BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU TEZLİ YÜKSEK LİSANS PROGRAMI

SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME VE BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇLARI

HAZIRLAYAN

CEREN NUR ENGİNAR

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

DOÇ. DR. EZGİ AYGÜN EŞİTLİ

ANKARA - 2023

BAŞKENT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS / DOKTORA TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih: 12 /09 /2023

Öğrencinin Adı, Soyadı:Ceren Nur ENGİNAR

Öğrencinin Numarası:22010301

Anabilim Dalı: Kamu Hukuku Anabilim Dalı

Programı: Kamu Hukuku Tezli Yüksek Lisans Programı

Danışmanın Unvanı/Adı, Soyadı: Doç. Dr. Ezgi AYGÜN EŞİTLİ

Tez Başlığı:Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme ve Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlama Suçları

Yukarıda başlığı belirtilen Yüksek Lisans/Doktora tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 134 sayfalık kısmına ilişkin, 05/09/2023 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 11.'dır. Uygulanan filtrelemeler:

1. Kaynakça hariç

2. Alıntılar hariç

3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:

ONAY

Tarih: 12 /09 / 2023

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Doç. Dr. Ezgi AYGÜN EŞİTLİ

TEŞEKKÜR

Bu çalışmayı bazı kişilerin desteği ve katkısı olmasaydı tamamlamam mümkün olamazdı. Bu nedenle benim için uzun ve zorlu olan bu süreçte yanımda olan herkese teşekkür etmek isterim.

Öncelikle tez konumun seçilmesinden çalışmamın tamamlanmasına kadar bilgisi ve tecrübesiyle rehberliğini esirgemeyen, tüm içtenliği ve hoşgörüsü ile desteğini daima hissettiren, kendisi ile çalışmaktan onur duyduğum değerli danışman hocam Doç. Dr. Ezgi AYGÜN EŞİTLİ'ye teşekkürlerimi sunarım.

Mesleki hayatımda olduğu gibi akademik hayatımda da her zaman yol gösterici olan, bu süreçte beni cesaretlendiren ve desteğini esirgemeyen Av. Dr. Y. Burak ASLANPINAR'a teşekkürü bir borç bilirim.

Son olarak hayatımın her döneminde kendi ayaklarım üzerinde durmayı öğrettikleri, her zaman tüm sevgi ve şefkatleriyle yanımda oldukları ve bu çalışmanın hazırlanmasında yaşadığımız tüm zorluklara rağmen büyük bir sabır ve fedakarlık gösterdikleri için annem Sevgi ENGİNAR ve babam Atila ENGİNAR'a, sevgisi ve anlayışıyla her daim yanımda olan en büyük destekçim kardeşim İrem ENGİNAR'a ve hayatım boyunca desteğini, sevgisini esirgemeyen teyzem Seher AKİL'e sonsuz teşekkür ederim.

ÖZET

Ceren Nur ENGİNAR, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme ve Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlama Suçları, Başkent Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Tezli Yüksek Lisans Programı, 2023

Eldeki çalışmada 5237 sayılı Türk Ceza Kanunu'nun *"Topluma Karşı Suçlar"* isimli başlık altındaki Üçüncü kısmın *"Bilişim Alanında Suçlar"* başlıklı Onuncu bölümünün *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* başlıklı 244. maddesindeki suçları öğretideki yaklaşımlar, yargı kararları ve teknolojideki güncel gelişmeler kapsamında değerlendirilmiştir.

Çalışmamız üç ana bölümden oluşmaktadır. İlk bölümde bilişim sistemleri ve bilişim suçlarının genel esaslarına yer verilmiştir. Bu doğrultuda bilişim, bilişim alanı ve bilişim sistemi kavramları izah edilmiştir. Bununla birlikte bilişim sistemlerine ilişkin teorik kavramlar olan bilgisayar, veri, internet kavramlarından bahsedilmiştir. Akabinde bilişim suçu tanımlanarak bilişim suçunun genel özellikleri ile karşılaştırmalı hukukta ve Türk hukukunda bilişim suçlarının değerlendirilmesi yapılmıştır.

Çalışmamızın ikinci bölümünde birinci bölümde izah edilen ve 5237 sayılı Türk Ceza Kanunu'nun *"Bilişim Alanında Suçlar"* başlığı altındaki *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* başlıklı 244. maddesinin birinci ve ikinci fıkrasındaki "*Bilişim sistemini engelleme, bozma ve verileri yok etme veya değiştirme suçları",* çalışmamızın üçüncü bölümünde ise ilgili maddenin dördüncü fıkrasındaki *"Bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu"* suç genel teorisi kapsamında suçun unsurlarına ayrılarak ayrı ayrı incelenmiştir. Bu kapsamda suçun özel görünüş biçimlerinden olan teşebbüs, iştirak ve içtima kurumlarına değinilerek suçun cezası ile suçta soruşturma ve kovuşturma evreleri açıklanmıştır.

Anahtar Kelimeler: Bilişim Sistemi, Bilişim Alanı, Bilişim Alanında Suçlar, Veri, Bilişim Suçu

ABSTRACT

Ceren Nur ENGİNAR, Crimes of Obstructing or Disrupting the System, Destroying or Changing Data and Gaining Unfair Benefits through the Information System, Başkent University, Institute of Social Sciences, Public Law Master's Program with Thesis, 2023

In this study, the crimes defined in Article 244 of the TCK titled "*Crimes against the Community"* under the Third Section entitled *"Crimes in the Field of Informatics"* and the Tenth Chapter entitled *"Obstruction, Disruption, Destruction or Alteration of the System"* will be evaluated in the scope of approaches in the doctrine, judicial decisions and current developments in technology.

Our study consists of three main parts. In the first part, general principles of information systems and informatics crimes will be addressed. In this context, the concepts of informatics, informatics field and informatics system will be explained. In addition, theoretical concepts related to information systems such as computer, data, and internet concepts will be mentioned. Then, the information crime will be defined and the general characteristics of the informatics crime will be evaluated in comparative law and the evaluation of informatics crimes in Turkish law will be made.

In the second part of our study, the first and second paragraphs of Article 244 titled *"Obstruction, Disruption and Destruction or Alteration of the Informatics System*" under the heading of *"Crimes in the Field of Informatics"* in the TCK explained in the first part of our study and the crime of *"Obtaining Unfair Benefit through Information Systems"* in the fourth paragraph of the relevant article will be examined by dividing the elements of the crime under the scope of the general theory of crime separately. In this context, the crime's punishment and the investigation and prosecution stages of the crime will be explained by addressing the institutions of attempt, participation, and concurrence, which are special appearances of the crime.

Key Words: Information System, Informatics Field, Informatics Crimes, Data, Informatics Crime

İÇİNDEKİLER

TEŞEKKÜR ..... **i**

ÖZET ..... **ii**

ABSTRACT ..... **iii**

KISALTMALAR ..... **x**

GİRİŞ **1**

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMLERİ VE BİLİŞİM SUÇLARINA İLİŞKİN GENEL ESASLAR

I. BİLİŞİM, BİLİŞİM SİSTEMİ VE BİLİŞİM ALANI **4**

A. BİLİŞİM **4**

B. BİLİŞİM SİSTEMİ **7**

C. BİLİŞİM ALANI **9**

II. BİLİŞİM SİSTEMİ KAVRAMLARI **10**

A. BİLGİSAYAR **10**

1. Tarihçe **12**

1.1. Birinci Dönem **12**

1.2. İkinci Dönem **13**

1.3. Üçüncü Dönem **13**

1.4. Dördüncü Dönem **14**

2. Donanım (Hardware) **15**

3. Yazılım (Software) **15**

3.1. İşletim/Uygulama Yazılımı (Operating System) **16**

3.2. Uygulama Yazılımı (Application Program) **16**

B. VERİ **17**

C. İNTERNET **19**

III. BİLİŞİM SUÇU VE BİLİŞİM SUÇUNA İLİŞKİN GENEL ESASLAR **20**

A. GENEL OLARAK 20

B. TANIM 22

C. BİLİŞİM SUÇLARININ EKONOMİK SUÇLARLA İLİŞKİSİ 22

D. BİLİŞİM SUÇLARININ SINIFLANDIRILMASI 23

E. BİLİŞİM SUÇLARININ GENEL ÖZELLİKLERİ 24

F. BİLİŞİM SUÇLARININ İŞLENİŞ YÖNTEMLERİ (MODUS OPERANDİ) 26

1. Genel Olarak 26

2. Bilişim Sistemlerine Müdahale Yöntemleri 27

2.1. Salam Tekniği (Salami Techniques) 27

2.2. Gizli Kapılar veya Hile Kapısı (Trap Door) 27

2.3. Bilişim Korsanlığı (Hacking) 28

2.4. Truva Atı (Trojan Horse) 28

2.5. Mantık Bombaları (Logic Bombs) 29

2.6. Çöpe Dalma/ Artık Toplama (Scavening) 30

2.7. Bukalemunlar (Chameleon) 30

2.8. Ağ Tavşanları (Network Rabbits) 31

2.9. Ağ Solucanları (Worm) 31

2.10. Gizlice Dinleme (Eavesdropping) 33

2.11. Hizmet Aksatma Saldırısı ve Hizmet Aksatma Atakları (DoS-DDoS) 33

2.12. Veri Aldatmacası (Data Diddling) 34

2.13. Süper Darbe (Super Zapping) 34

2.14. Eşzamanlı Saldırılar (Asyncronous Attacks) 35

2.15. Bilişim Virüsleri 35

2.16. İstem Dışı Alınan Elektronik İletiler (Spam) 36

IV. ULUSLARARASI HUKUKTA BİLİŞİM SUÇLARI 36

A. ULUSLARARASI ÖRGÜTLER 37
1. Avrupa Konseyi Tarafından Yapılan Çalışmalar 37
2. OECD Tarafından Yapılan Çalışmalar 38
3. Birleşmiş Milletler Tarafından Yapılan Çalışmalar 39
A. ULUSLARARASI DÜZENLEMELER 40
1. Avrupa Konseyi Siber Suç Sözleşmesi 40
2. Avrupa Siber Suç Sözleşmesi'ne Ek Protokol 42
3. Avrupa Konseyi Kişisel Bilgilerin Korunması Sözleşme 42
V. KARŞILAŞTIRMALI HUKUK 42
A. AMERİKA BİRLEŞİK DEVLETLERİ 43
B. İNGİLTERE 44
C. ALMANYA 45
D. İTALYA 45
E. FRANSA 46
F. İSVİÇRE 46
G. DANİMARKA 47
H. AVUSTURYA 47
VI. ULUSAL HUKUKTA BİLİŞİM SUÇLARI HAKKINDA DÜZENLEMELER 47
A. GENEL OLARAK 47
B. 765 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI 48
C. ÖZEL KANUNLARDA BİLİŞİM SUÇLARI 50
1. Fikir ve Sanat Eserleri Kanunu'nda (FSEK) Düzenlenen Suçlar 50
2. Elektronik İmza Kanunu'nda (EİK) Düzenlenen Suçlar 51
3. Kişisel Verilerin Korunması Kanunu'nda (KVKK) Düzenlenen Suçlar .. 52
D. 5237 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI 53
1. Bilişim Alanında Suçlar 53

2. Bilişim Yoluyla İşlenmesi Suçun Nitelikli Hali Olan Suçlar 54
3. Bilişim Yoluyla İşlenen Diğer Suçlar 55

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME, BOZMA VE VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

I. GENEL OLARAK 57
II. SUÇLARIN HUKUKİ KONUSU 59
III. SUÇLARIN MADDİ KONUSU 60
A. GENEL OLARAK 60
B. KRİPTO PARALAR 62
C. SANAL GERÇEKLİK OYUNLARINDAKİ KARAKTERLER VE NESNELER 63
IV. FAİL VE MAĞDUR 64
V. SUÇLARIN UNSURLARI 65
A. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SUÇU 65
1. Fiil 65
1.1. Bilişim Sisteminin İşleyişini Engellemek 69
1.2. Bilişim Sisteminin İşleyişini Bozmak 70
2. Hukuka Aykırılık 72
3. Kusurluluk 73
4. Kusurluluğu Kaldıran Nedenler 74
4.1. Fiille Fail Arasındaki Psişik/Manevi Bağı Ortadan Kaldıran Nedenler ... 74
4.2. Hata 75
4.3. Manevi Cebir ve Bu Temelde Kişiden Beklenenin Bulunduğu Koşullarda Kendisinden İstenememesi (İstenememezlik İlkesi) 76

B. BİR BİLİŞİM SİSTEMİNDEKİ VERİLERİ BOZMA, YOK ETME, DEĞİŞTİRME, ERİŞİLMEZ KILMA, SİSTEME VERİ YERLEŞTİRME VEYA VAR OLAN VERİLERİ BAŞKA BİR YERE GÖNDERME SUÇUNUN UNSURLARI 77

1. Fiil 77

1.1. Verileri Bozmak, Yok Etmek, Değiştirmek 80

1.2. Veriyi Erişilmez Kılmak, Sisteme Veri Yerleştirmek, Var Olan Verileri Başka Bir Yere Göndermek 83

2. Hukuka Aykırılık 86

3. Kusurluluk 88

4. Kusurluluğu Kaldıran Nedenler 89

4.1. Fiille Fail Arasındaki Psişik/Manevi Bağı Ortadan Kaldıran Nedenler ... 89

4.2. Hata 90

4.3. Manevi Cebir ve Bu Temelde Kişiden Beklenenin Bulunduğu Koşullarda Kendisinden İstenememesi (İstenememezlik İlkesi) 91

VI. SUÇLARIN ÖZEL GÖRÜNÜŞ BİÇİMLERİ 91

A. TEŞEBBÜS 91

B. İŞTİRAK 93

C. İÇTİMA 93

VII. SUÇLARIN NİTELİKLİ HALİ 101

VIII. YAPTIRIM, SORUŞTURMA VE KOVUŞTURMA 102

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SİSTEMLERİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU

I. GENEL OLARAK 104

II. SUÇUN HUKUKİ KONUSU 105

III. SUÇUN MADDİ KONUSU 108

IV. FAİL VE MAĞDUR 109

V. SUÇUN UNSURLARI 110

A. FİİL 110

B. HUKUKA AYKIRILIK 113

C. KUSURLULUK 114

D. KUSURLULUĞU KALDIRAN NEDENLER 114

1. Fiille Fail Arasındaki Psişik/Manevi Bağı Ortadan Kaldıran Nedenler . 115

2. Hata 115

3. Manevi Cebir ve Bu Temelde Kişiden Beklenenin Bulunduğu Koşullarda Kendisinden İstenememesi (İstenememezlik İlkesi) 116

VI. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ 116

A. TEŞEBBÜS 116

B. İŞTİRAK 117

C. İÇTİMA 117

V. BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇUNUN BENZER SUÇLAR İLE FARKI 119

A. HIRSIZLIK SUÇU İLE BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU 119

1. Bir Başkasının İnternet Bankacılığında Bulunan Paranın Başka Bir Hesaba Transfer Edilmesi 120

2. İnternet Vasıtasıyla Mağdura Ait Kontörlerin Bir Telefondan Diğer Bir Telefona Aktarılması 123

3. Oyun Karakterinin Ele Geçirilmesi 125

4. Kripto Paraların Çalınması 126

B. DOLANDIRICILIK SUÇU İLE BİLİŞİM SİSTEMLERİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU 127

VI. YAPTIRIM, SORUŞTURMA VE KOVUŞTURMA 129

SONUÇ 131

KAYNAKÇA 135

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
A.g.e	: Adı Geçen Eser
Akt.	: Aktaran
AKSS	: Avrupa Konseyi Siber Suç Sözleşmesi
Bkz	: Bakınız
C	: Cilt
CD	: Ceza Dairesi
CMK	: Ceza Muhakemesi Kanunu
Çev.	: Çeviri
E	: Esas
EİK	: Elektronik İmza Kanunu
ed.	: Editör
EDVAC	: Elektronic Discrete Variable Automatic Computer
FSEK	: Fikir ve Sanat Eserleri Kanunu
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K	: Karar
KVKK	: Kişisel Verilerin Korunması Kanunu
m	: Madde

OECD	: Convention on the Organisation for Economic Co-operation and Development
s	: Sayfa
S	: Sayı
www	: World Wide Web
TCK	: Türk Ceza Kanunu
TCKÖT	: Türk Ceza Kanunu Ön Tasarısı
TCMB	: Türkiye Cumhuriyeti Merkez Bankası
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
vd.	: ve devamı
vb.	: ve benzeri
Y	: Yıl
YCGK	: Yargıtay Ceza Genel Kurulu

GİRİŞ

Dünya genelinde ve ülkemizde bilişim çağı olarak adlandırılan bu dönemde teknolojinin gelişmesi, insanların bilişim araçlarını kullanım sıklığını arttırmaktadır. Özellikle internet sayesinde hayatın kolaylaşması ve bilgiye daha hızlı erişim sağlanması dikkat çekmektedir. Ancak, internetin ve bilişim teknolojilerinin hızla yayılması ve yaygınlaşması bilişim suçları kapsamında işlenen suçların sayısının da artmasına neden olmuştur.

Bilişim suçları bilişim sistemine karşı gerçekleştirilebildiği gibi bilişim sistemindeki verilere karşı da işlenebilmektedir. Yapılan bu saldırılar, verilerin çalınması, virüs yayılması gibi farklı şekillerde de gerçekleştirilebilir. Bu noktada bilişim hukuku ve ceza hukuku, bilişim suçlarıyla mücadele etmek için birbirleriyle multidisipliner olarak çalışırlar. Bilişim hukuku, bilişim suçlarına karşı yasal koruma sağlar ve bu suçlarla mücadele etmek için gerekli olan kanuni düzenlemeleri yapar. Ceza hukuku ise, bu suçlar için uygun cezaların belirlenmesini sağlar. Bu nedenle, bilişim suçlarıyla mücadele etmek için bilişim hukuku ve ceza hukukunun bir arada çalışması oldukça önemlidir. Dolayısıyla bilişim bilimleri alanına vakıf hukukçulara sahip olmak çok önemlidir.

Şu bir gerçek ki dünyada ve Türkiye'de mevzuat eksikliği kadar hukukçuların bilişim konusunda yetersiz kaldığı görülmektedir. Hukukçuların bilişim sistemleri konusunda yeterli düzeyde bilgi sahibi olmaması, bilişim alanında doğan hukuki problemlerin çözümünde aksaklıklara sebebiyet verebilmektedir. Dolayısıyla bilişim suçlarının oluşmasını engellemek, bilişim teknolojileriyle ilgili sorunları en kısa sürede çözmek ve mevzuat eksikliklerini gidermek için, bilişim hukuku konusunda uzmanlaşmış hukukçulara ihtiyaç vardır.

Bu çalışmada, bilişim suçlarından Türk Ceza Kanunu'nun *"Bilişim Alanında Suçlar"* başlıklı onuncu bölümünde düzenlenen *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* yan başlıklı 244. maddesi hakkında detaylı inceleme yapılacaktır. Zira bu hüküm, günümüzün gelişen ve hızla değişen teknolojisinde giderek artan bir önem kazanmaktır. Bu nedenle, bu çalışma, bilişim suçlarının önemine ve özellikle bu suçun etkilerine odaklanılacaktır.

Çalışmamız üç bölüme ayrılmıştır. İlk bölümde *"Bilişim Sistemleri ve Bilişim Suçlarına İlişkin Genel Esaslar"*, ikinci bölümde *"Bilişim Sistemini Engelleme veya Bozma ve Verileri Bozma, Yok Etme, Değiştirme veya Erişilmez Kılma, Sisteme Veri Yerleştirme, Var Olan Verileri Başka Bir Yere Gönderme Suçları"* ve üçüncü bölümde ise *"Bilişim Sistemleri Aracılığıyla Haksız Çıkar Sağlama Suçu"* incelenecektir.

Çalışmamızın birinci bölümünde bilişim sistemleri ve bilişim suçları incelenecektir. Bu kapsamda öncelikle bilişim, bilişim alanı, bilişim sisteminin kapsamının belirlenmesi akabinde bilişim sistemine ilişkin unsurlardan, tarihi gelişimiyle birlikte bilgisayar, veri ve internetten bahsedilerek konuya ilişkin kavramların tanınması amaçlanmaktadır. Bu bilgiler doğrultusunda tanımlanan bilişimin, bilişim suçu bakımından değerlendirilmesi yapılacaktır. Bir başka deyişle bilişim suçu kavramının tanımı ve kapsamı belirlenecektir. Dünyada ve mevzuatımızda nasıl düzenlendiği izah edilecektir. Bu kapsamda bilişim suçlarının genel özellikleri ortaya konmaya çalışılacaktır.

Çalışmamızın devamında ise birinci bölümde izah edilen mevzuatımızdaki bilişim alanında suçlar başlığı altında gösterilen 244. maddesindeki *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* başlığı altındaki üç suç tipi incelenecektir.

TCK'nin 244. maddesinin ilk iki fıkrasındaki benzerlikler nedeniyle çalışmamızın ikinci bölümünde "*Bilişim sistemini engelleme veya bozma ve verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçları"* birlikte incelenecektir. Bu kapsamda TCK m. 244/1 ve TCK m. 244/2 hükümlerinde belirtilen suçlar, suçun unsurları bakımından ayrı ayrı incelenmiştir. Buna karşın suçların hukuki konusu, maddi konusu, suçların faili ve mağduru, suçların özel görünüş biçimleri, teşebbüs, iştirak ve içtima, suçların nitelikli hali, yaptırım, soruşturma ve kovuşturma hususları iki suç bakımından benzer özellik gösterdiğinden ve tarafımızca öğretideki görüşler nedeniyle tekrardan imtina edildiğinden ilgili başlıklar altında birlikte inceleneceklerdir.

Çalışmamızın üçüncü bölümünde ise ikinci bölümde izah edilen mevzuatımızdaki bilişim suçlarından biri olan 244. maddesinin dördüncü fıkrasındaki *"Bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu"* incelenecektir. Bu kapsamda da suçun hukuki konusu, fail, konu, mağdur, fiil, hukuka aykırılık, kusurluluk, kusurluluğu kaldıran nedenler incelenecektir. Daha sonrasında suçun özel görünüş biçimleri, iştirak, teşebbüs ve

içtima hususları değerlendirilecektir. Akabinde suçun yaptırımı, soruşturulması ve kovuşturulması incelenecektir.

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMLERİ VE BİLİŞİM SUÇLARINA İLİŞKİN GENEL ESASLAR

I. BİLİŞİM, BİLİŞİM SİSTEMİ VE BİLİŞİM ALANI

A. BİLİŞİM

Bilişim kavramının Türkçemize nasıl kazandırıldığı konusunda öğretide birçok farklı görüş bulunmaktadır. Bazı yazarlar bilişim kavramının kökeninin Fransızcada aynı kökten gelen *"informatique"* olduğunu, daha sonra Türkçeye enformasyon olarak çevrilerek bu sözcüğün kullanıldığını, enformasyon yabancı bir sözcük olduğundan Türkçe karşılığı olan bilişim kavramının kullanıldığını belirmişlerdir.[1] Bazı yazarlar ise bilişim kavramının *"information"* (bilgi) ve *"automatique"* (otomatik) kelimelerinden türetildiğini ifade etmektedirler.[2] Bir başka görüşe göre ise Prof. Dr. Aydın Köksal tarafından bilişim kavramı *"bilmek"* fiilinden türetilerek Türkçemizde yer edinmiştir.[3]

Bilişimin kökenleri matematik, fizik ve elektroteknikten oluşan bir mühendislik alanıdır. Bilişim bilimi ise verilerin aktarıldığı, depolandığı ve algoritmalar aracılığıyla işlendiği makinelerin tasarımını yapar. Bilişim, bir yardımcı bilim gibi kabul edildiğinde bilişim dışındaki bilimlerde mevcut olguları soyutlaştırarak gerçekliğin simülasyonunu sağlar ve belirli algoritmalarla işlem yapar.[4]

TDK Sözlüğü'nde bilişim; *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik"* olarak tanımlanmaktadır.[5] Görüldüğü üzere Türk Dil Kurumu bilişimi, bilgi ve elektronik makine unsurlarını kullanarak tanımlamıştır. Dolayısıyla sözlük anlamı bakımından

[1] Değirmenci, Olgun: Bilişim Suçları, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul 2002, s.4.; Dülger, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, 10. Baskı, Seçkin Yayıncılık, Ankara 2023, s.73-74.
[2] Özen, Muharrem/Baştürk, İhsan: Bilişim-İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara 2011, s.12.
[3] Erdoğan, Yavuz: Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile), Legal Yayıncılık, İstanbul 2013, s.23.; Bensghir, Türksel Kaya: *"Türkiye'de Yönetim Bilişim Sistemleri Disiplinin Gelişimi Üzerine Düşünceler"*, *Amme İdaresi Dergisi*, Cilt: 35, Sayı:1, 2002, ss. 77-103, s.82.
[4] Özbek, Veli Özer: *"Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)"*, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C.9, Özel Sayı, İzmir 2007, s.1023.
[5] https://sozluk.gov.tr/, erişim tarihi: 30.04.2022.

bilişimin, bilginin elektronik makineler vasıtasıyla işlenmesi olarak tanımlanması mümkündür.

Bilişim terimleri sözlüğünde ise bilişim, çeşitli alanlarda iletişimde kullanılan ve bilimin esası olarak gösterilen bilgiyle bilişimi sınırlandırarak bu bilginin elektronik makineler vasıtasıyla işlenmesi olarak tanımlanmıştır.[6] Bilişim kavramına dair hukukçuların tanımlamaları ise şu şekildedir:

Tavukçuoğlu bilişim sözcüğünü; toplum ve insanlık yararını göz önünde bulundurarak, bilgi kavramını ve onu saklama, erişim, işleme, transfer etme ve kullanma yöntemlerini inceleyen bir bilim dalı olduğunu ifade etmiştir.[7]

Akbulut bilişimi, bilgisayar başta olmak üzere elektronik araçlarla işlenmesi ve verilerin iletişim hatlarıyla transfer edilmesi bilimi olduğu bir başka ifadeyle, verilerin işlenmesini yani veri iletişimini sağlayan ve bilgiyi inceleyen bir bilim dalı olduğunu belirtmiştir.[8]

Yazıcıoğlu ise bilişimi bilgisayarların kullanılması suretiyle bilginin saklanması, işlenmesiyle kullanılır hale gelmesi ve iletilmesini esas alan disiplin olarak tanımlamıştır .[9] Çalışmamızın devamında da ifade edileceği üzere yazarın bilişim alanındaki suçları bilgisayar suçları olarak tanımlamasının sebebi bilişimi bilgisayar üzerinden tanımlamasıdır.

