göz önünde bulundurulmaksızın, bu hüküm bir torba suç tanımı haline getirip bilişim sistemi kullanılarak elde edilen her türlü haksız

⁷⁵ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 996; Kurt, **a.g.e.**, s. 161.

⁷⁶ Erdoğan, **a.g.e.**, s. 247.

⁷⁷ Koca/Üzülmez, **a.g.e.**, s. 876; Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 990; Gül, **a.g.e.**, s. 96; Değirmenci, **a.g.m.**, s. 206.

⁷⁸ Koca/Üzülmez, **a.g.e.**, s. 877; Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6938; Avşar/Öngören, **a.g.e.**, s. 139; Ketizmen, **a.g.e.**, s. 179.

çıkar sağlama fiillerine uygulamak kanun koyucunun iradesine aykırılık oluşturur. TCK'da örneğin hırsızlık ve dolandırıcılık gibi bazı suçların bilişim sistemi kullanılması suretiyle işlenmesi bu suçların nitelikli hali sayılmıştır. Bu düzenlemeler esasında tali norm olan TCK m. 244/4'ün uygulama alanını daraltmak amacıyla yapılmıştır⁷⁹.

Fiillerin TCK'da bulunan çeşitli maddelerle karşılanamayacak olması halinde boşluk yaratmamak adına veya söz konusu fiiller hakkında geleneksel hükümlerin tipiklik unsuru açısından uygulanmasında tereddüde yer açmamak amacıyla ayrıca bir düzenleme yapılarak bağımsız bir norm teşkil etmek amaçlanmıştır. Bu madde gerekçesinden de anlaşılacağı üzere tali nitelikteki bir hükümdür, asli nitelikteki bir normun saptandığı suç tipine uygunluk gösteren bir fiil gündeme geldiği takdirde bu norm değil, asıl hüküm uygulama alanı bulacaktır⁸⁰.

Eğer bu suç bir suç işleme kararının icrası kapsamında değişik zamanlarda aynı kişiye karşı birden fazla kez işlenirse zincirleme suçtan bahsetmek gerekecektir⁸¹. Sistemin çalışmasının engellenmesi ya da veri yerleştirilmesi suretiyle haksız çıkar sağlanması için zaman aralıklarıyla ve aynı suç işleme kararıyla bilişim sistemine birçok kez etkiye bulunulmasıyla haksız çıkar birden fazla kere kazanılması durumu buna örnek gösterilebilir⁸².

F. Kusurluluk ve Cezalandırılabilirliğin Diğer Koşulları

Kusurluluğu etkileyen hallerden zorunluluk hali inceleme konusu yaptığımız suç için gündeme geleceği düşünülebilir. Zorunluluk halinin uygulanması için kişinin kendisinin veya başkasının hakkına yönelik olarak ağır ve muhakkak bir tehlikeden başka suretle korunmak olağanının bulunmaması gerekmektedir. Zorunluluk halinin

⁷⁹ Koca/Üzülmez, **a.g.e.**, 877; Koca, “Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları”, s. 7659.

⁸⁰ Eker, **a.g.m.**, s. 127.

⁸¹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6940.

⁸² Dülger, **a.g.e.**, s. 354.

bilişim sistemi aracılığıyla haksız çıkar sağlama suçu için gerçekleşeceğini söylemek mümkün değildir. Kişinin kendisinin ya da başkasının sahip olduğu hakka yönelik tehlikeyi uzaklaştırmak için başkasının sisteminde yapacağı müdahale ile haksız çıkar sağlamanın zorunlu olması bu tehlikeyi başka suretle defetme olanağının bulunmaması düşünülemez.

G. Yaptırım

Maddede fail için iki yıldan altı yıla kadar hapis cezası öngörülmüştür. Öngörülen adli para cezası ilk defa 5237 sayılı TCK ile getirilmiştir⁸³.

Dördüncü fıkra ilk iki fıkradan farklı olarak hapis ve adli para cezasına birlikte hükmolunması benimsenmiştir. Zira fail işlediği suç neticesinde haksız bir çıkar sağlamaktadır. Hâkim hapis cezasının alt sınırı olan iki yıl sonuç cezayı belirlemişse erteleme yetkisini kullanabilirse de bu durum adli para cezasını kapsamaz⁸⁴.

TCK m. 244/4'te belirtilen para cezasının asgari sınırı belirtilmediği için TCK m. 52/1 maddesi gereğince adli para cezasının beş günden az olamayacağı göz önüne alınarak en az bu kadara hükmolunacaktır⁸⁵.

H. Soruşturma ve Kovuşturma

Maddedeki yazılı tüm suçların soruşturması ve kovuşturulması re'sen yapılır⁸⁶.

Bu suçlarda özellikle soruşturma aşamasından kaybolacak delillerin, gecikmesizin ve hukuka uygun olarak toplanması gerekmektedir⁸⁷.

Müdahale edildiği söylenen sistem üzerinde herhangi bir değişiklik yapılmadan gerekli incelemenin yaptırılması, sisteme ya da içeriğine zarar verilip

⁸³ Kurt, **a.g.e.**, s. 245.

⁸⁴ Meran, **a.g.e.**, s. 583. Yılmaz, **a.g.e.**, s. 202.

⁸⁵ Kurt, **a.g.e.**, s. 246.

⁸⁶ Gül, **a.g.e.**, s.92.

⁸⁷ **A.e.**, s.93.

verilmediği, verilmiş ise ne şekilde gerçekleştiği (virüs, solucan vs.) , veri aktarıldıysa nereye aktarıldığı, başkasına yarar sağlanıp sağlanmadığı (hesaplar arası para transferi ya da faturalara ek ücret yansıtılması gibi) bu işlemler sırasında sisteme düşen IP adresi server ve log kayıtları üzerinde yapılacak inceleme ile tespit edilmeye çalışılmalıdır⁸⁸.

Sisteme düşen IP adresi kullanıcısı ilgili servis sağlayıcı şirketten (Vodafone, Turkcell, Superonline vs.) sorularak tespit edilebilse de uygulamada yurt dışı kaynaklı IP adresi ya da NAT uygulamasında kullanılan (ağ adresi dönüşüm uygulamasında kullanılan) IP adresi olması ya da toplu kullanım alanlarında sisteme girilmesi nedeniyle failin tespiti imkansızlaşmaktadır⁸⁹.

Bu durumda şüphelenilen şahıs varsa onun kullandığı dijital materyaller üzerinde inceleme yapılması ayrıca lehine yarar sağlanan kişiler yönünden araştırma yapılması gerekmektedir de bu da kesin çözüm değildir. Keza lehine yarar sağlanan kişilerin de çoğu zaman fiilden haberdar olmadıkları örneğin bir banka hesabından kendi hesabına para transferi yapılan şahsın bu fiilden haberdar olmadığı çünkü menfaatin daha sonra bir başka hesaba aktarıldığı görülmektedir⁹⁰.

Şüpheliye ait dijital materyallerde inceleme yapılırken olay tarihi ve zaman tespit edilmeli hangi kullanıcı ile internete bağlandığı, olaya ilişkin veri olup olmadığı belirlenmeli yine mağdur ya da başkalarına ait hesap bilgileri olup olmadığı, şifre kırıcı programın kullanılıp kullanılmadığı ya da başka kullanıcılar ile benzer konularda bağlantı kurulup kurulmadığı araştırılmalıdır⁹¹.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. maddesi gereğince davaya bakmaya görevli mahkeme asliye ceza mahkemeleridir⁹².

⁸⁸ Gül, **a.g.e.**, s.93.

⁸⁹ **A.e.**, s. 94.

⁹⁰ **A.e.**

⁹¹ **A.e.**

⁹² **A.e.**, s. 92.

II. SUÇLARIN BENZER SUÇLARLA KARŞILAŞTIRILMASI

A. Bilişim Sistemine Girme Suçu Sonucunda Sistemdeki Verilerin Yok Olması veya Değişmesi Suçu

TCK m.243/3'te *“Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur”* hükmü yer almaktadır. Bu suçun oluşabilmesi için failin verileri yok etme veya değiştirme kastıyla hareket etmemiş olması gerekmektedir. Burada suçun neticesi taksirle gerçekleşmektedir. *“yok olur veya değişirse”* ibareleri pasif niteliktedir ve faile değil fiile vurgu yapılmıştır⁹³.

TCK m. 244/2'de ise bir bilişim sistemindeki verinin kasten yok edilmesi veya değiştirilmesinin ayrı bir suç olarak düzenlendiği göz önüne alındığında, TCK m. 243/3'te düzenlenen suçun oluşması için failin yukarıda belirtilen seçimlik sonuçlar için kastının olmaması gerekir⁹⁴.

TCK m. 243/3'te gerçek neticesi sebebiyle ağırlaşan suça yer verilmiştir. Maddenin uygulanabilmesi için failin taksirle hareket etmesi gerekir. Şayet fail kasten hareket etmişse, bir başka suç oluşur ve doğrudan ilgili maddenin uygulanması gerekir⁹⁵. Dolayısıyla fail eğer verilere kasten zarar verirse, bu nitelikte fiiller zaten TCK m. 244/2'te düzenlendiğinden TCK m. 243/3'ün uygulanması mümkün değildir⁹⁶.

Tekrar belirtmek gerekirse yetkisiz olarak bilişim sistemine erişim sonucu verilerin değiştirilmesi veya yok edilmesine neden olan failin fiili TCK m. 243/3'te

⁹³ Karagülmez, **a.g.e.**, s. 212.

⁹⁴ **A.e.**, s. 213.

⁹⁵ Koca/Üzülmez, **a.g.e.**, s. 859, 875; Karagülmez, **a.g.e.**, s. 213.

⁹⁶ Dülger, **a.g.e.**, s. 266.

yer alan bilişim sistemine girme suçunun neticesi sebebiyle ağırlaştırılmış halini oluşturacaktır. Faili bu suçtan sorumlu tutabilmek için failin en azından taksirinin bulunması gerekir⁹⁷.

Bu maddede sayılan suçların kendi içinde ve diğer suçlardan incelediğimiz suçu ayırmada belirleyici etkenlerden biri faildeki manevi unsurdur. Sisteme hukuka aykırı giriş yapılması nedeniyle sistemdeki verilerin yok olması veya değişmesi halinde yani fiilin taksirli hali TCK m. 243/3'te neticesi sebebiyle ağırlaştırılmış suç olarak yaptırım altına alınmıştır⁹⁸. TCK m. 243/3'ün uygulanabilmesi için ilk olarak failin 244/1-2 fıkraları kapsamında bir kastının olmaması, ikinci olarak failin fiiline ilişkin kastının haksız olarak sisteme girip orada kalmaya devam etme şeklinde olması ve son olarak failin bu kast ile işlediği fiilin sonucunda sistemin içerdiği verilerin yok olması veya değişmesi koşullarının beraber gerçekleşmiş olması gerekir⁹⁹.

B. Mala Zarar Verme Suçu

1. Suçun Konusu

Mala zarar verme suçunun düzenlenmesinde taşınır ya da taşınmaz malın fiziki yapısı esas alınarak bunlara yönelik zarar verici fiillerin engellenmesi amaçlanmaktadır. Mala zarar verme suçu düzenlenirken ise bu suç seçimlik hareketli bir suç olarak ele alınmış ve bu yüzden mala zarar verme suçunun maddi unsuru belirlenmiştir. TCK m. 151'de düzenlenen mala zarar verme suçunda ise suçun maddi unsurunu oluşturan fiiller taşınır ya da taşınmaz malın kısmen ya da tamamen yıkılması, tahrip edilmesi, yok edilmesi, bozulması, kullanılmaz hale getirilmesi ve kirletilmesi olarak karşımıza çıkmaktadır¹⁰⁰.

Bilişim sistemlerinin yaygınlaşmasıyla veri ya da programları hedef alan müdahalelerin önlenmesi ve bu tür fiillerin cezalandırılabilirliği sorunu ortaya

⁹⁷ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6934.

⁹⁸ Akbulut, **a.g.e.**, s. 204; Erdoğan, **a.g.m.**, s. 1403.

⁹⁹ Karagülmez, **a.g.e.**, s. 240.

¹⁰⁰ Ketizmen, **a.g.e.**, s. 121.

çıkıştır. Klasik mala zarar verme suçunda genel olarak taşınır ya da taşınmaz malda fiziksel zarar aranırken, veri ya da bilişim sistemine yönelik zarar verici fiiller fiziksel değişikliğe yol açmayabilir¹⁰¹.

Bilişim sistemine yapılan müdahalelerde sorun, müdahale teşkil edecek fiillerin mala zarar verme suçunu oluşturup oluşturmayacağıdır. Bu tür müdahalelerde sistemin maddi varlığında değişiklik olmasa da sistemin fonksiyonlarını yerine getirememesi durumu vardır. Çözülmesi gereken husus, mala zarar verme suçunun unsurlarının bu tür fiilleri kapsayıp kapsamadığı noktasındadır¹⁰².

Sorunun bir diğer yönü ise maddi varlığı olmayan verinin, maddi varlığı olan taşınır ya da taşınmaz malın esas alınarak düzenlendiği mala zarar verme suçunun konusunu oluşturup oluşturmayacağı noktasındadır. Diğer deyişle verinin, verinin ele geçirilmesi suçunda da bahsedildiği üzere, mal olarak kabul edilip edilmemesi sorunun temelidir¹⁰³.

Verinin mal olarak kabul edilip edilmeyeceğine ilişkin sorun iki farklı yaklaşımla çözülmek istenmiştir. İlk yaklaşım, ekonomik değer taşıyan verinin mal/eşya olarak kabul edilmesidir. İkinci yaklaşım ise, veriye müdahalenin verinin bulunduğu mala yönelik bir zarar verme fiili olduğudur. Verinin bulunduğu maddi mal esas alınarak veriye müdahale ile verinin bulunduğu malın işlevine müdahale edilmesi hususu vurgulanmaktadır¹⁰⁴.

İlk görüşe göre eğer fail bilişim sistemine zarar vermek suretiyle verileri de yok etmiş ya da bozmuşsa hem mala zarar verme suçundan hem de verilere müdahale suçu oluşacaktır. Eğer fail kendine ait bilişim sistemine zarar vermek suretiyle sistemde bulunan başkasına ait verilere zarar vermişse kendi malına zarar vermesi mala zarar verme suçunu oluşturmadığından yalnızca TCK m. 244/2'yi ihlal etmiştir. Zira mala zarar verme suçunun oluşması için, başkasına ait taşınır veya

¹⁰¹ A.e., s. 121.

¹⁰² A.e., s. 122.

¹⁰³ A.e.

¹⁰⁴ A.e., s. 123.

taşınmazın suçun konusunu oluşturması gerekir. Eğer fail, başkasının mülkiyetinde olan bir sisteme zarar vermek suretiyle verileri yok etmişse hem mala zarar verme hem de verileri yok etme suçunu işlediği kabul edilir. Bu suçlar tek fiille gerçekleştiğinden fikri içtima hükümlerinin uygulanması gerekeceğini savunmaktadırlar¹⁰⁵.

Diğer görüş ise bilişim sistemindeki verilere müdahale suçu ile korunan hukuki değer soyut olarak sadece veriler olmayıp aynı zamanda somut olarak sisteme ait donanımlarından korunduğundan bahisle hem mala zarar verme hem de verileri yok etme veya değiştirme suçunun oluşacağını kabul etmektedir. Buradaki sorun özel normun genel norma önceliği prensibi gereğince bilişim sistemini özel olarak koruyan bir norm olan TCK m. 244'ün uygulanması ile çözülmesi gerektiğini savunmaktadır. Burada aynı hukuki değeri koruyan farklı iki normun ihlalinin söz konusu olduğunu belirtmektedir. Ancak TCK m. 244 mala zarar verme suçuna göre birtakım ek özelliklere sahip olan özel norm niteliğinde olduğundan bu durumda uygulama alanı bulacağını savunmaktadır¹⁰⁶. Bu görüşe göre, kanun koyucu verilere zarar verilmesini yaptırımsız bırakmak istemediği için TCK m. 244/2 maddesini düzenlemiştir ve bu suçu mala zarar verme suçunun bilişim alanındaki karşılığı olarak kabul etmektedirler¹⁰⁷.

Suçun kanuni tanımında bilişim sisteminden değil, bilişim sisteminin işleyişinin engellenmesinden ve bozulmasından söz edilmesi karşısında, suçun konusunu sistemin soyut unsurlarının oluşturduğunu kabul eden görüşe göre, soyut unsurlara zarar verme fiillerinin TCK m. 244 kapsamında olduğunu belirtmektedir. Her ne kadar maddenin gerekçesinde, bu madde ile sistemlere yöneltilen ızzar fiillerinin özel bir suç haline getirildiği ve “aracın fiziki varlığı ve işlemlerini sağlayan bütün diğer unsurların” bu suçun konusunu oluşturduğu belirtilmiş ise de maddi unsurlara yönelik zarar verme niteliği taşıyan fiillerin mala zarar verme suçunu oluşturduğunu savunmaktadır. Bu görüşe göre sistemin işleyişinin engellenmesi veya

¹⁰⁵ Akbulut, **a.g.e.**, s. 210, 211.

¹⁰⁶ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 869.

¹⁰⁷ Erdoğan, **a.g.e.**, s. 237.

bozulması ise ancak işler halde bulunan bir sistemin varlığını ve bunun soyut unsurlarına yönelik zarar verici fiillerin işlenmesini gerektirmektedir. Örneğin, bir kişinin diz üstü bilgisayarının yere fırlatılmak suretiyle parçalanması veya klavyenin tuşlarının sökülmesi halinde bilgisayar kişinin malvarlığında yer alan bir değer olarak tahrip edilmektedir. Bu durumda mala zarar verme suçu oluşur. Buna karşılık bilgisayarın fiziki varlığına zarar vermeksizin gönderilen bir virüs programı ile çalışamaz hale getirilmesi durumunda, bilgisayar bilişim sistemini sağlayan bir araç olarak etkisiz kılınmaktadır ve bu durumda TCK m. 244'te sayılan suç oluşmaktadır¹⁰⁸.