Değirmenci ise bilişimi teknik, ekonomik, sosyal ve hukuki alanlardaki verilerle sınırlandırarak bu verilerin işlenmesi, muhafaza edilmesi, organize edilmesi, değerlendirilmesi ve başka bir yere aktarılması olarak tanımlamıştır.[10]

Dülger ise öğretideki bilişim tanımlarında ortak yönleri veri işleme, veri aktarımı ve bunların bilgisayarla yapılması şeklinde belirlemiş ve bu belirlenen ortak yönler üzerinden

[6] Köksal, Aydın: Bilişim Terimleri Sözlüğü, Türk Dil Kurumu Yayınları, Ankara 1981, s.28.
[7] Tavukçuoğlu, Cengiz: Bilişim Terimleri Sözcüğü, Asil Yayın Dağıtım, Ankara 2004, s.55.
[8] Bozdoğan Akbulut, Berrin: *"Bilişim Suçları"*. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 8 (1-2 (Milenyum Armağanı), Haziran 2000, s.546.
[9] Yazıcıoğlu, Yılmaz: Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, Alfa Yayınevi, İstanbul 1997, s.131.
[10] Değirmenci, s.7.

(bilgi kavramı üzerinden) tanımlama yapmıştır. Dolayısıyla bilginin işlenmesi, aktarılması, bilgisayarda depolanması ve kullanıcının erişebilmesi bilimi olarak ifade etmiştir[11].

İstanbul Bölge İdare Mahkemesi 21. Ceza Dairesi'nin 02.03.2017 tarihli Kararı'nda da bilişim kelimesinin Fransızca informatigue sözcüğünden gelerek Türkçeye *"bilgi"* ve *"otomatik"* kelimeleri vasıtasıyla çevrilerek türetildiği belirtilmiştir. Kararda ayrıca bilişimin bilginin bir otomasyon sürecine dahil edilmesi neticesinde işlenmesini bir başka deyişle verinin muhafaza ve organize edilmesi, nakledilmesi, değerlendirilmesi, çoğaltılması gibi anlamları da içerdiğini belirtmektedir.[12]

Yine Yargıtay Ceza Genel Kurulu tarafından verilen 2017 tarihli Karar'da iletişimde kullanılan ve bilime dayanak olan bilgi kavramı üzerinden tanımlama yapılarak elektronik makineler vasıtasıyla bilginin işlenmesi, elektronik cihazlarda toplanması ve işlenmesi olarak tanımlanmıştır.[13]

Görüldüğü üzere, öğretide birden çok tanımlama olmasına rağmen yazarların *"bilişim"* kavramı tanımlanırken ortak paydada buluştukları unsurlar;

- bilginin işlenebilmesi,
- bilginin saklanabilmesi,
- bilginin aktarılabilmesi,

şeklinde olup öğretide bu özelikler çerçevesinde tanımlamalar yapılmıştır.[14]

Öğretide birçok yazar tarafından bilişim teriminin bilgisayara göre geniş bir kapsam alanı bulunduğu ifade edilmiştir.[15] Bu doğrultuda bazı yazarlar bir üst kavram olarak bilişimin bilgisayarı da kapsadığını, zira bilgisayarların verileri depo etmeyi, saklamayı, işlemeyi ve yeniden değerlendirmeyi sağladıklarını, bilişimin ise hem verileri işlemeyi

[11] Dülger, s.74-75. Aynı yönde Ergün, İsmail: Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008, s.10.
[12] İstanbul Bölge İdare Mahkemesi 21. CD'nin 02.03.2017 tarihli ve E:2017/530, K:2017/574 sayılı Karar. (Aynı yönde Yargıtay Ceza Genel Kurulu, 02.04.2013 tarihli ve E:2012/1293, K:2013/111) http://www.lexpera.com.tr erişim tarihi: 08.11.2022.
[13] Yargıtay Ceza Genel Kurulu'nun 17.01.2017 tarihli ve E:2015/867, K:2017/13 tarihli Kararı. https://www.corpus.com.tr/ erişim tarihi:10.11.2022.
[14] Kurt, Levent: Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, Seçkin Yayıncılık, Ankara 2005, s.25.
[15] Dülger, s.75.

hem de bu verileri aktarılmayı sağladığını ifade etmişlerdir.[16] Buna karşın bilişim ile bilgisayar teriminin iki farklı kavramlar olduğunu, bilişim bir bilim dalı iken bilgisayarın bir makineyi tanımladığını ve dolayısıyla iki terimin karşılaştırılmasının mümkün olmadığını vurgulayan yazarlar da bulunmaktadır.[17]

Kanımızca bilişimin bir bilim dalı, bilgisayarın da bir makine olduğunu kabul etsek de bilişim biliminin içerisinde bilgisayarın işlevi nedeniyle bilişim teriminin bilgisayarı kapsayıcı niteliği bulunmaktadır. Dolayısıyla bilişimin bir üst kavram olduğu görüşüne katılmaktayız.

B. BİLİŞİM SİSTEMİ

765 sayılı Kanun *"bilgileri otomatik işleme tabi tutan sistem"* ibaresini kullanmıştır. Buna karşın 5237 sayılı Kanun bu ibare yerine *"bilişim sistemi"* kavramını kullanmıştır.[18] 5237 sayılı TCK'nin 243. maddesinin gerekçesinde de bilişim sistemi kavramına ilişkin şu şekilde bir tanımlama yapılmıştır:

"Veri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir"

Öğretide yazarlar, bilişim sistemi için birçok tanımlamalar yapmıştır.

Ketizmen bilişim sistemini tanımlarken bilişimin Fransızca karşılığı olan *"enformatik"* kavramından hareketle bir enformasyon sistemi üzerinden tanımlama yapmıştır. Yazara göre enformasyon sistemi, enformasyonun toplanması, adlandırılması, düzenlenmesi, sınıflandırılması, dönüştürülmesi, arandığında kolay şekilde bulunması ve iletilmesi şeklindeki sınıflandırmaları içerebildiği ifade edilmektedir. Buradan hareketle yazar tarafından enformasyonun otomatik makineler vasıtasıyla ve otomatik bir biçimde işlenmesinin sağlandığı makineler, enformasyon sistemi olarak tanımlanabileceği belirtilmiştir.[19]

---

[16] Yenidünya, Caner/Değirmenci, Olgun: Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, İstanbul 2003, s.19. Aynı yönde dipnotta Özbek, "*Bilişim kelimesi, bilgisayardan faydalanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetini, bilgisayar ise bu faaliyetin gerçekleştirilmesinde en önemli etken olan cihazı ifade etmektedir. O halde, bilgisayar, bilişimin bir kısmını ifade etmektedir.*" s.1025.

[17] Dülger, s.74.

[18] Dülger, s.73.

[19] Ketizmen, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara 2008, s.10.

Işıklı/Küçükvardar, *"Bilişimde kullanılan tüm araç ve gereçlerin birleşiminden oluşan sistemdir."* şeklinde tanımlamıştır.[20]

YGCK'nin 2017 tarihli Kararı'nda da yerleşik kararlar ve öğretideki görüşlere vurgu yapılarak toplanan verilerin yerleştirilmesinin akabinde bilişim sisteminin bu verileri otomatik işleme tabi tutulması olanağı tanıyan manyetik sistemler olduğu belirtilmiştir.[21]

Görüldüğü üzere, verilerin toplanılarak yerleştirilmesi, bu verilerin otomatik işleme tabi tutulması ve manyetik bir sistem olması bilişim sisteminin özellikleri olarak gösterilebilmektedir.[22]

Buna karşın Avrupa Konseyi Siber Suç Sözleşmesinin 1. maddesinde *"bilişim sistemi*" kavramı kullanılmamıştır. Bu kavramın yerine *"bilgisayar sistemi"* kavramı kullanılmıştır. *"Bilgisayar sistemi"* ise söz konusu Sözleşme'de *"Bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbirleriyle ilişkili bir dizi cihazı ifade edecektir."* olarak tanımlanmıştır.[23]

Görüldüğü üzere, 5237 sayılı Türk Ceza Kanunu, yargı kararları ve öğretideki baskın görüş bilişim alanındaki suçları, bilgisayar ile sınırlandırmamış *"bilişim sistemi"* kavramını kullanarak bilişim suçlarını Avrupa Konseyi Siber Suç Sözleşmesindeki tanımdan daha geniş yorumlamıştır. Zira bilişimin bilgisayardan daha geniş bir kapsamı olduğu bilgisi ve günümüzdeki gelişen ve değişen teknoloji gerçeği karşısında *"bilgileri otomatik işleme tabi tutabilen cihazları"* bilgisayarlara indirgemek yetersiz kalacaktır. Zira akıllı cep telefonları[24], buzdolapları, navigasyon cihazları, POS cihazları (Point of Sale), ATM'ler (Automated Teller Machine), CCTV (Close Cicuit Television), kişisel sağlık takip cihazları, sesli yardım asistanları da bilgileri otomatik olarak işleme tabi tutabilen cihazlardan birkaçı olarak sayılabilmektedir.[25]

---

[20] Işıklı, Şevki/Küçükvardar, Mert: Bilişim Devrimi Teknolojinin Felsefi ve Sosyolojik Analizi, Birleşik Yayınevi, Ankara 2016, s.17.
[21] Yargıtay Ceza Genel Kurulu'nun 17.01.2017 tarihli ve E:2015/867, K:2017/13 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:22.05.2023.
[22] Özbek, s.1024.
[23]https://www.btk.gov.tr, s.20. erişim tarihi: 11.08.2023.
[24]YGCK'nin 19.06.2007 tarihli E:2007/6-136, K:2007/150 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:22.05.2023.
[25] Ekici, Şerafettin: Bilişim ve Teknoloji Hukuku, Seçkin Yayıncılık, Ankara 2022, s.23.

C. BİLİŞİM ALANI

5237 sayılı Kanunun TCK m. 243-246'nın yer aldığı onuncu bölümün başlığı *"Bilişim Alanında Suçlar"* olduğunda bilişim alanı kavramının da açıklanması gerekmektedir.

1989 tarihli Türk Ceza Kanunu Öntasarısı'nın 342. maddesinde *"Bilişim Alanı"*nı bilgilerin toplanılıp depo edilmesinin akabinde bu bilgilerin *"otomatik işleme tabi tutma"* sisteminden oluşan bir alan olduğu ifade edilmiştir"[26]

1997 tarihli TCK Öntasarısı'nın gerekçesinde ise bilişim alanı tanımı yapılırken bilgi yerine veri, sistem yerine manyetik sistem ibareleri kullanılarak verilerin toplanılıp depo edilmesinin akabinde bu bilgileri otomatik işleme tabi tutma olanağı veren manyetik sistemlerin oluşturduğu bir alan olduğu belirtilmiştir.[27]

Buna karşın bilişim alanı TCK'da tanımlanmamıştır. Yazıcıoğlu tarafından bilişim alanı tanımlarken aygıtlar özelinde bir açıklama yapmıştır. Yazara göre bilişim alanı, bilgisayar ve bilgisayar gibi aygıtların da içinde bulunduğu alandır.[28]

Özbek ise bilişim faaliyetini vurgulayarak bu faaliyetin gerçekleştirildiği yer olarak tanımlamış, bu alanın soyut bir alanı ifade ettiğini belirtmiştir.[29]

YCGK'nin 2009 tarihli Kararı'nda da bilişim alanı, kısaca bilgilerin depo edildikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alan olarak ifade etmiştir.[30] Dolayısıyla Yargıtay'ın bilişim sistemi tanımı ile birlikte düşünüldüğünde bilişim sistemlerinden oluşan alan olarak belirtilebilmesi mümkündür.

Bu doğrultuda öğretide bazı yazarlar[31] tarafından bilişim alanı kavramının kullanılmasının yerinde olduğu ifade edilirken bizim de katıldığımız görüşe göre bazı

[26] Ergün, s.11
[27] Ergün, s.11.
[28] Yazıcıoğlu, s.131.
[29] Özbek, s.1024.
[30]YCGK'nin 17.11.2009 tarihli ve E:2009/193, K:2009/268 sayılı Kararı, https://www.lexpera.com.tr, erişim tarihi: 15.05.2023.
[31] Yenidünya, A. Caner: "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243*)" Legal Fikri ve Sınai Haklar Dergisi, 2005, S.4, Yenidünya, s.1019

yazarlar[32] tarafından bilişim sistemi kavramının kullanılmasının daha doğru olacağı kanaatindedir.

II. BİLİŞİM SİSTEMİ KAVRAMLARI

A. BİLGİSAYAR

Bilgisayar, ülkemize 1960'lı yıllarda girmiş olup İngilizcede *"hesaplayarak sonuca ulaşma"* anlamına gelen *"to compute"* kelimesinden türeyen *"computer"* olarak adlandırılmıştır.[33] Önceleri bilimsel ve iş yaşamında kullanılmaya başlanılmıştır. Daha sonra yabancı etkisinde kalınarak ilk başlarda *"kompütür"*, *"sayısal makine"*, *"elektronik beyin"*, *"ordinatör"* vb. kelimeler kullanılmıştır. Daha sonrasında İngilizcede hesaplamak sözcüğünden türetilen ve Türkçeye hesaplayıcı olarak çevrilen *"computer"* kelimesine karşılık Türkçede *"bilgisayar"* kavramı tercih edilmiştir. Bilgisayar kelimesinin öz Türkçe olmasının yanı sıra yalnızca hesaplayıcı anlamına gelmeyen *"bilgiyi işlemek"* kökünden türetilen *"bilgi saymak, bilgi vermek"* anlamlarına da gelmesi makinenin gerçek yapılma amacına da hizmet verdiğinden yerinde bir seçim olmuştur.[34]

Buna karşın yalnızca bilgi işleyen bir araç olarak tanımlanması da bilgisayarın gerçek mahiyetini ve bu suretle elektronik hesap makineleri ile bilgisayar arasındaki farkını ortaya koymak bakımından yeterli olmayacaktır. Öte yandan programlama yeteneğini haiz makineler olarak tanımlamak da elektronik çamaşır makinelerinden bilgisayarları ayırmayacaktır. Bu kapsamda bilgisayarları, programlama yeteneği olan cihazlardan ve elektronik hesap makinelerinden ayıran husus, bilgisayarlar, genel amaçlı kullanılabilmektedir. Bir başka deyişle enformatik özelliğe sahiptir. Dolayısıyla bilgisayarlar, iyi kavramlaştırılmış ve tanımlanabilmiş problemler üzerinde çalışabilen aygıtlardır. [35]

Türk Dil Kurumu Sözlüğü'ne göre bilgisayarın tanımı *"Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"* şeklinde yapılmıştır. [36]

---

[32] Özbek, s.1024.
[33] The New Webster Encyclopedic Dictionary of The English Language, Vol.1, Ed: Virginia S.atvher/Alexander McQueen, New York, Grolier Incorparated, 1968, s.172 (akt. Dülger, s.62)
[34] Dülger, s.63.
[35] Yazıcıoğlu, s.27
[36] https://sozluk.gov.tr/, erişim tarihi: 01.05.2021.

Avrupa Konseyi Siber Suç Sözleşmesinin *"Terimlerin Kullanımı"* başlıklı Birinci Bölümünün *"Tanımlamalar"* başlıklı 1. maddesinde bilgisayar sistemini (computer system), *"bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi ifade edecektir."* İbareleri ile tanımlamıştır.[37]

Yazıcıoğlu ise bilgisayarı tanımlarken onu veri üzerinde yapabileceği özellikleri belirterek tanımlamıştır. Yazara göre bilgisayar, veri saklayan, muhafaza eden, bunları işleyen, depolanan, bir program işletebilen ve bu verileri otomatik olarak değiştiren özelliklere sahip bir cihaz olduğunu belirtmiştir.[38]

Tüm bu açıklananlar neticesinde bilgisayarın birçok tanımı yapıldığı görülmektedir. Ancak yapılan her tanımın gelişen ve değişen dünya ve teknolojide yetersiz kalması kaçınılmazdır. Ceza hukuku bakımından bir fiilin suç sayılabilmesi için suçun maddi konusunun *"suçların ve cezaların kanuniliği ilkesi"* gereğince kanunda tanımlanması gerekmektedir. Türk Ceza Hukukunda kıyas yasağı olması sebebiyle suç sayılacak fiilin cezasız kalmaması için kanunda boşluk bırakılmaması gerekmektedir.[39]

Kanımızca *"bilgisayar"* tanımının yapılması gerektiği görüşüne katılmakla birlikte daraltıcı bir yorumdan kaçınılması gerektiği düşüncesindeyiz. Zira Türk Ceza Kanunu'nda "*bilişim sistemi*" ibaresi kullanıldığından bilişim suçlarının yalnızca bilgisayarlara indirgenmesi hatalı olacaktır. Nitekim eskiden bilgisayar denilince masaüstü bilgisayarlar akla gelirken değişen ve gelişen dünya ve teknolojiyle birlikte bilgisayarların boyutları küçüldüğü gibi bilgisayarlar, akıllı bileklik, akıllı gözlük, akıllı saat vb. aksesuarlar da bilgisayar teknolojisi içermektedir. Bilişim sistemi başlığı altında da belirttiğimiz akıllı cep telefonları, buzdolapları, navigasyon cihazları, POS cihazları, ATM'ler, CCTV'ler, kişisel sağlık takip cihazları, IoT (internet of things) teknolojisine sahip akıllı aygıtlar da bilgisayarların özelliklerini haizdir.[40] Dolayısıyla gelişen teknoloji ve değişen dünya gerçeği karşısında bu değişimlere uyumlu kanunların yapılması gerekmektedir.

[37] https://polis.osce.org , erişim tarihi: 24.12.2022.
[38] Yazıcıoğlu, s.27-28.
[39] Doğan, Ramazan: 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Adalet Yayınevi, Ankara 2014, s.8-9.
[40] Yeldan, Didem: Siber Suçlar, Seçkin Yayıncılık, Ankara 2022, s.59.; Gün, Nagihan: Türk Ceza Hukukunda Bilişim Suçları, Çankaya Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, Haziran 2020, s. 30-31-32.

Bu düşünceden hareketle bilgisayarlar, bilişim suçları bakımından en çok kullanılan cihaz olduğundan bu başlık altında bilgisayarlara ilişkin genel geçer açıklamalara yer verilecektir.

1. Tarihçe

Bilgisayarın ortaya çıkması, bir anda olmamıştır. Bu doğrultuda birden çok icatla aynı döneme denk gelmesi, farklı fikir etkinliklerinin ve bilgi transferlerinin arka arkaya gelmesiyle oluşmuştur.[41]

Nitekim bilgisayarın ortaya çıkması yönündeki ilk adımın İngiliz matematikçi William Oughtred tarafından 1622 yılında abaküsü icat etmesiyle atıldığı da ifade edilmektedir. Buna karşın bazı kaynaklarda abaküsün, MÖ 2400 yıllarında Çin'de geliştirildiği ve denizaşırı ticaret yapan tüccarlar tarafından Avrupa ve Amerika'ya getirildiği de belirtilmektedir.[42]

Bilgisayarın tarihi gelişimi, sınırları kesin olmamakla birlikte öğretide dört döneme[43] ayrılarak incelenmektedir.

1.1.Birinci Dönem

Bilgisayarın tarihçesinde birinci dönem 1940–1959 arası döneme isabet etmektedir. Bu dönemde Dünya'da İkinci Dünya Savaşı etkisi bulunmaktaydı. 1942'de Pensilvanya Üniversitesi Moore Elektrik Mühendisliği Okulu'nda savaş sırasında atılan bombanın nereye düşeceğini hesaplayabilmek için J. Presper Eckert ile John W. Mauchly ve ekipleri tarafından bilinen *"ENIAC" ("Electronic Numerical Integrator And Calculator")* adıyla ilk bilgisayar üretildi. Atılan bombanın nereye düşeceğinin hesabı bir insanın 20 saatini almakta iken ENIAC bu işlemi 30 saniyede tamamlayabilmektedir.[44]

[41] Grolier International Americana Encylopedia, Sabah Yayınları, C. 3, Y.1993, s. 222.
[42] Yeldan, s.60.
[43] Bu çalışmada bilgisayarların tarihsel gelişimini dört dönem olarak incelemekteyiz. Buna karşın beşinci dönemin varlığını ileri sürenler de bulunmaktadır. Bu dönemi kabul edenler, kullanıcı ile interaktif olarak iletişime geçilen makineler üretilmektedir. (Aydın, s.23) Yine bu dönemde yapay zekalı bilgisayarların üretildiğini ancak bu tip bilgisayarlar için çalışmaların yeterli düzeyde olmadığını savunanlar da bulunmaktadır. (bkz: Madran, s.4)
[44] https://bilimgenc.tubitak.gov.tr, erişim tarihi: 24.12.2022.

ENIAC'la hemen hemen aynı dönemlerde Macar matematikçi J. Von. NEUMAN tarafından kesikli değişkenli elektronik otomatik bilgisayar olarak adlandırılan "EDVAC" (Elektronic Discrete Variable Automatic Computer) üzerinde çalışılmıştır.[45]

Birinci dönemdeki bilgisayarlar, günümüzdeki bilgisayarlara nazaran elbette ki ağır işlediği gibi pahalıdır. Bu bilgisayarlarda veri programları ise ana bellekte tutulmaktadır. Çevreye fazla ısı yayar ve daha fazla enerji harcamaktadırlar. Buna rağmen ENIAC, ilk elektronik devrelere sahip vakum tüplü bilgisayar olarak literatüre geçmiştir.[46]

1.2.İkinci Dönem

Bilgisayarın tarihsel gelişiminde ikinci dönem ise 1960–1964 yılları arasına tekabül etmektedir. Bu dönemde birinci dönemdeki vakum tüplerinin yerine, daha hızlı ve daha az elektrik üreten transistörlü bilgisayarlar kullanılmaya başlanmıştır. Bu dönemdeki bilgisayarlarda ASSEMBLY makine dili kullanılmış olup birinci dönemdeki bilgisayarlara nazaran ikinci dönemdeki bilgisayarlar daha az enerji kullanmakta ve daha az ısı yaymaktadır.[47]

Esasen bu dönemin en önemli özelliği programlamaya getirilen yeniliklerdir. Bu dönemdeki bilgisayarlarda birinci dönemden farklı olarak donanımdan ziyade yazılım unsurunda gelişme sağlanmıştır. Önceden her şey makinenin yapısına bağlı olarak yapılmakta iken donanımdan ari programlama dilleri yaratılmıştır. Bu diller geliştirilerek yazılımcıların yazılım dili bilmesine gerek olmaksızın yazılım üretebilmesi sağlanmıştır. Ayrıca işletim yazılımları da bu dönemde geliştirilmiştir.[48]

Türkiye'nin de ilk bilgisayarı olan *"IBM-650 Data"* 30 Ekim 1960' dan itibaren yol yapım çalışmaları için Karayolları Genel Müdürlüğü tarafından kullanılmaya başlanmıştır.[49]

1.3.Üçüncü Dönem

Bilgisayarın tarihsel gelişiminde üçüncü dönem ise 1965-1970 arasını kapsayan dönemdir. Bu dönemde transistörler bir araya getirilerek (tümleşik) entegre devreli

[45] Yazıcıoğlu, s.35.; Madran, R. Orçun: Bilgisayar Teknolojilerine Giriş, s.3. https://madran.net, erişim tarihi: 24.12.2022.
[46] Değirmenci, s.18-19.
[47] Madran, s.4.
[48] Yazıcıoğlu, s.36.; Dülger, s.95.
[49] Yeldan, s.60.

bilgisayarlar üretilmiştir. Dolayısıyla tümleşik devrelerin kullanılması ve silikon yongaların artmasıyla bilgisayarların hızı artmış ve boyutları küçülmüştür.[50] Ayrıca bilgisayarlarda manyetik diskler kullanılmaya başlanmıştır. Bunlar önceki bilgisayarlara kıyasla daha düşük maliyetli olup güvenilirliği yüksektir.[51]

Bu dönemdeki bilgisayarlar iş hayatında ve gündelik hayatta kullanılabilir hale getirilmiştir. Bu sayede bilgisayarlar, yalnızca bilimsel kurumların kullandığı erişilmesi zor makineler olmaktan çıkmıştır.[52] Zira Türkiye'nin ikinci bilgisayarı olan IBM 1620 de 1966 yılında İstanbul Teknik Üniversitesi tarafından akademik amaçlı olarak kullanılmaya başlanmıştır.[53]

Ayrıca belirtmek gerekir ki Amerika'da bir kişinin 18 Ekim 1966 tarihinde banka hesabında tahrifat yapması neticesinde ilk bilişim suçu işlenmiştir.[54]

1.4.Dördüncü Dönem

Bilgisayarın tarihsel gelişiminde dördüncü dönem ise 1970'den sonrasını kapsayan dönemdir. Bu dönemde işlem ve kontrol birimlerinin birlikte bulunduğu chipler geliştirilmesiyle mikroişlemcili bilgisayarlar üretilmiştir. Bu mikroişlemciler sayesinde bilgisayarlar, fiziksel olarak küçülmüş ve daha hızlı işlemler yapar hale gelmiştir. Aynı zamanda önceki dönem bilgisayarlara nazaran yüksek depolama hacimlerine erişmişlerdir. Ağ sistemleri oluşturularak başkaca bilgisayarlarla iletişim sağlanabilmiştir. Yapay zeka kavramı da bu dönemde hayata geçmiştir. [55]

Yine bu dönemde uygulama yazılımlarının geliştirilerek her tür iş için bilgisayarların kullanılabilir hale gelmesi büyük bir yenilik olmuştur. Zira önceki dönemlerde bilgisayarlar devlet desteğiyle askeri veya bilimsel amaçlı kullanılmaktayken artık ticari amaçla da kullanılmaya başlanılmıştır. Bu doğrultuda, 1978 yılında Apple ile başlayan süreç daha sonrasında diğer bilgisayar şirketleriyle devam ederek farklı sektörlerde de kullanılmaya başlanmıştır.[56]

[50] Yazıcıoğlu, s.37.
[51] Madran, s.4.
[52] Değirmenci, s.20-21
[53] Yeldan, s.60.
[54] Aydın, Emin Doğan: Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, Ankara 1992, s.13– 23.
[55] Madran, s.4.; Yazıcıoğlu, s. 38.
[56] Yazıcıoğlu, s.38; Dülger, s.92.

Mikroişlemcili bilgisayarlar, 1980'lerin sonuna doğru pazarlara girmiş ve 1990'lı yılların ortalarından itibaren ise kişisel bilgisayar olarak kullanılmaya başlanmıştır.[57]

2. Donanım (Hardware)

Türk Dil Kurumu sözlüğünde donanım, *"Bir bilgisayarda bulunan fiziksel birimler"*[58] olarak adlandırılmaktadır.

Öğretide ise donanımın birçok tanımı bulunmaktadır. Bir bilgisayarın fiziksel bileşenlerine verilen genel (ortak) isim olarak tanımlanabilmektedir. Genel olarak elle tutulabilen ve gözle görülebilen iç ve dış bileşenlere verilen isim olarak tanımlanmaktadır. Gözle görülebiliyor olması kasanın içerisinde bulunan parçaları donanımın bir parçası olmaktan alıkoymayacaktır. Zira kasanın içerisine bakıldığında o parçalar da görülecektir.[59]

Buna göre donanımın, dış donanım ve iç donanım olarak ayrılabilmesi mümkündür. Dış donanım, ekran, fare, yazıcı, mikro işlemci, sabit disk, bellek, klavye, joystick, tarayıcı, sürücü gibi parçaları ifade ederken; iç donanım ise anakart, ROM, RAM, işlemci, ekran kartı, ağ kartı gibi parçaları ifade etmektedir. [60] Bu parçaların her birinin ayrı bir özelliği olup farklı işlevleri bulunmaktadır.[61]

3. Yazılım (Software)

Bilgisayarlar, yukarıda belirtilen somut parçalardan oluşan donanımdan ibaret olmayıp soyut bileşenleri de bulunmaktadır. Bu soyut bileşenine de yazılım denilmektedir.[62]

TDK sözlüğünde yazılım, *"Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü"* ibareleriyle adlandırılmaktadır.[63]

Yazılım, bilgisayarlardan beklenilen bir işlemin yapılması amacıyla farklı algoritmalara bağlı komutlara bağlı olarak verileri işleyen ve bu işlemlerden bir sonuç çıkaran komut dizinleri olarak ifade edilmektedir.[64]

---

[57] Dülger, s.95.
[58] https://sozluk.gov.tr , erişim tarihi:29.02.2023.
[59] Ekici, Şerafettin: Bilişim ve Teknoloji Hukuku, Seçkin Yayıncılık, Nisan 2022, s.42.
[60] A.g.e, s.44.
[61] Yazıcıoğlu, s.31.
[62] Yazıcıoğlu, s.31.
[63] https://sozluk.gov.tr , erişim tarihi: 29.02.2023.
[64] Ekici, s.48.; Koçoğlu, s.15.

Yazılımı, uygulama yazılımı ve işletim yazılımı olarak ikiye ayrılmaktadır.

3.1.İşletim/Uygulama Yazılımı (Operating System)

İşletim sistemi –uygulama yazılımı olarak da bilinir- bilişim sisteminin çalışmasını ve temel fonksiyonları sağlayan yazılımlar olup bilişim sistemlerinin mütemmim cüzü bir başka deyişle, bütünleyici parçası olarak kabul edilmelidir.[65]

Bilgisayar kullanıcısının doğrudan temasta bulunduğu sistem yazılımına ise işletim sistemi denir. Bu sistem yazılımları bilgisayar ve kullanıcı arasında köprü oluşturmaktadır.[66] Bir başka deyişle bilgisayar kullanıcının komutları sayesinde yazıcı, hoparlör, monitör, tarayıcı gibi bilgisayarın donanım unsurları işletim sistemi içerisine sokulmaktadır. Dolayısıyla bir bilgisayarda işletim sistemi olmadığı takdirde hiçbir bilgisayar programı çalışamayacaktır. İşletim sistemlerine örnek olarak LİNUX/UNIX, Windows 3.1, Vista işletim sistemleri gösterilebilir. [67]

3.2.Uygulama Yazılımı (Application Program)

Bir program türü olan uygulama yazılımları, belli bir işlevi yerine getirmek için yazıldığı gibi belirli bir sorunu çözmek için de yazılmaktadır. Bununla birlikte bilgisayardaki işletim sistemi ile uyumlu çalışmaktadır.[68]

Uygulama yazılımları genellikle paket şeklinde hazırlanmışlardır.[69] Bu paket programlar olmasalardı bilgisayarda yapılması istenilen her işi kendimiz veya bir yazılımcı aracılığıyla yazdırmak zorunda kalacaktık.[70]

Bilgisayarın donanım ve yazılım unsurlarının parçası olmasa da bilgisayarla ilişkili kavramlar da bulunmaktadır. Bu çerçevede veri ve internet kavramlarının da bilgisayarla bağlantılı olmasından kaynaklı izah edilmesi gerektiği kanısındayız.

---

[65] Akıncı, Hatice/ Alıç A. Emre/ Er, Cüneyt*: "Türk Ceza Kanunu ve Bilişim Suçları"*, İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, s.156-275.
[66] Yenidünya/Değirmenci, s.23.
[67] Gürler, Fazıl: Yargıtay Kararları Işığında Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar. Yetkin Yayınevi, Ankara 2015, s.52. Pallı, Hayati: Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri 2008,
[68] Akıncı/Alıç/Er, s.172.
[69] Beygu, Şahin: Yayıncılıkta Bilgisayar El Kitabı, Yalçın Ofset Matbaası, İstanbul 1990, s.18.
[70] Yenidünya/Değirmenci, s.25.

B. VERİ

Veri, bilişim konusunda ve bilişim suçlarında en çok karşımıza çıkan kavramlardan biridir. Bu çerçevede İngilizcede *"data"* kelimesinin karşılığı olarak gösterilen veri, yukarıda ayrıntıları ile açıklanan veriyi işleyen, sonuç çıkaran ve saklayan bilişim sistemlerinin olmazsa olmazıdır.[71] Bu nedenle veri, bilişim suçları bakımından önemi haizdir. Zira suçun maddi konusu arasında bulunmaktadır.[72] Dolayısıyla çalışmamızda verinin de incelenmesi gerekmektedir.

Türk Dil Kurumu Sözlüğü'nde veri, *"olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi"* ibareleriyle tanımlanmıştır.[73]

Avrupa Konseyi Siber Suç Sözleşmesi (AKSS) ise *"bilgisayar verisi"* kavramı tercih edilerek hazırlanmıştır. Sözleşme'nin 1. maddesinde bilgisayar sisteminde işlenmeye hazır olan programları da içinde barındıran olgu, bilgi veyahut kavramların bilgisayar sisteminde her şekilde temsil edilmesi olarak tanımlanmıştır.[74]

Mevzuatımızda verinin tanımı, TCK'nın 243. maddesinin gerekçesinde yapılmıştır. Gerekçede bilişim sistemlerindeki soyut unsurların veri tanımına dahil olduğu vurgulanmıştır.[75] O halde, bilişim sistemlerindeki programların da veri olduğu söylenebilecektir.[76]

Yenidünya-Değirmenci'ye göre ise bilişim sistemi üzerinde muhafaza edilen, saklanan yazı, program ve resim gibi her şeyin bir veri olduğu ifade edilmiştir.[77]

Yine 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da da veri tanımı yapılmıştır.

---

[71] Yanar, Yasin: Ceza Hukuku ve Bilişim Hukuku Bağlamında TCK md.245/A Yasak Cihaz veya Programlar Suçu, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul 2019, s.19.
[72] Yavuz: Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri, Legal Yayıncılık, İstanbul 2018, s.56.
[73] https://sozluk.gov.tr , erişim tarihi:30.01.2023.
[74] https://polis.osce.org/ , erişim tarihi: 30.01.2023.
[75] *"Sistem içindeki bütün soyut unsurlar, fıkrada geçen veri teriminin kapsamındadır*" Erdoğan, s.39.
[76] Değirmenci, Olgun: *"Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi",* Türkiye Barolar Birliği Dergisi, C:18, S:58, s.197-198.
[77] Yenidünya/Değirmenci, s.48. https://www.resmigazete.gov.tr, erişim tarihi: 30.01.2023.
[77] Dülger, s.79.

Söz konusu Kanun'un 2. maddesine göre verinin *"bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri"* ifade ettiği belirtilmiştir.[78] Dikkat edilirse bu tanımlama bilişim sistemi yerine bilgisayar kavramı üzerinden yapılmıştır.

Dülger ise veriyi, bilişim sistemleriyle üzerinde işlem yapılabilen, neticesinde sonuçlar üretilebilen bu sonuçların saklanarak daha sonra yeniden işlenebilen ve başkaca bilişim sistemlerine aktarılabilen her türlü bilgi olarak tanımlamıştır.[79]

Dülger veri tanımlaması yaparken yalnızca *"bilgisayar verisi"* olarak ifade edilmesinin bilgisayarın dışında ancak sistem içerinde mevcut olan araçlardaki verileri kapsamadığını vurgulamıştır. Böyle olunca bu araçlarda bulunan verilerin suçun maddi konusunu teşkil ettiği durumların yaptırımsız kalabileceğini belirtmiş olup yalnızca *"veri"* ibaresinin kullanılmasının daha uygun olacağı kanaatindedir.[80]

Bizce de mevzuattaki bilişim suçları yalnızca bilgisayar ile işlenebilen suçları içermemektedir. Zira Kanunumuz *"bilişim sistemi"* olarak ele alarak *"bilgisayar verisi"* teriminden farklı olarak daha geniş kapsamda ve bizce daha üst kavram olan *"veri"* terimini kullanıldığından Kanun koyucunun da iradesinin bu yönde olduğu açıktır.

Hafızoğulları-Özen, Dülger'in tanımına benzer bir şekilde *"veri"* nin tanımını veriyi, bilişim sistemleri üzerinde işlem yapılabilen, bu işlemler sonucunda sonuçlar üretebilen, muhafaza edebilen ve daha sonra tekrar işleyebilen ve başkaca bilişim sistemlerine aktarabilen, her türlü bilgi olarak tanımlamıştır. Akabinde verilerin bilgisayarın üzerinde çalıştığı bilgiler olduğunu ve bilişim dahilinde, rakamsal veya alfabetik nitelikteki işaretlerin de veri olduğunu belirtmek suretiyle bir tanımlama yapmışlardır.[81]

Hafızoğulları-Özen'in veriyi tanımlarken bilişim sistemini ve bilgiyi bir unsur olarak aldığı görülmektedir. Bu noktada yazarlar tarafından yapılan bu tanımlamanın Kanun koyucunun mevzuatımızda kullandığı kavramlarla yapılan en uygun tanımlama olduğu kanaatindeyiz.

---

[78] Erdoğan, s.37-38; https://www.resmigazete.gov.tr, erişim tarihi: 30.01.2023.
[79] Dülger, s.83.
[80] Dülger, s.84.
[81] Hafızoğulları, Zeki/ Özen, Muharrem: Türk Ceza Hukuku Özel Hükümler-Topluma Karşı Suçlar, Ankara 2016, s.454.

C. İNTERNET

İnternet, İngilizceden Türkçemize geçmiş bir kavram olup Türk Dil Kurumu tarafından *"genel ağ"* olarak tanımlanmıştır.[82]

İnternet terimini, İngilizcedeki *"İnter"* kelimesi Türkçede *"arasında"*, *"net"* kelimesi ise Türkçede *"ağ"* olmak üzere, *"Ağlar Arasında"* şeklinde de tanımlayabiliriz.[83] *"Ağların ağı"* şeklinde *"international"* ve *"network"* kelimelerinin birleşiminden oluştuğu da ifade edilmektedir. [84]

Siber Suç Sözleşmesinin Açıklayıcı Raporu'nda *"ağ"* kavramının tanımı iki ya da daha fazla bilgisayar sisteminin birbirilerine bağlı olması şeklinde tanımlanmıştır. Bu çerçevede internetin de aynı protokolü kullanan ve birbirleriyle bağlantılı olan çok sayıdaki ağdan oluşan küresel bir ağ olduğu ifade edilmiştir.[85]

Öğretide hukukçular tarafından internetin birçok tanımı yapılmıştır. Şöyle ki:

Yenidünya-Değirmenci tarafından internet, belli esaslar çerçevesinde bilişim ağları ile bilgisayarların bağlantılanarak kendine özgü bir dil vasıtasıyla iletişim kurulması şeklinde tanımlanmıştır.[86]

Demir ise interneti birçok haberleşme ağının bir arada oluşturdukları dosyalar ile bilgisayar programları arasında kurulan bir ağ olduğunu belirtmiş ve bütün insana dair bilginin ve birikimin de paylaşıldığını vurgulamıştır.[87]

İnternet Servis Sağlayıcıları (IHS'ler) olarak adlandırılan kuruluşlar, internet ortamına bağlantı sağlamaktadırlar. Öte yandan her bilgisayarın kendine özgü ve değişmeyen bir IP numarası da bulunmaktadır. Bu doğrultuda internet ortamına

[82] https://sozluk.gov.tr , erişim tarihi:29.02.2022.
[83] Yeldan, s.53.
[84] Yenidünya/Değirmenci, s.36.
[85] Özen/Baştürk, s.14,
[86] Yenidünya/Değirmenci, s.36-37.
[87] Demir, Önder: *"İnternet Servis Sağlayıcısının Hukuki Sorumluluğu",* Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayınları, 21-22 Mayıs 2001, İzmir 2022, s.29.

bağlanılmasının akabinde web[88] sayfalarını kullanmak için bir standart olması gerekir ki o da *"http"*dir.[89]

Bilgisayar ağlarından en bilinen internet olup ilk bilgisayar ağı *"ARPANET (Advanced Research Projects Agency Network)"*tir. Amerikan Savunma Bakanlığı için askeri amaçlı bir proje kapsamında İleri Araştırma Projeleri Ajansı tarafından geliştirilmiştir. Bu projede bir nükleer saldırıda haberleşmenin sağlanabilmesi adına kullanılmıştır.[90]

Türkiye'de ise internet ilk kez 1993 yılında TÜBİTAK'ın desteklediği bir projede Orta Doğu Teknik Üniversitesi tarafından kullanılmıştır. 1994 yılında ise Ege Üniversitesi tarafından kullanılmıştır.[91]

İnternet, çoklu iletişim ağlarının bir kombinasyonudur; grafik, metin, resim vb. dosyaların ve bilgisayar programlarının bilgisayarlar arasında paylaşıldığı ve değiş tokuş edildiği bilgisayarlar arasındaki bir ağdır. İnternet bir bilgisayar kümesi olup IP[92] (İnternet Protokolü) vasıtasıyla birbirlerine paket göndermektedir.[93]

III. BİLİŞİM SUÇU VE BİLİŞİM SUÇUNA İLİŞKİN GENEL ESASLAR

A. GENEL OLARAK

Öğretide bu alandaki suçları tanımlamada bir kavram karmaşası bulunmaktaydı. Bu alandaki suçları tanımlamak için *"siber suç"*[94], *"sanal suç"*[95], *"internet suçu"*[96],

[88] Web, ses, görüntü veya metin biçiminde değişen nitelikteki verileri iletebilen bir sistemdir. (dipnotta Kurt, s.43.
[89] Sırabaşı, Volkan: İnternet ve Radyo – TV Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Adalet Yayınevi, Ankara 2003, s.56.
[90] Türkoğlu, Süleyman: Bilgisayar ve İnternet Medya ve İletişim Ön Lisans Programı (akt. Yeldan, s.54.)
[91] Sınar, Hasan: İnternet ve Ceza Hukuku, Beta Yayınları, İstanbul 2001, s. 111.; Yeldan, s.61.; Koçoğlu, Seda: Bilişim Sistemine ve Sistemdeki Verilere Müdahale ile Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlama Suçları (TCK m. 244), İstanbul Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, İstanbul 2019, s.43.
[92] "IP adresi, interneti ya da TCP/IP protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres" https://tr.wikipedia.org , erişim tarihi: 20.05.2021.
[93]KARAHAN, Mehmet, *"Bilişim Kavramları",* http://www.web.inonu.edu.tr 1, (aktaran Tunç, Demircan: Bilişim Alanında Suçlar, Selçuk Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, Konya 2007, s.20.)
[94] Çeken, Hüseyin: *"ABD'de İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası"* (Çevrimiçi) http://archiv.jura.uni-saarland.de, erişim tarihi:04.03.2023; Çakır, Hüseyin/ Kılıç, Mehmet Serkan: Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara 2014, 7. Bölüm, (Aytekin, Akın/ Kılıç, Mehmet Serkan/ Aytekin, Akın: Karşılaştırmalı Hukuk Açısından Siber Suçlar), s.181.

bilgisayar suçu"[97], *"bilişim suç hukuku"*, *"bilişim sistemi aracılığıyla işlenen suç"*, *"bilgisayara karşı işlenen suç"*, *"bilişim alanında işlenen suç"*, *"bilgisayarlar aracılığıyla işlenen suç ve bilişim suçu"* kavramlarının bir dönem kullanıldığını görmekteyiz.[98]

Oysa günümüz teknolojisinde *"siber suç"*, *"bilgisayar suçu"*, *"sanal suç"*, *"internet suçu"* gibi tanımlamalar bu alandaki suçları tanımlamak için yetersiz kalmaktadır. Zira son zamanlarda *"hi-tech crime"* yani *"yüksek teknoloji suçu"*, *"e-crime"* ve *"multi-jurisdictional crime"* (çok yargısal suçlar) gibi kavramlar bu alanı tanımlamak için kullanılmaya başlanmıştır[99]. Buna karşın günümüzde çoğunlukla bilişim suçları üzerinde uzlaşma sağlanmıştır. Nitekim Kanun koyucunun görüşünün de bu yönde olduğu, öğretide de bu kavramın tercih edildiği ve genel kabul gören bir kavram olduğu görülmektedir.[100]

"Bilişim suçu" kavramının kullanılması kanımızca da yerindedir. Şöyle ki:

- Siber suç kavramı, bilişim ağları bilhassa internet yoluyla gerçekleştirilen fiiller bakımından kullanılması,
- Bilgisayar suçu kavramı, hem kapsamının dar olması[101] hem de birtakım yazarlar bakımından bilgisayarın başlı başına suç işleyemeyeceği, anılan kavram ile kastedilenin bilgisayar arayıcılığıyla işlenen suç olduğu düşüncesi[102]
- İnternet suçu kavramı ise esasında internetin bilişim suçlarını işlemeye elverişli en yaygın ağ olduğu, buna karşın internet dışında başkaca ağların da bulunduğu,[103]

dolayısıyla *"bilişim suçu"* kavramına kıyasla yeterli olmayacaklardır. Zira bu kavramın kullanılması sayesinde bu isim altında incelenen suçların sosyo-ekonomik dönüşüm nedeniyle bilişim suçları ile ilişkilendirilmesi daha kolay olacaktır.[104]

---

[95] Yazıcıoğlu, Yılmaz: *"Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı"*, Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001, İzmir Dokuz Eylül Üniversitesi Yayını, 2002, s.452.
[96] Sınar, s.129; Yenisey, Feridun: *"İnternet Suçlarının Yeni İşleniş Biçimleri"*, Uluslararası İnternet Sempozyumu, 21-22 Mayıs 2001, İzmir Dokuz Eylül Üniversitesi Yayını, 2002, s. 447.
[97] Yazıcıoğlu, Bilgisayar Suçları, s.53 vd.
[98] Dülger, s.76-77.
[99] Yeldan, s.43.
[100] Yeldan, s.36.
[101] Yenidünya/Değirmenci, s.31; Yeldan, s.36.
[102] Değirmenci, s.55.
[103] Yenidünya/Değirmenci, s.32.
[104] Ketizmen, s.39.

Bu itibarla, tarafımızca çalışmamızda da bilişim suçu kavramı tercih edilmiştir.

B. TANIM

İlk olarak Türk Ceza Hukuku Literatürüne *"3756 sayılı 765 sayılı Türk Ceza Kanununun Bazı Maddelerinin Değiştirilmesine Dair Kanun Kanun"* ile giren bilişim suçu kavramı, ülkelerin mevzuatlarında tanımlanmış bir suç şekli değildir. Bilişim suçu kavramı hakkında birçok tanımlama yapılsa da üzerinde uzlaşma sağlanan ortak bir tanım bulunmamaktadır.[105]

Bu çerçevede bilişim suçlarını Akbulut, *"verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar"* olarak tanımlamıştır.[106]

Dülger ise bilişim suçu, bilişim sistemleri aracılığıyla veri, veri işlem ile bağlantılı olan sistem ve sistemin işleyişine karşı işlenen suçlar olduğu şeklinde ifade edilmiştir.[107]

Tavukçuoğlu tarafından ise bilişim suçları, bilişimdeki gelişim ve değişimlere neticesinde artış gösteren ve teknoloji vasıtasıyla çoğunlukla sanal ortamda kişilere veyahut kurumlara zarar verici davranışlarda bulunmak olarak tanımlanmıştır. Bu zararın maddi veya manevi olabileceğini de belirtmiştir.[108]

Karagülmez ise bilişim suçu kavramının kapsayıcı olması gerektiğini belirterek, bilişim suçunun bilişim sisteminin kullanıldığı veyahut bilişim sistemlerine karşı işlenen suç olarak tanımlamıştır.[109]

Tüm bu açıklamalar neticesinde bilişim suçları, sisteminin kendisini veya sistemdeki verileri hedef alan ve bilişim teknolojileri kullanılarak veya bilgi araçlarına doğrudan müdahale edilerek işlenen suçlardır.[110]

C. BİLİŞİM SUÇLARININ EKONOMİK SUÇLARLA İLİŞKİSİ

Ekonomik suçlar,[111] ekonomik hayatta geçerli olan ve mecburi güven öğesinin suiistimalinden doğan suçlardır.[112] Küçüktaşdemir ise ekonomik suçları mesleki ve teknik

[105] Ergün, s.12.
[106] Bozdoğan Akbulut, s.551.
[107] Dülger, s.82.
[108] Tavukçuoğlu, s.56.
[109] Karagülmez, s.46.
[110] Erdoğan, s.52; Kurt, 53.

yetenekleri olan failler tarafından işlendiğini belirtmesinin akabinde şiddet içeriği bulunmayan, genellikle aldatıcı filler aracılığıyla ekonomik kazanç amacı güdülen, iktisadi bir etkinlik ile işlenen ve iktisadi menfaatleri ihlal eden suçlar şeklinde tanımlamıştır.[113]

Öğretide bilişim suçlarını ekonomik suç olarak nitelendiren yazarlar bulunmaktadır. Bu görüşe göre bilişim suçları haksız ve ekonomik menfaat sağlamak amacıyla işlenmektedir. Bununla birlikte bilişim suçlarının ekonomik suç olarak nitelendirilmesinde finans kurumlarına veya bu kurumlarla irtibatlı şekilde kişilere özgü işlenmesi sebebi yatmaktadır. Bu yazarlar, bilişim suçlarının işlenmesindeki asıl amacın hukuka aykırı olarak gelir elde etmek olduğunu vurgulamaktadırlar.[114]

Bilişim suçlarının ekonomik suç olarak kabul edildiği görüşlere göre bu suçlar;

- *"Bireysel ya da finansal kazanç veya zarar verme amaçlarıyla*
- *İnternet ya da elektronik ortamlarda,*
- *Bilgisayar veri ile sistemlerinin gizlilik, bütünlük, elde edilebilirlik ve erişilebilirliğine karşı"*,
- Bilgisayarlarla ilgili fiillerle gerçekleşmektedir.[115]

Bazı yazarlarımız ise bilişim suçlarının sadece malvarlığı suçlarıyla sınırlandırılması görüşüne katılmamaktadır. Örneğin sisteme yetkisiz girişler veyahut veriler üzerindeki sahtecilik fiillerinde bu durumun oluşmayacağı ifade etmektedirler.[116]

Bizce de bilişim suçlarının malvarlığı suçlarıyla sınırlandırılması görüşüne katılmak mümkün değildir. Zira ekonomik bir amaç güdülmeyerek de bilişim suçları işlenebilecektir.

D. BİLİŞİM SUÇLARININ SINIFLANDIRILMASI

Öğretide bilişim suçlarının sınıflandırılmasında esas alınan hususun, bilişim teknolojilerinin *"amaç"* ve *"araç"* olarak kullanılması olduğu görülmektedir. Bu

---

[111] Öğretide bu alanı tanımlamak bakımından ticari suç, ekonomik suç, ticari hayatı ilgilendiren suçlar, mali suçlar gibi kavramlar kullanılmakta olup bir terim birliği bulunmamaktadır. Hal böyle iken ekonomi kavramının ticaret kavramını da kapsaması nedeniyle bu çalışmamızda ekonomik suç kavramı kullanılacaktır. (bkz. Özbek, Veli Özer: Ekonomi Ceza Hukuku Birinci Kitap Genel Hükümler, Seçkin Yayıncılık, Ankara 2020, s.21, 30-31)

[112] Dönmezer, Sulhi: *"Ekonomik Suçlar",* Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1985, S.7, ss.19-30, s.21.

[113] Küçüktaşdemir, Özgür: Ekonomik Suçlar Bağlamında Türk Ticaret Kanununda Düzenlenen Suçlar ve Cezalar, Ankara 2018, s.61.

[114] Dülger, s.143-144.

[115] Koçoğlu, s. 38.; Turan, Metin: Alman Bilişim Hukuku, Adalet Yayınevi, Ankara 2017, s. 25.

[116] Akbulut, s.70.

doğrultuda, *"dar ve geniş anlamda"*[117], *"doğrudan ve dolaylı"*[118], *"bilişim sistemine karşı suçlar ve bilişim sistemi aracılığıyla işlenen suçlar"*[119] olarak sınıflandırıldığı görülmektedir.