İkinci yaklaşımda, veri mala zarar verme suçunun konusunu oluşturabilecek bir mal olarak kabul edilmemektedir. Veriye yönelik müdahale doğrudan mala zarar verme olarak kabul edilmemiştir. Bu yaklaşıma göre, veriye müdahale verinin bulunduğu mal, içerdiği veri ile birlikte bir işleve sahip olup veriye müdahale sonucunda bu işleve zarar verilmekte bu haliyle mala zarar verme söz konusu olmaktadır. Aynı yaklaşım sisteme müdahale bakımından geçerlidir. Sistemin yazılım unsuruna yönelik müdahale söz konusu olsa da sistemin işlevini yerine getirememesi söz konusu olduğundan mala zarar verme suçunun oluştuğunu belirtmektedirler¹⁰⁹.

Mala zarar verme suçunun ancak bir mal üzerinde işlenebilecek olması, verilerin ise mal olarak değerlendirilememesi ve bu sebeple de bilişim alanındaki hareketlerin mala zarar verme suçuyla karşılanamayacak olması sebebiyle bu husus ayrıca düzenlenmiştir. TCK m. 244'te suçun konusu veri olup soyut nitelik taşımaktadır. Mala zarar verme fiilleri ise kanun gereği şeyler üzerinde yani fiziki varlığı olan cisimler üzerinde işlenebileceğinden eğer özel düzenleme bulunmasaydı kanunilik ve kıyas yasağı gereği bu fiillerin klasik düzenlemelerle karşılanması mümkün olmayacaktı¹¹⁰. Bu nedenle verilere ya da sisteme zarar verilmesi durumunda TCK m. 244'te düzenlenen suçlar gündeme gelecektir¹¹¹.

¹⁰⁸ Koca/Üzülmez, **a.g.e.**, s. 870.

¹⁰⁹ **A.e.**, s. 124.

¹¹⁰ Kurt, **a.g.e.**, s. 166,167.

¹¹¹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s.662.

TCK m. 151’de düzenlenen suçun konusunu “başkasına ait taşınır ya da taşınmaz mal” oluşturur. TCK m. 244/1’in konusu ise bilişim sistemidir. Bilişim sistemini mal ya da eşya olarak kabul etmeyen bu görüşe göre bu iki madde aslında birbirinden tamamen farklı iki suç tipini düzenlemekte ve suç politikasıyla belirlenen iki farklı hukuki değeri koruma altına almaktadır. Dolayısıyla iki madde arasında özel hüküm- genel hüküm ilişkisi bulunmadığı gibi salt mala zarar verme kastıyla yapılan bir eyleme TCK m. 151’in uygulanması gerekirken TCK m. 244’ün gerekçesindeki “ızzar” kelimesini gerekçe göstererek söz konusu fiile TCK m. 244’ün uygulanması gerektiğini savunmak isabetli olmadığını belirtmektedirler. Bu görüş gerekçeyi değil de kanun maddesini temel alarak, failin kastının bilişim sisteminin işleyişine ya da içerdiği verilere zarar vermek olmadığı salt mala zarar vermek kastıyla hareket ettiği durumlarda mala zarar verme suçunun oluştuğunu kabul ettiğini söyleyebiliriz¹¹².

Suçun konusunu oluşturan verilerin mutlaka bilişim sisteminde yer alan veriler olması gerektiğini savunan görüşe göre, yalnızca veri saklama işlevine sahip cihazlardaki verilere müdahale edilmesi mala zarar verme suçunu oluşturacaktır¹¹³. Bu görüşe göre CD, USB bellek gibi cihazların içerisinde bulunan verilere ulaşılamaması amacıyla bozulması veya fiziki olarak kullanılmaz hale getirilmesi halinde TCK m. 151’de düzenlenen mala zarar verme suçu oluşur¹¹⁴. Bu görüşe katılmayan görüş ise içindeki verileri bozmak için bir disketi kıran kişi, veri şey olarak değerlendirilmediğinden veriye karşı yaptığı fiili mala zarar verme suçu kapsamında sayılmayacak, TCK m. 244’ten cezalandırılacağını savunmaktadır¹¹⁵. Bu görüş, sistemde yer alan veri kavramına USB bellek ve CD-ROM gibi aygıtların girdiğini savunarak suçun oluşacağını kabul ettiği gibi TCK m. 244/2’de düzenlenen neticelerden birinin gerçekleşmesi durumunda suçun mala zarar verme suçunu da oluşturacağından bahisle içtima kapsamında değerlendirilmesi gerektiğini kabul etmektedirler. Örnek vermek gerekirse verilere zarar vermek amacıyla cihazlara zarar verilmesi halinde mala zarar verme suçu ile sistemi engelleme, bozma, verileri yok

¹¹² Dölger, **a.g.e.**, s. 317, 338; Taşkın, **a.g.e.**, s. 55.

¹¹³ Koca/Üzölmez, **a.g.e.**, s. 871.

¹¹⁴ **A.e.**, s. 869.

¹¹⁵ Kurt, **a.g.e.**, s. 167.

etme veya deęiřtirme suçları arasında fikri içtima ilişkisinin varlığını kabul etmektedirler¹¹⁶.

2. Hareket

TCK m. 244/1 ile TCK m. 151’de düzenlenen mala zarar verme suçu arasındaki ilişki doktrinde çokça tartışılmıştır.

TCK m. 244/1 incelendiğinde, AKSSS’den farklı olarak, sisteme müdahalenin sistemin yazılımına yönelik olarak sisteme veri gönderilmesi, yerleştirilmesi gibi hareketlerle gerçekleştirileceğine ilişkin bir düzenlemeye yer verilmedięi görölmektedir. Bu nedenle sistemin yazılımına veri aracılığıyla müdahalenin ya da her türlü müdahalenin sisteme müdahale oluşturup oluşturmayacağı tespit edilmesi gereken noktadır¹¹⁷.

TCK m. 244/1’in yazılıma yönelik fiiller yanında donanıma yönelik mala zarar verme suçunun konusunu oluşturabilecek fiilleri kapsayan özel bir suç mu olduęu yoksa bu fıkranın sadece sistemin yazılım unsuruna yönelik fiillerin esas alınarak mala zarar verme suçunu tamamlayan bir suç olarak mı düzenlendiğinin tespiti bu hususun çözümü bakımından önem arz etmektedir¹¹⁸.

Bu fıkra kapsamında hangi fiillerin düzenlendiğinin belirlenmesi, mala zarar verme suçu ile bu suçun ayrılmasında önem arz eder. Eğer bu fıkranın yazılıma yönelik veri aracılığıyla gerçekleştirilen fiilleri kapsadığı kabul edilecek olursa, TCK m.244/1’de suçun konusunun sistemin yazılım yönünün esas alındığı sonucuna varılacaktır. Fakat bu fıkranın donanıma ve yazılıma yönelik fiilleri bir bütün olarak kapsadığı ya da sadece donanıma yönelik fiilleri kapsadığı kabul edilecek olursa, mala zarar verme suçuna göre biliřim sistemini bir bütün olarak konu edinen özel bir hüküm olduęu sonucuna varılabilecektir¹¹⁹.

¹¹⁶ Akbulut, **a.g.e.**, s. 189.

¹¹⁷ Ketizmen, **a.g.e.**, s. 130.

¹¹⁸ **A.e.**

¹¹⁹ **A.e.**, s. 131.

TCK m. 244/1'in fiziksel müdahaleleri kapsam dışı bırakacak şekilde sadece yazılım dolayısıyla veriye müdahale yoluyla gerçekleştirilen fiilleri esas aldığı kabul eden görüş bulunmaktadır. Bu görüşe göre, yazılıma yönelik hareketler sonucunda sistemin işleyişinin engellenmesi ya da bozulması halinde TCK m. 244/1, donanıma yönelik fiillerde ise TCK m. 151 uygulama alanı bulacaktır. Bu görüş, sistemin işleyişinden, yazılım unsuruna bağlı veri işleme faaliyeti anlaşılması gerektiğini, TCK m. 244/1'de düzenlenen bilişim sisteminin işleyişine müdahale edilmesinden de sistemin yazılım yönüne işaret ettiği anlaşılması gerektiğini savunmaktadır¹²⁰.

Diğer görüş, TCK m. 244/1'de düzenlenen hareketin somut bileşenlere yani donanıma yönelik olduğunu, ikinci fıkradaki fiillerin ise yazılım yani soyut bileşenlere yönelik olduğunu kabul etmektedir¹²¹.

Diğer görüş ise TCK m. 244/1'de sistemin işleyişinin engellenmesi ve bozulmasından bahsedildiğini, bu fiilleri sınırlayıcı hükme yer verilmediğini belirtmektedir. Bu görüşe göre sistemin işleyişini sağlayan yazılım ya da donanım unsurlarından herhangi birisine zarar verilmesiyle suç oluşmaktadır. Ancak somut unsurlara (donanım) zarar verilmesi halinde hem sistemin işleyişinin bozulması hem de mala zarar verme suçunun oluştuğundan bahisle fikri içtima gereği TCK m. 244/1'in uygulanacağını ileri sürmektedir. Bu görüşe göre fail örneğin bir program vasıtasıyla bilişim sisteminin programlarına zarar verip işlemlerini bozar ya da engellerse sadece TCK m. 244/1'te tanımlanan suç oluşur. Eğer fail engel olmak ya da bozmak kastıyla bilgisayarı yere atıp kırsa veya klavyenin tuşlarına zarar verirse bu durumda hem mala zarar verme suçu hem de bilişim sistemini engelleme suçu oluşacaktır. Faile fikri içtima kuralları gereğince TCK m. 244/1'den ceza verilecektir. Örnekte de görüldüğü üzere failin kastının iyi belirlenmesi gerekir. Failin kastı sadece makineye zarar vermek ise artık fikri içtima kurallarına gidilmez ve TCK m. 151 hükmü gereğince cezalandırılır¹²².

¹²⁰ Ketizmen, **a.g.e.**, s. 132, 133; Koca/Üzülmez, **a.g.e.**, s. 871.

¹²¹ Bıçkın, **a.g.m.**, s.153.

¹²² Erdoğan, **a.g.e.**, s. 206; Kurt, **a.g.e.**, s. 165; Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6928.; Bayındır, **a.g.m.**, s. 72

Kanaatimizce bilişim sistemi ilk bölümde ayrıntılı olarak açıkladığımız üzere donanım ve yazılım unsuru ile bir bütündür. Bir sistemin düzgün çalışması için her iki unsurun birbiriyle uyumlu ve doğru çalışması gerekmektedir. Bu nedenle bu hükümle hem donanım hem de yazılım unsuru koruma altına alınmıştır. Bu nedenle sadece soyut unsurlara müdahalenin (veri/yazılım) suçu oluşturacağını kabul eden görüşe katılmıyoruz. Diğer yandan önemli olan failin kastıdır. Fail sadece mağdurun bilgisayarını kullanılmaz hale getirmek için bilgisayarını kırarsa mala zarar verme suçu oluşmaktadır. Ancak failin sisteme girişi engellemek için kabloları kesmesi durumunda fikri içtima gereği TCK m. 244/1'in uygulanacağını söyleyebiliriz.

C.Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu

TCK m. 141'e göre hırsızlık, zilyedinin rızası olmadan başkasına ait taşınır bir malın, failin kendisine veya başkasına yarar sağlamak maksadıyla bulunduğu yerden alınması suretiyle işlenebilir. Bu suçun oluşabilmesi için, failin kendisine veya başkasına bir yarar sağlamak amacıyla hareket etmesi yeterlidir, suçun tamamlanması için bunun fiilen temini şart değildir¹²³.

TCK m. 142/2-e bendinde ise hırsızlık suçunun bilişim sistemleri kullanılmak suretiyle işlenmesine yer verilmiştir. Bu düzenleme; “ (2) Suçun.... e) Bilişim sistemlerinin kullanılması suretiyle, İşlenmesi hâlinde, beş yıldan on yıla kadar hapis cezasına hükmolunur.” şeklindedir.

Kanun metninde hırsızlık suçunun konusu taşınır mal olarak belirtilmiştir. Verinin taşınabilir mal sayılıp sayılmayacağı ve buna bağlı olarak hırsızlık suçunun nitelikli halinin hangi durumlara uygulanabileceği tartışılması gereken noktalardandır.

Verinin hırsızlık suçuna konu olup olamayacağı konusunda doktrinde görüş birliği bulunmamaktadır.

¹²³Karagülmez, a.g.e., s. 216.

İlk görüş, veri somut nesne olmadığından hırsızlık suçu kapsamında taşınabilir mal olarak kabul edilemeyeceğini savunmaktadır. Bu görüşe göre, 765 Sayılı TCK'nın 525/b-2 maddesindeki hukuka aykırı yarar sağlama suçuyla düzenlenen fiillerden biri de bilişim sistemi aracılığıyla gerçekleştirilen hırsızlık suçudur. Bu görüş bilişim hırsızlığı olarak isimlendirilebilecek bu suç tipine TCK m. 142'de hırsızlık suçunun nitelikli hallerinden birisi olarak yer verilmesinin yerinde olmadığını ileri sürmektedir. Hırsızlık suçunun tanımlandığı 141. maddede suçun konusu olarak somut nesneler gösterilmesine rağmen bilişim hırsızlığının konusunu oluşturan veriler somut nesne özelliği taşımadığını belirtmektedirler. TCK m. 244/4'ün bağımsız bir suç tipi olarak düzenlenmesi ve suçun konusunun neler olduğu ile hangi fiillerin cezalandırılmak istendiğinin açıkça ifade edilmesi gerektiğini ileri sürmektedirler¹²⁴.

İkinci görüşe göre verinin ekonomik değerinin önemi de günümüz dünyasında kabul edilmiştir ve veri hırsızlık suçuna konu olabilmektedir. TCK m. 142/2-e'nin düzenlenmesinde bilişim sisteminin hırsızlık suçunun işlenmesinde sağladığı kolaylık nedeniyle ayrıca düzenlendiğini belirtmektedirler¹²⁵.

Bu görüşe göre, içerisinde veri yüklü olan bilgisayar, disket veya CD'nin herhangi bir yerden alınması halinde, TCK'nın 142/2-e bendi uygulanmayacaktır. Buradaki örnekte hırsızlıkta bilişim sistemi kullanılmamıştır. Hırsızlıkla ilgili diğer hükümler uygulama alanı bulacaktır¹²⁶. Ancak bilişim sisteminin kullanılmadığı, harici bir hard diskin içinde bulunan verinin ele geçirilmesi amacıyla bu hard diskin alınması halinde TCK m. 244/2, bu fiilden haksız bir çıkar sağlanması durumunda ise TCK m. 244/4 maddesi uygulanmalıdır¹²⁷.

Bu nitelikli hırsızlığın oluşabilmesi için bir kimsenin zilyedi olduğu bir malın “bilişim sistemi kullanılarak” ondan alınması veya o mal üzerinde fiili hâkimiyetin bu şekilde kurulması gerekmektedir. Burada kastedilen husus, bilişim sisteminin

¹²⁴ Dülger, **a.g.e.**, s. 461.

¹²⁵ Karagülmez, **a.g.e.**, s. 217.

¹²⁶ **A.e.**, s. 218.

¹²⁷ Dülger, **a.g.e.**, s. 463.

kullanılması suretiyle verinin değil, taşınabilir şeylerin çalınmasıdır¹²⁸.

1. Kontör Transferi

Bir görüş kontör transferi olarak bilinen internet üzerinden girdiği şifre ile telefon sahibinin numarasından başka bir numaraya oradan da yine şifre vasıtasıyla kendi numarasına hat sahibinin bilgisi ve rızası dışında kontör transferi yapmak şekilde gerçekleştirilen fiilin TCK 142/2-e’de düzenlenen suç oluşturduğunu savunmaktadır¹²⁹. Kontör transferi fiili de banka hesabından paranın havale edilmesi gibi rızaya aykırı bir şekilde malvarlığında azalmaya neden olarak verinin temsil ettiği paranın alınarak mal edinilmesi fiilidir. Kontör gibi GSM hattına TL yüklenmesi şeklinde gerçekleşen fillerde TCK m. 142/2-e uygulanmalıdır¹³⁰.

Yargıtay bu konuda sanığın internet üzerinden girdiği şifre ile bir başka kişinin telefon numarasından başka bir kişinin telefon numarasına oradan da kendi telefon numarasına transfer yaptığı durumda, TCK m. 142/2-e’nin oluştuğunu kabul etmiştir. Doktrinde bu görüşü savunmayıp fiilin TCK 244/4’ün kapsamına girdiğini savunan karşıt görüş de bulunmaktadır¹³¹.

Bu görüşe göre, bilişim sisteminin araç olarak kullanılması suretiyle ekonomik değer taşıyan ve başkasının malvarlığından azalmaya neden olan her türlü verinin transferini TCK m. 142/2-e kapsamında kabul etmemek gerekir. Buradaki ölçüt sağlanan ekonomik yararın dış dünyada maddi bünyeye sahip bir eşya ile ilgili olmasıdır. Örneğin internet bankacılığı işlemleriyle başkasının hesabından havale edilen para hırsızlık suçuna konu olabilecek bir maldır. Bu paranın bir kimsenin cebinden çekilip alınmasıyla bankadaki hesabından alınması arasında bir fark yoktur. Bunlara rağmen dış dünyada maddi bir varlığı olmayan ama parayla ölçülebilen bir değer internet aracılığıyla transfer edilmesi hırsızlık suçunu oluşturmayabilir. Böyle bir durumda suçun temel şekli oluşmadığından nitelikli halin oluştuğundan da söz

¹²⁸ Parlar, **a.g.e.**, s. 106, 108.

¹²⁹ Gül, **a.g.e.**, s.90.

¹³⁰ Dülger, **a.g.e.**, s. 470.

¹³¹ Akbulut, **a.g.e.**, s. 251, 252.

edilemez. İnternet üzerinden bir telefonda diğer telefona kontör transferi yapılması olayında ise TCK m. 142/2-e değil, TCK m. 244/4'ün oluştuğunu savunmaktadırlar¹³².