Buna karşın bilişim suçlarının sınıflandırılmasında farklı sınıflandırma yapan yazarlar da bulunmaktadır. Örneğin Ersoy, *"bilgisayarın maddi konusu teşkil ettiği suçlar"*, *"bilgisayarların araç olarak kullanılması suretiyle işlenen suçlar"*, *"bilgisayar ortamında işlenen suçlar"* olarak gruplandırmıştır.[120] Önder ise *"bilgisayarın araç olarak kullanıldığı mala karşı suçlar"*, *"bilgisayarın araç olarak kullanılarak kişiye karşı işlenen suçlar"* ve *"bilgisayarın araç olarak kullanılması suretiyle kişisel hakların üstünde topluma ait haklar üzerinde işlenen suçlar"* olarak üç grupta toplamaktadır.[121]Dönmezer, *"bilgisayar sistemi içinde işlenen suçlar"* ve *"bilgisayara karşı işlenen suçlar"* olarak sınıflandırmıştır.[122] Karagülmez ise *"bilgisayarın fiziki yapısına zarar verme fiilleri"*, *"bilgisayarın tek başına çalışma sistemine ilişkin fiilleri"* ve *"bilgisayar ağlarına yönelen (internet yoluyla/ortamında) işlenen fiiller"* olarak üç gruba ayırmıştır.[123]

Her ne kadar öğretide farklı sınıflandırmalar olsa da *"amaç-araç"* ilişkisinin bulunduğu görülmektedir.[124] Bu kapsamda bilişim suçları ve bilişim yoluyla işlenen suçlar şeklindeki sınıflandırmanın yerinde olduğu kanaatindeyiz. [125]

E. BİLİŞİM SUÇLARININ GENEL ÖZELLİKLERİ

Bilişim suçlarının kendine has özellikleri bulunmaktadır. Bunları sıralayacak olursak;

1. Bilişim suçunu işleyen failin yakalanması riski diğer suçlara kıyasla daha az olduğu söylenebilir. Zira bu suçlarda genellikle müdahale edenle müdahalenin

[117] Yeldan, s.35.
[118] Yeldan, s.35.
[119] Erdoğan, s.102.
[120] Ersoy, Yüksel: *"Genel Hukuki Koruma Çerçevesinde Bilişim Suçları"*, Prof. Dr. Yılmaz GÜNAL'a Armağan, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, C:49, No:3-4, 1994, s.160; Erdoğan, s.101.
[121] Önder, Ayhan: Şahıslara ve Mala karşı Cürümler ve Bilişim Alanında Suçlar, Filiz Kitapevi, İstanbul 1994, s.505; Erdoğan, s.101.
[122] Dönmezer, Sulhi: Kişilere ve Mala Karşı Cürümler, Beta Yayıncılık, Tıpkı 17.B, İstanbul 2004, s.101; Gün, s.353; Erdoğan, s.101.
[123] Karagülmez, s.61; Gün, s.353.; Erdoğan, s.101.
[124] Aynı doğrultuda Özen/Baştürk, s.91.
[125] Bkz: Akarslan, Hüseyin: Bilişim Suçları, Seçkin Yayıncılık, Ankara 2012, s.39-40

konusu farklı mekanlarda olduğundan fiziki mekânın getirdiği sınırlamalar ortadan kalkmakta ve failin yakalanması zorlaşmaktadır. [126]

2. Bu suçların diğer suçlara kıyasla az emek ve masrafla işlenmekte ise de daha çok zarar verebilmektedir.[127] Bu sebeple suçlar yaygınlaşma tehlikesini içinde barındırmaktadırlar. Zira klasik suçlar genellikle dar bir alanda görülür ve akabinde sonra erer. Buna karşın bu suçlar, sayısı, türleri, işlenebilme imkanları bakımından çeşitlilik göstermektedir. Bilişim suçlarının etki alanı ve sonuçları tahmin edilemez niteliktedir. Bu da bilişim suçlarının en belirgin özelliklerindendir.[128] Bir üniversitede bir öğrenci tarafından 1 milyon dolar üzerindeki bilgisayar yazılımının internet yoluyla dağıtımının yapılması bu duruma örnek verilebilir.[129]
3. Bilişim sistemi kullanılan her alanda bilişim suçları işlenebilmektedir.[130]
4. Bilişim suçlarının en önemli özelliği suç işlenmesinden sonra arkada herhangi bir iz bırakılmaması nedeniyle modus operandinin (suçun işlenme şekli) tespitinin zorlaşmasıdır.[131] Zira bu suçlar genellikle *"köstebek"* adı verilen kurum içi kişiler tarafından işlenmekte olup takibinin ve tespitinin yapılması mümkün değildir.[132]
5. Bilişim suçları bakımından yasa yapılmasında teknolojinin hızla gelişmesi nedeniyle yasalar yetersiz kalabilmektedir.[133]
6. Bilişim suçları ile ilgili yasal düzenlemeler yapılırken hukukçuların yanında bilişim konusunda uzman kişilerin de bulunması gerekmektedir.[134]
7. Bilişim suçları devamlılık arz etmektedir. Zira fail sisteme girdikten sonra yakalanana kadar fiiline devam etmektedir.[135]
8. Bilişim suçlarının failleri bakımından bilişim suçları için beyaz yakalı suçlar da denilmektedir.[136] Zira sanığın mesleki veya iş dünyasını ilgilendirmektedir.[137]

---

[126] Erdoğan, s.87-88.
[127] Erdoğan, s.88.; Koçoğlu, s.36.
[128] Karagülmez, Ali: Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, 5. Baskı, Seçkin Yayıncılık, Ankara 2014, s.69.
[129] İnanıcı, s.518; Doğan, s.18.
[130] Aydın, s.46.
[131] Kurt, s.58.
[132] Dursun, Hasan: *"Bilgisayar ile İlgili Suçlar",* Yargıtay Dergisi, C.24, S.3, Y.1998, s.337.
[133] Erdoğan, s.89.
[134] Erdoğan, s.90.
[135] Tiedemann, Klaus: *"Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi"*, Çev. Yenisey, Feridun: **İÜHFM**, C. XLI, S. 1-4, Y.1975, s. 324.
[136] Doğan, s.18.
[137] Kurt, s.57.

9. Bu eylemleri işleyen failler, adli makamlara bildirilmediğinden gizlenebilmektedir.[138] Bazen de suçun mağdurlarının topluma deşifre olmamak istemeleri nedeniyle yetkili mercilerin önüne bu suçların gelmediğini görmekteyiz. Bu suçlardan genellikle tesadüfen ya da bir kişinin ihbarı üzerine haberdar olunmaktadır.[139]

F. BİLİŞİM SUÇLARININ İŞLENİŞ YÖNTEMLERİ (MODUS OPERANDİ)

1. Genel Olarak

Bilişim suçları başlangıçta hukuka aykırı menfaat sağlamak amacıyla işlenmekteydi. Bununla doğru orantılı olarak internetin ortaya çıkması ve değişik amaçlarla gerçekleştirilmesiyle birlikte suç oranlarında artış meydana geldiği gibi fiillerin yerine getirilmesinde farklı yöntemler kullanılmaya başlanmıştır.[140]

Bilişim suçları diğer suç türlerinden farklı işleniş biçimlerine sahiptir. Zira klasik suç türlerinde bir suçun fiil unsurunu oluşturan eylemler, failin fiziksel fiilleri ile ortaya çıkmakta iken bilişim suçlar genellikle internet üzerinden gerçekleştirildiği için bu işi yapmak üzere yıkıcı yazılımlar (vandalware) oluşturulmuştur.[141]

Bu yazılım ya da tekniklere örnek olarak;

- Bilişim korsanlığı (hacking)
- Truva atı (trojan horse)
- Hizmet aksatma saldırısı veya atakları (DoS-DDoS)
- Salam tekniği (salami techniques)
- Bukalemunlar (chamelon)
- Mantık bombaları (logic bombs)
- Tavşanlar (rabits)
- Virüsler
- Gizli kapılar (trap door)
- Çöpe dalma (scavening)
- Ağ solucanları (network worm)

[138] Doğan, s.18.
[139] Yazıcıoğlu, s.62.
[140] Bozdoğan Akbulut, s.7.
[141] Dülger, s.109-110.

- Gizli dinleme (eavesdropping)
- Veri aldatmacası vs. verilebilir

2. Bilişim Sistemlerine Müdahale Yöntemleri

2.1. Salam Tekniği (Salami Techniques)

Salam tekniği adı verilen bu yöntem genellikle bankacılık alanında gerçekleştirilen bir usuldür.[142] Özellikle bankalardaki bilişim sistemlerinde kullanılır. Bu sayede haksız çıkar sağlama suçlarında kullanılan bir yöntemdir.[143]

Bu yöntemle, kişilerin hesaplarındaki rakamların küsuratları, son rakamı, son iki rakamındaki kuruşlar fail tarafından kendisinin belirlediği başka bir hesaba transfer edilerek orada biriktirilmesi sağlanmaktadır. Özellikle bankalarca faizler değiştirildiğinde veyahut müşteriler hesaplarında işlem gerçekleştirdiğinde meydana gelen yeni kuruşlar hesaba dahil edilmediklerinde veya edilse de kişilerce değer ifade etmeyen bu rakamlar nedeniyle çok değersiz görünen küçük meblağlar milyonlarca işlem sonucu çok yüksek meblağlara ulaşabilmektedirler.[144]

Bu teknik için Truva atı ve ona benzer diğer başkaca yazılımlar kullanılmaktadır.[145]

2.2. Gizli Kapılar veya Hile Kapısı (Trap Door)

Bilgisayar programcılarının işletim sistemi veya kullanıcı sistemi oluştururken ileride oluşabilecek durumlara karşı sistemlerin şifrelerinde değişiklik yapmak veyahut yeni şifreler koyabilmek için bu sisteme önceden bıraktıkları giriş olanaklarıdır. Bu sayede değişikliliğe kapalı olan şifreler bakımından yeni duruma göre ayarlama yapılabilmektedir. Genellikle yasal bir amaca hizmet için bırakılmaktadır. Buna karşın kötü niyetli programcı için hukuk dışı tasarruflar bakımından iyi bir olanak sağlayacaktır.[146] Dolayısıyla bu mekanizmaların program veyahut işletim sistemi tamamlandığında yok edilmesi gerekir ki kötü niyetli kişilerce hukuk dışı faaliyetlerde kullanılması önlenmiş olsun.[147]

[142] Doğan, s.25.
[143] Dülger, s.111.
[144] Yazıcıoğlu, s.155.
[145] Değirmenci, s.89.
[146] Yazıcıoğlu, s.156-157.
[147] Değirmenci, s.85.

2.3.Bilişim Korsanlığı (Hacking)

Hacking bir İngilizce kavram olup bilişim korsanlığı olarak ifade edilmektedir. Burada bilişim korsanlığından kasıt kişilerin yetkisiz ve izinsiz olarak bilişim sistemlerindeki verilere ve fonksiyonlara ulaşılmasıdır.[148] Söz konusu fiili gerçekleştirenlere *"hacker"* denilmektedir.

Bunun yanı sıra *"cracker"*ler de bulunmaktadır. Kelime *"crack"* sözcüğünden gelmekte olup crakerler kötü niyetli olarak kendilerine veya üçüncü kişi yararına haksız çıkar sağlamak amacıyla bilişim sistemlerine veya internet sitelerine saldırarak güvenlik duvarını aşmaktadırlar. *"Hacker"* ve *"Cracker"* kavramı günümüzde birbiri içerisine geçmiştir. Böylece tüm faaliyetler için hacker kavramı kullanılmaya başlanmıştır. Genel olarak hacker ve crackerleri ifade etmek için de *"bilişim korsanı"* kavramı kullanılmaktadır.[149]

Hacking olayında üç adım bulunmaktadır. Hacker tarafından öncelikle keşif yapılmaktadır. Bu sayede önemli bilgilere ulaşılmaktadır.[150] Sonrasında ikinci adım olarak tarama yapılmaktadır. Tarama yapılmasındaki amaç ise açık portların, işletim sisteminin, çalışan servislerin paylaşılan kaynakların ve kullanıcı isimlerinin belirlenmesini sağlamaktır.[151] Üçüncü adım ise şifre kırmak, oturum çalmak, Dos saldırıları yapmak, tampon belleği taşırmak, gibi yöntemler ile sisteme sızabilmektir.[152]

2.4.Truva Atı (Trojan Horse)

Truva atı yazılımının çalışma mantığı Truva Savaşı'nda kullanılan Truva atının Truvalılara hediye edilmesinin akabinde Truva atı kaleye girdikten sonra Truva atının içine gizlenmiş düşman askerleri kaleyi ele geçirmesinden esinlenilmiştir. [153]

Bunlar, internet veya e-posta yoluyla bilgisayarınıza gizlice giren ve siz fark etmeden dışarıya veri gönderen programlardır.[154]

---

[148] Kurt, s.73.
[149] Dülger, s.112.
[150] Yılmaz, s.151.
[151] Yılmaz, s.227.
[152] Yılmaz, s.372. Kurt, s.19-20.
[153] Dülger, s. 110.
[154] Sun, Frank: Canavarın İnternetteki Sayısı: 666 (Kutsal Kitap Gözüyle İnternet), (Çev. Özgül Erman) Cep Kitapları, İstanbul 2001, s.38 aktaran Ergün, s.17.

Bilgisayara kurulan Truva atı, bu bilgisayarın tüm açıklarından faydalanarak tüm sisteme hakim olabilmektedir. Kendisini gönderen kişinin tüm komutlarını yerine getirerek bu kişinin bütün sisteme hakim olabilmesini sağlamaktadır.[155]

Truva atlarının zararlı bir yazılım olduğu açıktır. Buna karşın çoğalma özellikleri bulunmamaları ve zararlı bir yazılım olarak görülmemeleri nedeniyle diğer bilişim virüslerinden bu noktada ayrıldığı söylenebilmektedir.[156] Truva atı TCK m. 244/1 gereğince sistemin işleyişini bozma suçunu oluşturacaktır.[157]

2.5.Mantık Bombaları (Logic Bombs)

Mantık bombaları, önceden belirlenen olasılıklara göre zararlı işler yapan programlardır. Bu programlar, oluşturulurken belirlenen hallerin oluşması ile çalışmaya başlamaktadırlar. Öte yandan truva atı yönteminin de bir türüdür.[158]

Mantık bombaları esasında hasar verici sonuçlar için bilgisayar programları içine yerleştirilen kasten seri komutlar olup bunlar bilgisayar sistemini bozmak amacıyla programlanmaktadırlar.[159]

Mantık bombaları, yaratıcının maaş kayıtlarını izleyebilmektedir. Yaratıcının maaşı belli sınırın altına indiğinde yükseltme, silme veyahut biçimlendirme gibi bilişim suçu oluşturacak işlemlerde bulunabilir.[160] Bu yöntemi kullananlar genellikle hırsızlık, istihbarat, şantaj, ızrar veya eğlence amacında olabilmektedir.[161]

"Omega Engineering" isimli Amerikan şirketinde çalışan EDP görevlilerinden birinin işten çıkartılması üzerine, bu işçinin kendisine ait bilgileri silmesi ve diğer tüm çalışanların kimlik bilgilerini de sabote etmesi ve 10 milyon dolarlık zarar verdiği olay mantık bombası eylemine örnek olarak verilebilir.[162]

Yine 2016 yılında bir kişi Siemens firmasına ait bir şubenin bilişim sistemlerine mantık bombası yerleştirerek hesap tablolarında belirli zamanlarda hata verilmesine sebep

[155] Değirmenci, s.79.
[156] Dülger, s.110.
[157] Uçar, Hüdaverdi: 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Çankaya Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, Ankara 2014, s.20.
[158] Kurt, s.73.
[159] Yazıcıoğlu, s.157.
[160] Aydın, s.13.
[161] Kurt, s.73.
[162] Yazıcıoğlu, s.157; Yazıcıoğlu, *"Hukukumuzda TCK'nun 24. Madde Kapsamında Bilişim Sitemine Girme Eylemi",* s.71.

oldu. Bu sorunu düzeltsin diye işe alındı. Ancak tesadüf eseri zarar verici kod bulundu. Bu aşamaya kadar kimse o kişinin yaptığından şüphelenmedi.[163]

Bu fiil TCK m. 244/2 uyarınca verileri bozma suçunu oluşturacaktır.[164]

2.6.Çöpe Dalma/ Artık Toplama (Scavening)

Çöpe dalma tekniği, bir bilgisayar sisteminin veri-işlem neticesinde sonda kalan bulguların toplanması işlemi olarak tanımlanabilir. Bir başka deyişle artık toplama olarak da adlandırılabilmektedir. Örneğin bilgisayar çıktısının etraftan toplanması ya da bilgisayarda işlem görüp silinen bir dosyanın yeniden elde edilmesi şeklinde olabilmektedir.[165]

Bu yöntem ile özellikle askeri, ticari, istihbarı önemli sırlar öğrenilebilir, haksız menfaatler sağlanabilir. Dahası kişilerin dokunulmaz alanına müdahale oluşturabileceği gibi sırların dokunulmazlığını da ihlal edebilmektedir.[166] Bu fiil ile TCK m. 244/2 suçu oluşabilir.[167]

2.7.Bukalemunlar (Chameleon)

Bukalemun güvenilir bir program gibi davranmaktadır. Buna karşın gerçek birtakım hile ve aldatmalar içerir. Truva atı özelliğine yakındır.[168] Zira yasal bir programın tüm hareketlerini taklit edebilmekte, gizli bir şekilde girdiği sistemdeki kullanıcı ad ve şifreler gibi verileri kopyalayarak saklayabilir.[169] . Daha sonra yaratıcısı, kendi hukuka aykırı amaçları için elde ettiği veriler sayesinde programlara istediği gibi girip çıkabilmektedir.[170]

Bukalemunlar, sistemin içine girene kadar sistem için normal çalışan ve zararsız, onun niteliklerini haiz gibi görünmektedir. Buna karşın sistemin içine girdikten sonra zarar verici faaliyetlerine başlayarak esasen zararlı bir yazılım olduğunu göstermektedir. Kendisi çok iyi saklanabildiği için bu ad verilmiştir. Bukalemunlar düzgün bir biçimde

[163] https://www.kaspersky.com.tr, erişim tarihi: 18.05.2023.
[164] Uçar, s.22.
[165] Yazıcıoğlu, s. 159; https://cahitcengizhan.com, erişim tarihi: 18.05.2023.
[166] Kurt, s.62.
[167] Uçar, s.46.
[168] Aydın, s.52-53.
[169] Kurt, s.75.
[170] Dülger, s.117.

programlandığı takdirde meşru yazılımların tüm hareketlerini taklit edebilirler.[171] Bu fiil TCK m. 244/1'deki *"Bilişim sisteminin işleyişini bozma suçu"*na sebebiyet verecektir.[172]

2.8.Ağ Tavşanları (Network Rabbits)

Bilgisayar virüslerinden biri olup ismini aldığı hayvan gibi çok hızlı üremektedirler.[173] Bu yazılımlar, kısa süre içerisinde kolonileşmek suretiyle sistemin bilgi işleme gücünü azaltmakta ve sisteme durmadan gereksiz işler yapması için komutlar vermektedirler. Buradaki asıl amaç, özellikle birden fazla kullanıcılı sistemlerin, işleyişini bozmaktır. Bununla birlikte bir diğer amacı da veri aktarım ağını koparmaktır. Başka deyişle, sistemin kaynaklarını çalışmaz hale getirmektir.[174]

Tavşanlar, kendi kendilerine yetebilmekte olup virüsler gibi asalak olmayan programlardır. [175] Bu özellik virüs ve tavşanları birbirinden ayıran en belirgin özellik olup tavşanların kullanıcı veri kütüklerinin sonuna eklenmemeleri de ayırıcı özellikleri arasındadır.[176]Ağ tavşanları ile TCK m. 244/1 suçu oluşabilecektir.[177]

2.9.Ağ Solucanları (Worm)

Ağ solucanları, kullanıcının müdahalesine ihtiyacı bulunmaksızın kendi kendine çalışabilmekte olup bir kopyasını, veri iletim ağıyla bağlantılı olan başkaca bilişim sistemine kopyalayabilen bir programdır.[178]

1988 yılında 23 yaşında üniversite öğrencisi olan Robert Morris tarafından tarihte ilk solucan (worm) programı yazılmıştır. Morris tarafından 99 satırlık bir deme projesi olarak ortaya salınmış olup solucanların bilgisayardan diğer bir bilgisayara bulaşma özelliği bulunmaktadır.[179]

Ağ solucanları, iletişim ağındaki sistemler arasında dolaşmaktadırlar. Bu dolaşım esnasında da herhangi bir donanım veya yazılıma zarar verme zorunlulukları

---

[171] Dülger, s. 117.
[172] Uçar, s.25.
[173] Değirmenci, s.103.
[174] Kurt, s.75.
[175] Kurt, s.75.
[176] Levin, Richard B., Bilgisayarda Virüs-Antivirüs, (Çev. Ferhat Okan Sezer), Doruk Yayınları, Ankara 1992, s.27 aktaran Kurt, s.75.
[177] Uçar, s.25.
[178] Dülger, s.115.
[179] Yazıcıoğlu, Recep Yılmaz: *"Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi"* 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara 2009, s.71.

bulunmamaktadır.[180] Ağ solucanları, öncelikle iletişim ağları üzerinden bilişim sistemine gelirler. Daha sonra virüs gibi davranarak yazılıma zarar verebileceği gibi sisteme Truva atı da bırakabilmektedir. Yalnızca gezilerini sürdürebilmek için ürerler ve çok hızlı yayılırlar. Girdikleri sistemde verileri toplayabildikleri gibi gizemli mesajlar bırakırlar. Yakalanmamak için de kendilerinden kalan her şeyi silerler.[181]

Gerçekten diğer programlara atlamadan, verileri ve iletişimi bertaraf etmektedirler. Bu doğrultuda esasen temel işlevi iletişimi yok etmek olsa da verileri yok etme özelliği de zaman zaman ön plana çıkmaktadır.[182]

İnternette ve e-postalarda birçok ağ solucanı örneği görmekteyiz. Örneğin internette dolaşırken küçük pencerelerde kullanıcıların karşına ilgi çekici reklamlar çıkar. Bu reklamlara tıklandığında içinde solucan olan dosyalar bilgisayara iner ve tıklandığı andan itibaren solucan etkinleştir. İnternetteki solucanlara örnek olarak;

- *"Tebrikler! 250 SMS kazandınız. Telefonunuza indirmek için tıklayınız.*
- *Tebrikler! Amerika'ya gitme hakkını yakalamak için ücretsiz çekiliş kazandınız.*
- *Tebrikler! Amerika kapınızda.*
- *Visa kartınıza bonus kazandınız.*
- *Sitemize giren 1.000.000. kişisiniz. Bizden sürpriz hediye kazandınız.*
- *Bugün şanslı gününüzdesiniz. Bizden büyük para ödülünü kazandınız.*
- *Tebrikler! Bizden saat kazandınız."*

verilebilir.[183]

Bazı solucanların kendilerini çoğaltmak için e-postaları da tercih edildiği de görülmektedir. Özellikle;

- *"Bin Ladin yakalandı.*
- *Fidel Castro (veya herhangi bir insan) öldü.*
- *İlk defa nükleer terör saldırısı gerçekleşti.*
- *Üçüncü Dünya Savaşı çıktı."*[184]

[180] Sezer, s.27.
[181] Kurt, s.68.
[182] Çankaya, Ayhan: *"Bilişim Suçlarının Dünü, Bugünü ve Türkiye'deki Durumu",* Polis Dergisi, 2002, S:30, s.8.; Kurt, s.76.
[183] Uçar, s.43. https://tr.wikipedia.org, erişim tarihi:05.03.2023.

bu başlıklarla yayıldığı görülmektedir.

2.10. Gizlice Dinleme (Eavesdropping)

Veri iletiminde kullanılan ağlara girerek veya bilişim sistemlerinin yaydığı yüksek dalgaları yakalayarak veri elde etme tekniğidir. Bu yöntem en çok bilgisayar monitörlerinden çıkan elektromanyetik dalgaların yakalanması vasıtası ile ekran görüntüsüne dönüştürülmesi şeklinde olabileceği gibi fiziksel müdahaleler sonucunda ağda kaydolunan bilginin elde edilmesi şeklinde de karşımıza çıkabilmektedir.[185]

Öte yandan bu fiil ile işlenen suç hem başka suçlara aracı olmak için hem de bizzat dinlenme saikiyle işlenebilmektedir. Bu suç, telefon konuşmalarının gizlice dinlenmesinin bilişim sistemindeki karşılığı olmaktadır.[186] Dolayısıyla bu fiil kapsamında TCK m. 133 ile TCK m. 135'te düzenlenen suçlar oluşturulabilecektir.[187]

2.11. Hizmet Aksatma Saldırısı ve Hizmet Aksatma Atakları (DoS-DDoS)

Hizmet aksatma saldırısı olarak bilinen DoS saldırıları, bir bilişim sistemi tarafından diğer bir sisteme sürekli veya düzenli olarak yaptığı saldırılar sonucunda onu işlevsiz hale bir başka deyişle hizmet veremez hale getirmeye yönelik yapılan saldırılardır. Bu saldırı birçok yöntem kullanılarak yapılabilmektedir.[188]

Hizmet aksatma atakları olarak bilinen DDoS (Distributed Denial Of Service) saldırıları ise bir saldırgan tarafından daha önce tasarlanmış olan makine ile bir diğer bilgisayara saldırı yapmak suretiyle o hedeflenen sistemi hizmet veremeyecek hale getirmektedir.[189] Sistemin kaldıramayacağı bir başka deyişle artık hizmet veremez duruma getirilmesini amaçlayan bu saldırılara *"sistem kaynaklarını tüketme"* saldırıları da denilmektedir.[190]

---

[184] Uçar, s.25.
[185] Değirmenci, s.75.
[186] Kurt, s.62.
[187] Uçar, s. 31.
[188] Dülger, s.123.
[189] Dülger, s.123.
[190] Gürler, s.105.

Bu saldırılar daha çok internet üzerinden internet protokolleri kurallarının kötüye kullanılarak gerçekleştirilmektedir. Bu saldırılar Kullanılan yöntemlere göre Ping Of Death, ICMP Flood gibi isimler alabilmektedirler.[191]

Genellikle DoS saldırısı yapan failler, kredi kartı ödeme sistemleri, banka vs. web site veya hizmetlere karşı müdahalede bulunmaktadırlar.[192]

2.12. Veri Aldatmacası (Data Diddling)

Bilişim suçlarının işlenme yöntemleri arasında en basit ve en kolay olması nedeniyle çok tercih edilmektedir. Buna karşın çıkartılması en zor olandır.[193] Veri aldatmacası ile verinin bilgisayara veya bilgisayar hafızasına kayıt esnasında yanlış girilmesi, değiştirilmesi veya bazı verilerin kasten bırakılması gerçekleşmektedir.[194]

Veri aldatmacası yöntemiyle bir şirket veya kişi tarafından vergi veya diğer mali belgeleri doldururken fayda sağlanmak amacıyla gelir veya giderlerin şişirilmesi yahut eksik beyan edilmesi sağlanabilmektedir.[195]

2.13. Süper Darbe (Super Zapping)

Bu yöntemin adı İngilizce'deki *"super zap"* ibaresinden gelmektedir. Bilgisayar sistemleri birtakım işletme hatalarından veya kendilerinden kaynaklı nedenlerle çalışmaz hale gelmekte başka bir deyişle kilitlenmektedir. İşlevini yerine getirebilmek için *"super zap"* programlarına ihtiyaç bulunmaktadır. Bu programlar sayesinde güvenlik tedbirleri aşılarak sistemde meydana gelen sorunlar hızlı bir şekilde düzeltilmektedir.[196] Dolayısıyla gizli kapılar gibi meşru amaçlıdır.[197] Buna karşın program bitip teslim edildiğinde kapatılması önem arz etmektedir. Zira bu yapılmadığında suçlular tarafından suç işlemeye elverişli bir araç haline gelmektedir. [198]

Yine her ne kadar faydalı olsalar da kötüye kullanımı halinde ciddi sıkıntılar oluşturabilmektedirler. Zira güvenlik tedbirleri aşarak sistemde istenilen değişiklikleri

[191] Elbahadır, Hamza: Hacking Interface. Kodlab Yayınları, İstanbul 2016, s.118-121 aktaran Karagöz, Mehmet Can: Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, On İki Levha Yayıncılık, 2020, s.110-111.
[192] https://tr.wikipedia.org, erişim tarihi:05.03.2023.
[193] Yazıcıoğlu, s152.
[194] Kurt, s.62.
[195] https://www.computerhope.com, erişim tarihi:05.03.2023.
[196] Yazıcıoğlu, s.156.
[197] Değirmenci, s.85.
[198] Kurt, s.67.

yapabilmeyi sağlamaktadırlar. Örneğin bir Amerikan bankasında bilgisayar sistemindeki bir hatayı düzletmek için kullanılan super zap programının banka görevlisi tarafından güvenlik tedbirlerini aşarak banka görevlisi, bazı arkadaşlarının banka hesaplarına yüklü para transferleri yapmıştır.[199]

2.14. Eşzamanlı Saldırılar (Asyncronous Attacks)

Bilindiği üzere, bilgisayar sistemleri mevcut programları eş zamanda bir başka deyişle aynı anda kullanamamaktadır. Bilgisayardaki sistemler, bilgisayar kaynaklarını farklı usuller kullanmak suretiyle sırasıyla işlem yapmaktadır. Böyle olunca kullanıcıların taleplerini yerine getirirken yaşanan bekleme sırasında verilerin değiştirilmesi bu yöntem ile olabilmektedir. Bir başka deyişle bu bekleme sırasında yeterli bilgi ve beceriye sahip olan kimselerce çeşitli işlemler vasıtasıyla bu veriler üzerinde değişiklik sağlanabilmektedir.[200] Bu yöntem aracılığıyla TCK m. 244/1-2 fıkralarındaki suçlar oluşabilecektir.[201]

2.15. Bilişim Virüsleri

Birtakım yazarlar tarafından bilgisayar virüsleri[202] olarak da adlandırılan bu virüsler, ilk olarak bir yüksek lisans öğrencisi olan Frederick Cohen tarafından tez danışmanının önerisiyle kendi kendini kopyalayabilen yazılımlar için tezinde kullanılmıştır.[203] Öte yandan doktor olan babası tarafından biyolojik virüslerle benzerliği ifade edilerek onu yönlendirmiştir.[204] Virüsler, kendi kendilerini çoğaltabilmekte olup farklı yöntemlerle diğer sistemlere ulaşarak bu sistemleri de etkileyebilmektedirler.[205]

Virüslerin tespiti zor olup ancak özel programlarla tespit edilebilmektedirler. Bazı virüsler, kullanıcıya var olmayan donanım ve yazılım hataları iletirken, bazı virüsler doğrudan bir yol izlemek suretiyle ekranda zıplayan toplar ile gülümseyen suratlar görüntülenmesine sebebiyet verir. Bilhassa bazı virüsler işlevini yerine getirdikten sonra izlerini silerek arkada hiçbir emare bırakmazlar. Bir kısım virüsler ise sistemi yavaşlatırlar.

---

[199] Yazıcıoğlu, s.156.
[200] Yazıcıoğlu, s.158.
[201] Uçar, s.27.
[202] Yazıcıoğlu, s.161; Kurt, s.69.
[203] Clough, Bryan /Mungo, Paul: Sıfıra Doğru: Veri Suçları ve Bilgisayar Yeraltı Dünyası, Çev. Emel Kurma, İletişim Yayınları, İstanbul 1999, s.100-101.
[204] Sırımcıyan, Alis: *"Tehlikeli Alışveriş Turları",* CHIP Dergisi, S:12, s.158.
[205] Değirmenci, s.88; Akbulut, s.76-77.; Yazıcıoğlu, s.161.

Dolayısıyla bahsedilen ilk virüsler tahrip edici, ikinci kısımdaki virüsler ise sisteme rahatsızlık verici olarak nitelendirilmesi mümkün bulunmaktadır.[206]

2.16. İstem Dışı Alınan Elektronik İletiler (Spam)

Kelime karşılığı olarak Türkçesi esasen "*baharatlı domuz eti ve jambon*"dur. Buna karşın "*sistem dışı ileti"* veya *"yığın ileti"* olarak kullanılmaktadır. Dolayısıyla istem dışı ve rahatsız edici her türlü ileti ve ekleri için spam adı vermekteyiz.[207] Spam eylemi "*spamming",* spam eylemini gerçekleştirene ise "*spammer*" denilmektedir. Spamların içeriğini genellikle ürün-hizmet reklamları, hemen zengin ol-evinden para kazan yöntemler ve illegal içerik-pornografi gibi içerikler oluşturmaktadır.[208]

Spam çoğunlukla bir ürünün reklamını, pazarlamasını yapmak ve pornografik içerikli reklam ve mesajların dünyaya ulaşmasını sağlamak gayesiyle kullanılmaktadır. Bu mesajlar, daha çok bünyesinde fazlaca e-posta adresi bulunduran kuruluşların veri tabanlarını satmaları nedeniyle artmaktadır.[209] *"Sistemi engelleyecek boyuta ulaştığı takdirde TCK m. 244'teki bilişim sisteminin engellenmesi kapsamında değerlendirilebilecektir"*.[210]

IV. ULUSLARARASI HUKUKTA BİLİŞİM SUÇLARI

Bilişim suçları internet ortamının kullanılmasıyla birlikte suçun işlendiği yer bakımından bütün dünyaya yayılabilen tek suç türü olduğu söylenebilmektedir. Bu özelliği nedeniyle de bu suçlarla mücadelede tek bir ülkenin bu hususta kanuni düzenleme yapması yeterli olmayacaktır. Bu noktada bilişim suçları ile uluslararası mücadelede iş birliği yapılması gerekmektedir. Bu iş birliğinin sağlanabilmesi için de en az iki ülke arasında iş birliğini uygun kılacak yazılı anlaşmalar veyahut sözleşmeler hazırlanması gerektiği açıktır.[211]

Bu doğrultuda bilgisayarların anavatanının Amerika olduğundan bilişim suçlarına dair ilk çalışmalar Amerika'da yapılmıştır. Dolayısıyla ilk bilişim uyuşmazlıkları da ABD'de olduğu görülmektedir. Örneğin yazılımların hukuki korunmasına ilişkin uyuşmazlığı 1972 yılında *"Gottschalk v. Benson davası"*nda Amerikan Yüksek

[206] Aydın, s.54; Kurt, s.69.
[207] Kurt, s.72.
[208] Pallı, s.61.
[209] Değirmenci, s.117.
[210] Kurt, s.73; Uçar, s.23.
[211] Akarslan, s.152-151.

Mahkemesi incelemiş iken aynı konuyu İtalyan Mahkemesi on bir yıl sonra *"Atari Inc. & Bertolino c. Sidam davası"* ile, İngiltere 1981 yılında, Fransa 1982 yılında ve Almanya ise 1976 yılında yargı önünde inceleme fırsatı bulabilmiştir. Dolayısıyla Avrupa'da bilişim uyuşmazlıklarının ortaya çıkışı ABD'ye kıyasla yenidir. Bu doğrultuda Amerika'da bilişim uyuşmazlıklarına ilişkin düzenlemeler de Avrupa'ya kıyasla daha eskiye dayanmaktadır. Zira ABD'deki birçok eyalet 70'lerden itibaren bilişim uyuşmazlıklarına ilişkin hukuki düzenleme yoluna gitmişlerdir. Örneğin 1978'den itibaren Arizona, Florida Kuzey Karolina, Rhode Island, California, Virginia Eyaletleri bilişim suçları hakkında özel hukuki düzenlemeler yapmışlardır.[212]

Bilim, teknoloji ve bilişim alanındaki gelişmeler nedeniyle insanları birtakım işlemleri daha kolay yapabilme ve ulaşım sayesinde bir ülkeden başka bir ülkeye hareket etmeleri kolaylaşmıştır. Bu da bazı suçların uluslararası işlenebilir hale gelmesi nedeniyle *"uluslararası toplum"* denilen bir kavramın ortaya çıkmasına sebebiyet vermiştir. Bu doğrultuda bilişim suçları yapısı gereği sınır aşan özelliği nedeniyle uluslararası bir unsur barındırmaktadır. Hal böyle olunca suçla mücadele için uluslararası bir adli iş birliği kaçınılmaz olmuştur.[213]

Bilişim suçları ile mücadele kapsamında Birleşmiş Milletler (BM), Avrupa Birliği (AB) ve O.E.C.D. gibi uluslararası örgütlerin çalışmaları bulunmaktadır.[214]

A. ULUSLARARASI ÖRGÜTLER

1. Avrupa Konseyi Tarafından Yapılan Çalışmalar

Avrupa Konseyi, Avrupa ülkelerinin siyasi, hukuki ve sosyal alanlarda iş birliğini artırmak amacıyla oluşturulmuş bir uluslararası organizasyondur. 1949 yılında kurulmuştur. Bu Konseyin merkezi Fransa'da bulunmaktadır. Avrupa Konseyi'ne 47 devlet üyedir. Avrupa Konseyi insan haklarının korunması, demokrasi, hukukun üstünlüğü, kültürel çeşitlilik, çevrenin korunması ve sürdürülebilir kalkınma için kurulmuş Avrupa Birliğinden farklı bir kuruluştur. Avrupa Konseyi, üye ülkeler arasındaki iş birliğini

[212] Yazıcıoğlu, s.52.
[213] Dülger, s.205. Buna karşın uluslararası ceza hukuku kaynaklarında bilişim suçları, uluslararası bir suç olarak düzenlenmemekte ve uluslararası ceza mahkemelerinin yargılama yetkisine dahil suçlardan değildir. Buna karşın bu durum bilişim suçlarının uluslararası nitelikte olduğu gerçeğini değiştirmemektedir. Zira bilişim suçları ve bilişim sistemlerinin araç olarak kullanıldığı birçok suç tipinde uluslararası düzenlemeler yapılmış ve bu düzenlemeler fiili olarak harekete geçilmiştir. (Dülger, s.205)
[214] Dülger, s.203.

güçlendirmek amacıyla çeşitli çalışmalar yürütmektedir. Bu projeler arasında bilişim suçları da yer almaktadır.[215]

Avrupa Konseyi elektronik bilgi bankalarında çalışan verilerden dolayı 1970'li yıllarda bireyin özel hayatının korumak amacıyla bir dizi çalışma başlatmış, bu yönde iki tavsiye kararı almış ve Almanya, Avusturya, Fransa, Norveç ve Danimarka gibi ülkeler verilerin korunması hususunu mevzuatlarına dahil etmişlerdir. [216]

Kişisel verilerin saklanması ve hukuka aykırı mücadelelere karşı korunması açısından mevcut düzenlemelerin yetersiz hale gelmesi sebebiyle kişisel verilerin korunmasını uluslararası boyutta ele almak için 28 Ocak 1981 tarihinde *"Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin Sözleşme"* hazırlanmış ve aynı tarihte başka ülkelerle birlikte Türkiye tarafından da imzalanmıştır.[217] Öte yandan Avrupa Konseyi, özel hayatın gizliliği ilkesi gereğince yayınladığı tavsiye kararları vasıtasıyla internet ortamında anonim olmanın önemini de belirtmiştir.[218]

Avrupa Konseyinin en geniş kapsamlı çalışması ise aşağıda ayrıntılarına yer verilecek olan 11 Kasım 2010 tarihinde *"Avrupa Konseyi Siber Suç Sözleşmesi (Convention on Cybercrime)"* ve *"Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesine Ek Protokol"*dür ve Türkiye tarafından da imzalanmıştır.[219]

2. OECD Tarafından Yapılan Çalışmalar

Savaş sonrası Avrupa'nın yeniden kalkınması için Marshall Planı kapsamında 14 Aralık 1960 tarihinde Paris Sözleşmesi'nde dayanılarak oluşturulan bir örgüttür. 1947 ila 1960 yıllarında etkinliği bulunmaktadır. *"Avrupa Ekonomik İşbirliği Örgütü (OEEC)"* nin fonksiyonunu tamamladıktan sonra 30 Eylül 1961 yılında *"Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)"* kurulmuştur. Bu örgüt üye ülkelerle sürekli iş birliği halinde olabilmek için üye ülkeler nezdinde temsilcilikler açmaktadır. Buna karşın OECD'nin yalnızca üye

[215] Akarslan, s.151-152.
[216] Değirmenci, s.40.
[217] Dülger, s.207.
[218] Demir, s.481-484.
[219] Akarslan, s.152.; Dülger, s.208.

ülkelerle ilişki içerisinde olmadığı, üye olmayan birçok ülke ile de ilişki içerisinde bulunduğunu ifade etmek de gerekmektedir.[220]

OECD, bilişim ile ilgili uluslararası çalışmaların yapıldığı ilk örgüt olup ülkemiz de bu örgüte üyedir. Bu çalışmalardaki asıl amaç, bilişim suçlarında ceza kanunlarında paralellik ve bir uyum sağlamaktır.[221]

Bu çerçevede OECD, *"Computer-Realted Crime: Analysis of Legal Policy"* ile çalışmalarını somutlaştırmıştır. Bu Rapor, bazı ihlallerin cezai müeyyideye bağlanması gerektiği bununla birlikte söz konusu ihlallerle sınırlı da olmadığı hususunda mutabık kalınmıştır. İlgili raporda belirtilen ihlaller ise *"bilgisayar yoluyla dolandırıcılık, sahtecilik, bilgisayardaki program ve verilerde değişiklik yapılması, bilgisayardaki programlarda telif haklarına aykırı olarak kopyalama yapmak, çoğaltmak ve dağıtmak, bilgisayar ve diğer iletişim sistemlerinin iletişiminin veyahut diğer işlevlerinin engellenmesi"* olarak sayılmıştır.[222]

3. Birleşmiş Milletler Tarafından Yapılan Çalışmalar

Birleşmiş Milletler, 24 Ekim 1945'te kurulmuştur. Dünyadaki barışı, ekonomik kalkınmayı, güvenliği, adaleti ve sosyal eşitliği tüm ülkelere sağlamayı amaçlayan örgüttür.[223]

Birleşmiş Milletler, bilişim suçları ile ilgili çalışmaları 1980'li yılların ortalarından itibaren yapmaya başlamıştır. Milan Eylem Planında tanımlanan birtakım suçlara karşı ulusal eylem raporunda bilgisayar suçları tartışılmıştır.[224]

Bu çalışmada daha önceden ifade edildiği üzere bilişim suçları, sınır aşan bir özelliğe olduğundan bu hususta Birleşmiş Milletler tarafından sınırları aşan organize suçlarla mücadele edebilmek amacıyla tanzim edilen *"The United Nations Convention against Transnational Organized Crime (Birleşmiş Milletler Sınıraşan Organize Suçlarla Mücadele Sözleşmesi"* önemi haizdir. Zira bu sözleşmede teknolojik suçlarla ilgili birtakım düzenlemeler yapılmıştır. Örneğin 27. maddesinde yasa uygulamada iş birliğini hükme

[220] Dış Ekonomik İlişkiler Kurulu, *"İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD)",* https://www.mfa.gov.tr, erişim tarihi: 24.04.2023.
[221] Akarslan, s.155.
[222] Yıldız, Sevil: Suçta Teknik Bir Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, Nobel Yayınevi, Ankara 2007, s.128.; Erdoğan, s.64.
[223] Birleşmiş Milletler, https://tr.wikipedia.org, erişim tarihi:25.04.2023.
[224] Beceni, Yasin: Siber Suçlar, http://www.hukukcu.com, erişim tarihi: 24.04.2022.

bağlamış olup sözleşmeye taraf olan devletlerin teknoloji kullanılarak işlenmiş sınıraşan suçlarda işbirliği yapması düzenlenmiştir. Türkiye de bu sözleşmeyi *"Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesine Ek Kara, Deniz ve Hava Yoluyla Göçmen Kaçakçılığına Karşı Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun"* ile kabul etmiştir.[225]

Öte yandan Birleşmiş Milletler çatısı altında bulunan *"Birleşmiş Milletler Suçun Önlenmesi ve Ceza Adaleti Komisyonu"*, Ekonomik ve Sosyal Konsey'e bağlı olup her yıl yaptığı kongrelerde siber suçlara ilişkin çalışmalar yapmakta ve üye ülkelere tavsiye kararları almaktadır.[226]

Komisyon tarafından *"On İkinci Birleşmiş Milletler Suçu Önleme ve Ceza Adaleti Kongresi"* düzenlenmiştir. Söz konusu kongrede, siber suçları önleme amacı taşıyan bir anlaşma önerisi atılmış ancak *"Avrupa Konseyi Siber Suç Sözleşmesi"* yürürlükte olduğundan yeni bir anlaşmaya gerek bulunmadığı gerekçesiyle söz konusu teklif AB, ABD ve Kanada tarafından reddedilmiştir.[227]

A. ULUSLARARASI DÜZENLEMELER

1. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa'da bilişim suçları hakkında yapılan ilk çalışma, 1976 yılında *"Ekonomik Suçun Kriminolojik Yönü Üzerine Yapılan Avrupa Konseyi Konferansı"* olup bu konferans ile bilişim suçlarının tanıtımı yapılmıştır.[228]

Buna karşın söz konusu suçlarla mücadele edilebilmesi için *"Avrupa Konseyi Suç Sorunları Komitesi"* tarafından bu alanda çalışılmak üzere bir uzmanlık komitesi oluşturulmasına karar verilmiştir. Böyle olunca 1996 yılında *"Siber Suç Uzmanlar Komitesi"* kurulmuştur. Komite kurulduktan sonra suç, internet ve bilgisayar konularını bir arada ele alan ve bu konuda ilk uluslararası düzenleme olan Avrupa Konseyi Siber Suç Sözleşmesi Haziran 2001'de hazırlanmış ve 8 Kasım 2001 tarihinde onaylanarak 42 ülke tarafından imza edilmiştir. Bu sözleşme ile toplumun siber suçlara karşı korunmasını

[225] Akarslan, s.159-160.; Erdoğan, s.64.
[226] Computer Crime Research Center, *"UN reccomendations on fighting cybercrime",* https://www.crime-research.org, erişim tarihi.25.04.2023.
[227] Akarslan, s.161.
[228] Schjolber, Stein/ Hubbard, Amanda M.: *"Harmonizing National Legal Approaches on Cybercrime",* İnternational Telecommunication Union WSIS Thematic Meeting on Cybercrime Geneva 28 June-1 July 2005, s.8 (akt. Erdoğan, s.66.)

sağlanması, müşterek bir ceza hukuku politikası üzerinde birleşmesi ve bu doğrultuda uluslarca gereken mevzuatın kabul edilerek siber suçlara karşı iş birliğinin sağlanması amaçlanmaktadır.[229]

Avrupa Konseyi Siber Suç Sözleşmesi'nde *"İnternet Ortamında Ceza Sorumluluğunun Avrupa Ana İlkeleri"* olarak da isimlendireceğimiz bazı ilkeler bulunmaktadır. Bu ilkeler;

İlke	Açıklama
1	*"Suçlarla ilgili ceza sorumluluğunun sınırlarının başta düşünce ve söz özgürlüğü ile iletişim özgürlüklerin gereklerine uyulması"* [230]
2	*"Bilgisayarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak bir minimum standarda uyulması"*[231]
3	*"Fiilin hukuka aykırı olması"*[232]
4	*"Fiilin kasten işlenmesi"*[233]

Henüz hiçbir ülke tarafından bildirimde, beyanda ve çekincede bulunulmamıştır. Sözleşme, 23 Kasım 2001'de Budapeşte'de imzaya açılmıştır. Türkiye de bu sözleşmeyi 2010 yılında imzalamıştır. *"6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Daire Kanun"* ile birlikte 2014 yılında yürürlüğe girmiştir.[234]

[229] Ergün, s.59.; Erdoğan, s.66-67.
[230] Erdoğan, s.68.
[231] İçel, Kayıhan: İÇEL, Kayıhan: "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 59, S. 1-2, Y. 2001, s.7, https://dergipark.org.tr, erişim tarihi: 04.05.2023.
[232] İçel, s.8.
[233] Erdoğan, s.68.
[234] Dülger, s.212.; Erdem, Merve/ Özocak, Gürkan: Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri, http://ozocak.com, erişim tarihi: 04.05.2021.

2. Avrupa Siber Suç Sözleşmesi'ne Ek Protokol

Avrupa Konseyi özellikle 1990 sonrasında Berlin Duvarının yıkılmasından sonra örgütlü ırkçılık düşüncesi artmıştır. Bu doğrultuda yabancı düşmanlığı eylemleri ortaya çıkmıştır. Bu örgütler, birbirleri arasında bilişim sistemleri ile internet ağını kullanmak suretiyle iletişim kurmaları nedeniyle bu konuda bir düzenleme yapılması ihtiyacı oluşmuştur. Bunun üzerine Konsey, Siber Suç Sözleşmesine ilave olarak *"Bilişim Sistemleri Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşmesine Ek Protokol"* hazırlamıştır. Söz konusu Ek Protokol de 28 Ocak 2003'te imzaya açılmış olup protokolde her çeşit ırkçı söylem ile yabancı düşmanlık ihtiva eden verinin üretilmesi, bu verilerin bilişim sistemleri vasıtasıyla yayılması ve bu ırkçı ve düşmanlık içeren düşüncelerin sanal alemde propagandası yaptırıma bağlanmıştır.[235]

3. Avrupa Konseyi Kişisel Bilgilerin Korunması Sözleşme

Kişisel bilgiler hakkındaki en önemli düzenleme ise Avrupa Konseyinin *"Kişisel Bilgilerin Otomatik İşlenmesine Karşı Bireylerin Korunması Sözleşme"*dir. Daha çok 108 sayılı sözleşme olarak bilinmektedir. Her ne kadar bu belge sonradan yeterli olmasa da yalnızca AB üyesi ülkeler tarafından değil, tüm dünyada kabul görerek ulusal mevzuatlarının hazırlanmasında göz önünde bulundurulmuştur.[236]

V. KARŞILAŞTIRMALI HUKUK

Çalışmamızda önceden de ifade edildiği üzere, bilişim suçlarının uluslararası nitelik taşıması sebebiyle uluslararası alanda kuruluşlar ve devletler birtakım düzenlemeler yapmıştır.[237]

Bilişim suçlarının sınır aşan özelliği sebebiyle birçok ülkede önemli çalışmalar yapılmıştır.[238] Bu noktada mevcut hükümlerinde değişiklik meydana getiren ülkeler ile yeni ve özel düzenleme yapılan ülkeler olarak iki yöntem benimsendiği görülmektedir. Bu çerçevede genellikle ABD, İngiltere, İrlanda gibi Anglosakson Hukuku uygulanan ülkelerde özel düzenleme yapılması söz konusu iken İtalya, Almanya, Danimarka,

[235] Dülger, s.212.; Ergün, s.62-63.
[236] Ergün, s.63; Yıldız, s.190.
[237] Erdoğan, s.54.
[238] Dülger, s.223.

Avusturya, Finlandiya, İsveç, Hollanda, Norveç, Yunanistan, gibi Avrupa devletlerinde mevcut hükümlerde değişiklik yapılarak sorun çözülmeye çalışılmıştır.[239]

A. AMERİKA BİRLEŞİK DEVLETLERİ

Bilgisayarın ABD'de gelişmesi[240] ve internetin de anavatanının ABD olması[241] nedeniyle bilgisayar suçlarına ilişkin ilk düzenlemelerin yine ABD'de olduğu görülmektedir.[242]

ABD bilişim suçları ve soruşturması ile ilgili federal düzeyde ve eyaletler düzeyinde birçok düzenlemeler yapmıştır.[243]

Bunlardan ilki 1984 tarihli *"Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Kanunu"* dur. Bu kanun kamu kurumları ile özel kuruluşlarının bilgisayarlarına karşı korsanlık müdahalesinin önlenmesi amacıyla düzenlenmiştir.[244]

Diğer bir düzenleme ise yürürlük tarihi 08.02.1996 olan İletişim Ahlak Kanunu'dur. Bu kanun sayesinde çocukların internette kendilerine zararlı olacak içeriklere ulaşması engellenmek istenmiş ve bu tür yayınlar yapanlara iki yıl hapis cezası ve 250.000 dolara kadar para cezası öngörülmüştür. [245] Bu yasa ile internet üzerinde müstehcen resim, video klip, yazı gibi gereçlerin yayını, iletimi ve şiddet içeren yayınların sunulması yaptırıma bağlanmıştır. [246]

ABD'de çocuk pornografisi hususunda da 30.09.1996 tarihli *"Çocuk Pornografisinin Önlenmesi Yasası"* bir başka yasal düzenlemedir. [247] Bu yasa, düşünce ve ifade özgürlüğünün sınırsız kısıtlamalara tabi tutulmaması gerektiğini göz önünde bulundurmakla birlikte internet ortamındaki çocuk pornografisine ilişkin yayınların önlenmesine ilişkin düzenlemeler de barındırmaktadır.[248]

---

[239] Yazıcıoğlu, s.170.
[240] Yazıcıoğlu, s.51.
[241] Sınar, s.92.
[242] Yazıcıoğlu, s.52.
[243] Dülger, s.224.
[244] Dülger, s.224.
[245] Dülger, s.224.
[246] Mahmutoğlu, s.41-42.
[247] Mahmutoğlu, s.42.
[248] Sınar, s.95.