Yargıtay Ceza Genel Kurulu 2013/13-448 Esas 2014/524 Karar sayılı 25.11.2014 tarihli kararı şu şekildedir; “ *“kontörleri temsil eden verinin Abdullah Çelik isimli kişiye ait olan 0536 367 numaralı telefona, bu telefona ait şifreyi de kullanmak suretiyle kendisine ait 0536 975 numaralı telefona aktarıp kullanması şeklinde gerçekleşen, bu işlem nedeniyle bilişim sisteminin doğru ve işlevine uygun olarak çalışmasına engel bir durumun da meydana gelmediği somut olayda, sanığın eylemi, telefonun kullanılmasını sağlayan, ekonomik bir değer ifade eden ve bilişim sisteminde veri ile temsil edilen kontörleri, bilişim sistemini kullanıp veriyi yer değiştirmek suretiyle kendi telefon hattın geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği ve ekonomik bir değeri olan, ancak bir bedel ödemek suretiyle alınabilecek olan kontörleri alarak mal edinmeye yöneliktir. Kaldı ki sanığın mağdurun telefonunda kullandığı kontörleri almak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCK'nun 142/2-e maddesinde düzenlenmiş bulunan “bilişim sistemleri kullanılmak suretiyle hırsızlık” suçunun gerçekleştiği kabul edilmelidir.*”¹³³

Yargıtay Ceza Genel Kurulu bu kararıyla kontör transferinde kontörün temsil ettiği paranın alındığından bahisle bilişim sistemleri kullanarak gerçekleşen hırsızlık suçu olduğuna karar vermiştir. Diğer deyişle YCGK burada failin veriyi başka bir yere göndermekten ziyade mağdurun malvarlığında azalmaya yol açarak verinin yani onu

¹³² Koca/Üzülmez, **a.g.e.**, s. 879.

¹³³ “Çoğunluk görüşüne katılmayan Genel Kurul Üyesi V. Dirim; Kanunilik Prensibi uyarınca veriyi taşınır mal sayan herhangi bir kanuni düzenleme olmadan, bir verinin zilyedinin rızası olmaksızın bulunduğu yerden alınması fiilini hırsızlık olarak kabul edilmesinin mümkün değildir. Kontör, ekonomik bir değer ifade etmekte ise de; taşınır bir mal değildir. Bilgisayar ortamından temin edilen kontör, sahibine belirli süreler için telefonda görüşme yapma hakkı sağlayan bir veridir. Üstelik bulunduğu yerden fiziken de alınmış değildir. Buna karşılık sanığın işlemiş olduğu fiil; TCK'nın 244. maddesinin 2. fıkrasında düzenlenen seçimlik hareketlerden olan 'varolan verileri başka bir yere'” göndermek olup, aynı Kanun'un 4. fıkrasında belirtilen 'haksız bir çıkar sağlama' söz konusu olduğu için TCK'nın 244. maddesinin 4. fıkrasında düzenlenen bilişim suçunu oluşturmaktadır.” www.corpus.com.tr (Çevrimiçi) 22.03.2019.

temsil eden parasal değeri mal edinmeye yönelik fiili dolayısıyla TCK m. 142/2-e'nin oluştuğunu belirtmektedir.

Sonuç olarak failin mağdura ait GSM şirketlerindeki hesabına hukuka aykırı olarak girip cep telefon kontörlerini kendisine transfer etmesi halinde de söz konusu hırsızlık suçu oluştuğunu söyleyebiliriz¹³⁴.

2. ATM'den Para Çekilmesi veya İnternet Üzerinden Yapılan Havalelerde Durum

Bir kimsenin banka kartı kullanmadan ATM'den para çekmesi halinde bilişim sistemi aracılığıyla hırsızlık suçu oluşmaktadır. Elinde bulundurduğu başkasına ait banka kartını ve şifresini kullanarak ATM'den para çekilmesi ya da başkasına ait kredi kartıyla alışveriş yapılması durumunda banka veya kredi kartlarının kötüye kullanılması suçu oluşacaktır. Banka görevlisinin bankada hesapları bulunan kişilerin sistemine girerek kendi hesabına para aktarması durumunda Bankacılık Kanunu m. 160'ta düzenlenen bankacılık zimmeti suçu oluşmaktadır. İnternet üzerinden başka birinin hesabına girerek başkasının hesabına para aktarması durumunda bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu oluşur. Burada bilişim sistemi bu suçların işlenmesinde sadece bir araçtır. Paranın kişinin cebinden çekilip alınmasıyla bankadaki hesabından alınması arasında fark bulunmamaktadır¹³⁵. Ancak doktrinde bu görüşe karşıt olarak, dış dünyada maddi varlığı olmayan ama parayla ölçülebilen değerlerin internet aracılığıyla transfer edilmesi hırsızlık suçunu oluşturmayıp TCK m. 244/4'ün kapsamına girdiğini savunan görüş de bulunmaktadır¹³⁶.

Bu görüşe göre, TCK m. 244/4 verilere veya sistemin işleyişine müdahale etmek suretiyle çıkar sağlamasını cezalandırır. Bu nedenle hırsızlık, dolandırıcılık suçlarına göre daha özel niteliktedir. Bu norm varken diğer normlara gidilmesi doğru

¹³⁴ Hüseyin Eker, **Açıklamalı-İçtihatlı Hırsızlık Suçları**, Ankara, Adalet Yayınevi, 2014, s. 241.

¹³⁵ Koca/Üzülmez, **a.g.e.**, s. 877, 878; Taşkın, **a.g.e.**, s. 117; Artuk/Gökçen/Alşahin/Çakır, **a.g.e.**, s. 485.

¹³⁶ Akbulut, **a.g.e.**, s. 224, 225.

değildir. Bir hesaptan diğer hesaba yetkili olmayan kişi tarafından havale yapılması durumunda verilerde değişiklik yapılarak, veriler üzerinde oynama yapılarak TCK m. 244/4 anlamında çıkar sağlanması söz konusudur¹³⁷. Bu görüş havale işlemleri ile kişinin haksız çıkarda sağlaması durumunda, havalenin aslında sistemde bulunan verilerin değiştirilmesi olduğundan bahisle TCK m. 244/4'ün uygulanacağını savunmaktadır. Bankalara veya kamu kurum kuruluşlarına karşı işlenen fiiller TCK m. 244/3'te düzenlendiğinden bu görüş, internet aracılığıyla havale gibi bankacılık işlemleri yoluyla çıkar sağlama fiillerine kanunun sistematigi uyarınca TCK m. 244/4'ün uygulanacağını savunmaktadır¹³⁸.

Kullanım yaygınlığı bakımından online bankacılık sistemine de değinmek gerekir. İnternet bankacılığı, bankacılık hizmetlerini internet üzerinden ve mobil uygulamalar ile sunabilen, müşterilerine 7/24 bankacılık hizmeti verebilen alternatif bankacılıktır¹³⁹.

Online bankacılık kullanmak isteyen bir kişi, internet aracılığıyla banka tarafından kendisine verilen müşteri numarasını ve şifreyi girmekte, daha sonra kendisine gönderilen sms şifresini girerek işlemlerini gerçekleştirmektedir. Bu şifre sistem tarafından otomatik olarak verilmekte ve banka personeli dâhil hiç kimse tarafından bilinmemektedir. Hesap sahibine kendisine özel tahsis edilen bu şifreyi kırmak mümkün olduğundan veya sistemdeki güvenlik önlemlerinin aşılması gerçekleşebildiğinden bunları ele geçiren kişinin verilerde oynama yaparak sistemin işleyişini engellemek suretiyle TCK m. 244/4'te düzenlenen suçu gerçekleştirmesi mümkündür¹⁴⁰.

Online bankacılık suçlarından tek kullanımlık şifre güvenliğini aşmak için failler ilk yol olarak elde edilen kişisel bilgiler doğrultusunda sahte belgeler ile SIM

¹³⁷ Akbulut, **a.g.e.**, s. 224; Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 615.

¹³⁸ Akbulut, **a.g.e.**, s. 225.

¹³⁹ Harun Aksaya, Kadir Burak Olgun, Mehmet Elibol, "İnternet Bankacılık Hizmetleri ve Paydaşların Sorumlulukları", **Enformatik, Toplum ve Hukuk**, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016, s. 120.

¹⁴⁰ Akbulut, **a.g.e.**, s. 250; Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 991.

kart çıkartmaktadır. Böylelikle banka tarafından gönderilen tek kullanımlık mesajların yeni çıkarılan SIM karta gelmesi sağlanmaktadır. İkinci yol ise bilgileri alınan kişilerin cep telefonu numarasına mesaj gönderilmesi usulüdür. Mesajın içeriğinde kişinin cihazına virüs bulaştıracak bir internet bağlantı adresi bulunmaktadır. Kişi bağlantıya tıkladığı zaman virüs otomatik olarak telefona bulaşmakta ve cep telefonuna gelen tüm mesajlar hat sahibinin bilgisi dışında başka bir telefon numarasına yönlendirilerek bilgilerin alınması sağlanmaktadır. Dolayısıyla tek kullanımlık şifrelerin sanıldığı kadar güvenli olmadığını söylenmektedir¹⁴¹.

Bu kapsamda online satış konusuna da değinmek gerekecektir. İnternette alışveriş hizmetlerinde gerçek alıcının şifresinin ve diğer bilgilerinin ele geçirilerek satış işleminin failin lehine yapılması durumunda bu suç oluşur. Ancak TCK m. 244/1 ve m. 244/2’de sayılan fiillerin gerçekleştirilmesi suretiyle haksız çıkar kazanılırsa bu suç oluşur. Aksi halde TCK m. 142/2-e’nin uygulanacağını söyleyebiliriz. Zira Yargıtay da bu tür fiillerde bu sonuca varmıştır. Karara konu olayda “web sitesine girişte abone olan katılan tarafından kullanılan kullanıcı adı ve parola bilgilerinin sanık tarafından ele geçirilmesi sonucu web sitesinden tek şifre uygulanmasından faydalanarak site tarafından abonelerine ücreti karşılığında sunulan ürün ve servis hizmetlerinden olan oyun satın alınarak, buna ilişkin ücretin katılanın internet faturasına yansıtılmak suretiyle haksız menfaat temin etmek şeklindeki eylem” Yargıtay tarafından bilişim sistemi kullanmak suretiyle hırsızlık suçu kapsamında kabul edilmiştir¹⁴².

Yargıtay’a göre TCK m. 142/2-e hükmü altın, hisse senedi, para gibi ekonomik değeri olan malları fiziki temasta bulunmadan, verileri değiştirme suretiyle hâkimiyetinin değiştirilmesi durumlarını kapsar.

5237 sayılı TCK’nın yürürlüğe girmesinden sonraki birkaç yıl içinde Yargıtay’ın 6. ve 11. Ceza Daireleri arasında başkasının banka hesabına internet üzerinden girerek hesaptaki paraların başka bir hesaba gönderilmesi şeklinde

¹⁴¹ Yiğitbaşı/Gürsul, **a.g.m.**, s. 198.

¹⁴² Akbulut, **a.g.e.**, s. 250, 251.

gerçekleşen olaylarda iki daire arasında içtihat farklılığı bulunmaktaydı. Yargıtay 6. Ceza Dairesi bu tür olayları genellikle hırsızlık suçu olarak nitelendirirken, 11. Ceza Dairesi bilişim sistemi aracılığıyla yarar sağlama suçu olarak kabul ediyordu. Ancak Yargıtay CGK, 2009 yılında verdiği kararında¹⁴³, bu tür olaylarda TCK m. 244/4 anlamından bir veri transferi değil, bu veri tarafından temsil edilen paranın mal edinilmesine yöneldiğini belirterek, olaya uygulanacak hükmün TCK m. 142/2-e bendinde düzenlenen bilişim sistemi aracılığıyla hırsızlık suçunun oluştuğunu kabul etmiştir¹⁴⁴.

Yargıtay Ceza Genel Kurulu söz konusu 17.11.2009 tarih 2009/11-193 Esas 2009/268 Karar sayılı kararında sanığın şirket hesabının internet şifresini kırarak bu hesaptan kendi adına açtırdığı hesaba havale yaparak haksız çıkar elde etmesi fiilini “... maddede başka bir suçu oluşturmaması halinde denilerek tali norm niteliğinde bir düzenleme yapılmıştır. Yani bilişim sistemleri aracılığıyla bir çıkar sağlandığından öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık, zimmet gibi asli olan önce uygulanması gereken bir başka suçun oluşup oluşmadığı tartışılmalı eylem başka bir suç oluşturmamışsa o zaman TCK.nın 244/4 maddesi irdelenmelidir. Temyiz davasına konu olayda sanık, bilişim sistemine zarar verme veya verilen yok etme, bozma, erişilmez kılma amacıyla hareket etmemektedir. Hedefi bilişim sistemi olmayıp, amacı bilişim sistemini kullanarak şikayetçinin bankadaki parasını çalmak, ele geçirmektir. Tamamıyla malvarlığına yöneliktir. Bu amaçla yani şikayetçinin parasına ulaşmak için bankanın sistemine girmiş, banka sistemi ve verilere yönelik bir eylemde bulunmamış, hesaptaki parayı kendi hesabına havale etmiştir. Hırsızlık suçu bilişim sisteminden yararlanılarak işlenmiş olup dolaylı bilişim suçu mevcuttur ve sanığın eylemi tali norm niteliğinde bulunan 244/4 maddesindeki suça uygun olmayıp daha ağır cezayı gerektiren 142/2-e maddesindeki suça uygun bulunmaktadır. Öte yandan eylemin 765 sayılı Ceza Yasası döneminde 525/b-2 maddesine uygun bulunması, yeni yasada bu suçun karşılığı olan 244/4 maddenin uygulanmasını gerektirmemektedir.

¹⁴³ Yargıtay CGK, 17.11.2009 tarih, 2009/11-193 Esas 2009/268 Karar sayılı kararı.

¹⁴⁴ Koca/Üzülmez, **a.g.e.**, s. 878.

Çünkü 765 sayılı Yasada 525/b maddesi asli norm olarak düzenlenmiştir ve 765 sayılı Yasada bilişim sistemlerinin kullanılması suretiyle hırsızlık suçuna yer verilmemiştir.” denilerek TCK m. 142/2-e maddesinde düzenlenmiş bulunan “bilişim sistemi kullanılmak suretiyle hırsızlık” suçunun gerçekleştiğini kabul etmiştir. Burada veriyi başka bir yere göndermekten ziyade verinin temsil ettiği parayı alarak mal edinme fiili olduğu gibi failin de katılanın internet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka bir alternatifi olmaması gerekçe gösterilmiştir¹⁴⁵.

Yargıtay’da oluşan görüş birliği sayesinde TCK m. 244/4’ün uygulanma alanı çok daralmıştır. Verinin temsil ettiği değer esas alınıp bu yolla işlenen suçlar TCK m. 142/2-e kapsamında değerlendirilmiştir¹⁴⁶.

Bizim de katıldığımız görüşe göre, gönderilen verinin temsil ettiği değer olan paranın failin hâkimiyetine havale yoluyla geçmesiyle TCK m. 142/2-e’de düzenlenen suç oluşur. Bu nedenle Yargıtay Ceza Genel Kurulu kararı da isabetlidir.

¹⁴⁵ Serdar Mermut/Osman Berk Alpaslan, “Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Çıkar Sağlama Suçu ile İlgili Bir Yargıtay Ceza Genel Kurulu Kararının İncelenmesi”, **Suç ve Ceza Dergisi**, 2010, S. 2, İstanbul, s. 107 vd; Akbulut, **a.g.e.**, s. 229,230.

Çoğunluk görüşüne katılmayan kurul üyesi Kubilay Taşdemir ise ‘*Hırsızlık suçunun maddi konusu başkasına ait taşınır maldır. Taşınır mal mevcut ve maddi varlığı olan bir cisimdir. Veri taşınabilir mal olarak düzenlenmemiş ve tanımlanmamıştır. Verinin sahibinin rızası olmaksızın bilişim sisteminden başka bir yere gönderilmesinde hırsızlık suçunun oluştuğunu söyleyebilmek için verinin taşınır mal olarak kabulü zorunludur. TCK’da verinin taşınır mal olarak tanımlanmaması nedeniyle bu fiil hırsızlık suçuna ait norm öncelikle uygulanması gereken asli norm niteliğini taşımaz. 5237 sayılı TCK veriyi taşınır bir mal olarak tanımlamadığına göre, veriyi temel almak suretiyle bilişim sistemleri kullanılarak elde edilen haksız edinimleri hırsızlık suçu olarak nitelendirmek TCK’daki suçta ve cezada kanunilik ve kıyas yasağı ilkeleri karşısında olanaklı değildir.*’ görüşünü ileri sürerek fiilin 5237 sayılı TCK’nın 244/4 maddesine uyan suçu oluşturduğu yönünde oy kullanmıştır. Mermut/ Alpaslan, **a.g.m.**, s. 120 vd.

¹⁴⁶ Yılmaz, **a.g.m.**, s. 95. Yargıtay 17. Ceza Dairesi 2015/10051 Esas 2016/9471 Karar sayılı 23.06.2016 tarihli kararı; “müştekilerin de işyeri olan Kepez Elektrik Santralinde kurulu bilgisayarların harddiskinde şifre kırmaya yarayan "Keylogger" programının bulunduğu tespit edildiğinin ve program sayesinde elde edilen klavye bilgilerinin önceden belirlenen bir e-mail adresine yönlendirildiğinin, diğer bir deyişle bu program sayesinde müşterilerin hesabına girildiğinin anlaşılmasına karşın, anılan programı yükleyen kişinin kimliğinin ve ele geçirilen bilgilerin hangi adreslerle irtibatlı bulunduğu incelenmesi gerekirken bu hususlarda herhangi bir araştırma ve incelemeye girilmemesi, müşterilerin banka hesaplarından internet bankacılığı şifresi kırılarak hesapta bulunan paraların sanıkların banka hesabına aktarıldığının anlaşılması karşısında; sanıkların eylemleri 5237 sayılı TCK’nın 142/2-e maddesindeki suçu oluşturduğu halde, aynı Yasa’nın 244/4. maddesi ile uygulama yapılması bozmayı gerektirmiştir.” www.corpus.com.tr (Çevrimiçi) 17.03.2019.

Bir banka ya da kredi kurumunun bilişim sisteminde yer alan para söz konusu sistemde veri olarak bulunur. Bilişim sisteminde veri olarak bulunan para da hırsızlık suçunu oluşturan mal kavramının içinde yer alır. Dolayısıyla failin bu suçu işlemekteki kastı mağdurun aslında verilerini değil parasını hâkimiyeti altına almaktır. Suçun konuluş amacı da dikkate alındığında YCGK'nın 17.11.2009 tarihli kararının yerinde ve amaca uygun olduğu söylenebilir¹⁴⁷.

TCK m. 142/2-e ile TCK m. 244/4 arasında asli norm-tali norm ilişkisi bulunmaktadır. Bilişim sistemini kullanmak suretiyle bir hırsızlığın gerçekleşmesi durumunda, fail hırsızlığın bu bentte düzenlenen nitelikli şeklinden sorumlu olacaktır¹⁴⁸.

Bu karara katılmayan görüş ise havale edilen şeyin her halükarda veri olduğunu belirtir. Bu görüşe göre, TCK m. 244 hırsızlık ve dolandırıcılık suçlarına göre özel norm niteliği taşır. Aynı konuda özel norm varken genel norma gidilemez. TCK m. 244'ün getirilme amacı bilişim alanında gerçekleşen suç niteliği taşıyan her türlü fiili cezalandırmaktır. Bu suçlarda ortak payda suçun bilişim sisteminde işlenmesi ve hukuki konunun da veri niteliğinde bulunmasıdır. Bu şekilde transfer edilen parayı bir malvarlığı değeri olarak kabul edecek olursak TCK m. 244/4'ün bir anlamı kalmaz. Kanun koyucu bu tür para transferlerinin de yapılacağını öngörerek fiillerin bir banka veya kredi kurumuna ait bilişim sistemi üzerinde işlenmiş olmasını daha fazla cezayı gerektiren nitelikli hal saydığı gibi bu suretle haksız yarar elde edilmesini de ayrıca cezalandırmıştır. Bu nedenle bu görüş internet bankacılığı yolu ile havale işlemlerini TCK m. 244/4 kapsamında olduğunu ileri sürmektedir¹⁴⁹.

Verinin taşınabilir mal sayılmayacağından bahisle bir başkasının banka hesabından kendi hesabına para transferinin hırsızlık suçunu oluşturmayacağını ileri sürülmesi doğru değildir. Bilişim sistemlerine karşı ya da bunların araç olarak kullanıldığı tüm suçlar, veriler kullanılarak işlenir. Kişi başkasının hesabından kendi

¹⁴⁷ Dülger, **a.g.e.**, s. 469.

¹⁴⁸ Koca/Üzülmez, **a.g.e.**, s. 603.

¹⁴⁹ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 994.

hesabına para aktarırken, bu verileri değil bu verileri kullanarak başkasının parasını aktarmaktadır. Burada bilişim sistemi paranın alınması bakımından araç fonksiyonu görmektedir¹⁵⁰. Bu örnekte veri hırsızlık suçunun konusu olmayıp suçun tamamlanmasında araç niteliği taşımaktadır. Fail sadece veriyi taşıma amacı güdüyorsa ve hırsızlık suçunun konusu dışında bir menfaat temin ediyorsa burada TCK m. 244/4'ün ihlal edildiğinden bahsedilecektir¹⁵¹.

Bu görüşe göre bilişim sisteminin kullanılması suretiyle malın alınması ibaresinin, örneğin bir yere girmek için kullanılan sistemin devre dışı bırakılması suretiyle girilip para veya diğer taşınır malların fail tarafından egemenliği altına alınmasını ifade etmektedir. Hırsızlık suçundaki nitelikli halin söz konusu olabilmesi için temel şeklinin unsurlarına ilave unsurlar eklenmesi, nitelikli hal gerçekleşmediğinde temel şeklinin uygulanabilmesi gerekir. Bilişim sistemi aracılığıyla çıkar sağlanmasında nitelikli hal uygulanmadığından temel şeklinin uygulanamayacağını savunmaktadır¹⁵². Bu görüşe göre hırsızlık suçu ancak taşınabilir eşyalar üzerinde işlenebilmektedir. Örneğin bir şirketin üretimini yaptığı beyaz eşyaları muhafaza ettiği ve şirketin bilişim sistemine bağlı merkezi kilit sistemi ile kilitli deposundaki malları çalmak üzere ağ üzerinden şirketin bilişim sistemine ulaşan hırsızların kilit sistemini kontrol eden bilişim sistemini tahrip ederek devre dışı bırakmaları ve depo kapılarının açılması üzerine beyaz eşyaları çalması olayında hırsızlık suçu bilişim sistemi kullanılarak işlenmektedir¹⁵³.

Bu görüş kanunda veri taşınabilir bir mal olarak tanımlanmadığından veriyi temel almak suretiyle bilişim sistemleri kullanılarak elde edilen haksız kazanımları hırsızlık suçu kapsamında saymak mümkün olmayacağını savunmaktadır. Örneğin bir bilgisayar sistemine yanlış veri girerek ya da mevcut veriler değiştirilerek kişinin

¹⁵⁰ Koca, “Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları”, s. 1657.

¹⁵¹ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 881, 882.

¹⁵² Akbulut, **a.g.e.**, s. 227.

¹⁵³ Kurt, **a.g.e.**, s. 171.

kendine haksız yarar sağlaması durumunda ortada taşınabilir bir mal bulunmadığından hırsızlık suçu oluşmayacağını belirtmektedir¹⁵⁴.

Bu görüşe göre diğer yandan hırsızlık suçuna konu olan taşınır mal, zilyedin rızası dışında tamamen onun hâkimiyet alanından çıkmaktadır. Zilyedin rızası dışında malı olan kişi kendi hâkimiyet alanına taşıdığı mal üzerinde orada rahatça tasarruf edebilme imkânına sahip olabilecektir. Oysa sistemde yer alan veriler başka bir yere taşınmakla beraber, bu verileri oluşturan kişinin koyacağı kodlar veya şifreler nedeniyle taşınılan yerde rahatça kullanılmayabilir. Bu durumda ise fiil hırsızlık olarak nitelendirilemeyeceğini savunmaktadır¹⁵⁵.

Kısaca kişinin rızası dışında failin kendisine veya başkasına yarar sağlamak amacıyla hareket edip kişinin eşya üzerinde egemenliğine bilişim sistemi aracılığıyla son verilmesi halinde bu bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu oluşur¹⁵⁶.

TCK m. 143'te hırsızlık suçunun gece vakti işlenmesi durumunda cezanın artırılacağı hükmü bulunmaktadır. Suçun gece vakti işlenmesi, mağdurun karşı koyabilmesi gücünün azalması, failin gecenin karanlığından istifade ile suçun icrasını kolaylaştırması nedenleriyle nitelikli hal olarak kabul edilmiştir. Bu nitelikli halin bilişim sistemlerinin kullanılması suretiyle hırsızlık suçuna uygulanmaması gerekmektedir. Çünkü bilişim sisteminin gece kullanılması fail için bir avantaj olmadığı gibi mağdurun da suçun icrasına karşı koymasına etki eden bir unsur olmayacaktır¹⁵⁷.

Son olarak, TCK m. 142/2-e'de söz konusu olan veri parayı temsil eden veri olduğunu söyleyebiliriz.

¹⁵⁴ Yazıcıoğlu, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, s. 398.

¹⁵⁵ Biçkin, **a.g.m.**, s. 155.

¹⁵⁶ Kızıltan, **a.g.t.**, s. 90.

¹⁵⁷ Değirmenci, **a.g.m.**, s. 208.

D.Bilişim Sistemlerinin Araç Olarak Kullanılması Suretiyle Dolandırıcılık Suçu

TCK m. 244/4'te düzenlenen suçun yardımcı norm olarak düzenlenmiş olması ve dolandırıcılık suçunun özel bir şekli olarak düşünülmemesi karşısında bu suçun unsurlarının ve klasik dolandırıcılık suçuna göre sınırının belirlenmesi gerekmektedir¹⁵⁸.

Sisteme ve veriye müdahalenin yapılmasıyla bir yarar sağlanmıyor ve yararın sağlanmasına ilişkin işlem bir kişi tarafından gerçekleştiriliyorsa bu durumda klasik dolandırıcılık suçu kapsamında fiilin düşünülmesi gerekir. Ancak sisteme ya da veriye müdahale teşkil etmeyen fakat bir bilişim sisteminin kullanılması sonucunda yarar sağlama durumları da dolandırıcılık suçunu oluşturmaktadır. Örneğin; internet üzerinden alışveriş imkânı sağlayan bir sitenin taklit edilmesi sonucunda buradan alışveriş yapılabileceğine ilişkin hileli hareketlerle kişileri aldatıp yarar sağlanması durumunda klasik dolandırıcılık suçunun olduğu kabul edilir¹⁵⁹.

Ağ üzerinden rezervasyon ve ödeme imkânı sunan bir otelin bilişim sistemine girilmesi ve rezervasyondan sonra sanki ödeme yapılmış gibi gerçeğe aykırı veri yerleştirilmesi ve otel yetkilisinin bu kaydı görüp yanılarak kişinin ücretini ödemediği otelde kalmasına izin vermesi durumunda bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu işlenmiş kabul edilir. Burada her ne kadar TCK m. 158/1-f maddesindeki suçla beraber TCK m. 244/2 gerçekleşse de 244/4'te bulunan “başka bir suç oluşturmaması halinde” ibaresinden dolayı fail dolandırıcılık suçunu işlemiş kabul edilir¹⁶⁰.

Dolandırıcılık suçunun söz konusu olabilmesi için hilenin varlığı ve muhatabının mutlaka insan olması gerekmektedir. Mevcut veriler değiştirilerek veya yeni veriler girilerek bir manipülasyon yapıldığında bu hileler insana karşı değil

¹⁵⁸ Ketizmen, **a.g.e.**, s. 183.

¹⁵⁹ **A.e.**

¹⁶⁰ Kurt, **a.g.e.**, s. 171, 172.

bilişim sistemine karşı gerçekleştirilmektedir. Bilişim sistemleri kullanılarak haksız çıkar elde edilmesi suçları bakımından kişinin rolü suçta araç teşkil etmekten öteye gidememektedir¹⁶¹.

Dolandırıcılık suçunun oluşması için fiilin muhatabının gerçek kişi olması gerektiği görüşüne katılmaktayız. Yargıtay 23. Ceza Dairesi'nin 2015/4528 Esas 2015/8082 Karar sayılı 14.12.2015 tarihli kararı da şu şekildedir; “*Sanığın, katılan şirkete ait Mağazasında bilgisayar sorumlusu olarak çalıştığı, şubelerde yapılan satışların yine şubelerde bulunan bilgisayar vasıtasıyla, şirket merkezindeki server üzerinde bulunan veri tabanına işlendiği ve bu işlem sonunda merkezdeki programdan şubelerdeki günlük satış ve stok miktarının takip edildiği, yapılan kayıtların merkezde görevli “....” isimli kullanıcı olan sanık tarafından bilişim sisteminin işleyişi değiştirilerek sisteme gerçeğe aykırı veri yerleştirmek suretiyle haksız çıkar sağlandığı, haksız yararın doğrudan katılana yönelik hileli davranışlarla gerçekleşmemesi karşısında eylemin dolandırıcılık olarak nitelendirilemeyeceği gibi, katılan tarafından sanığın zilyetliğine devredilmiş bir mal bulunmaması karşısında eylemin güveni kötüye kullanma suçunu da oluşturmayacağı belirlenmiş olmakla sanığa yüklenen eylemin TCK'nın 244/4. maddesinde düzenlenen bilişim sistemini aracı kılarak yarar sağlama suçunu oluşturduğu gözetilmeden*”¹⁶² Karara konu olayda sanığın fazladan satış yapılmış gibi göstererek menfaat elde etmesinden dolayı TCK m. 224/4'ten hüküm kurulmuştur. Kararda da görüleceği üzere dolandırıcılık suçunun oluşabilmesi için hileli davranışlarla mağdurun yanılgıya düşürülmesi ve bu yanılgı sonucunda fail veya başkasına haksız yarar sağlanması gerekmektedir. Bu nedenle sisteme veri yükleyerek hile ile gerçekleştirilen fiiller dolandırıcılık suçuna konu

¹⁶¹ Yazıcıoğlu, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, s. 399. Yargıtay 11. Ceza Dairesi 2009/1616 Esas 2009/11328 Karar sayılı 07.10.2009 tarihli kararı; “*Bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunda, verileri otomatik işleme tabi tutma olanağı veren sistemler araç olarak kullanılıp gerçek kişiler aldatılarak çıkar sağlanmaktadır. Bankaların etkin işlevi bulunan çek, hesap cüzdanı, dekont gibi maddi varlıklarının kullanılması halinde ise, banka vasıta kullanılarak dolandırıcılık suçu oluşur. Gerçek bir kişiyle karşı karşıya gelmeden bir başka vasıta kullanılarak görüşmeden, konuşmadan, kişilere yönelik hileli davranışlarla aldatılmadan sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde, bilişim sistemine girerek haksız çıkar sağlama suçu gerçekleşir.*” www.corpus.com.tr (Çevrimiçi) 22.02.2019.

¹⁶² www.corpus.com.tr (Çevrimiçi) 22.02.2019.

olmaz, eğer şartları varsa TCK m. 244/4 gündeme gelebilir. Dolandırıcılık suçunun nitelikli halinin oluşabilmesi için örneğin internet sitesinin kişiyi aldatmakta aracı olması diğer deyişle hilenin bu site ya da bilişim sistemi kullanılarak mağdura yönelmesi ve bu hile sonucunda haksız yararın sağlanması gerekmektedir.

Dolandırıcılık suçundaki kişiye karşı hile mağdura ait verilerin erişilmez kılınması ya da değiştirilmesi ile gerçekleştirilmiş ise hem dolandırıcılık suçunun nitelikli hali hem de TCK m. 244/2’de düzenlenen verilere müdahale suçu oluşur. Burada iki ayrı suç tek fiille gerçekleştiğinden farklı neviden fikri içtima hükümlerinin uygulanması gerekir. Ancak Yargıtay’ın aksi yönde kararları da bulunmaktadır. Yargıtay 15. Ceza Dairesi’nin 2015/6793 Esas 2017/25773 Karar sayılı 04.12.2017 tarihli kararı da şu şekildedir; “ Sanıkların, müşteki ...’ın ..., müşteki ...’nın ... isimli MSN adresleri ile bu adreslere bağlı facebook hesaplarının şifrelerini kırmak suretiyle ele geçirdikleri, müşteki ...’nın hesaplarına bağlı arkadaşlarından müşteki ... ile müşteki ... gibi görüşerek para talep ettikleri, müşteki ...’ın eşi müşteki ...’ın da talep edilen 700 TL’yi sanık ...’a ait hesaba yatırdığı, yatırılan paranın sanık ... tarafından çekildiği, bu şekilde sanıkların nitelikli dolandırıcılık ve bilişim sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarını işledikleri... ’’¹⁶³

Fiilde eğer banka kartı veya kredi kartı kullanmak suretiyle bir bilişim sistemi kullanılmaksızın örneğin slip makinelerinin kullanılması gibi mağdurun iradesini etkileyecek surette hile söz konusu olursa, bu takdirde fiil bir bilişim sistemine karşı işlenmiş olamaz, zira henüz bir bilgisayara veri yüklemek veya mevcut verileri manipüle etmek söz konusu olmamıştır, bu sebeple burada sadece mağdurun iradesi etkilendiğinden dolandırıcılık suçu söz konusu olacaktır¹⁶⁴.

“Fake mail” olarak adlandırılan ve kişide bankanın internet şubesine girdiği kanısını uyandıran maillerin kullanılması yoluyla çıkar elde edilmesi durumunda failin nitelikli dolandırıcılık suçundan cezalandırılacağını söyleyebiliriz¹⁶⁵. “Phishing”

¹⁶³ www.corpus.com.tr (Çevrimiçi) 22.02.2019.

¹⁶⁴ Yazıcıoğlu, “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, s. 411.

¹⁶⁵ Taşkın, **a.g.e.**, s. 192.

siteleri de aynı şekilde müşteriye bankası adına inandırıcılığı yüksek bir kurumdan elektronik posta iletilmesi gönderildiği izlenimiyle kişiyi aldatmaktadır¹⁶⁶.

Örneğin, mal alımı için kendisine gelen satıcının mobil pos cihazından kredi kartı ödemesi yapacak müşterinin, kartını satıcıya vermesinin ardından satıcının hileli hareketlerle alıcıyı kandırıp müşteri bilgilerini ele geçirmesi ve kendisine haksız menfaat temin etmesi durumunda TCK m. 158/1-f oluşur. Bu suçun maddi unsurunun oluşması için hareketin gerçek bir kişiye yöneltilmiş olması, onun kandırılarak çıkar sağlanması gerekmektedir. Burada gerçek kişiye yöneltilmiş bir hileli hareket ve bu fiilin gerçekleşmesi için bir bilişim aracı olan pos cihazı vasıta olarak kullanıldığı için TCK m. 158/1-f oluşmuştur¹⁶⁷.

TCK’da nitelikli dolandırıcılık suçunun düzenlendiği 158. maddesinin 1 numaralı fıkrasının (f) bendinde, dolandırıcılık suçunun *“bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle”* işlenmesi halinde üç yıldan on yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunacağı ifade edilmiştir. Söz konusu (f) bendinde ise birden fazla nitelikli hal düzenlenmiştir. İlki bilişim sistemlerinin, ikincisi ise banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılıktır¹⁶⁸.

Madde gerekçesinde *“bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir.”* denilmiştir¹⁶⁹.

Bu suçun gerçekleşebilmesi için fail tarafından bilişim sistemi üzerinde hileli bir işlemin yapılması gerekir. Örneğin internet üzerinden elektronik ortamda sipariş

¹⁶⁶ Mahmutoglu, “TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, s. 885.

¹⁶⁷ A.e.

¹⁶⁸ Karagülmez, a.g.e., s. 219.

¹⁶⁹ A.e.

vermek ve dijital ödeme yapmak mümkün olduğundan internetteki aldatıcı reklam veya gönderilen e-posta ile sonradan bir takım avantajlar sağlanacağı vaadiyle bir kişinin sözleşme yapmaya ikna edilmesi durumunda bu elektronik sözleşme ve buna bağlı ödeme yapılmasında hile kullanılmış olur nitelikli dolandırıcılık suçu gerçekleşmiş olur¹⁷⁰.

Bilişim sistemlerinin araç olarak kullanılmasından maksat, bilgileri otomatik işleme tabi tutan manyetik sistemlerden araç olarak yararlanmak suretiyle belli bir malvarlığı üzerinde tasarrufta bulunma yetkisine sahip olan kişi veya kişilerin aldatılması ve bu yolla haksız bir kazancın sağlanmasıdır. Örneğin internet üzerinden yayın yapan bir siteye girmenin bedava olduğu yazdığı halde, buraya giren kişilere kıtalar arası yapılan telefon görüşmesi faturasının yansıtılmış olması halinde dolandırıcılık suçunun nitelikli hali oluşmuş olur¹⁷¹.