Bir başka çocuk pornografisi ile mücadele kapsamında hazırlanan düzenleme ise *"Çocukların Online Olarak Korunması Yasası"*dır. 1998 yılında hazırlanan bu yasa ile aynı zamanda çocuk pornografisi ticaretini de engellemek amaçlanmıştır.[249]

ABD'nin bir diğer düzenlemesi ise 23.07.1997 tarihli *"İnternet Kumarının Yasaklanması Yasası"*dır.[250] Bu düzenleme ile ABD sınırları içerisinde, Las Vegas ve Atlantic City gibi belli sınırların haricinde, internet vasıtasıyla şans ve kumar oyunlarına erişimi tüm bireyler için engellenmek istenmiş ve bu hususta yaptırımlar getirilmiştir.[251]

Bir diğer düzenleme ise kişilerin tek bir sosyal güvenlik numarası ile her türlü kimlik bilgilerine ulaşılabilen ABD'de, 1998 yılında kabul edilen *"Hüviyet Hırsızlığı Yasası"* ile bireylerin hukuka aykırı olarak kimlik bilgilerine ulaşılması ve bu bilgilerin hukuka aykırı amaçlarda kullanılması ve kullandırılması suç olarak nitelendirilmiştir.[252]

B. İNGİLTERE

29 Ağustos 1990 yılında yürürlüğe giren 29 Temmuz 1990 tarihli *"Bilgisayarın Kötüye Kullanılması Yasası"* vasıtasıyla bilişim suçları düzenlenmiştir.[253] Üç tip suç tipi belirlenen bu düzenlemede; ilk suç tipi, kasten bir bilgisayara veya içindeki veri veyahut programa yetkisiz erişilmesi; ikincisi, *"kasten bir başka bir suçun işlenmesini kolaylaştırmak"* için bilişim cihazına yetkisiz olarak girilmesi; üçüncüsü ise kasten bilgisayarın yetkisiz olarak bozulması, verilere erişimin engellenmesi veyahut veri üzerinde değişiklik yapılması olduğu görülmektedir.[254]

Bu kanun haricinde pornografi ve çocuk pornografisi hususuna ilişkin çalışmalar da yapılmıştır. *"Müstehcen Yayınlar Kanunu"* (1964) ile *"Telekomünikasyon Kanunu"*nda (1984) değişiklikler yapılmıştır. Bu değişiklikler ile sanal *"yayınlama"* kavramının içerisine bilişim sistemindeki veriler de dahil edilerek sanaldaki pornografik yayınların kontrol altına alınması sağlanmıştır.[255]

---

[249] Mahmutoğlu, s.42-43.
[250] Sınar, s.96.
[251] Çeken, Hüseyin: *"Amerika Birleşik Devletlerinde Siber Suçlar",* http://www.jura.uni-sb.de, erişim tarihi:05.05.2023
[252] Dülger, s.233.
[253] Dülger, s.233.
[254] Karagülmez, s.116.
[255] Dülger, s.234.; Erdoğan, s.59.

C. ALMANYA

Almanya, internet dünyasındaki suçlar bakımından Kıta Avrupası'nda ilk çalışmaları yapan ülkedir. Çalışmalar internet ortamında işlenen suçların ne olduğu, kimler tarafından işlenebileceği, internet ortamında işlenen suçlar ve bu suçlardan kimlerin sorumlu olacağı hususlarını içermektedir. 13 Haziran 1997 yılında kabul edilen "*Teleservisler Kanunu*" nun 5. paragrafında internetteki yayınlarda süjelerin cezai sorumluluğuna açıklık getirmiştir. Daha sonra da 08.06.2000 tarihli 2000/31 Direktifi göz önüne alınarak 14.12.2001 tarihinde Teleservisler Kanunu'nda sorumluluğu genişletecek ve detaylı esaslar getirilen değişiklikler yapılmıştır.[256]

Yine 15.05.1986 tarihli 2. Ekonomik Suçlarla Mücadele Kanunu kapsamında Alman Ceza Kanunu ve Haksız Rekabete İlişkin Kanun'da siber suçları yaptırım altına almak için çeşitli düzenlemeler yapılmıştır.[257]

D. İTALYA

İtalya'da bilişim suçları ile ilgili düzenlemelerde, yeni bir düzenlemeye gidilmekten çok mevcut hukuki düzenlemelerin bilişim sahasındaki suçları da kapsadığı savunulmuştur. Bu halde bazen yorum ve içtihatlarla, suçta ve cezada kanunilik ilkesine ve kıyas yasağına aykırı bir şekilde uygulamalarla bu hususa yön verilmiştir.[258]

Bu kapsamda İtalya'da bilişim sahasındaki ilk düzenleme 1993 tarihinde 547 sayılı *"Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema dicriminalita informatica"* isimli Kanun ile yapılmıştır.[259]

İtalyan Ceza Kanunu, bilgisayar ve buna ilişkin sistem, veri ve programlarını tamamen veya kısmen tahrip edici, değiştirici, silici veya sistemin işleyişini engelleyici yahut bozucu fiilleri mala zarar verme suçları içinde kabul etmiştir. Yine bilişim sistemlerine kişinin rızası olmaksızın hukuka aykırı olarak girme veyahut bu sistemde kalmaya ilişkin fiiller de İtalyan Ceza Kanunu'nda suç olarak düzenlemiştir.[260]

---

[256] Mahmutoğlu, s.43-44; Erman, Barış: *"Alman Hukukunda İnternetten Kaynaklanan Ceza Sorumluluğu, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası",* İstanbul 2001, C: LIX, S: 1-2, s.206-208.; Erdoğan, s.59.
[257] Yazıcıoğlu, 1997, s.172-173.
[258] Kurt, s.104.
[259] Akıncı/Alıç/Er, s.208; Kurt, s.104.
[260] Erdoğan, s.61.; Ünver, Yener: *"Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul 2001, C: LIX, S: 1-2, s.67-68.

E. FRANSA

Fransa'da internet ortamına ilişkin ayrıca bir ceza hukuku düzenlemesi bulunduğu söylenememektedir. Bu doğrultuda Yeni Fransız Ceza Kanunu'nun öngördüğü suç tiplerinden internet vasıtasıyla işlenen suçların da öngörülerek hazırlandığı ifade edilebilmektedir.[261]

Fransız Ceza Kanunu'nda "*otomatik sisteme bağlı kişisel verilerin ihlali"*, "*kişilik haklarının bilişim sistemi aracılığıyla ihlali*", *"resim veya sözlerinin kişinin rızasına aykırı biçimde montajının yayınlanması"*, "*küçüğün resminin pornografik nitelikte kullanılması"*, *"küçük tarafından görülmeye elverişli şiddet ve pornografik nitelikli mesaj yayımı*", *"otomatik bilişim sistemine tamamen veya kısmen hakız biçimde girme*", *"girilen sisteme kaydedilmiş verileri silme*", "*sistem fonksiyonlarını değiştirme veya verileri değiştirme*", *"bilişim sisteminin işlenmesini önleme veya farklı yönlendirme*", "*sistemdeki verileri hukuka aykırı olarak değiştirme ve silme"* gibi eylemler suç olarak düzenlenmiş olup bu metinlerde *"hangi yolla olursa olsun, hangi araç ile olursa olsun"* kavramları kullanılarak internet de kapsanmıştır.[262]

Söz konusu sistemin ihtiyacı karşılamaması nedeniyle *"01.08.2000 tarih ve 2000-19 sayılı Kanun"* ile iletişim özgürlüğü konusunda 30.09.1986 tarihli Kanun'da değişiklik yapılarak dört maddeden oluşan *"link üzerinde özel haberleşme dışındaki iletişim servisleriyle ilgili hükümler"* şeklinde ilave başlık eklenmiştir.[263]

F. İSVİÇRE

İsviçre bu alanda en son değişiklik gerçekleştiren devletlerdendir. İsviçre Federal Ceza Kanunu'nda değişiklik öngören Kanun ile *"Mal Aleyhine İhlaller"* başlıklı bölümünde bilgisayar suçları bakımından düzenlemeler bulunmaktadır. Bu Kanun ile verilerin aşındırılması, bilişim sistemine izinsiz girilmesi, verilerin tahribi bilgisayarın hileli kullanılması, kredi kartlarının ve bankamatik kartlarına karşı suistimaller yaptırıma bağlanmıştır.[264]

---

[261] Sınar, s.98.
[262] Ünver, s.71.
[263] Kangal, Zeynel T.: *"Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu",* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul 2001, C: LIX, S:1-2, s.228-229.
[264] Yazıcıoğlu, s.174.

G. DANİMARKA

Danimarka'da da bilgisayar suçlarına ilişkin 05.06.1985 tarihli Ceza Kanunu ile *"bilgisayar marifetiyle dolandırıcılık yapılması, bilgisayar, veri ve programları üzerinde gerçekleştirilen işlemler aracılığıyla bilgisayarın fonksiyonları üzerinde değişiklikler yapılması"* fiilleri yaptırıma bağlanmıştır. Yine *"ticari ve kişisel nitelikteki sır aleyhine işlenen fiiller"* de cezalandırılmaktadır.[265]

H. AVUSTURYA

Avusturya Ceza Kanunu ise bilişim sistemindeki verilere zarar verilmesini, bilişim sistemini kötüye kullanılması suretiyle işlenen dolandırıcılığı, ispat araçlarında sahteciliği ile bu araçların kovuşturma organlarına ibrazından kaçınılmasını, bu araçlara zarar verilmesini ve bu araçların gizlenilmesini suç olarak düzenlemiş ve yaptırıma bağlamıştır.[266]

VI. ULUSAL HUKUKTA BİLİŞİM SUÇLARI HAKKINDA DÜZENLEMELER

A. GENEL OLARAK

Dünyadaki teknolojik gelişmelerle birlikte bilgisayarlar, Türkiye'de de olumlu ve olumsuz yönleriyle yaygınlaşmıştır. Bu duruma bilgisayarların hem kişisel hem kurumsal yönde kullanılması yol açmıştır. Bilgisayarların bu denli yaygınlaşması nedeniyle bulunduğumuz çağın adı *"Bilişim Çağı"* olarak adlandırılmıştır.[267] Böyle olunca bir yandan mevzuattaki ihtiyaç bir yandan Türkiye'nin de taraf olduğu uluslararası düzenlemelere uyum sağlamak için hukuken birtakım düzenlemeler yapmak gerekmiştir.

Gerçekten 765 sayılı TCK ile Kanun koyucu tarafından bu hususa ilişkin iki düzenleme yapılmıştır. İlk düzenleme 3756 sayılı Kanun ile TCK'nin ikinci kitabına *"Bilişim Alanında Suçlar"* başlıklı bazı bilişim suçlarını öngören kısım 1991 yılında eklenmesi ile olmuştur.

---

[265] Yazıcıoğlu, s.173.
[266] Ünver, s.72.
[267] Dülger, s.55.

İkinci düzenleme ise 1995 yılında 4110 sayılı Kanun ile Fikir ve Sanat Eserleri Kanunu'nda *"bilgisayar programlarının"* da *"eser"* sayılmasıdır. Dolayısıyla bu Kanun ile bilgisayar programlarına karşı müdahaleler de yaptırıma bağlanmıştır.[268]

Akabinde 01 Haziran 2005 tarihinde 5237 sayılı Türk Ceza Kanunu yürürlüğe girmesinden sonra ise 765 sayılı Kanun'a ilişkin hükümler uygulanmaya başlayınca 765 sayılı TCK'ye ilişkin hükümler yürürlükten kalkmıştır. Bununla birlikte bilişim suçlarının büyük bir çoğunluğu TCK'de düzenlense de özel kanunlarda da bilişim suçlarına yer verilmiştir.

B. 765 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

Türk Hukukunda bilişim suçlarına ilişkin ilk düzenleme, 1989 Türk Ceza Kanunu Ön Tasarısı (TCKÖT) ile olmuştur. 1989 tarihli TCKÖT ile bilişim suçlarına ilişkin düzenleme, *"Özel Hükümler"* başlıklı ikinci kitabın *"Topluma Karşı Suçlar"* başlıklı ikinci kısmın dokuzuncu bölümünde 342–346. maddelerinde 5 madde halinde yer almaktadır.[269] Bu maddelerde hile ile bilgi elde etme ve bunları haksız kullanma, yarar sağlama ve zarar verme, sahtecilik, feri cezalar, bu suçlardan ötürü tüzel kişilerin sorumlu olduğu ve teşebbüs halinde suçun tamamlanmış hali cezalandırılacağı belirtilmiştir.[270]

06.06.1996 tarihinde oluşturulan komisyon tarafından 1997 tarihli TCKÖT'de bilişim suçları için yeni düzenlemeler öngörülmüş olup 347-352. maddelerinde bilişim suçlarına yer verilmiştir. Bu düzenlemede bilişim sistemlerine münhasıran girmek de suç olarak sayılmıştır. Yine bilişim sistemine girme, verileri tahrip etme ve bozma, bilişim sisteminin işleyişini engelleme, bozma ve bilişim sistemlerinden haksız çıkar sağlama, bilişim sistemleri marifetiyle sahtecilik, feri cezalar, tüzel kişilerin sorumluluğu ve bu suçları işlemek üzere teşekkül oluşturma hususları düzenlenmiştir.[271]

1989 tarihli TCKÖT bütünüyle yasalaşmamış olsa da bilişim suçlarına ilişkin bölümü önemli değişikliklere uğramaksızın 06.06.1991 tarihli ve 3756 sayılı Kanun ile Türk Ceza Kanunu'na girmiştir. Bu Kanun, 14.06.1991 Resmî Gazete tarihli ve 20901 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Böylece 765 sayılı Türk Ceza

[268] Yazıcıoğlu, s.205.
[269] Ayrıntılı kanun maddesi için bkz. Kurt, s.295; Erdoğan, s.74-76.
[270] Kanun maddelerinin tam metni için bkz. Kurt, s.117.
[271] 1997 TCKÖT, TBMM Matbaası Basımı, Yayınlanmamış Metin, s.282-283.

Kanunu'na 525/A, B, C ve D maddeleri eklenmiştir.[272] 525/A[273] maddesinde *"bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme"* fiili, ikinci fıkrasında ise *"bilgileri otomatik olarak işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanma, nakletme ve çoğaltma fiilleri"* suç olarak düzenlenmiştir. 525/B maddesinde ise *"bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru tahrip etme, değiştirme veya silme fiili, ikinci fıkrasında ise bilgileri otomatik işleme tutmuş sistemi kullanarak kendisi veya başkası lehine haksız çıkar sağlama fiilleri"* suç olarak tanımlanmıştır. 525/C maddesinde *"hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sistemi kullanma suçu"* düzenlenmiştir. 525/D maddesinde ise 525/A ve B maddelerindeki suçları işleyenler hakkında feri cezalara yer verilmiştir.[274]

1997 tarihli TCKÖT'de bilişim suçları[275], *"Topluma Karşı Suçlar"* başlıklı ikinci kısmın *"Bilişim Alanında Suçlar"* başlıklı 9. bölümünde 347–352. maddeleri arasında toplam 6 maddede düzenlenmektedir. Bu tasarıda ilk kez 1989 tarihli TCKÖT'in ve 765 sayılı Kanunu'nun kullandığı *"bilgileri otomatik olarak işleme tabi tutmuş sistem"* yerine *"bilişim sistemi"* kavramının kullanıldığı görülmektedir. Bu tasarıdaki bir diğer değişiklik ise bilişim sistemlerindeki kişiye özel alanlara karşı fiillerin cezalandırılması amacıyla ayrıca verileri ele geçirme koşulu olmaksızın bilişim sistemine girme fiilinin suç haline getirilmesidir.[276]

2000 TCKÖT'de[277] bilişim suçlarının yeri ve bölüm başlıklarıyla önceki tasarıdaki yer ve bölüm başlıklarıyla aynıdır. Bu tasarının diğerlerinden farkı ilk ve tek bağımsız düzenleme olan *"Banka ve Kredi Kartlarının Kötüye Kullanımı"* başlıklı 349. maddesinin eklenmesidir.

---

[272] Kanun maddelerinin tam metni için bkz. Kurt, s.297

[273] *"Verilerin ele geçirilmesi suçu"*nda *"bilgileri otomatik işleme tabi tutan sistem"* kavramına yer verilmiş olup bu kavramın ne olduğu açıkça ifade edilmemiştir. Buna karşın ilgili düzenlemenin gerekçesinde *"bilgileri otomatik işleme tabi tutan sistem"* kavramının yanında *"(bilgisayar)"* ibaresi eklendiğinden Kanun koyucunun bilgisayarı kastettiği anlaşılmaktadır. (Ekinci, Mustafa/ Esen, Sinan: Anlatımlı ve Gerekçeli Yeni Türk Ceza Kanununda Yer Alan Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Adalet Yayınevi, Ankara 2005, s.347.)

[274] Kanun maddelerinin tam metni için bkz. Kurt, s.121-123.

[275] Kanun maddelerinin tam metni için bkz. Kurt, s.299-300; Erdoğan, s.78-79.

[276] Değirmenci, *"Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi",* s.197-198.

[277] Kanun maddelerinin tam metni için bkz. Kurt, s.301-302, Erdoğan, s.80-81.

Yine 2003 tarihli TCKÖT'[278]de birtakım küçük değişikler yapılmıştır. [279]

C. ÖZEL KANUNLARDA BİLİŞİM SUÇLARI

Bilişim suçları esas olarak TCK'de bulunmakla birlikte bazı özel kanunlarda da bilişim yoluyla işlenmesi dolayısıyla bilişim suçları kapsamında değerlendirilmesi mümkün olan suçlara rastlamak mümkündür.

Bunlardan ilki 5846 sayılı Fikir ve Sanat Eserleri Kanunu'dur. Bu kanunda bilgisayar programları ve verileri, eser olarak nitelendirildiğinden bilgisayar programlarına ve verilerine FSEK kapsamında yapılan müdahaleler bilişim suçu olarak nitelendirilebilmektedir.

İkinci Kanun ise 5070 sayılı Elektronik İmza Kanunu'dur. Elektronik imzaya yönelik esasları düzenleyen EİK'te elektronik imza bir elektronik verisi olup mahiyeti itibarıyla bilişim temellidir. Dolayısıyla elektronik imzaya yönelik EİK kapsamında yapılan müdahaleler de özel kanunlarda düzenlenen bilişim suçları olarak nitelendirilebilmektedir.

Diğer bir kanun ise 6698 sayılı Kişisel Verileri Koruma Kanunu'dur. Anılan Kanun *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak adlandırılan kişisel verilerin işlenmesinde veri işleyenlerin yükümlülükleri ve kişisel verilerin işlenmesindeki esasları düzenlemektedir. Söz konusu kanuna göre verilerin işlenmesi, kişisel verilerin otomatik olan veya belirli bir veri kayıt sisteminde olmak kaydıyla otomatik olmayan yollarla depolanması, aktarılması, kullanımının engellenmesi gibi kişisel veriler üzerindeki yapılan her türlü işlem olarak tanımlanmaktadır. Dolayısıyla bilişim sistemine kaydedilen ve işlenen kişisel verilere yönelik KVKK kapsamında hukuka aykırı bir müdahale, bilişim suçu olarak değerlendirilebileceği kanaatindeyiz.

Çalışmamızın devamında bahsi geçen özel kanunlardaki hükümlere yer verilecektir.

1. Fikir ve Sanat Eserleri Kanunu'nda (FSEK) Düzenlenen Suçlar

*"5846 sayılı Fikir ve Sanat Eserleri Kanunu"*nda *"07.06.1995 tarihli ve 4110 sayılı Kanun"* ile FSEK'in 71, 72 ve 73. maddelerinde değişiklikler yapılmıştır. Bu değişiklik ile

[278] Kanun maddelerinin tam metni için bkz. Kurt, s.303-304); Erdoğan, s.82-83.
[279] Kurt, s.129, 132.

bilgisayar programları ve verileri eser kavramına dahil edilmiştir.[280] Dolayısıyla söz konusu bilgisayar programları ve verilerine karşı FSEK kapsamında yapılan müdahaleler bilişim suçu olarak nitelendirilebilmektedir. Bu halde Kanun'un 71. ve 72. maddeleri bilişim suçu olarak kabul edilebilir. Zira *"Manevi, mali veya bağlantılı haklara tecavüz"* başlığı altındaki 71. maddesinde hak sahibinin bir bilişim yazılımıyla ilgili maddi ve manevi hakları ile bağlantılı haklarına çeşitli fiillerle tecavüz hallerini suç olarak kabul edilmiştir.[281]

"Teknolojik önlemleri etkisiz kılma" başlıklı 72. maddesinde ise korsa yazılımların hukuka aykırı olarak çoğaltılmasını engellemek amacıyla oluşturulan programları işlevsiz kılmaya yönelik fiiller suç kapsamına alınmıştır.[282]

2. Elektronik İmza Kanunu'nda (EİK) Düzenlenen Suçlar

İnternet kullanımının yaygınlaşması ve verilerin internet ortamında paylaşılabilmesinin kolaylaşması nedeniyle e-ticaret ve elektronik sözleşmeler yapılmaktadır. Bu işlerin güvenilirliğini arttırmak ve hukuki bir boyut kazandırmak adına Kanun koyucu tarafından 5070 sayılı Elektronik İmza Kanunu (EİK) ile elektronik imza geçerli bir imzalama sistemi olarak belirlenmiştir.[283]

Kanun'un 3. maddesinde tanımlanan elektronik imza "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan"* bir elektronik veridir. Anılan maddede ayrıca elektronik veri de *"Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları"* şeklinde tanımlanmıştır.[284] Tanımlardan da görüleceği üzere elektronik imza mahiyeti gereği bilişim sistemleri ile bağlantılı olup elektronik imzaya olan güvenin korunması ve doğruluğunun sağlanması açısından söz konusu Kanun'da iki madde halinde bilişim suçuna yer verilmiştir.

[280] Karagülmez, s.162.; Dülger, s.591-592.
[281] Dülger, s.592-593.
[282] Dülger, s.614.
[283] Başlar, Yusuf: "Elektronik İmza Kanunu'nda Düzenlenen Bilişim Suçları", Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, C.4, S.7, Y.2016, s.41.
[284] https://www.mevzuat.gov.tr, erişim tarihi:22.08.2023

Kanun'un *"İmza oluşturma verilerinin izinsiz kullanımı"* başlıklı 16. maddesi *"imza oluşturma verisi veya imza oluşturma aracını elde etmeyi, vermeyi, kopyalamayı, bu araçları yeniden oluşturmayı ve izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturmayı"* suç olarak düzenlemiştir. Kanun'un 17. maddesinde ise *"Elektronik Sertifikalarda Sahtekarlık"* başlığı altında *"Tamamen veya kısmen sahte elektronik sertifika oluşturma veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif etme ve bu elektronik sertifikaları bilerek kullanma"* suç olarak düzenlenmiş ve yaptırıma bağlanmıştır. EİK m. 19'da ise tüzel kişilerle ilgili güvenlik tedbirlerine yer verilmiştir.[285]

3. Kişisel Verilerin Korunması Kanunu'nda (KVKK) Düzenlenen Suçlar

Bilişim teknolojisinin gelişmesiyle birlikte kullanımının da yaygınlaşması nedeniyle kişisel verilerin daha sıkı korunması ön plana çıkmıştır. Zira bilişim teknolojisinin sağladığı depolama, eşleştirme ve işleme gibi fonksiyonlar sayesinde *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"*[286] olarak tanımlanan kişisel verilerin toplanması ve işlenmesi kolaylaşmaktadır.[287] Bu nedenle kişisel verilerin korunması amacıyla kişisel verilerin işlenmesinde veri işleyenlerin yükümlülükleri ve kişisel verilerin işlenmesindeki esasların hüküm altına alındığı 07.04.2016 tarihli Resmi Gazetede *"6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)"* yayınlanarak yürürlüğe girmiştir.[288]

Bu çerçevede anılan Kanun'un *"Suçlar"* başlıklı 17. maddesinde, *"Kişisel Verilere İlişkin Suçlar"*da Türk Ceza Kanunu'nun 135 ile 140. maddeleri arasındaki hükümlere atıf yapılarak TCK'nin ilgili hükümlerinin uygulanacağı belirtilmiştir.

KVKK'ye göre *"kişisel verileri silmeyen veya anonim hale getirmeyen"* kişilere de TCK m. 138 gereğince yaptırım uygulanacağı ifade edilmiştir.[289]

---

[285] Başlar, s.62. Ergün, s.77.
[286] KVKK m.3/1-d hükmünde kişisel veri bu şekilde tanımlanmıştır. https://www.mevzuat.gov.tr, erişim tarihi: 22.08.2023.
[287] Ketizmen, s.189.
[288] https://www.kvkk.gov.tr, erişim tarihi:22.08.2023
[289] Bük, Alaattin: Bilişim Alanında Kişisel Verilerin Korunması, Seçkin Yayıncılık, Ankara 2018, s.59.

D. 5237 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SUÇLARI

5237 sayılı Türk Ceza Kanunu 01.06.2005 tarihinde yürürlüğe girmiş olup bu tarih itibarıyla söz konusu Kanun'a ilişkin hükümler uygulanmaya başlayınca 765 sayılı TCK'ye ilişkin hükümler yürürlükten kalkmıştır.[290]

5237 sayılı TCK'de ise bilişim suçları üçe ayrılmaktadır:

1- Bilişim alanında suçlar.
2- Bilişim yoluyla işlenmesi suçun nitelikli hali olan suçlar.
3- Bilişim yoluyla işlenen diğer suçlar.

1. Bilişim Alanında Suçlar

Bilişim alanındaki suçlar, 5237 sayılı Kanun'un ikinci kitabının *"Topluma Karşı Suçlar"* başlıklı üçüncü kısmının *"Bilişim Alanında Suçlar"* başlıklı dokuzuncu bölümünde yer almaktadır.

Bu Kanun'un ilk yayımlandığı tarihteki halinde ilgili bölümün 243. maddesinde *"Bilişim sistemine girme suçu"*, 244. maddesinde *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu"*, 245. maddesinde *"Banka ve kredi kartlarının kötüye kullanılması suçu"* düzenlenmiştir. 246. maddesinde ise *"Tüzel kişiler hakkında güvenlik tedbiri"* hükmü bulunmaktadır.

İlgili hükümde bugüne kadar değişiklikler olmuştur. Nitekim 243. maddesinde *"6698 sayılı Kanun"*un 30. maddesiyle *"bilişim sistemine hukuka aykırı olarak giren ve orada kalmaya devam eden"* ibaresindeki *"ve", "veya"* olarak değiştirilmiştir. Yine aynı Kanun ile anılan maddeye bilişim sisteminin içinde veyahut sistemler arasındaki verilerin transferlerini, hukuka aykırı olarak izlenmesini yaptırım altına alınan 4. fıkra eklenmiştir.[291]

244. maddesinde herhangi bir değişiklik olmasa da 245. maddesinin ikinci fıkrasındaki değişiklik ve üçüncü fıkranın eklenmesi ile kapsamı genişletilmiş ve 4. fıkra ile cezasızlık sebepleri düzenlenmiştir. 5560 sayılı Kanun'un 11. maddesi ile yapılan

[290] Kurt, s.136.
[291] https://www.lexpera.com.tr, erişim tarihi:07.05.2023

değişiklikle de birinci fıkradaki fiiller hakkında TCK'deki malvarlığına karşı suçlara uygulanan etkin pişmanlık hükümlerinin uygulanacağı belirtilmiştir.[292]

Son olarak 5237 sayılı TCK'ye *"Yasak cihaz veya programlar"* başlıklı 245/A maddesi eklenmiştir. Bu madde ile yasak cihaz ve programlara ilişkin cezalara ilişkin birtakım fiiller yaptırım altına alınmıştır.[293]

Dolayısıyla son hali ile TCK'nin *"Bilişim Alanında Suçlar"* başlıklı onuncu bölümünde 243. maddesinde *"Bilişim sistemine girme suçu"*, 244. maddesinde *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu"*, 245. maddesinde *"Banka ve kredi kartlarının kötüye kullanılması suçu"*, 245/A *"Yasak cihaz veya programlar"* ve 246. maddesinde ise *"Tüzel kişiler hakkında güvenlik tedbiri uygulanması"* düzenlenmiştir.

2. Bilişim Yoluyla İşlenmesi Suçun Nitelikli Hali Olan Suçlar

TCK'de bilişim alanında suçlar dışında *"Bilişim yoluyla işlenmesi suçun nitelikli hali"* olan suçlar da bulunmaktadır. Örneğin bu suçlardan biri TCK'nin 142. maddesinde düzenlenen nitelikli hırsızlık suçudur. Bu hüküm ile fail, bilişim sistemleri kullanılmak suretiyle hırsızlık suçunu işlediği takdirde suçun nitelikli halinden sorumlu tutulacaktır. TCK m. 142/2-e maddesi hükme uyan suçun sübut bulması için hırsızlık suçunun yanında bilişim sistemlerinin de kullanılması gerekmektedir.[294]

Nitekim Yargıtay bir kararında, katılanın internet üzerinden banka hesabına giren sanık, katılana ait 30.000 TL'yi kendi hesabına havale ederek çekmesi olayında kastın katılanın rızası dışında mal varlığında azalmaya neden olma olduğuna, bir başka deyişle verinin temsil ettiği parayı elde etmek olduğuna, bu nedenle TCK m. 142/2-e maddesindeki suçun oluştuğu gözetilmeden TCK'nin 244/4. maddesi gereğince hüküm kurulmasının hukuka aykırı olduğuna hükmetmiştir.[295]

---

[292] https://www.lexpera.com.tr, erişim tarihi:07.05.2023
[293] https://www.lexpera.com.tr, erişim tarihi:07.05.2023
[294] Yeldan, s.125.
[295] Yargıtay 6. Ceza Dairesi'nin 14.06.2022 tarihli ve E:2021/12444, K: 2022/9092 sayılı Kararı. https://www.corpus.com.tr, erişim tarihi: 05.05.2023. Yargıtay 8. Dairesi'nin 03.11.2021 tarihli ve E:2021/754, K:2021/20284 sayılı Kararı da aynı doğrultudadır.

Bir diğer bilişim yoluyla işlenmesi nitelikli hal olan suç ise günümüzde özellikle internet yoluyla yapılan alışverişlerde en çok karşılaşılan TCK m. 158/1-f hükmündeki *"Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçu"* dur. Bu suçun oluşabilmesi için dolandırıcılık suçuyla birlikte bilişim sistemlerinin de kullanılması gerekmektedir.[296] Yargıtay'ın 2020 tarihli bir kararında, sanık internet ortamında bir siteden Samsung Galaxy S3 marka cep telefonu satışını yapmaktadır. Katılan ile ilanda yazılı cep telefonunun 150 TL'ye satışı hususunda anlaşılmıştır. Buna karşın sanık tarafından katılana cep telefonu yerine sigara bırakma cihazı gönderilmiştir. Bu olayda Yargıtay, TCK m. 158/1-f hükmünde belirtilen *"bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçunu işlediği"* dikkate alınmaksızın beraat verilmesini hukuka aykırı bulmuştur.[297] Benzer bir başka Yargıtay kararında, sanığın sahibinden.com isimli sitede verdiği araba ilanını gören katılanın, sitede yazan telefon numarası ile sanığı aradığı ve satış konusunda anlaşıldığı, katılanın sanığa kapora gönderdiği buna mukabil daha sonra sanığa ulaşamadığı olayda, fiilin *"bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu*" nu oluşturup oluşturmayacağının gözetilmesi gerektiği vurgulanmıştır.[298]

TCK'nin *"Kumar oynanması için yer ve imkan sağlama"* başlıklı 228. maddesinde düzenlenen suç, günümüzde genellikle internet kafelerde kumar oynatılması, yaşça küçüklere internet ortamında kumar oynaması amacıyla yer ve imkan sağlanması, kumar sitelerinde kumar oynayabilmesi için başkaca kişilerin hesaplarına para aktarılması gibi birçok fiille işlenebilmektedir.[299] 01.02.2018 tarihli ve 7078 sayılı Kanun ile anılan hükme üçüncü bir fıkra eklenerek suçun *"Bilişim sistemlerinin kullanılması suretiyle işlenmesi"* nitelikli hal olarak düzenlenmiştir.[300]

3. Bilişim Yoluyla İşlenen Diğer Suçlar

Türk Ceza Kanunu'nda bazı suçları salt bilişim suçu olarak tanımlamak mümkün olmasa da gelinen çağda teknolojinin gelişmesi nedeniyle bu suçların bilişim yoluyla işlenerek suçun işlenişi kolaylaşmaktadır. Örneğin TCK'nin 124. maddesindeki

[296] Yeldan, s.132.
[297] Yargıtay 15. Ceza Dairesi'nin 11.11.2020 tarihli ve E:2017/24850, K:2020/11377 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:05.05.2023.
[298] Yargıtay 15. Ceza Dairesi'nin 05.02.2019 tarihli ve E:2018/9016, K:2019/388 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi: 05.05.2023.
[299] Yeldan, s.261-263.
[300] https://www.mevzuat.gov.tr, erişim tarihi: 08.05.2022.

"Haberleşmenin engellenmesi suçu"[301], 125. maddesindeki *"Hakaret suçu"*[302], 132. maddesinde düzenlenen "*Haberleşmenin gizliliğini ihlal suçu*", 133. maddesinde düzenlenen *"Kişiler arasındaki konuşmaların dinlenmesi veya kayda alınması suçu*"[303], 134. maddesinde düzenlenen "*Özel hayatın gizliliğini ihlal suçu*"[304], 135. maddesinde düzenlenen *"Kişisel verilerin kaydedilmesi suçu"* [305], 136. maddesinde düzenlenen "*Kişisel verileri verme veya ele geçirme suçu*"[306], 138. maddesinde düzenlenen *"Verilerin yok edilmesi suçu"* ve 226. maddesinde düzenlenen *"Müstehcenlik suçu"* gibi bazı suçlarda doğrudan bilişim sisteminden bahsedilmemiştir. Buna karşın hüküm incelendiğinde suça konu fiilin bilişim sistemi aracılığıyla oluşması daha kolaylaştığı görülmektedir.

---

[301] Özellikle elektromanyetik girişim (enterferans) yoluyla sinyaller yayarak birtakım sistem ve/veya cihazların faaliyetini engelleyen haberleşmede kesinti veya kaliteyi azaltma fiiliyle gerçekleşmektedir. (https://www.btk.gov.tr/elektromanyetik-girisim-enterferans, erişim tarihi: 08.05.2023) Yargıtay 4. Ceza Dairesi'nin 21.01.2013 tarihli ve E:2012/12008, K:2013/820 sayılı Kararı örnek olarak verilebilir. (https://www.corpus.com.tr, erişim tarihi: 01.05.2023)

[302] Sosyal medyanın yaygınlaşması ile internet yoluyla hakaret suçunun işlenmesi oldukça kolaylaşmıştır. Özellikle aleniyet nitelikli hali bakımından bilişim ciddi rol oynamaktadır. Nitekim Yargıtay 18. Ceza Dairesi'nin 22.01.2019 tarihi ve E:2016/15711, K:2019/1839 sayılı Kararı'nda sanığın Twitter isimli sosyal medya platformunda katılan milletvekiline hitaben yazdığı *"sayın vekilim@.... ... ve ... gibi insan müsveddelerinin de sizin ile aynı sıfata sahip olmaları ne iğrenç"* şeklindeki sözlerinin hakaret suçunu oluşturduğuna hükmedilmiştir. (https://www.corpus.com.tr, erişim tarihi: 01.05.2023)

[303] Gelinen çağda kiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçunun işlenebilirliği ses kayıt cihazları, telefon uygulamaları sayesinde oldukça kolaylaşmıştır. Nitekim Yargıtay 12. Ceza Dairesi'nin 14.04.2021 tarihli ve E:2020/974, K:2021/3641 sayılı Kararı'na konu olayda sanığın eşine ait telefona casus program ekleyerek telefon görüşmelerini kayıt altına alması nedeniyle TCK m.133'te belirtilen suçu işlediği iddia olunmuşsa da boşanma davasında delil olarak sunma amacı taşıdığı kanaatine varılarak beraat kararı verilmesi gerektiğine ilişkin hüküm kurulmuştur. (https://www.corpus.com.tr, erişim tarihi: 07.05.2023)

[304] Yargıtay 12. Ceza Dairesi'nin 26.05.2021 tarihli ve E:2020/5206, K:2021/4328 sayılı Kararı'na konu olayda bir süredir sevgili olan sanık ile mağdur yaptıkları görüntülü sohbet sırasında sanığın, katılanın rızası dışında çıplak görüntülerini kaydetmiştir. Yargıtay tarafından cinsel ve fiziksel mahremiyete ilişkin görüntülerin kişisel veri olmayacağı, dolayısıyla somut olaydaki fiilin özel hayatın gizliliğini ihlal suçunu oluşturduğu açıkça hükme bağlanmıştır. (https://www.corpus.com.tr, erişim tarihi: 07.05.2023)

[305]Mağdur, nişanlı olan sanıktan ayrılmadan önce sanığı facebook hesabından silmiş olmasına rağmen sanık mağdura ait fotoğrafları kendi facebook hesabında paylaştığı Yargıtay 12. Ceza Dairesi'nin 14.04.2021 tarihli ve E:2020/10149, K:2021/3642 sayılı Kararı'na konu olayda, isnat edilen fiilin *"verileri hukuka aykırı olarak verme veya ele geçirme suçu"*nu oluşturacağı belirtilmiştir. (Yeldan, s.212)

[306] Yargıtay 12. CD'nin 14.02.2018 tarihli ve E:2017/2960, K:2018/1541 sayılı Kararı'nda sanığın internet üzerinden tanıştığı ve arkadaş olduğu katılanın daha kendi sosyal medyasında yayınladığı fotoğrafları tartışmaları nedeniyle katına adına açtığı sahte hesapta katılanın rızası dışında yayınlaması, sanık hakkında *"verileri hukuka aykırı olarak verme veya ele geçirme suçu"*ndan mahkumiyetine karar verilmesi gerektiğine hükmedilmiştir. (https://www.corpus.com.tr, erişim tarihi: 07.05.2023)

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME, BOZMA VE VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

I. GENEL OLARAK

5237 sayılı Türk Ceza Kanunu'nun *"Bilişim Alanında Suçlar"* başlık onuncu bölümünün *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"* başlıklı 244. maddesi şu şekildedir:

"(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 adlî para cezasına hükmolunur"

Yukarıda görüldüğü üzere ilk fıkrada bilişim sistemini engelleme, bozma; ikinci fıkrada bilişim sistemindeki verileri yok etme veya değiştirme; üçüncü fıkrada nitelikli hal ve dördüncü fıkrada ise birinci ve ikinci fıkradaki neticelere sebebiyet verebilecek fiillerin işlenmesiyle failin kendisine veya başkasına haksız çıkar sağlanması halleri düzenlenmiştir.

Buna göre ilk fıkrada *"Bilişim sisteminin işleyişini engelleme veya bozma"* suç olarak nitelendirilmiş iken ikinci fıkrada *"Bilişim sistemindeki verileri bozma, yok etme,*

değiştirme veya erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka yere gönderme" hükme bağlanmıştır.

Üçüncü fıkrada ise suçların nitelikli hali düzenlenmiştir. Söz konusu hükme göre birinci ve ikinci fıkradaki suçların *"Bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi"* hali nitelikli hal olarak belirtilmiştir. Dördüncü fıkrada ise diğer fıkralarda tanımlanan suçlara ilişkin elverişli hareketlerle haksız çıkar sağlamasının başka bir suç oluşturmaması hali yaptırıma bağlanmıştır. Yani bu fıkrayla da ayrı bir suç olarak düzenlenmiştir. Esasen madde incelendiğinde görülecektir ki tek bir maddede aralarında ortaklık bulunan üç farklı suç düzenlenmiştir.[307]

Öte yandan ikinci fıkradaki hususlara dikkat edildiğinde maddenin başlığı ile uyum sağlamamaktadır. Zira madde başlığında yalnızca verileri *"yok etme veya değiştirme"* hususlarına yer verilirken ikinci fıkrada bunların yanı sıra *"erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme"* hususları da bulunmaktadır. Yine ilgili maddenin dördüncü fıkrası incelendiğinde birinci ve ikinci fıkralardaki neticelere sebebiyet verecek fiillerin işlenmesi nedeniyle haksız çıkar sağlanması hali de madde başlığında yer verilmemiştir. Dolayısıyla kanaatimizce TCK'nin 244. maddesinin "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"* başlığı, söz konusu madde hükmünde düzenlenen suçları tanımlamak noktasında yetersiz kalmaktadır.

Bu bilgiler ışığında çalışmamızın devamında yukarıda belirtilen eleştirilerimiz doğrultusunda maddede belirtilen üç suç tipi "*Bilişim sisteminin işleyişini engelleme ve bozma", "Bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme"* ve *"Bilişim sistemleri aracılığıyla haksız çıkar sağlama"* şeklinde ayrı ayrı suçun unsurlarına ayrılarak izah edilecek olup bu bölümde aralarında benzerlik olması nedeniyle yalnızca TCK'nin 244. maddesinin birinci ve ikinci fıkrasındaki suçlar incelenecektir. Dördüncü fıkrasındaki *"Bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu"* ise bir sonraki bölümde değerlendirilecektir.

Bilişim sisteminin işleyişini engelleme, bozma ve verileri yok etme veya değiştirme suçları sırasıyla Türk Ceza Kanunu'nun 244. maddesinin birinci ve ikinci fıkralarında

[307] Hafızoğulları/Özen, s.451.

düzenlenmiştir. Öğretide söz konusu suçları tanımlamak için bilişim sistemine ve bilişim sistemindeki verilere müdahale suçları[308] olarak nitelendirildiği de görülmektedir. Söz konusu suçlar bakımından suçun hukuki konusu ve fail ile mağdurun özellikleri, suçların kusurluluğu kaldıran nedenleri, suçların özel görünüş biçimleri, suçların nitelikli halleri ve yaptırım, soruşturma ve kovuşturma hususları benzer özellik gösterdiğinden tekrardan imtina ederek tek başlık altında izah edilecektir. Buna karşın TCK'nin 244. maddesinin birinci ve ikinci maddesinde belirtilen suçların unsurları ayrı ayrı incelenecektir.

II. SUÇLARIN HUKUKİ KONUSU

TCK'nin gerekçesi incelendiğinde *"Bilişim Alanında Suçlar"* bakımından suçun hukuki konusuna dair hiçbir açıklama bulunmamaktadır.[309]

Öğretide de TCK m. 244'te birden fazla suç tipi bulunmaktadır. Bu nedenle bu suçun hukuki konusu bakımından birden fazla görüş bulunmaktadır.[310]

Hafızoğulları-Özen, bilişim alanındaki suçlar *"Topluma Karşı Suçlar"* başlığı altında düzenlenmişse de toplumsal alandaki olması gereken güveni zedelemesi nedeniyle ayrı bir suç başlığı altında değil de *"Kamunun Güvenine Karşı Suçlar"* başlığı altında bir alt kategoride bulunması gerektiğini ifade etmiştir. Bu halde suçun hukuki konusu, bilişim ortamının güvenliğinin sağlanması ve sağlıklı işlemesine ilişkin ferdi-kamusal yarar olduğunu ifade etmiştir.[311]

Özbek-Doğan-Bacaksız ise TCK m. 244'te iki hukuki değerin korunduğunu, ilkinin bilişim sistemi ve veri güvenliğinin olduğunu belirtmiş olup ikinci fıkrasındaki verilerin bilişim sistemi unsusu içerisindeki veriler olmadığı, bilişim sistemi içerisindeki münhasıran bulunan unsur olduğuna dikkat çekmiştir. İkincisinin ise TCK m.244/4 gereği mülkiyet hakkı olduğunu ifade etmiştir. [312]

[308] Ketizmen, s.112, Koçoğlu, s.81. Kurt "*Bilişim sistemine veya burada yer alan verileri zarar verme suçu",* Güler ise *"Bilişim sisteminin işleyişini engelleme veya bozma ve bilişim sistemindeki verilere zarar verme suçu"* olarak nitelendirmiştir.
[309] Özen/Baştürk, s.112.
[310] Özbek/Doğan/Bacaksız, s.974.
[311] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.452.
[312] Özbek, Veli Özer/ Kanbur, Nihat/ Doğan, Koray/ Bacaksız: Pınar, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara 2022, s.995-996.

Yenidünya-Değirmenci, bu maddede düzenlenen suçların suçun hukuki konusu bakımından karma bir nitelikte olduğunu,[313] anılan maddedeki suçun genel anlamda bir maddi zarar ya da faydaya yol açtığı, bu nedenle de korunan hukuki değerin ekonomik çıkarla ilintili olduğunu belirtmiştir. Bununla birlikte, suça ilişkin fiilin özel hayatın gizliliği, kişi ve haberleşme hürriyetini etkilediğinden bahisle bu çıkarları zedeleme tehlikesi barındırdığından Kanun koyucunun bu tehlikeyi önlemek istediğini belirtmiştir.[314]

Dülger de karma niteliği bulunduğunu ifade etmiş olup bu maddede belirtilen suçlarda ceza yaptırımı ile korunan hukuki değerin bilişim sistemi, bilişim sistemindeki veriler ve diğer unsurların güvenli bir şekilde çalışabilmesi olduğunu ifade etmiştir.[315]

Taşkın ise ceza yaptırımı ile korunan hukuki değerin bilişim sistemi içerisindeki soyut ve somut unsurlar olduğunu zira bu unsurların Kanun koyucu tarafından bu unsurların zarar görmemesinin amaçlandığını ifade etmiştir.[316]

Kurt ise suçun hukuki konusunun bilişim sistemiyle içerisinde verilerin dokunulmazlığı olduğunu ifade etmiştir.[317]

Bu konuda suçun hukuki konusunun karma nitelikli olduğu kanaatindeyiz. Zira Hafızoğulları-Özen'in de ifade ettiği üzere *"Sistemi engelleme, bozma verileri yok etme veya değiştirme"* başlıklı TCK'nin 244. maddesi "Topluma Karşı Suçlar" başlığı altında düzenlenmesi sebebiyle esasen bilişim sisteminin güvenilirliği sağlanarak toplum düzeni ve kamu barışını sağlanılması ile birlikte özel hayatın ve sırların gizliliğinin, mülkiyet hakkının korunmasının ve haberleşme özgürlüğünün sağlanılması da istenilmektedir.

III. SUÇLARIN MADDİ KONUSU

A. GENEL OLARAK

TCK m. 244'te belirtilen suçların maddi konusu hakkında öğretide birçok yazar tarafından görüş bildirilmiştir.

Bir görüşe göre suçların konusunu bilişim sisteminin soyut ve somut unsurları ile sistemdeki yer alan veriler olduğu ifade edilmektedir.[318] Aynı doğrultuda bir başka görüş

[313] Aynı yönde, Dülger, s.335.
[314] Yenidünya/Değirmenci, s.93.
[315] Dülger, s.335.
[316] Taşkın, Şaban Cankat, Bilişim Suçları, Beta Yayıncılık, Bursa 2008, s.42.
[317] Kurt, s. 161-162.

ise AKSSS'nin 4. ve 5. maddelerine dair dayanak raporu ve madde gerekçesine dayanılarak TCK m. 244/1 ve 2. maddelerindeki suçların konusunu bilişim sistemi, sistem içerisindeki veriler ve diğer unsurlar olduğu belirtilmektedir.[319] Özbek-Doğan-Bacaksız da TCK m. 244/1'de hüküm altına alınan suçun konusunun bilişim sistemi olduğunu ifade etmiştir. Yazarlar bu doğrultuda suçun maddi konusunun bilişim sistemindeki gerek yazılım gerekse donanım ögelerini kapsadığını, TCK m. 244/2'de düzenlenen suçun konusunun ise veri olduğunu belirtmişlerdir.[320] TCK m. 244/3 bakımından ise suçun maddi konusu, banka ve kredi kurumuna veyahut kamu kurum veya kuruluşuna ait bilişim sitemindeki veriler olduğu ifade edilmektedir.[321]

Görüldüğü üzere bizim de katıldığımız görüşe göre, öğretideki yazarlar tarafından suçun maddi konusunun TCK m. 244/1'de bilişim sistemi olduğu, TCK m. 244/2'deki suçta ise veri olduğu noktasında mutabık kalınmıştır. Genellikle bilişim sisteminin yazılımı ve donanımıyla bir bütün olduğu da ifade edilerek donanımın da suçun konusunu oluşturduğu ifade edilmekteyse de aksi görüşte olan yazarlarımız da bulunmaktadır.

TCK'nin 244. maddesinin gerekçesinde *"Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka yere bir yere gönderme erişilmez kılma, değiştirme ve yok etme fiilleri suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç haline getirilmiştir, aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."*[322] demek suretiyle bilişim sisteminin donanımı ve yazılımı bir başka deyişle bilişim sistemine ait olan soyut ve somut tüm unsurların suçun konusunu oluşturduğu belirtilmektedir.

Buna karşın öğretideki bazı yazarlar gerekçenin hatalı olduğunu savunmaktadır. Madde metninden yola çıkarak Kanun koyucunun yalnızca bilişim sistemine ait soyut unsurlardan olan veri ve sistemin işleyişinde oluşan zararları cezalandırmak istediği belirtilmiştir. Dolayısıyla içerisinde hiçbir veri bulunmayan ve çalışmayan bilişim sistemine zarar verildiğinde TCK'nin 244. madde hükmü ile cezalandırılmaması gerektiği,

---

[318] Kurt, s.162.
[319] Karagülmez, s.215.; Artuk/Gökcen/Yenidünya, s.4673.
[320] Özbek ve diğ, s.997, Aynı yönde Dülger, s.339.
[321] Çakıcı, Mert: *"Türk Ceza Kanunu m. 243 ve m. 244'te Düzenlenen Bilişim Suçları",* Ceza Hukuku Dergisi, Nisan 2014, C:9, S:24, s.326.
[322] Özbek ve diğ, s.998.

aksi halde TCK'nin 151. maddesi ile uygulamada uyumsuzluk yaşanacağı belirtilmektedir.[323]

TCK'nin 244. maddesi kapsamında suçun konusunu oluşturan verilere, yazılımlar gösterilebilmektedir. Zira yazılımlar, verilerden meydana gelmektedir.[324] sistem yazılımları ve uygulama yazılımları olarak ikiye ayrılan yazılımlar da çalışmamızın *"Yazılımlar"* başlığında detaylı olarak incelendiğinden tekraren yeni bir açıklama yapılmayacaktır.

B. KRİPTO PARALAR

Son yıllarda geleneksel para birimlerine alternatif bir değer olarak popüler hale gelmiş bir kavram olan kripto para blok zincir teknolojisinin bir ürünüdür. Kripto para, dijital bir temsilci olarak işlev görebilecek bir değerdir ve değişim aracı olarak kullanılabilir. Kripto para bir dijital temsilci olarak işlev görür ve işlem yapmak için merkezi bir otoriteye ihtiyaç duymaz. Bunun yerine blok zinciri olarak adlandırılan merkeziyeti bulunmayan küresel bilgisayarlar ağı üzerinden çalışarak kullanıcılar arasında doğrudan transferler gerçekleştirilebilir.[325] Kripto paralara en yaygın kullanım alanı olan bitcoin örnek olarak verilebilir.

Kripto paralar, Irak, Nepal, Tunus, Cezayir, Çin, Bangladeş, Fas, Katar ve Mısır, gibi bazı ülkelerde tamamen yasaklanmıştır.[326] Bununla birlikte El Salvador, Orta Afrika Cumhuriyeti gibi bazı ülkelerde ödeme aracı olarak kabul edilmiştir.[327] Buna karşın Türkiye tarafından ise kripto para, ödeme aracı olarak kabul edilmemiştir.[328]

Ülkemizde Türkiye Cumhuriyet Merkez Bankası'nın (TCMB) hazırladığı *"Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik"* kripto paralara ilişkin ilk düzenlemedir. Anılan Yönetmelik 16.04.2021 tarihli Resmi Gazetede yayımlanmıştır. Bu Yönetmelik ile ülkemiz kripto paraları bir ödeme aracı olarak kabul etmediği gibi mevzuatta *"kripto varlık"* tabirine yer vermiştir.

---

[323] Dülger, s.340.
[324] Dülger, s.339.
[325] İçel, Kayıhan/Ünver, Yener/ Öz, Kerem: Kripto Para ve Ceza Hukuku, *"Hochman, Nathan J.: "Kripto Paranın Vahşi Batı Görünümünü Düzenlemek"* (Çev. Boulanger, Özge Didem), Seçkin Yayıncılık, Ankara 2022, s.64.
[326] *"Kriptoyu yasaklayan ülkeler çoğalıyor"* https://www.sozcu.com.tr, erişim tarihi:13.05.2023
[327] *"Bitcoin, Orta Afrika Cumhuriyeti'nin resmi para birimi oldu",* https://www.bbc.com, erişim tarihi:13.05.2023.
[328] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, https://www.resmigazete.gov.tr , erişim tarihi:13.05.2023.