TCK m. 244/4'te ise düzenlenen suçun oluşması için bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi fiillerinden birinin veya birkaçının gerçekleşmesi ve bu fiil sonucunda failin mali veya manevi haklara yönelik haksız bir yarar sağlaması gerekir. Dolayısıyla bu suç tipinde manipölasyon fiilleri yapılarak gerçekleştirilen hileler insana karşı değil bilişim sistemine karşı gerçekleştirilmektedir¹⁷².

Veri, program ve sisteme müdahaleler yoluyla yarar sağlanması, genel olarak dolandırıcılık suçu çerçevesinde ele alınmış ancak bu suçun unsurlarının söz konusu fiilleri kapsayamamasından hareketle ayrı bir suç olarak düzenlenmiştir. Bu suçun ayrı bir suç olarak düzenlenme nedenlerini iki başlık altında toplayabiliriz. İlki, bilişim sistemi aracılığıyla hileli ya da aldatıcı hareketler yapılarak haksız çıkar sağlanmasında bu hareketlerin kişiye karşı yapılmaması nedeniyle klasik dolandırıcılık suçunun unsurlarının bu tür fiilleri kapsamaması yönündendir. İkinci olarak, ceza kanunlarında yer alan güveni kötüye kullanma, hırsızlık ve dolandırıcılık suçlarında elde edilen

¹⁷⁰ Parlar, **a.g.e.**, s. 119.

¹⁷¹ Koca/Üzülmez, **a.g.e.**, s.703

¹⁷² Parlar, **a.g.e.**, s. 119.

şeylerin cismani olması bilişim suçları bakımından ise durumun farklı olmasını gösterebiliriz¹⁷³.

İlk unsuru açıklamak gerekirse bilişim sistemi aracılığıyla yarar sağlama fiillerinde kişiye karşı bir hile yapılması sonucunda kişinin aldatılmasının söz konusu olmaması nedeniyle, kişiye karşı hileli hareketin yapılması unsurunun yerini bilişim sisteminin işleyişine veya veriye müdahale edilme unsuru almaktadır¹⁷⁴.

Kişiye karşı hileli hareketlerin olmaması karşılıksız yararlanma suçu bakımından da gündeme gelmiştir. 765 sayılı TCK m. 521/b’de düzenlenen otomatların kötüye kullanılması suçunda hareketler gerçek kişiye karşı gerçekleştirilmez. Kişinin hile ile kandırılmasından bahsedilemeyeceğinden bu suç dolandırıcılık suçundan ayrılmaktadır¹⁷⁵.

1997 Ön tasarısının 218. maddesinde ve 12.05.2003 tarihinde TBMM’ye sunulan Türk Ceza Kanunu Tasarısının 233. maddesinden yer verilen bu suçun, her iki tasarıda bulunan gerekçesi incelendiğinde, açıklamaların bilişim sistemleri aracılığıyla yarar sağlama bakımından da gündeme geldiği görülmektedir. Ön tasarıdaki gerekçenin ilgili kısmında; *“Mesela bir bankanın elektronik cihazlarını programlamakla görevli yükümlü memuru, yanıltıcı bilgileri alete vermek suretiyle belirli bir hesapta mevcut olmayan bir paranın bulunduğu yolunda ilgili memura bilgi verilmesini ve bu suretle bu hesaptan para çekmek isteyen kimseye ödeme yapılmasını veya başka bir şubeye ya da bankaya havale gönderilmesini sağlayabilir.”* örneği verilmiştir. Aynı gerekçe bahsi geçen tasarıda da mevcuttur. 5237 sayılı TCK’da ise gerekçede bu örneğe yer verilmemiştir¹⁷⁶.

Otomatların kötüye kullanılmasının dolandırıcılık suçunu oluşturmayacağına ve bu sebeple ayrı bir düzenleme yapıldığına ilişkin gerekçe TCK m. 244/4’te düzenlenen suç için de geçerlidir. Her iki suçun düzenlenmesinde gerekçe, kişiye karşı

¹⁷³ Ketizmen, **a.g.e.**, s. 147.

¹⁷⁴ **A.e.**, s. 149.

¹⁷⁵ **A.e.**, s. 150.

¹⁷⁶ **A.e.**

bir hilenin ya da aldatmanın söz konusu olmamasıdır. Gerekçedeki örnekte programa müdahale sonrasında memura bilgi verilmesi ve bu şekilde para çekilmesini sağlamaktan bahsedilmektedir. Bu örnek bir kişiyi aldatacak şekilde hileli hareketlerin olması karşısında dolandırıcılık suçu kapsamında değerlendirilmelidir. Bu örnek genel olarak bilgisayar aracılığıyla yarar sağlamanın dolandırıcılığın özel şekli olarak düzenlenmesinde gerekçe olarak ileri sürülmektedir¹⁷⁷.

Bu suçun ayrı olarak düzenlenmesinde diğer etkenin de verinin eşya olarak kabul edilmemesi olduğundan yukarıda bahsedilmişti. Verinin eşya/mal olmaması karşısında bunların ele geçirilmesinin klasik hırsızlık suçunu oluşturmayacağı gerekçesi gerçeği yansıtmamaktadır. Sorun veri hırsızlığı ya da verinin ele geçirilmesi şeklindeki suçlar ile çözümlenmeye çalışılmıştır¹⁷⁸.

Nitelikli dolandırıcılık suçunun düzenlenmesinin nedeni, verinin eşya/mal olmamasına bağlı olarak dolandırıcılık suçunda elde edilecek şeyin cismani varlığının bulunması gerektiği gerekçesi değil, burada gerçek gerekçe gerçekleşen fiilde kişiye karşı hile içeren fiilin olmamasıdır¹⁷⁹.

Bu hükümle, 765 sayılı TCK m. 525/b-2'nin uygulamada ortaya çıkardığı sorunları çözmek amaçlanmıştır. Bu sorunların çözümü için özellikle içtima bahsini kolaylaştırmak amacıyla bilişim sistemlerinin kullanılmasının hırsızlık ve dolandırıcılık suçunun daha ağır cezayı gerektiren nitelikli hal olarak düzenlenmesi, 245. maddede düzenlenen banka ve kredi kartlarının kötüye kullanımına ilişkin suçların düzenlendiğini söyleyebiliriz¹⁸⁰.

Bu kapsamda bilişim sistemlerinin işleyişine ve veriye müdahale edilerek kişiye karşı herhangi bir hileli hareketin yapılması ve kişinin aldatılması söz konusu olmadan yarar sağlanmasının incelemeye esas suçu oluşturacağını söyleyebiliriz¹⁸¹.

¹⁷⁷ Ketizmen, **a.g.e.**, s. 151.

¹⁷⁸ **A.e.**, s. 152.

¹⁷⁹ **A.e.**, s. 152, 153.

¹⁸⁰ **A.e.**, s. 174.

¹⁸¹ Ketizmen, **a.g.e.**, s. 175.

Yargıtay'ın bilişim sistemlerinin kullanılması suretiyle işlenen dolandırıcılık suçuyla (TCK m. 158/1-f) bilişim sistemi kullanarak haksız çıkar sağlama suçu (TCK m. 244/4) arasındaki farkı belirlemek için geliştirdiği ölçüte değinmek yerinde olacaktır. Yargıtay TCK m. 244//4 ile TCK m. 158/1-f arasındaki farkı ortaya koyan kararlarında bu iki suç arasındaki ayırımın suçun kime ve neye karşı işlenmiş olduğuna göre yapılacağını ortaya koymuştur. Dolandırıcılık suçunun temel şeklinin oluşması için fail tarafından bir insana karşı hileli hareketlerin yapılması gerekmektedir. Hileli davranışlar eğer bir bilişim sistemi kullanılmak suretiyle gerçek kişiye karşı gerçekleştiriliyor ve bu fiil sayesinde kişi yanıltılarak haksız bir kazanç elde ediliyorsa nitelikli dolandırıcılık suçu oluşur. Buna karşılık bir gerçek kişiye karşı hileli davranışlar sergilenmeksizin sırf bilişim sistemi kullanılarak haksız yarar sağlanıyorsa bilişim sistemi aracılığıyla haksız yarar sağlama suçu oluştuğu kabul edilir¹⁸².

Yargıtay, banka görevlilerine karşı hileli hareketler sonucunda daha önce açtığı hayali hesaplara karşılığın yatırılmadan para aktarılması durumunda dolandırıcılık suçunun oluştuğunu kabul etmiştir. Bu olayda paranın bir bilişim sistemi kabul edilen ATM'den çekilmiş olması fiilin hukuki niteliğini etkileyen bir unsur olarak görülmemiştir. Aynı şekilde salam tekniğinde, fiilin failin sahte bir talimat ile bankaya giderek banka çalışanına bu talimatın gösterilmesi suretiyle gerçekleştirilmesinde dolandırıcılık suçu oluşur. Burada sahte talimat hileyi oluşturmakta ve bu hile ile banka çalışanına para transfer işlemi yaptırılmaktadır¹⁸³.

Yargıtay son dönemde verdiği kararlarda TCK m. 244/4 ile bilişim sistemlerini kullanmak suretiyle gerçekleştirilen nitelikli dolandırıcılığın düzenlendiği TCK m. 158/1-f arasındaki farkı ortaya koyarken gerçekleştirilen fiilin kime veya neye karşı gerçekleştirildiği kriteri üzerinden hareket etmektedir. Buna göre hile ve desise içerikli fiil bir bilişim sistemi kullanılmak suretiyle bir kişiye karşı gerçekleştiriliyor ve bu fiil neticesinde haksız bir kazanç elde ediliyorsa burada 158/1-f 'nin gerçekleştiğini

¹⁸² Koca/Üzülmez, **a.g.e.**, s. 880; Akbulut, **a.g.e.**, s. 228.

¹⁸³ Ketizmen, **a.g.e.**, s. 167.

söyleyebiliriz. Zira dolandırıcılık suçunun gerçekleşmesi için hile ve desise içerikli fiillerin bir insana karşı yapılması gerekmektedir¹⁸⁴.

Dikkat edilmesi gereken husus her ne kadar bilişim sistemleri kullanılıyor olsa da hileli davranışların muhatabının gerçek bir kişi olması zorunluluğudur. Örneğin bir kişi başka bir kişinin MSN parola ve şifresini ele geçirdikten sonra o kişinin listesindeki kişilerle kurduğu internet iletişimi esnasında sanki o hesabın gerçek kullanıcısıymış gibi kendisine ait bir hesaba havale yapmalarını istemiş ve bu isteği yerine getirilerek haksız kazanç elde etmişse artık burada nitelikli dolandırıcılık hükümlerinin uygulanabileceğini söyleyebiliriz¹⁸⁵.

Dolayısıyla TCK'da dolandırıcılık suçunun ve bilişim sistemlerinin araç olarak kullanması suretiyle işlenmesi ayrıca yaptırıma bağlandığından TCK m. 244/4'ün uygulanması pek mümkün değildir¹⁸⁶.

Diğer bir görüşe göre, 244. madde kapsamındaki bir suç, kimi zaman zimmete ya da hırsızlığa veya dolandırıcılığa ya da güveni kötüye kullanmaya çok benzeyebilir. Bu suçlardan, hırsızlığın mal üzerinde işlenmesi zorunlu iken, verinin mal olmaması; aynı şekilde dolandırıcılıkta da hile ile mağdurun kandırılması gerekirken, bilişim sistemlerinin ise kandırılmasının söz konusu olamaması sebebiyle klasik hırsızlık ve dolandırıcılık suçları hiçbir zaman gerçekleşemeyecektir¹⁸⁷.

E. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu

Eski TCK döneminde, haksız olarak ele geçirilen banka kartları ile ATM'lerden para çekilmesi fiillerinin, ATM'lerin bir bilişim sistemi olması ve bu kartlarla bilişim sisteminin kullanıldığının kabulü sonucunda, 525/b-2 maddesinde

¹⁸⁴ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 992.

¹⁸⁵ **A.e.**

¹⁸⁶ Artuk/Gökçen/Yenidünya, **Ceza Hukuku Özel Hükümler**, s.892.

¹⁸⁷ Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi", s. 399, 400; Akıncı/Alıç/Er, **a.g.m.**, s. 189; Malkoç, **a.g.e.**, s. 1681.

düzenlenen bilgisayar aracılığıyla yarar sağlama suçunu oluşturduğu sonucuna varılmıştı¹⁸⁸.

TCK'nın yeni sisteminde ise bilişim suçları yeniden düzenlenmiş ve TCK m. 244/4'te düzenlenen bilişim sistemi aracılığıyla yarar sağlama suçunun unsurlarının, 765 sayılı TCK m. 525/b-2'ye göre daha belirgin hale getirilmiş ve yardımcı norm olarak düzenlenmesi nedeniyle uygulama alanı daraltılmıştır. Ayrıca TCK'da banka ve kredi kartlarının hukuka aykırı kullanılması suretiyle yarar sağlanmasına ilişkin birtakım fiiller 245. maddede ayrıca düzenlenmiştir¹⁸⁹.

TCK m. 245'te düzenlenen banka veya kredi kartını kullanmak suretiyle çıkar sağlandığında ise failin cezası üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasıdır. Ancak nitelikli hırsızlık suçunu oluşturan TCK m. 142/2-e'ye göre bir hesaptan başka bir hesaba para aktarmak suretiyle fiil gerçekleştirildiğinde beş yıldan on yıla kadar hapis cezasının verilmesi gündeme gelecektir. İnternet aracılığıyla havale yapıldığında daha fazla hapis cezası alınmakta, banka veya kredi kartlarıyla işlem yapılarak para alınmasında ise daha az ceza uygulanmaktadır. Kanun koyucu bu fiillerin niteliği ile ilgili yapılan tartışmalara son vermek amacıyla banka veya kredi kartlarıyla çıkar sağlanmasını özel olarak düzenleme ihtiyacı hissetmiştir. Banka veya kredi kartlarıyla çıkar sağlanmasını özel olarak düzenleyen bu sistemde, diğer kartların kullanılması veya hesaptan başka hesaba havale yapılması suretiyle çıkar sağlanması da TCK m. 244/4 kapsamında ele alınmalıdır. Doktrinde bu görüşü savunan görüş, TCK m. 244/4'te hangi fiillerle suçun işleneceğinin açıkça ifade edilmesine rağmen bu kapsama giren bir fiilin sırf kanun koyucunun tali norm olduğuna ilişkin düzenlemesi sebebiyle başka madde kapsamına girdiğini kabul etmemektedir¹⁹⁰.

Haksız olarak ele geçirilen kartın kullanılması suretiyle ATM'den para çekilmesi durumuna da burada değinmek gerekir.

¹⁸⁸ Ketizmen, **a.g.e.**, s. 184.

¹⁸⁹ **A.e.**, s. 185.

¹⁹⁰ Akbulut, **a.g.e.**, s. 227.

765 sayılı TCK'nın yürürlükte bulunduğu dönemde bilişim suçları bakımından en çok uygulanan hüküm 525/b-2'dir. 525/b-2'in 765 sayılı TCK'da bilişim sistemlerinin kullanılmasıyla ortaya çıkan boşluğu doldurmaktan ziyade özellikle banka ve kredi kartlarının kullanılması suretiyle haksız yarar sağlanan fiillere yönelik olduğu söylenebilir¹⁹¹.

Kısaca "ATM" olarak adlandırılan otomatik para çekme makinelerinden başkası ait kart ile para çekilmesi fiilinin, 765 Sayılı TCK m. 493/2'de düzenlenen suçu mu yoksa m. 525/b-2'de düzenlenen suçu mu oluşturacağı tartışmalıdır¹⁹².

Yargıtay 6. Ceza Dairesi kararlarında bu tür fiillerin 765 sayılı TCK m. 493/2'de düzenlenen suçu oluşturduğunu ve bu tür fiillerin işlenmesinde banka kartının alet olduğunu ifade etmişlerdir. Otomatik para çekme makinelerinden para çekilmesi fiilini hırsızlık olarak nitelendirmiş, banka kartının kullanılmasını 493/2'de düzenlenen anahtar ve diğer aletler kavramına dâhil olduğunu ifade etmişlerdir¹⁹³.

Yargıtay Ceza Genel Kurulu ise 11.4.2000 tarih 2000/6-62 Esas K. 2000/72 Karar sayılı kararında, ATM'den para çekilmesi fiili ile ilgili olarak banka kartının anahtar ya da sair alet kavramına dâhil olup olmadığını ve bilişim sisteminin kullanılmış olup olmadığını tartışmıştır. Anılan karara göre; *"Kısaca ATM olarak adlandırılan Automated Teller Machine sisteminin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura gereksinim vardır, bunlardan birincisi kart diğeri ise kullanıcı şifresidir. Bu iki araca sahip olmadan, bir bilgi işlem parçası olan ve ana sisteme bağlı bulunan ATM makinelerini kullanma olanağı yoktur. Belirtilen karta ve şifreye sahip olan kişi, kartı makineye takıp şifreyi de yazdıktan sonra işlem sürecini başlatabilir. Ancak, kartı elinde bulunduran kişinin makine vasıtasıyla sisteme verdiği komutların yerine getirilebilmesi için ana kumanda merkezinin de bu komutları onaylaması gerekmektedir. Örneğin nakit para çekilmek istendiğinde hesapta para yoksa veya günlük çekme limiti dolmuş ya da herhangi bir nedenle hesap*

¹⁹¹ Ketizmen, **a.g.e.**, s. 159.

¹⁹² **A.e.**

¹⁹³ **A.e.**, s. 160.

ana merkez tarafından kullanıma kapatılmışsa işlem, komut onaylanmayacağından yapılamaz. Bu olgu da gösteriyor ki ATM makineleri bir bilgi işlem sisteminin ünitesidir. Yine, sistem harekete geçirmede kullanılan kartların geleneksel hırsızlık suçları bakımından “sair alet” olarak kabul edilmesi olanaklı değildir. Gelişen teknoloji ürünü olsalar da bu kartlar şifre olmadan kullanılamazlar, diğer bir söylemle sistemi tek başına harekete geçiremezler. Sistem harekete geçirilmeden bundan bir yarar sağlanması da söz konusu edilemez. Burada bilgisayar sistemini harekete geçirebilen kartlar ile belirli bir yere girilmesi için kullanılan diğer kartların, fonksiyonları itibariyle yek diğerine benzemediği de belirtilmelidir. Ayrıca anahtar benzeri sair bir aletten söz edebilmek için mantiken bir kilidin de bulunması gereklidir. Bu bakımdan da ATM makinelerinde kullanılan kartları sair alet olarak saymaya olanak yoktur.”

Karara konu olayda sanık, bir bankanın şubesindeki ATM’nin kart konulan bölümüne önceden kâğıt yerleştirmiş, işlem yapmak isteyen şikâyetçinin kartının sıkışmasını sağlayıp böylece sistemle iletişimi ve işleme geçilmesini engellemiş, yardımcı olmak bahanesiyle bankayı arıyor izlenimi verip önceden anlaştığı arkadaşını arayarak şikâyetçi ile görüşmesini sağlamış, şikâyetçiye banka görevlisi gibi davranan arkadaşının yaptırdığı şifre kodlama işlemi sırasında şikâyetçinin şifresini öğrenmiş ve onun ayrılmasından sonra da kredi kartını yuvadan çıkartıp banka şubesindeki ATM’lerden farklı tarihlerde nakit para çekmiştir. Yargıtay Ceza Genel Kurulu bu tür fiillerin sair alet kullanmak suretiyle hırsızlık suçunu oluşturmadığına karar verirken, ATM’lerin ve kartların özelliğinden hareket etmiştir¹⁹⁴.

Kararın gerekçesinde de görüleceği üzere, Yargıtay CGK, 6. CD kararlarından farklı olarak, haksız şekilde ele geçirilmiş banka kartı ile ATM’lerden para çekilmesi fiilinin 765 sayılı TCK m. 493/2’de düzenlenen hırsızlık suçunu değil aynı Kanunu’nun 525/b-2’de düzenlenen suçu oluşturduğu kanaatine varılmıştır¹⁹⁵.

¹⁹⁴ Koca, “Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları”, s. 1652, 1653.

¹⁹⁵ Ketizmen, **a.g.e.**, s. 161.

Kararda, her iki suç kapsamına girecek olan fiil, 525/b-2 maddesindeki özel düzenleme nedeniyle ilgili madde kapsamında kabul edilmiştir. Bu açıdan incelendiğinde aslında hırsızlık suçu kapsamında olan bir fiili, sadece bilişim sisteminin kullanılmış olması nedeniyle bu suçun kapsamına alındığını sonucuna varılır¹⁹⁶.

Ancak Yargıtay 11. Ceza Dairesi 28.05.2008 tarih 2006/8259 Esas 2008/5350 Karar sayılı kararında “*Ayrıntıları Ceza Genel Kurulu’nun 28.12.2004 gün 2004/173-228 sayılı kararından açıklandığı üzere; ATM’nin kart konulan bölümüne önceden kâğıt yerleştiren sanığın, işlem yapmak isteyen şikâyetçinin kartının sıkışmasını sağlayıp, hile ile şifresini öğrendikten sonra şikâyetçiyi uzaklaştırarak hileli davranışlarla ele geçirdiği kart ve şifresini kullanıp para çekerek haksız menfaat sağlamaktan ibaret eyleminin bankanın maddi varlığı olan kartı kullanarak gerçekleştirilmesi nedeniyle 765 sayılı TCK’nın 504/3 maddesinde öngörülen suçu oluşturup oluşturmadığına ilişkin delilleri takdir ve tartışmanın üst dereceli Ağır Ceza Mahkemesine ait olduğuna...*” karar vermiştir. Ceza Genel Kurulu hileli yollarla ele geçirilen kart ve şifresini kullanarak bankamatiklerden para çekilmesi halinde bankayı vasita kılarak dolandırıcılık suçunun oluşacağına karar vermiştir. Daha önceki kararlarında bu tür fiillerin bilişim sistemini kullanarak haksız yarar sağlama suçunu oluşturacağına hükmetmişti¹⁹⁷.

Yeni kanunun yürürlüğe girmesiyle aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü içeren tartışmalı fiiller TCK m. 245’te bağımsız suç haline getirilmiştir. Böylece kartın ne şekilde ele geçirildiğine bakılmaksızın başkasına ait bir banka veya kredi kartını kullanarak kendisine ya da başkasına yarar sağlama fiilleri yani sadece kartla ATM’lerden para çekilmesi şeklindeki fiiller değil, bu kartları kullanarak elde edilen her türlü haksız yararlanmalar bu hükme göre cezalandırılabilir hale gelmiştir¹⁹⁸.

¹⁹⁶ A.e., s. 162.

¹⁹⁷ Koca, “Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları”, s. 1653.

¹⁹⁸ A.e., s. 1654.

Failin hukuka aykırı şekilde elde ettiği kredi kartı bilgilerini internet üzerinden alışveriş yaparken kullanması ya da telefon bankacılığı kullanarak işlem yapması durumunda da TCK m. 245'te düzenlenen suç oluşur. Yargıtay 8. Ceza Dairesi 2014/28971 Esas 2015/18007 Karar sayılı 01.06.2015 tarihli kararı şu şekildedir; “*Sanığın ...'na ait kredi kartı bilgilerini hukuka aykırı olarak ele geçirdikten sonra bu kart bilgilerini kullanarak internet üzerinden değişik zamanlarda harcama yapması eyleminin, zincirleme olarak TCK.nun 245/1 maddesinde tanımlı suçu oluşturduğu gözetilmeden yazılı şekilde TCK.nun 244/4. maddesi uyarınca uygulama yapılması... yasaya aykırı*”¹⁹⁹.

Diğer görüşe göre banka veya kredi kartlarının kullanılması, bu kartların fiziki olarak ATM ve POS cihazı gibi makinelerden geçirilmesini gerektirmektedir. Bu suç ancak banka veya kredi kartlarının bilişim sistemleri üzerinden kullanılmasıyla işlenebileceğini savunmaktadırlar. Bu nedenle, kartın fiziki olarak kullanılmayıp karta ilişkin bilgilerin elde edilerek bilişim sistemi yoluyla haksız yarar sağlanması halinde TCK m. 245 oluşmayacağını belirtirler. Bu durumda somut olayın işleniş şekline göre bilişim sistemini kullanarak hırsızlık, dolandırıcılık veya bilişim sistemleri kullanarak haksız yarar sağlama suçlarına ilişkin hükümler uygulanmalıdır. Suçun kanuni tanımında da açıkça banka veya kredi kartını ele geçiren veya elinde bulunduran kimseden ve rıza olmaksızın bunun kullanılması veya kullandırılmasından söz edildiğinden bahisle tanımdaki bu ifadelerden kanun koyucunun bu suç bakımından kartın fiili olarak kullanılması gerektiğini kastettiğini savunmaktadırlar²⁰⁰.

Yargıtay ise yukarıda açıklandığı gibi aksi görüştedir²⁰¹. Haksız olarak ele geçirilen kart bilgilerinin kullanılması suretiyle internet üzerinden alışveriş yapılması

¹⁹⁹ www.corpus.com.tr (Çevrimiçi) 22.03.2019.

²⁰⁰ Koca/Üzülmez, a.g.e., s.895.

²⁰¹ Yargıtay 8. Ceza Dairesi 2013/15238 Esas 2014/9843 Karar sayılı 16.04.2014 tarihli kararı; “*Başkasına ait kredi kartının kötüye kullanılması suretiyle yarar sağlama suçunun oluşabilmesi için kartın fiziken kullanımı gerekmeyip kart bilgilerinin kullanılması yeterli olduğu cihetle; katılana ait kredi kartı bilgileri ile internet üzerinden değişik tarihlerde birden çok kez kontör transferi yapan sanığın zincirleme banka veya kredi kartlarının kötüye kullanılması suçundan cezalandırılması gerektiği gözetilmeden, bilişim sistemine hukuka aykırı müdahale suretiyle haksız çıkar sağlama suçundan hüküm kurulması hukuka aykırıdır.*” www.corpus.com.tr (Çevrimiçi) 22.03.2019

halinde de TCK m. 245/1’de düzenlenen suçun oluşacağını kabul etmektedir. Yargıtay bu görüşüne gerekçe olarak 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu’nun 3. maddesindeki kredi kartı tanımlamasını işaret eder. Bu kanunda kredi kartı hem basılı kart hem de “fiziki varlığı bulunmayan kart numarası” şeklinde tanımlanmıştır. Bu tanımlı yalnızca 5464 sayılı Kanun’un uygulanması bakımından kabul etmek gerekir. Zira hem TCK m. 245/1’de bulunan ifadeler hem de bu suçla ticari hayatta nakit para yerine kullanılan bu kartların doğru olduğuna yönelik güvenin korunması bu suçun oluşabilmesi için kartın fiziki olarak kullanılmasını gerekli kılmaktadır²⁰².

Failin başkasına ait kartı kullanması aynı zamanda TCK m. 244/1-2’yi de ihlal edebilir. Bu durumda farklı neviden fikri içtima hükümlerinin uygulanması gerekir²⁰³.

F. Zimmet Suçu

5237 sayılı TCK’nın 247. maddesinde düzenlenen zimmet suçunun konusu madde metninde mal olarak ifade edilmiştir. 765 sayılı TCK’da zimmet suçunun konusu “para veya para yerine geçen evrak veya senetler veya diğer mallar” şeklinde düzenlenmişti. Aslında mal ibaresi; para, para yerine geçen evrak, senet ve sair diğer ekonomik değerleri kapsayan üst bir kavram olarak anlaşılması gerekmektedir. Bu nedenle 5237 sayılı Kanun’daki düzenlemede zimmetin konusunun sadece mal olarak ifade edilmesi gereksiz tekrarların önüne geçmek bakımından yerindedir. Ayrıca maddede geçen mal ifadesini de sadece taşınır olarak değil, gerekçede belirttiği gibi taşınır veya taşınmaz mal olabileceği şeklinde anlamak gerekir²⁰⁴. Ekonomik değeri olan ve şey kavramına giren bütün nesneler bu suçun konusuna girer. Misli eşya niteliğinde olan paranın da bu suça konu olabileceği açıktır²⁰⁵.

²⁰² Koca/Üzülmez, **a.g.e.**, s.895.

²⁰³ Koca/Üzülmez, **a.g.e.**, s.902. Yargıtay 15. Ceza Dairesi 2015/8674 Esas 2017/25774 Karar sayılı 04.12.2017 tarihli kararı; “İncelenen dosya içeriğine göre; sanığın, katılan ...'e ait facebook ve MSN hesaplarının şifresini ele geçirip, şifreyi değiştirerek erişimi engellemesi ve müşteki Madlen'in bilgisi dışında kredi kartından harcamalar yaptığıının iddia edilmiş olması karşısında, eylemlerinin, 5237 sayılı TCK'nın 244/2 ve 245/1 maddelerine göre bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçu ile banka ve kredi kartlarının kötüye kullanılması suçunu oluşturduğu anlaşılmakla...” www.corpus.com.tr (Çevrimiçi) 20.03.2019.

²⁰⁴ Koca/Üzülmez, **a.g.e.**, s. 923; Sevik, **a.g.e.**, s.446.

²⁰⁵ İzzet Özgenç, **Zimmet Suçu**, Ankara, Seçkin Yayınları, 2009, s.14.

Zimmet suçunun işlenmesi dolayısıyla elde edilecek menfaatin mutlaka faile sağlanması gerekmez, fiil sonucunda menfaat üçüncü kişiye de sağlanabilir²⁰⁶.

Bir görüş ise daha önce hırsızlık ve mala zarar verme suçlarında bahsedildiği gibi zimmet suçunu düzenleyen TCK m. 247 açıkça mal kavramından bahsettiğinden verilerin ise mal olmaması nedeniyle zimmet suçu söz konusu olamayacağını savunmaktadır²⁰⁷.

Bu görüşe göre, TCK m. 247’de düzenlenen zimmet, bir kamu görevlisinin görevi nedeniyle kendisine devredilmiş olan ve koruma ve gözetimiyle yükümlü olduğu malı kendisinin veya başkasının mülkiyetine sokması unsurlarını içeren suç tipidir. Suçun konusu madde gerekçesinde de belirtildiği üzere taşınır ya da taşınmaz maldır²⁰⁸.

Bilişim sisteminin kullanılması yoluyla hırsızlık suçunda yaptığımız açıklamalarda burada da geçerlidir. Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu tali norm olarak düzenlenmiştir. Sistemdeki verilerin temsil ettiği değer maddi nitelikteki para olduğundan eğer zimmet suçu gerçekleşmişse ayrıca TCK m. 244/4’ten faile ceza verilemez.

G. Kişisel Verilerin Kaydedilmesi Suçu

TCK m. 135’in sadece kişisel verileri koruma altına aldığını söyleyebiliriz. Bu nedenle hükümde yer alan veri ibaresi, doğrudan kişiye ait olan ve kişinin üzerinde tek başına tasarrufta bulunabileceği verilerdir. Bazı bilgiler veri niteliğinde olmakla birlikte kişisel olmaktan çok kurumsal olabilir. Örneğin, bir anonim şirketin ticari sırları bu mahiyettedir. Ticari sır, bankacılık sırrı veya müşteri sırrı ile fenni keşif ve buluşlar veya sınai uygulamaya ilişkin bilgiler ayrı bir hükümde koruma altına

²⁰⁶ Mehmet Emin Artuk/Ahmet Gökçen/Mehmet Emin Alşahin/Kerim Çakır, **Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018, s. 905.

²⁰⁷ Erdoğan, **a.g.e.**, s. 238.

²⁰⁸ Kurt, **a.g.e.**, s. 172.

alındığından bu türdeki bilgilere karşı TCK m. 135 ve devamındaki hükümlerde yer alan suçlar oluşmaz²⁰⁹.

TCK'nın 244/2'de düzenlenen suçun konusu bu suçları kişisel verilerin kaydedilmesi suçunu düzenleyen TCK m. 135 ve kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçunu düzenleyen TCK m.136'dan ayırır. TCK m. 244/2'de her türlü veri suçun konusunu oluşturmaktayken TCK m. 135 ve m. 136'da yalnızca kişisel veriler suçun konusunu oluşturabilmektedir. Öte yandan TCK m. 135 ve m.136'da her türlü yer ve araçta kayıtlı kişisel veriler suçun konusunu oluşturuyorken, TCK m. 244/2'de yalnızca bilişim sisteminde yer alan veriler suçun konusunu oluşturmaktadır²¹⁰.

Bir bilişim sisteminde bulunan verilerin başka bir yere gönderilmesi aynı zamanda TCK m. 136'da düzenlenen “verileri hukuka aykırı olarak verme veya ele geçirme” suçunu oluşturan fiillerin zeminini hazırlayabilir²¹¹. Geçit suç oluşturup oluşturmayacağı suç tipini oluşturan her hareket bakımından ayrı ayrı ve olayın özellikleri dikkate alınarak belirlenmelidir²¹².

Yargıtay 12. Ceza Dairesi'nin 2016/10576 Esas 2017/7642 Karar sayılı 18.10.2017 tarihli kararında geçit suç olarak kabul etmemiş, suçların ayrı ayrı oluştuğunu belirtmiştir. Karar şu şekildedir; “*sanığın, katılanın cep telefonunu katılandan habersiz kendi kullandığı bilgisayara bağlayarak içerisinde bulunan rehber ve media dosyalarının tamamını ele geçirdiği ve cep telefonundaki kayıtları sildiği iddia ve kabul edilen olayda, sanığın sübut bulan eylemleri nedeniyle TCK'nın 244/2. maddesinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirme, aynı Kanunun 134/1 maddesinde düzenlenen özel hayatın gizliliğini ihlal*

²⁰⁹ Özbe/ Doğan/ Bacaksız/ Tepe, **a.g.e.**, s.570.

²¹⁰ Dülger, **a.g.e.**, s. 315. Yargıtay 8. Ceza Dairesi'nin 2014/23 Esas 2014/17639 Karar sayılı 07.07.2014 tarihli kararı; “*ATM cihazına banka ve kredi kartları bilgilerini kopyalamak için sistem kuran, ancak ihbar edilmeleri neticesinde herhangi bir kartın kopyalamasını yapamadan yakalanan sanığın eyleminin TCK.nun 136, 35. maddelerine uyan suçu oluşturduğu gözetilmeden yazılı şekilde TCK.nun 244/2-3. Maddeleri uyarınca hüküm kurulması BOZULMASINA*” www.corpus.com.tr (Çevrimiçi) 22.03.2019.

²¹¹ Artuk/Gökçen/Yenidünya, **Türk Ceza Kanunu Şerhi**, s. 6936.

²¹² Dülger, **a.g.e.**, s. 338.

ve 136/1 maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçlarını oluşturduğu gözetilmeden’’²¹³

Kanaatimizce kişisel verilerin başka bir sisteme gönderilerek kaydedilmesi gibi durumlarda tek hareketle hem kişisel verilerin kaydedilmesi hem de verilere müdahale suçu oluşacağından failin farklı neviden fikri içtima gereği cezası ağır olan suçtan cezalandırılması gerekmektedir.

H. Güveni Kötüye Kullanma Suçu

Güveni kötüye kullanma suçunun konusunu “başkasına ait olup da, muhafaza etmek veya belirli bir şekilde kullanmak üzere zilyedliği kendisine devredilmiş olan mal” oluşturmaktadır²¹⁴. Bu nedenle hırsızlık ve mala zarar verme suçlarında suçun konusu yönünden yaptığımız tartışmalar burada da geçerlidir. Verinin tek başına silinmesi bu suçu oluşturmaz.

Sözleşme ile veriler üzerinde değişiklik yapma yetkisi kendisine verilen kişinin yetkisini aşarak kendisinin veya başkasının yararına zilyetliğin devri amacı dışında tasarrufta bulunması durumunda suçun oluşabileceği düşünülse de²¹⁵ güveni kötüye kullanma suçunun konusu mal olarak belirlendiğinden bu suç oluşmaz.

İçinde veri bulunan bir bilgisayarın faile teslimi sonrasında içine verilerin de olduğunu bilerek bilgisayarı başkasına satan failin durumunda iki suçun da gerçekleştiğini düşünülebilir. Bu durumda faile fikri içtima gereği daha ağır cezayı gerektiren suçtan ceza verilecektir.

²¹³ www.corpus.com.tr (Çevrimiçi) 20.03.2019.

²¹⁴ Özbek/Doğan/Bacaksız/Tepe, **a.g.e.**, s. 692.

²¹⁵ Biçkin, **a.g.m.**, s. 155, 156.

SONUÇ

Bilişimin sistemlerinin günümüz dünyasında kullanımının giderek yaygınlaşmasına bağlı olarak bilişim suçlarının görünürlüğü de artmıştır. Bu suçların önemli boyutta bireysel ve toplumsal sonuçları bulunmaktadır. Çalışmamızda bilişim suçları kapsamında TCK m. 244 kapsamında düzenlenen bilişim sistemine müdahale suçu, bilişim sistemindeki verilere müdahale suçu ile bilişim sistemi aracılığıyla haksız çıkar sağlama suçu olmak üzere üç farklı suç tipi incelenmiştir. Ancak bu suçlara değinilmeden önce bilişim kavramı ile bu kavram ile bağlantılı unsurlar açıklanmaya çalışılmıştır. Kavramlardan sonra bilişim suçlarını diğer suçlardan ayıran özelliklerden olan suçların işleniş biçimlerinden en yaygın kullanılanları açıklanmaya çalışılmıştır. Çok kısa bir sürede işlenen bu suçların yaygın olmasının nedeni bu işlenme biçimlerinin getirdiği kolaylıktır. Çalışmamızın devamında ise bilişim suçlarının hukukumuzda yer alan düzenlemeleri hakkında bilgi verilmeye çalışılmıştır.

Çalışmamızın ikinci bölümünde TCK m. 244/1-2’de düzenlenen bilişim sistemine müdahale ile bilişim sistemindeki verilere müdahale suçları arasındaki bağlantı sebebiyle bu suç tiplerini suçların ortak özellikleri ve farklılıklarına dikkat çekerek birlikte açıklamaya çalıştık.

Bilişim sistemine müdahale suçu bakımından bilişim sisteminin, sistemin güvenliği ve işleyişinin korunmak istendiğini; bilişim sistemindeki verilere müdahale suçu bakımından ise sistemde bulunan verilerin bütünlüğü ve herhangi bir engel olmadan verilerin kullanılmasındaki yararın korunduğunu söyleyebiliriz. Bu suçlarla veri ve sistem bir bütün olduğundan hem yazılım hem de donanım unsurunun korunduğundan suçlarla korunan hukuki değer karma nitelik taşımaktadır. Bilişim sistemleri günümüzde insanların hem özel yaşamları hem de toplum ve devletle olan ilişkilerinde önemli bir rol oynadığından suçlarla korunan hukuki değeri mülkiyet hakkı ile sınırlandırmak maddenin düzenlendiği yer bakımından da isabetli değildir. Bu fıkralar ile veri veya sistem sahibinin mülkiyet hakları korunduğu gibi bunun yanında tasarruf yetkisine sahip olan kişilerin sistemi veya veriyi kullanmasındaki yarar da ayrıca korunmaktadır.

Suçların topluma karşı suçlar bölümünde düzenlenmesi ise isabetlidir. Günümüz toplumunda hem kamusal hem de bireysel ilişkilerin çoğu artık bilişim sistemleri üzerinden gerçekleşmektedir. Bu madde ile toplumun bilişim sisteminin işleyişine güveni de korunmaktadır. İlk fıkrada düzenlenen suçun konusunu bilişim sistemi oluştururken ikinci fıkrada düzenlenen suçun konusunu veri oluşturmaktadır. Maddedeki veri kavramı hem bilişim sistemindeki hem de CD ve USB bellek gibi veri taşıma aygıtlarında bulunan veriyi kapsamaktadır. Sistemler yazılım ve donanım unsuru ile bir bütündür. Bu nedenle veri taşıma aygıtlarında bulunan veriler sisteme girdiğinde sistem kullanıcısının tasarruf edeceği konumda olacaktır. Burada bulunan verilerin silinmesi, başka bir taşıyıcı cihaza aktarılması mümkün olduğundan suça konu verilerin mutlaka sistemde bulunması şartının suçun oluşması bakımından aranmaması gerekmektedir.

TCK m. 244/1-2'deki suçlar serbest hareketli olarak düzenlenmiştir. Maddede sayılan neticeler her türlü müdahale ile gerçekleştirilebilmektedir. Bilişim sistemini engellemek neticesi ile kastedilen bilişim sisteminin verimli çalışmasının önlenmesi yapılan müdahaleyle sistemin kapasitesinin sınırlandırılmasıdır. Sistemin yavaşlatılması sistemin istenildiği hızda kullanılmasının engellemesi olduğundan engellenme kapsamındadır. Sistemin bir an bile çalışmaması sistemi aksatacağından geçici süreli de olsa sistemin engellenmesi suçu oluşturmaktadır. Sistemin bozulması ise engellemekten öteye geçerek sistemin işleminin olanaksız hale getirilmesidir. Bu durumda sistem, verilen komutlara işleyecek durumda bile değildir. Sisteminin işleyişinin bozulması fiziksel müdahale ya da soyut unsurlarına müdahale ile gerçekleşmesi arasında bir fark bulunmamaktadır. Her iki unsura müdahale bu suçu oluşturmaktadır.

Verinin bozulması durumunda veri sistemde bulunmaktadır ancak verinin kısmen ya da tamamen komutlara uygun sonuç vermemesi yani işlevini yerine getirememesi durumu bulunmaktadır. Verileri gerçekten tamamıyla ortadan kaldırmak mümkün değildir. Verinin silindiği durumda bile silindiğine dair e-kalıntı sistemde kalmaktadır. Bu nedenle verileri yok etmeden anlaşılması gereken silinme de dâhil olmak üzere sistem kullanıcısının verisine istediği gibi ulaşmasının engellenmesi

durumudur. Verinin deęiştirilmesi ise veride daha önce bulunmayan bilgilerin eklenmesi, verinin mevcut niteliğinin deęiştirilmesidir. Verileri erişilmez kılma ise verilerin komutlara uygun işlem üretmesini sağlayan kodların kullanıcının erişemeyeceğı şekilde deęiştirilmesidir. Veri yerleřtirmek ise sisteme sistemde bulunmayan verinin dıřarıdan ya sistem ierisinden daha önce mevcut olmayan verinin girilmesiyle gerekleşmektedir. Verileri başka bir yere göndermek sistemdeki verileri başka bir dosyaya ya da başka bir sisteme transfer edilmesidir. Yok etmeden farklı olarak halen o veri varlığını sürdürmektedir.

Biliřim suçlarının faili suçların niteliğı gereğı önem arz etmektedir. İncelemeye konu yaptığımız suçların işlenebilmesi için en azından sistem veya veri unsurlarının bulunması gerekmekte olduğı gibi bunları nitelikli kullanabilme becerisinin de kiřide bulunması gerekmektedir. Biliřim sistemleri her ne kadar ok yaygınlařmış olsa da nitelikli sistemi engelleme olaylarında failin becerisi suçun gerekleşmesinde önem kazanmaktadır. Sistemin işleyişini bozan, engelleyen, verileri yok eden, deęiřtiren, veri yerleřtiren, verileri erişilmez kılan, başka yere veri gönderen herkes bu suçun faili olabilir.

Biliřim sistemine veya verilere müdahale suçlarının mağduru sistem veya veri sahibidir. İkisinin birbirinden farklı olması durumunda mağdurun belirlenebilmesi için ayrı ayrı her ikisinin mülkiyet, kullanım ve tasarruf haklarının araştırılması gerekmektedir. Sistemi kullanan kiři malik olmasa da sisteme müdahale durumunda mağdur konumunda olabilecektir.

Her iki suç da kasten işlenebilir. Suların taksirle işlenebileceğinin kabulü suçların kapsamının öngörülemez biçimde artmasına neden olacağından kanunda bu tür düzenlemenin yapılmamış olması yerindedir. Kanunda herhangi bir amaç unsuruna yer verilmediğı için suçların manevi unsurlarında amaç aranmasına gerek yoktur, fail sisteme veya veriye müdahale etmesinin hangi amaçla yapıldığının suçun oluşması bakımından önemi bulunmamaktadır.

İlgilinin rızasının incelediğimiz suç tipleri bakımından gerekleşmesi mümkündür. Veriler üzerinde tasarruf yetkisi bulunan kiři verilerin yok edilmesine,

değiştirilmesine veya maddede sayılı diğer fiillere rıza göstermişse suç oluşmayacaktır.

Kanunun hükmünü icra da uygulanması mümkün olan hukuka uygunluk nedenlerindendir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da web sitelerine erişimin engellenmesi yolu buna örnek olarak gösterilebilir.

Meşru savunmanın bu suçlara uygulanıp uygulanmayacağı doktrinde tartışmalı olsa da meşru savunma için TCK m. 25/1'de yer alan *“o anda hal ve koşullara göre saldırı ile orantılı biçimde defetmek zorunluluğu”* şartı arandığından sisteme ve verilere müdahale suçlarında uygulanması mümkün değildir. Veriye ya da sisteme müdahale durumunda kişinin ilk olarak 5651 sayılı Kanun vasıtasıyla engelleme imkânı bulunduğundan meşru savunmanın uygulanması mümkün değildir.

TCK'nın 244. maddesinin 3. fıkrasında, birinci ve ikinci fıkradaki tanımlanan fiillerin *“bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi”* suçların nitelikli hali olarak öngörülmüştür. Ülkemizde insanlar adli yargı mercilerine başvurmadan vergi borçlarına kadar birçok işlemi internet üzerinden resmi sitelerden kurumlara gitmeden gerçekleştirebilmektedir. Mobil bankacılık ise birçok kişi tarafından kullanılmakta, kişiler bu yazılımlar üzerinden çeşitli yatırımlar yapmaktadır. Toplum hayatını kolaylaştıran ve ekonomik düzeni koruyan bu tür sistemlerin kamu kurumlarına ya da banka veya kredi kurumuna ait olması durumun ayrıca korunması isabetli olmuştur.

Bilişim sistemine müdahale suçu ile bilişim sistemindeki verilere müdahale suçlarının teşebbüs aşamasında kalması mümkündür. İcra hareketlerinin failin elinde olmayan nedenlerle yarıda kalması ve bu nedenle sisteme veya veriye etki edememesi durumunda teşebbüs gündeme gelecektir. Örneğin sistemi ele geçirmek için kurulan bir yazılımın sisteme girmesi fakat eksiklik nedeniyle çalışmaması durumunda teşebbüsten bahsedilecektir.

TCK m. 243'te düzenlenen bilişim sistemine girme veya orada kalma suçunun tezimizin konusunu oluşturan suç tipleri açısından geçit suç oluşturup oluşturmayacağı tartışma konusu yapılabilir. Bilişim sistemine veya sistemdeki verilere müdahale suçlarının gerçekleşebilmesi için mutlaka sisteme girme veya orada kalmaya devam etme hareketlerinin gerçekleşmesi gerekmediğinden geçit suç ilişkisi bulunup bulunmadığı her somut olayda ayrı ayrı değerlendirilmesi gerekmektedir.

Fail eğer tek bir hareketle hem bilişim sistemine hem de verilere müdahale etmişse failin farklı neviden fikri içtima kuralları gereğince daha ağır cezayı öngören TCK m. 244/1'den cezalandırılması gerekmektedir.

TCK m. 244/4'te ise bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu düzenlenmiştir. Doktrinde bazı yazarlar bu fıkrayı nitelikli hal olarak kabul etse de biz bu görüşe katılmıyoruz. Madde metninde “başka bir suç” ifadesi kullanılırken gerekçede “fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması” ifadesine yer verilerek kanun ile gerekçe arasında çelişki oluşturulsa da gerekçe bağlayıcı olmadığından madde metninin esas alınması gerekmektedir.

Bu suç bilişim sisteminin işleyişinin engellenmesi, bozulması, sistemdeki verilerin bozulması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi, erişilmez kılınması, değiştirilmesi ve yok edilmesi suretiyle kişinin kendisinin veya başkasının yararına haksız çıkar sağlama suçu olarak işlenebilir. Haksız çıkarın ise yalnızca maddi olması gerekmez. Maddi ya da manevi her türlü çıkar bu suç sonucunda elde edilebilir. Bu nedenle bu suçla korunan hukuki değer de mağdurun hem manevi hem de maddi hakkıdır.

Suçun konusunu bilişim sistemi veya bu sistemde bulunan verilerdir. Fail bilişim sistemi ve veriler üzerinde gerçekleştirdiği hareketler neticesinde haksız çıkar elde etmektedir.

Suç tanımında yazılı hareketleri gerçekleştirerek haksız çıkar sağlayan herkes suçun faili olabilmektedir. Bu çıkar sonucunda maddi veya manevi hakları zarara uğrayan kişi suçun mağdurudur.

Suçun oluşması için kast unsurunun dışından ayrıca amaç unsuru aranmaz. Faildeki suç işlemeye yönelik kast suçun manevi unsurunu oluşturmaktadır. Failin haksız çıkar sağlama suçu oluşması bakımından yeterlidir, failin hangi amaçla hareket ettiği önemli değildir. Böyle bir amacı bulunmayan failin sistemi engelleme veya bozma hareketlerini gerçekleştirdikten sonra çıkar sağlama durumunda bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu oluşmuş olacaktır.

Suçun tamamlanabilmesi için haksız çıkarın sağlanması şarttır. Fail bilişim sistemi ve verilere müdahale etmesine rağmen menfaati elde edememişse suçun teşebbüs aşamasında kaldığını söyleyebiliriz.

TCK m. 244/4'te düzenlenen bilişim sistemleri aracılığıyla haksız çıkar sağlama suçunu tali norm olarak düzenlemiştir. Bilişim sistemleri aracılığıyla haksız çıkar sağlama şeklinde bir olayla karşılaşıldığında ilk olarak bu failin kanunda düzenlenen başka suçları oluşturup oluşturmadığı araştırılmalıdır. Olayın gerçekleştiriliş şekli bu suçlardan birisine uygunsa bu suç aksi durumunda TCK m. 244/4 oluşacaktır.

Çalışmamızın son kısmında inceleme konusu yaptığımız üç suç tipini benzer suçlarla karşılaştırması yapılarak konunun daha iyi anlaşılabilmesi amaçlanmıştır. TCK m. 151'de düzenlenen mala zarar verme suçunun konusunu başkasının taşınır ya da taşınmaz malı oluşturmaktadır. İnceleme konusu yaptığımız suç tipleri açısından suçların konusunu bilişim sistemi ve veri olarak kabul ettiğimizden bu unsurlara zarar verme fiilleri TCK m. 244 kapsamındadır. Salt mala zarar vermek kastıyla yapılan hareketler her ne kadar sistemi engellemiş olsa da mala zarar verme suçunu oluşturmaktadır. Buna karşılık sistemin fiziksel yapısına zarar verilmeksizin dışarıdan gönderilen bir yazılım ile sisteme etki edilmesi durumunda bilişim sistemine müdahale suçu oluşacaktır.

TCK m. 142/2-e'de hırsızlık suçunun bilişim sistemleri kullanılmak suretiyle işlenmesine yer verilmiştir. Doktrinde verinin, bilişim sistemleri kullanılmak suretiyle hırsızlık suçunun konusunu oluşturup oluşturmayacağı tartışmalıdır. Bir görüşe göre, veri somut nesne olmadığından hırsızlık suçu kapsamında taşınabilir mal olarak kabul

edilemez. Bizim de katıldığımız ikinci görüş ise verinin temsil ettiği paranın hırsızlık suçuna konu olabileceğini savunmaktadır. Günümüz dünyasında paranın artık kişilerin yanında değil banka hesaplarında bulunan veri olarak bilişim sisteminde görülmesi olağandır. Bu nedenle banka hesabında bulunan verilerin transferi durumunda bilişim sistemleri kullanılmak suretiyle hırsızlık suçunun oluştuğunu kabul etmek gerekir. Kişinin başkasının hesabından kendi hesabına para aktarması durumunda verilerin değil onun temsil ettiği paranın aktarılması durumu söz konusu olduğundan bilişim sistemi kullanılarak hırsızlık suçunun gerçekleştiğini kabul etmek gerekmektedir.

Bir diğer tartışmalı konu ise kişinin telefon hattından başka bir hatta yapılan kontör transferinin durumudur. Burada da kontörün temsil ettiği paranın gönderilmesi söz konusu olduğundan bilişim sistemleri kullanarak hırsızlık suçunu oluşturmaktadır.

TCK m.158/1-f'de ise bilişim sistemlerinin araç olarak kullanılması suretiyle gerçekleşen dolandırıcılık suçu düzenlenmiştir. Bu suçun gerçekleşebilmesi için hilenin varlığı ve muhatabının mutlaka insan olması gerekmektedir. Bilişim sisteminin aldatılmasından söz edilemeyeceği için, ancak bu sistemin araç olarak kullanılarak bir insanın aldatılması yani dolandırılması halinde bu bendin uygulanması mümkündür. İnternet site adresinin yanlış gösterilmesi veya kişinin ilgili yere şifresini yazdığı anda maddi kazanç sağlayacağına yönelik reklamlar buna örnek olarak gösterilebilmektedir.

Dolandırıcılık suçundaki kişiye karşı hile mağdura ait verilerin erişilmez kılınması ya da değiştirilmesi ile gerçekleştirilmiş ise hem dolandırıcılık suçunun nitelikli hali hem de TCK m. 244/2'de düzenlenen verilere müdahale suçu oluşur. Burada iki ayrı suç tek hareketle gerçekleştiğinden farklı neviden fikri içtima hükümlerinin uygulanması gerekmektedir. Sonuç olarak hileli hareketlerin bilişim sistemi kullanılmak suretiyle bir kişiye karşı gerçekleştirilmesi durumunda nitelikli dolandırıcılık suçu oluşmaktadır.

Eski TCK döneminde haksız olarak ele geçirilen banka kartları ile ATM'lerden para çekilmesi fiillerinin, ATM'lerin bir bilişim sistemi olması dolayısıyla bilgisayar aracılığıyla yarar sağlama suçunu oluşturduğu kabul ediliyordu. TCK m. 245'in düzenlemesi ile kartın ne şekilde ele geçirildiğine bakılmaksızın

başkasına ait bir banka veya kredi kartını kullanarak kendisine ya da başkasına yarar sağlama fiillerinin banka ve kredi kartlarının kötüye kullanılması suçu olarak kabul edilmiştir.



KAYNAKÇA

Altıntaş, Hakan/

Mehmet, Tan : “Bilişim Suçları ve Güvenlik Önlemleri”, **2. Polis Bilişim Sempozyumu Bildirileri**, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, Ankara, s. 220-225.

Akbulut, Berrin : **Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2017.

Akbulut, Berrin : “Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme”, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, C. XXIV, S. 2, 2016, s. 7-55.

Akdeniz, Gökşin : “Hacker Etiği”, **Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Biçimi**, Mustafa Akgül’e Armağan, Der. Ali Rıza Keleş, Yetkin Sal, İstanbul, Alternatif Bilişim, 2013, s. 8-16.

Akıncı, Hatice/Kılıç

A. Emre/Er, Cüneyd : “Türk Ceza Kanunu ve Bilişim Suçları”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 157-275.

Aksaya, Harun/

Olgun Kadir, Burak/

Elibol Mehmet : “İnternet Bankacılık Hizmetleri ve Paydaşların Sorumlulukları”, **Enformatik, Toplum ve Hukuk**, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016, s.119-143.

Aktürk, Cemal/

Talan, Tarık : “Mobil Bilişim Suçları”, **Enformatik, Toplum ve Hukuk**, Ed. Fatih Gürsul, İstanbul, Legal Yayıncılık, 2016, s.145-169.

Artuç, Mustafa/

Bayyurt, Yıldırım : **Gerekçeli, Karşılaştırmalı, Tablolu, Eski ve Yeni Metinleriyle 5237 sayılı TCK**, Ankara, Seçkin Yayınları, 2008.

Artuk ,Mehmet Emin/

Gökçen, Ahmet/

Yenidünya, Caner : **Türk Ceza Kanunu Şerhi**, 2. bs. , C. V, Ankara, Adalet Yayınları, 2014. (**Türk Ceza Kanunu Şerhi**)

Artuk, Mehmet Emin/

Gökçen, Ahmet/

Yenidünya, Caner : **Ceza Hukuku Özel Hükümler**, 15. bs., Ankara, Adalet Yayınevi, 2015. (**Ceza Hukuku Özel Hükümler**)

Artuk, Mehmet Emin/

Gökçen, Ahmet/

Alşahin, Mehmet

Emin/ Çakır, Kerim : **Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018.

Aşıcioğlu, Faruk/

Arslan, Murat Nihat/

Dokurer, Semih : **Meraklılar ve Hevesliler İçin Adli Bilimler**, İstanbul, Türkiye İş Bankası Yayınları, 2012.

Avşar, Zakir/

Öngören, Gürsel : **Bilişim Hukuku**, İstanbul, Türkiye Bankalar Birliği, 2010.

Aydın, Emin Doğan : **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yayınları, 1992.

Bayındır, Aslı : “Türk Ceza Kanunu’nda Düzenlenen Bilişim Suçları”, **Suç ve Ceza Hukuku Dergisi**, S.2, 2010, s.55-107.

Beceni, Yasin : “Bilgi Toplumunda Hukukun Değişen Yüzü”, **Bilişim Hukuku**, Der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 96-100.

Berber, Leyla Keser : **Adli Bilişim (Computer Forensic)**, Ankara, Yetkin Yayınları, 2004.

Biçkin, İnci : “Siber Suç Sözleşmesi ve 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları”, **Yargıtay Dergisi**, C. XXXII, S. 1-2, Ocak-Nisan 2006, s.145-168.

Canberk, Gürol/

Sağiroğlu, Şeref : “Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma”, **Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi**, C:22, No:1, 2007, s. 121-136.

Çakır, Hüseyin/

Kılıç, Mehmet

Serkan : **Güncel Tehdit: Siber Suçlar**, Ankara, Seçkin Yayıncılık, 2014.

Değirmenci, Olgun : “Bilişim Suçları”, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2002.

Değirmenci, Olgun : “2004 Türk Ceza Kanunu’nun Bilişim Suçları Bakımından Değerlendirilmesi”, **TBB Dergisi**, S:58, Mayıs/Haziran 2005. s. 195-208.

Demircan, Tunç : Tunç Demircan, **Bilişim Alanında Suçlar**, İstanbul, Legal Yayıncılık, 2016.

Dilek, Halil İbrahim : “Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri”, Dicle Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Diyarbakır, 2007.

Doğan, Koray : “Bilişim Suçları ve Yeni Türk Ceza Kanunu”, **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y. 2, S. 6-7, Ekim 2005, s. 290-319.

Dönmezer, Sulhi : **Kişilere ve Mala Karşı Cürümler**, 17. bs., İstanbul, Beta Yayınları, 2004.

Dursun, Selman : “Türk Ceza Hukuku’nda Emrin İfasının Hukuki Niteliğinin Alman ve İtalyan Ceza Hukuku’yla Karşılaştırmalı Olarak İncelenmesi”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XVIII, Y. 2014, S.2, s.203-252.

Dülger, Murat

Volkan : **Bilişim Suçları ve İnternet İletişim Hukuku**, 7. bs., Ankara, Seçkin Yayıncılık, 2018.

Eker, Hüseyin : **Açıklamalı-İçtihatlı Hırsızlık Suçları**, Ankara, Adalet Yayınevi, 2014.

- Eker, Umut : “Türk Ceza Hukuku’nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 sayılı Yeni Türk Ceza Kanunu’nun İlgili Hükümlerinin Yorumu”, **TBB Dergisi**, 2006, s. 101-132.
- Erdağ, Ali İhsan : “Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)”, **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.XIV, S. 2, 2010, s. 275-303.
- Erdoğan, Yavuz : “Bilişim Sistemine Girme ve Kalma Suçu”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. XII, Özel Sayı, 2010 (Basım yılı:2012), s. 1363-1433.
- Erdoğan, Yavuz : **Türk Ceza Kanunu’nda Bilişim Suçları** (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile), İstanbul, Legal Yayıncılık, 2012, s.11.
- Ergün, İsmail : **Siber Suçların Cezalandırılması ve Türkiye’deki Durum**, Ankara, Adalet Yayınevi, 2008.
- Ergün, İsmail : “Yeni Türk Ceza Kanunu’nda Bilişim Suçları”, **2. Polis Bilişim Sempozyumu Bildirileri**, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s. 23-29.
- Ersoy, Yüksel : “Genel Hukuki Koruma Çerçevesinde Bilişim Suçları”, **Ankara Üniversitesi SBF Dergisi**, C. XLIX, 1994, s. 149-183.
- Esen, Sinan : **Malvarlığına Karşı Suçlar Belgede Sahtecilik ve Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2007.
- Gemalmaz H.Burak : **Sanal Dünyalarda İktidar ve Özgürlük**, İstanbul, Beta Yayıncılık, 2011.
- Gerche, Marco : “Siber Suç Sözleşmesi ile 10 Yıl: Avrupa Konseyi’nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarıları ve

Kusurları”, Çev. Kerem Öz, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 59-87.

Gözüşirin, Mesih : “5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi”, Kara Harp Okulu Savunma Bilimleri Enstitüsü Güvenlik Bilimleri Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2011.

Gül, Ahmet : **Doğrudan Dolaylı Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2016.

Helvacıoğlu, Aslı

Deniz : “Avrupa Konseyi Siber Suç Sözleşmesi- Temel Hükümler İncelenmesi”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 277-340.

Hilgendorf, Eric : Grundfalle zum Computersstrafrecht, JuS, 1996, Heft 10, s. 893.

İçel, Kayıhan : “Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri”, **İÜHFM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 3-10.

İçel, Kayıhan/

Sokulu-Akıncı,

Fusun/ Özgenç,

İzzet/ Sözüer,

Adem/ Mahmutoğlu,

Fatih Selami/

- Ünver Yener : **Suç Teorisi**, 3. bs. , İstanbul, Beta Yayıncılık, 2004.
- İnanıcı, Haluk : “Bilişim ve Yazılım Hukuku, Uygulamanın İçinden Görünüşü”, **İBD**, C. LXX, S. 7-8-9, 1996.
- Karagülmez, Ali : **Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri**, 5. bs., Ankara, Seçkin Yayıncılık, 2014.
- Karagülmez, Ali : “Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular”, **2. Polis Bilişim Sempozyumu Bildirileri**, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s. 31.
- Ketizmen,
Muammer : **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008.
- Kızıltan, Mehmet
- Burak : “5237 Sayılı TCK’da Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları”, İstanbul Üniversitesi SBE Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2007.
- Koca, Mahmut : “Avrupa Konseyi Siber Suç Sözleşmesi’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku”, **Bilgi Toplumunda Hukuk**, Ünal Alptekin’e Armağan, C. III, İstanbul, Beta Yayınları, 2003, s. 785-816. (AKSSS’nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku)
- Koca, Mahmut : “Yargıtay Kararları Işığında Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Yarar Sağlama Suçları”, **Prof. Dr. Ali Güzel’e Armağan**, C. II, İstanbul, Beta Yayıncılık, 2010, s.1651-1660.

Koca, Mahmut/

Üzülmez, İlhan : **Türk Ceza Hukuku Özel Hükümler**, 5. bs., Ankara, Seçkin Yayıncılık, 2018.

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

Lenckner, Theodor/

Wolfgang,

Winkelbauer : Computerkriminalitat- Möglichkeiten und Grenzen des 2. WiKG, CR, 1986, Heft 10, s. 656.

Mahmutoğlu, Fatih

Selami : “Türk Ceza Kanunu’nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi”, **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Prof. Dr. Füsun Sokullu-Akıncı’ya Armağan, C. LXXI, S. 1, 2013, s. 855-889. (TCK’da Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi)

Mahmutoğlu, Fatih

Selami : “Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Sorumluluğu”, **İÜHFM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 39-49.

Malkoç, İsmail : **Açıklamalı- İçtihatlı 5237 sayılı Yeni Türk Ceza Kanunu**, C. II, Ankara, Malkoç Kitapevi, 2007.

Meran, Necati : **Zimmet-Rüşvet-İrtikap ve Güveni Kötüye Kullanma Suçları**, Ankara, Seçkin Yayıncılık, 2014.

Meran, Necati : **Yeni Türk Ceza Kanununda Sahtecilik-Malvarlığı Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar**, Ankara, Seçkin Yayınları, 2008.

Mermut, Serdar/

Alpaslan, Osman

Berk : “Bilişim Sistemlerinin Kullanılması Suretiyle Haksız Çıkar Sağlama Suçu ile İlgili Bir Yargıtay Ceza Genel Kurulu Kararının İncelenmesi”, Suç ve Ceza Dergisi, 2010, Sayı:2, İstanbul

Möhrenschlager,

Manfred : Das neue Computerstrafrecht, wistra, 1986, Heft 4.

Mungo, Paul/

Clough, Byran : **Sıfıra Doğru Veri Suçları ve Bilgisayar Dünyası**, İstanbul, İletişim Yayınları, 1999.

Nizam, Feridun : “Avrupa Siber Suçlar Konvansiyonu ve Türk Ceza Kanunundaki Bilişim Suçlarının Karşılaştırılması”, **2. Polis Bilişim Sempozyumu Bildirileri**, Ankara, Emniyet Genel Müdürlüğü Bilgi İşlem Dairesi Başkanlığı, 2005, s. 217-219.

Orta, Mesut : **Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim)**, Ankara, Yetkin Yayınları, 2015.

- Önok, Murat : “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Prof. Dr. Nur Centel’e Armağan, Özel Seri, C. XIX, S. 2, 2013, s. 1229-1269.
- Özbek, Veli Özer : “Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.IX, Özel Sayı, İzmir, 2007, s. 1019-1063.
- Özbek, Veli Özer : “İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C. IV, S. 1, 2002, s. 101-158.
- Özbek, Veli Özer : “Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi”, **İÜHFİİ İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 184.
- Özbek, Veli Özer /
- Koray Doğan/Pınar
- Bacaksız/İlker Tepe: **Türk Ceza Hukuku Özel Hükümler**, 13. bs., Ankara, Seçkin Yayıncılık, 2018.
- Özel, Cevat : “Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 341-361.
- Özel, Cevat : “Bilişim Suçlarının Türk Ceza Kanunu ve Tasarıdaki Hükümler Yönünden Mukayeseli Olarak Değerlendirilmesi”, **Bilişim Hukuku**, Der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 85-92.
- Özgenç, İzzet : **Zimmet Suçu**, Ankara, Seçkin Yayınları, 2009.

Parlar, Ali /

Hatipoğlu, Muzaffer : **Türk Ceza Kanunu Yorumu**, C. IV, Ankara, Seçkin Yayıncılık, 2008.

Pallı, Hayati : “Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları”, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Kayseri, 2008.

Parlar, Ali : **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Bilge Yayınevi, 2011.

Popp, Andreas : Bilgi Teknolojisi ve Ceza Hukuku, Çev. Hakan Hakeri, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 87-103.

Schuhr, Jan C : “Bilgisayar Ceza Hukukunda Kıyas ve Davranış Normu: Verilerin Değiştirilmesi Örneği (Alman Ceza Kanunu madde 303a ve Siber Suç Sözleşmesi madde 4)”, Çev. Ahmet Mert Duygun, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 309-347.

Sevük, Handan

Yokuş : **Türk Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018.

Sınar, Hasan : “İnternetin Ortaya Çıkardığı Hukuki Sorunlara Bir Ceza Hukuku Yaklaşımı”, **Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni (MHB)**, Yılmaz Altuğ’a Armağan Y:17-18, S. 1-2, 1997-1998, s. 355-372.

- Sınar, Hasan : “Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme”, Prof. Dr. Çetin Özek Armağanı, İstanbul, Galatasaray Üniversitesi Yayınları, 2004, s. 765-786.
- Sınar, Hasan : **İnternet ve Ceza Hukuku**, İstanbul, Beta Yayınları, 2001.
- Sieber, Ulrich : Bilgisayar Suçluluğu, Çev. Yener Ünver, **İnternet Hukuku**, Ankara, Seçkin Yayıncılık, 2013, s. 13-59.
- Sokullu-Akıncı,
Fusun : “Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi”, **İÜHFİM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 11-38.
- Soyaslan, Doğan : **Ceza Hukuku Özel Hükümler**, Ankara, Yetkin Yayınları, 2010.
- Sutherland,
Edwin H.: “Beyaz Yaka Suçluluğu”, Çev. Selman Dursun, **Suç Politikası**, Karşılaştırmalı Güncel Ceza Hukuku Serisi, Prof. Dr. Claus Roxin’e Armağan, Ankara, Seçkin Yayıncılık, 2006, s. 295-306.
- Taşkın, Şaban
Cankat : **Bilişim Suçları**, İstanbul, Beta Yayınevi, 2008.
- Şentürk, Aysan/
Korcuklu, Neşe/
Balay, Mustafa : Bilgisayar Kullanımı ve İnternet, Bursa, Ekin Kitapevi, 2005.

- Tanşu, Okan : “Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s.139-154.
- Taşkın, Şaban
- Cankat : “Bilişim Hukuku Uluslararası Uyuşmazlıklar”, TBB Dergisi, S. 85, 2009, s. 332-372.
- Tezcan, Durmuş/
Ruhan, Mustafa
- Erdem/Önok, Murat : **Teorik ve Pratik Ceza Özel Hukuku**, Ankara, Seçkin Yayıncılık, 2016.
- Tepe, İlker : “İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku’ndaki Yeni Gelişmeler”, **Alman- Türk Karşılaştırmalı Ceza Hukuku**, İstanbul, Yeditepe Üniversitesi Hukuk Fakültesi, İstanbul, 2010, C.I, s. 267-288.
- Tiedemann, Klaus : “Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi”, Çev. Feridun Yenisey, **İÜHFM**, C. XLI, S. 1-4, 1975, s. 319-332.
- Topaloğlu, Mustafa : **Bilişim Hukuku**, Ankara, Karahan Kitapevi, 2005.
- Turan, Metin : **Bilişim Hukuku**, Ankara, Seçkin Yayıncılık, 2017.
- Turan, Metin : **Alman Bilişim Hukuku**, Ankara, Adalet Yayınevi, 2017.
- Uçkan, Özgür/
Beceni, Yasin : “Bilişim-İletişim Teknolojileri ve Ceza Hukuku”, **İnternet ve Hukuk**, Der. Yeşim Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayını, 2004, s. 363-430.

- Ünver, Yener: “Türk Ceza Kanunu’nun ve Ceza Kanunu Tasarısı’nın İnternet Açısından Değerlendirilmesi”, **İÜHFM İnternet Özel Bölümü**, C. LIX, S. 1-2, 2001, s. 51-153.
- Yaycı, Esra : “Bilişim Suçları”, Gazi Üniversitesi SBE Kamu Hukuku Anabilim Dalı, Yayınlanmamış Yüksek Lisans Tezi, Ankara, 2007.
- Yazıcıoğlu, Yılmaz: “Dialler, Key Logger Programları- İnternet Bankacılığı Dolandırıcılığı”, **Bilişim Hukuku**, Der. Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayınları, 2006, s. 80-85.
- Yazıcıoğlu, Yılmaz : “Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirilmesi”, **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, C:II, S:2, 2005, s. 393-412.
- Yazıcıoğlu, Yılmaz : **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, İstanbul, Alfa Yayınevi, 1997.
- Yazıcıoğlu, Yılmaz : “Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi”, **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y:1, S:1, İstanbul, Ocak- Mart 2004, s. 172-185. (2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi)
- Yenidünya, Caner/
- Değirmenci, Olgun : **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2003.
- Yılmaz, Sacit : 5237 sayılı TCK’nın 244. Maddesinde Düzenlenen Bilişim Alanında Suçlar, **TBB Dergisi**, 2011, s.62-100.
- Yiğitbaşı, İsmet/

Gürsul, Fatih : “Online Bankacılık Suçlarının İncelenmesi: İstanbul Örneği”,
Enformatik, Toplum ve Hukuk, Ed. Fatih Gürsul, İstanbul,
Legal Yayıncılık, 2016, s. 174-206.

www.hurriyet.com.tr/gundem/e-miting-yapacak-40846416

www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5cb9cb614006d3.66854511

www.corpus.com.tr

www.kazancı.com