Yönetmelik'e göre kripto varlık ise *"dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak sanal olarak oluşturulup dijital ağlar üzerinden dağıtımı yapılan, ancak itibari para, kaydi para, elektronik para, ödeme aracı, menkul kıymet veya diğer sermaye piyasası aracı olarak nitelendirilmeyen gayri maddi varlıkları ifade eder."* olarak tanımı yapılmıştır.[329]

Görüldüğü üzere, kripto para ülkemizde bir para birimi olarak kabul edilmemekle birlikte maddi olmayan bir varlık şeklinde tanımlanmıştır.[330] Dolayısıyla tüm bu açıklamalardan sonra kripto varlıkları teknik olarak sistemdeki verileri değişim aracı olarak kullanmayı sağlayan yazılımlar olarak tanımlayabilmekteyiz.[331] Yazılımlar TCK m. 244 kapsamında olduğuna göre kripto varlıkların da TCK m. 244 kapsamında olduğu kanaatindeyiz.

C. SANAL GERÇEKLİK OYUNLARINDAKİ KARAKTERLER VE NESNELER

Bilindiği üzere, son zamanlarda dünyada sanal gerçeklik teknolojisi epey ilgi görmektedir. Sanal gerçeklik, gerçek dünyanın veyahut içindeki ögelerin üç boyutlu biçimdeki sanal temsilcilerini ifade etmektedir.[332] Sanal gerçeklik oyunları da bu teknoloji kullanılarak sanal ortamlarda oynanan oyunlardır.

Sanal gerçeklik oyunlarında avatar ad verilen karakterler ve bu oyunlarda kullanılan dijital ögeler bulunmaktadır. Bu oyunlara girişte yapılan sözleşmelerde, karakterlerin ve oyun malzemelerinin sahibinin oyunun sahibi (yaratıcısı) olduğu söylenmektedir. Buna kaşın mevzuatımızda bu sözleşmenin borçlar hukuku bakımından tartışmalı olması nedeniyle karakterlerin ve malzemelerin oyun yaratıcısına ait olduğunun söylenmesi mümkün değildir. Her ne kadar özel hukuk bakımından tartışmalar bulunmakta ise de bunların ceza hukuku bakımından veri olduğu gerçeğini değiştirmeyecektir. Bu halde söz

[329] Ödemelerde Kripto Varlıkların Kullanılmamasına Dair Yönetmelik, https://www.resmigazete.gov.tr, erişim tarihi:13.05.2023.
[330] Esasen bu durum birçok yönüyle eleştiriye açıktır. Buna karşın çalışmamızın akıcılığını ve konu bütünlüğünü bozacağı için bu tartışmaya girilmeyecektir.
[331] Şahin, Muhammet: *"Kripto Para Yeni Bir Vergi Sığınağı mı? Bilişim Teknolojilerindeki Gelişmeler Temelinde Bir Değerlendirme,"* Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, S. 34, 2019, s. 174.
[332] Şişman, Burak: Bilim Kurgudan Gerçeğe: Artırılmış Gerçeklik, Sanal Gerçeklik ve Karma Gerçeklik, Bilim ve Teknik, Mart 2021, s. 5. https://bilimteknik.tubitak.gov.tr, erişim tarihi:15.05.2023.

konusu karakterlere ait şifrelerin kırılması veya ele geçirilmesi TCK'nin 244. maddesi kapsamında değerlendirilebilecektir.[333]

IV. FAİL VE MAĞDUR

Kanun koyucu tarafından TCK'nin 244. maddesinde düzenlenen suçlar hakkında suçun faili veyahut mağduru bakımından herhangi bir kısıtlamada bulunulmamıştır.[334] Dolayısıyla fail bakımından hükümde *"kişi"* ibaresi kullanıldığından fail, bilişim sistemine müdahalede bulunan herkestir.[335] Buradaki herkesten kasıt gerçek kişidir. Zira tüzel kişiler fail olamayacaktır.

Suçun mağduru bakımından da herhangi bir özellikli durum bulunmamaktadır. Dolayısıyla suçun mağduru da fail tarafından bilişim sistemine karşı müdahalede bulunulan herkestir.[336]

Bu noktada bazı yazarlar, TCK m. 244/1 ve 2'de yaptırım altına alınan fiillerin banka, kredi kurumu, kurum veya kuruluşun bilişim sistemine karşı işlenmesi halinde mağdurun bilişim sisteminin ait olduğu kurum veya kuruluş olduğunu belirmektedirler.[337]

Koca/Üzülmez, bir tüzel kişinin malvarlığında bulunan bilişim sisteminin bozulması veya engellenmesi halinde, tüzel kişiyi suçtan zarar gören olarak kabul etmek gerekeceğini belirtilmiştir. Böyle olunca suçun mağdurunun tüzel kişiyi oluşturan gerçek kişiler olabileceği ifade edilmiş olup devlete ait bir kurumun bilişim sistemine karşı bir saldırı yapılması halinde toplumdaki herkesin suçun mağduru olacağı belirtilmiştir. [338]

Hafızoğulları/Özen ise güvenli bir bilişim ortamının temini kamu düzeninden olduğundan kamu idaresinin suçun mağduru olduğunu ifade etmiştir. Zira söz konusu suçların *"Topluma Karşı Suçlar"* kısmı altında düzenlendiği ifade edilmiştir. Dolayısıyla

---

[333] Dülger, s.340-341.
[334] Dülger, s.338-339.
[335] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.451.
[336] Kurt, s.163. Bununla birlikte aynı yazar mağduru tanımlarken bilişim sistemi *"üzerinde hak sahibi olma"* kavramını kullanmıştır. Tersinden bir ifadeyle söz konusu fiiller nedeniyle bilişim sistemi üzerinde hak sahibi olmayan kişi mağdur da olamayacaktır. Yazara göre, hak sahipliğinden kasıt kişinin bilişim sistemi üzerindeki mülkiyetini haiz olma olabileceği gibi sözleşmeler vasıtasıyla zilyetliğini haiz olma da olabilmektedir. (Kurt, s.163.)
[337] Özbek ve diğ, s.998.
[338] Koca, Mahmut/ Üzülmez, İlhan: Türk Ceza Hukuku Özel Hükümler, Adalet Yayınevi, Ankara 2015, s.810.

suçların *"Kişilere Karşı Suçlar"* kısmında olmaması sebebiyle kişi veya kişilerin sadece suçtan zarar gören olabileceğini belirtilmiştir.[339]

Kanun koyucu bu suçları Kanun'un *"Topluma Karşı Suçlar"* kısmında ele alması nedeniyle kamu idaresinin suçun mağduru olması haklı bir görüş olmakla birlikte gelişen teknoloji nedeniyle kanaatimizce söz konusu suçların mağdurunun karma nitelikte olduğunu söylemek mümkündür. [340] Zira bilişim sisteminin işleyişi engellenen veyahut bozulan ya da bilişim sistemindeki verileri bozulan, yok edilen, değiştirilen, erişilmez kılınan veyahut bu sisteme veri yerleştirilen kişi suçun mağdurudur. Devlete ait bir bilişim sistemi söz konusu ise bu halde toplumu oluşturan herkes iken üçüncü fıkrada ise ilgili banka veya kredi kurumu veyahut kamu kuruluşudur.

V. SUÇLARIN UNSURLARI

A. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SUÇU

1. Fiil

TCK m. 244/1'de fiil *"bir bilişim sisteminin işleyişini engellemek veya bozmak"* olarak tanımlamıştır. Kanunda bilişim sisteminin bir tanımı yapılmamaktadır. TCK m. 243'ün gerekçesinde bilişim sistemi;

"Verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler" şeklinde tanımlanmış olup TCK m.244'ün gerekçesinde de suçun konusunun hem donanım hem de yazılımı içerdiği şu şekilde ifade olunmuştur:

"Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."

Tanımdan da görüleceği üzere, bir bilişim sisteminde hem donanımı (fiziki varlığı) hem de yazılımı ifade ettiği açıktır.

---

[339] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.452.

[340] Nitekim Yargıtay 8. Ceza Dairesi'nin 15.05.2014 tarihli ve E:2013/2959, K:2014/12412 sayılı Kararı'nda *"Sanığın, müştekilere karşı TCK'nın 244/2 maddesi kapsamında kalan eylemlerinin birbirinden bağımsız ayrı suçları oluşturduğu halde tek suç kabul edilerek mahkumiyet hükmü kurulması bozmayı gerektirmiştir"* olarak hüküm kurulmuştur. Görüldüğü üzere söz konusu kararda her bir mağdura karşı fiilin farklı bir suça vücut verdiği, suç sabit ise ayrı ayrı mahkumiyet kararı verilmesi gerektiği vurgulanmıştır.

Buna karşın Hafızoğulları-Özen, bilişim sistemi kavramından yalnızca yazılımın anlaşılması gerektiğini, zira *"bir bilişim sisteminin donanımına zarar vermek, bilişim sistemine zarar vermek olmakla birlikte, suçun hukuki konusu ele alındığında işleyişine zarar verilen bilişim sisteminin donanımı değil, yazılımı"* ifade ettiğini belirtmişlerdir. Dolayısıyla yazarlar donanımın işleyişini engellemenin veya bozmanın TCK'nin 151. madde hükmü yani mala zarar verme suçu kapsamında olduğunu belirtmişlerdir.[341]

Ancak bizim de katıldığımız görüşe göre, bilişim sistemi yazılımı ve donanımıyla bir bütündür. Zira yazılıma verilecek bir zarar kuşkusuz donanımın işlevselliğini de olumsuz etkileyecektir. Örneğin, hard disk bilgisayarın bir donanım unsuru olup teknik bir müdahale olmaksızın bilgisayardan ayrılamamaktadır. BIOS yazılımı olmaksızın da yüksek hızlı ve kapasiteli bilgi okuyup yazan hard disk tek başına çalışamaz. Dolayısıyla yazılım ve donanımın uyumlu ve iş birliği içerisinde olması gerekmektedir. Öte yandan bilgisayarın şifresinin değiştirilmesi ve erişimin engellenmesi de bu suça örnek olarak gösterilebilmektedir[342]

Suçun serbest hareketli mi veya seçimlik hareketli suç mu olduğu hususu öğretide tartışmalıdır. Bir görüşe göre suçun oluşması için anılan fıkradaki iki hareketten yalnızca birinin gerçekleşmesi yeterli olduğundan seçimlik hareketlidir.[343] Nitekim TCK m. 244'ün gerekçesinde de *"Fıkrada seçimlik hareketli bir suç meydana getirilmiştir"* denilmek suretiyle seçimlik hareketli bir suç olduğu ileri sürülmüştür.[344]

Başka bir görüşe göre ise anılan fıkrada düzenlenen suçun neticeleri oluşturan elverişli her hareketle işlenebileceğinden serbest hareketli bir suç olduğu ifade edilmektedir.[345] Bir başka deyişle suçun hareketinin bozma veya engelleme değil, hareket sonucu oluşan netice olduğu belirtilmektedir. Dolayısıyla buradaki suçun serbest hareketli olduğu, neticenin de bozma veya engelleme olduğu ifade edilmektedir.[346] Biz bu görüşe katılmaktayız.

---

[341] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.452-453. Aynı yönde Koca/Üzülmez, s.812.
[342] Özbek ve diğ, s.997.
[343] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453.; Kurt, s.164. Ayrıca bağlı hareket olduğu görüşü için bkz. Özbek ve diğ, s.1001.
[344]https://www.lexpera.com.tr, erişim tarihi:18.08.2023.
[345] Koca/Üzülmez, s.915. Tezcan, Durmuş/ Erdem, Mustafa Ruhan/ Önok, Murat: Teorik ve Pratik Ceza Özel Hukuku, Seçkin Yayıncılık, Ankara 2021, s.1167.; Dülger, s.342.
[346] Erdoğan, s.186.

Kanaatimizce bilişim sisteminin işleyişinin bozulması veya engellenmesi hareket değil, hareketin neticesi olmalıdır. Zira Kanun koyucu, bilişim sisteminin engellenmesi veya bozulmasının hangi hareketlerle olacağını belirtmemiştir. Dolayısıyla bilişim sisteminin işleyişini engelleyecek veya bozacak elverişli bir hareket ile söz konusu suç işlenmiş olacaktır. Böyle olunca madde gerekçesinde her ne kadar seçimlik hareketli bir suç olduğu ifade edilse de bizce serbest hareketli bir suçtur. Zira kanun maddesinde belirtilen birden çok netice seçenekli kılınmıştır. Söz konusu hükümde belirtilen neticelerden biri gerçekleştiğinde suç oluşmuş olacaktır. Nitekim Kanun koyucu tarafından gerekçede de ifade edildiği üzere, TCK m. 244 bilişim sistemlerine yöneltilen ızrar fiillerinin özel bir hali olduğu, yargı kararlarında[347] da *"TCK.nın 244. maddesinin bir ve ikinci fıkralarında klasik mala zarar verme suçunun özel bir şekli düzenlenmiş 3. fıkrada nitelikli haline, 4. fıkrada ise haksız çıkar sağlanmasına yer verilmiştir"* denilmek suretiyle klasik "*Mala zarar verme suçu*"nun özel bir şekli olduğu ifade edilmiştir. Dolayısıyla TCK m. 151'de düzenlenen mala zarar verme suçunun da serbest hareketli bir suç[348] olduğu göz önüne alındığında, TCK m. 151'e göre özel bir norm olan TCK m. 244/1 de serbest hareketli bir suç olması gerektiği kanaatindeyiz.

Anılan suçun tehlike mi zarar suçu mu olduğu hususunda da öğretide tartışma bulunmaktadır. Bir görüşe göre, TCK'nin 244. maddesinin birinci fıkrasında yer alan bu suç tipi, tipte ayrıca bir neticenin meydana gelmesi gerektiğine yönelik ibarenin bulunmadığı düşüncesinden hareketle tehlike suçu olarak nitelendirilmektedir.[349] Tehlike suçu olduğunu savunan bir diğer görüşe göre, engelleme veya bozma nedeniyle bir kimse bir yarar elde edebilir, bu yararın karşıtı da zarar olabilir ancak bu husus ilgili maddenin dördüncü fıkrasında düzenlendiğinden bu fıkrada belirtilen suç, salt hareket suçudur.[350] Bazı yazarlara göre ise sistemin bozulması veya engellenmesi sistemin zarar görmesi anlamına gelmesine neden olacaktır. Zira sistem sahibi tarafından sisteme girilememesi veya istenildiği gibi kullanılamaması söz konusu olacağından zararın da olduğu kabul edilmektedir. [351] Zarar suçu olduğunu savunan bir diğer ise bozma veya engelleme hareketi

[347] Yargıtay 8. Ceza Dairesi'nin 10.05.2022 tarihli ve E:2019/26683, K:2022/6848 sayılı Kararı, Yargıtay 8. Ceza Dairesi'nin 11.06.2020 tarihli ve E:2017/21566, K:2020/13171 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi: 18.08.2023.
[348] Hafızoğulları, Zeki/Özen, Muharrem: Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, US-A Yayıncılık, Ankara 2016, s.369
[349] Özbek ve diğ, s.1001.
[350] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453.
[351] Özbek ve diğ, s.1001.

nedeniyle bir zararın meydana gelmesi gerekir ki bu halde de bozma ve engelleme hareketi oluşturacak iken zarar da neticeyi meydana getirecektir.[352]

Kanaatimizce söz konusu suç bir zarar suçudur. Zira bilişim sistemine karşı yapılan bozma veya bilişim sistemini engellemeye yönelik hareketler neticesinde bilişim sisteminin işleyişinin bozulması veya engellenmesi söz konusu olacaktır. Böyle olunca bilişim sistemine ya geri dönülemez bir hale sebebiyet verilecek ya da bilişim sistemine girişte zorlanma söz konusu olacaktır. Bir başka deyişle bilişim sisteminde bir zarar söz konusu olacaktır.

Nitekim Yargıtay 8. Ceza Dairesi'nin bir kararında *"Maddede yazılı suçun oluşması için, bir bilişim sisteminin işleyişine yönelik engelleyici ve zarar verici fiiller bulunmalıdır. Diğer bir anlatımla bilişim sistemine yapılan müdahalelerle sistemin; veri işleme fonksiyonu yerine getirmesi engellenmeli, fonksiyonunu tamamen veya kısmen kaybetmeli veya verilere zarar verilmelidir."* denilmek suretiyle zarar suçu olarak kabul edildiği belirtilmiştir.[353]

Öğretide bu suçun icra hareketi ile işlendiği hususunda görüş birliği bulunmaktadır.[354] Dülger'in görüşü de bu yönde olsa da teknik ekibin bilişim sistemine karşı yapılan virüs saldırısını bilinçli olarak gerekli olan yazılımları eklemeyerek önlememesi veya bilişim sistemini dışarıdan gelen zararlı müdahalelere karşı savunmasız bırakması hallerinde suçun istisnai olarak ihmal suretiyle işlenebileceğini de ifade etmiştir.[355]

Söz konusu suç, ani suçtur. Buna karşım öğretide bazı yazarlar tarafından suçta süreklilik olabileceği belirtilmektedir. Bu halde mütemadi suçun varlığı söz konusu olacağı, dolayısıyla failin sisteme girerek çıkmaması veya sistemdeyken yakalanması hallerinde suçun temadi edeceğini savunmaktadırlar. Böyle olunca suçun gerçekleştiği an temadinin kesildiği an olacağı ve zamanaşımının bu tarih esas alınarak belirleneceğini belirtmektedirler. [356] Buna karşın biz bu görüşe katılmıyoruz. Zira bir suç hem ani hem de kesintisiz olabilmesi mümkün olmayıp hareketin süreklilik göstermesi suçu kesintisiz suç

[352] Dülger, s.355.
[353] Yargıtay 8. Ceza Dairesi'nin 23.02.2023 tarihli ve E: 2020/11307, K: 2023/772 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi: 18.08.2023
[354] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453. Aynı yönde Dülger, s.352.; Erdoğan, s.185.;
[355] Dülger, s.352.
[356] Kurt, s.153; Taşkın s.32.

yapmayacaktır. Bir başka deyişle, bilişim sisteminin bozulmasının veya engellenmesinin süre gelmesi bu suçun kesintisiz suç olacağı anlamına gelmeyecektir.[357]

Öğretide bu suçun neticeli mi neticesiz mi olduğu hususunda da görüş birliği bulunmamaktadır. Nitekim bazı yazarlar bu suçun neticesiz bir suç olduğunu belirtmektedirler.[358] Buna karşın bazı yazarlar ise maddede belirtilen hareketlerin sonucu olarak bir neticenin meydana geldiğini savunmaktadırlar.[359] Kanaatimizce söz konusu suçta belirtilen hareketler neticesinde bilişim sisteminin bozulması veya bilişim sisteminin engellenmesine sebebiyet verileceğinden neticeli bir suç olarak kabul etmek mümkündür.

1.1.Bilişim Sisteminin İşleyişini Engellemek

"Engellemek" ibaresinin sözlükteki anlamı, bir şeyin gerçekleşmesinin veyahut yapılmasının önlenmesi olarak tanımlanmaktadır. Bununla birlikte Koca-Üzülmez, bilişim sisteminin sağlıklı bir şekilde çalışmamasının da engelleme olabileceğini belirtmiştir.[360]

Erdoğan, Türk Dil Kurumu sözlüğündeki anlamından yola çıkarak bilişim sisteminin varlığına dayanak teşkil eden görevini yapamaz hale getirilmesi olarak tanımlayarak amaçsal bir yorum yapmıştır.[361]

Nitekim Dülger de buna ek olarak engel olmanın DDoS saldırısı gibi yalnızca çalışmasına yönelik değil ayrıca söz konusu bilişim sistemine ilişkin unsurların örneğin ethernet kartın işleyişine zarar vererek sanal ağlara bağlanılmasına engel olunmasını da bu kapsama dahil etmiştir.[362] Bir başka deyişle esasen sistemin bozulması söz konusu değildir. Yalnızca sistem normalde yerine getirebileceği fonksiyonları hiç ya da gereği gibi yerine getirmemektedir. Örneğin hızının yavaşlaması, performansının zayıflaması, dosyanın açılmaması bilişim sisteminin işleyişinin engellenmesine örnek olarak gösterilebilir. Dolayısıyla bozulan bir sistemden bahsedilmesinin mümkün olmadığının altını çizmek gerekmektedir.[363]

Yargıtay 23. Ceza Dairesi sanığın katılana ait facebook hesabının yalnızca şifresini değiştirdiği olayda, TCK m. 244/1 uyarınca *"bilişim sisteminin işleyişini engelleme suçu"*

[357] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453.
[358] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453.; Özbek ve diğ, s.1001.
[359] Koca/Üzülmez, s.915.; Tezcan/Erdem/Önok, s.1167.; Erdoğan, s.187.; Gürler, s.141.
[360] Koca/Üzülmez, s.811-812.
[361] Erdoğan, s.189.
[362] Dülger, s.343.
[363] Kurt, s.164.

oluştuğuna, dolayısıyla TCK m. 244/2 gereğince cezalandırılmasının hukuka aykırı olduğuna karar vermiştir. [364] Söz konusu karara katılmıyoruz. Zira bizce çalışmamızın devamında da belirtilecek olan söz konusu maddenin ikinci fıkrasında düzenlenen veriyi erişilmez kılmak suçunu oluşturmaktadır.

1.2.Bilişim Sisteminin İşleyişini Bozmak

"Bozmak" kavramının anlamı TDK'nin sözlüğünde *"bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek"* olarak tanımlanmıştır. [365]

Bilişim sisteminin faaliyetinin o sırada kalıcı olarak çalışamaz hale gelmesi bilişim sisteminin işleyişinin bozulması olarak ifade edilebilir. Bu halde bilişim sistemin çökertilmesi, virüs gibi zararlı yazılımlarla sistemin işlemez hale gelmesi gibi durumlar meydana gelmektedir. [366]

Ketizmen ise bilişim sisteminin işleyişinin bozulmasını, bilişim sisteminin işletim sistemini ve sistem içerisindeki veri işleme faaliyetini yahut işlem yapabilmesini sağlayan diğer unsurlarına yapılan zararlı müdahaleler sonucunda işlem yapabilme yeteneğinin tamamen yahut kısmen ortadan kaldırılması olarak değerlendirmiştir.[367]

Bazen sistem engellenmesi söz konusu olduğunda bilişim sistemi çalışamaz hale gelmektedir. Ancak bu halde sistemin bozulmasından söz edilmemesi gerekmektedir. Zira bu hal, sistemin çalışamaz halde olması arızi sebeplerden kaynaklanmaktadır.[368]

Bazı yazarlar sistemin fiziki unsurlarına zarar vererek veya yalnızca soyut unsurlarına müdahale ederek sistemin çalışamaz hale getirilmesi yoluyla bilişim sisteminin işleyişinin bozulacağını ifade etmektedir. [369] Örneğin SSD diskin ezilmesi, sabit diskin kırılması halinde de sistemin işleyişinin bozulmasından söz edileceğinden bahsetmişlerdir.[370] Ayrıca sistemin donanımı da dahil olmak üzere tüm fiziki bileşenlerinin

[364] Yargıtay 23. Ceza Dairesi'nin 24.05.2016 tarihli ve E:2015/9146, K:2016/6542 sayılı Kararı, Dülger, s.342.
[365] https://sozluk.gov.tr/, erişim tarihi: 09.05.2023.
[366] Özbek ve diğ, s.999.
[367] Ketizmen, s.135.
[368] Kurt, 164.
[369] Bkz. Akbulut, Berrin: *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme",* Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Konya 2016, C: 24, S:2, s.30.
[370] Dülger, s.344.

bozulmasının yanı sıra içerisindeki programların bozulmasının da bu kapsama dahil edilmesi gerektiği ifade edilmektedir.[371]

Diğer bir görüşe göre ise madde gerekçesinden yola çıkarak bilişim sisteminin maddi unsurlarına yöneltilen fiziki müdahalelerin mala zarar verme suçunu oluşturduğu dolayısıyla sistemin işleyişini sağlayan soyut unsurlara yapılan müdahalenin TCK m. 244/1 hükmüne göre cezalandırılacağı savunulmaktadır.[372] Bir başka deyişle esasen fiziki olarak verilecek bir zararın sistemin işleyişine verilmesi gerekmektedir.[373] Zira bu görüşe göre bozma fiili dışındaki suçun oluşumuna sebebiyet veren müdahaleler açısından TCK m. 244 ile TCK m. 151 arasında fark bulunmaktadır.[374]

Yargıtay 11. Ceza Dairesi'nin 2014 tarihli Kararı'nda Avrupa Siber Suçlar Sözleşmesi'ne uygun olarak bilişim sisteminin işleyişinin engellenmesi veyahut bozulması, herhangi bir yarar sağlama amacı şartına bağlanmaksızın ayrı bir suç olarak düzenlendiği belirtilmiştir. Bu doğrultuda sistemin işleyişinin engellenmesinden kastın bilişim sisteminin verimli bir şekilde çalışmasının önlenmesi, kapasitesinin ve icra yeteneğinin sınırlanması, yavaşlaması veya bütünüyle kilitlenmesi olduğunu belirtmiştir. Buna karşın bilişim sisteminin bozulmasının ise bilişim sistemindeki mekanik bir parçanın veya bir yazılım programının yapması gereken işi yapamayacak duruma gelmesi, sistemin çökmesi, zarara uğraması, işlemez hale gelmesi, fiziki olarak da zarar verilmesi olarak tanımlamıştır. Bilişim sisteminin işleyişinin bozulması, engellemenin en üst noktası olan durma noktası olduğunu belirtmiştir. Madde gerekçesi doğrultusunda bu suçun bilişim sistemlerine yöneltilen ızrar fiillerinin seçimlik hareketli özel bir suç olduğu vurgulanmıştır. Dolayısıyla bilişim sistemlerinin fiziki varlığına, işlemesini sağlayan diğer unsurları bu suçun maddi konusunu oluşturduğu belirtilmiştir.[375]

Görüldüğü üzere, bozmak kavramından bilişim sisteminin kendisinden beklenilen ve görevinde olan işleri yapamayacak hale getirilmesinin anlaşılması gerekmektedir. Bu noktada bilişim sisteminin işleyişinin bozulmasının gerçekleştirilmesine en elverişli müdahaleler virüsler ve kurtçuklardır. Virüs gönderilerek birçok kişinin bilişim sistemleri

[371] Değirmenci, 2002, s.189.
[372] Koca/Üzülmez, s.811-812.
[373] Kurt, s.165.
[374] Ketizmen, s.137.
[375] Yargıtay 11. Ceza Dairesi'nin 24.03.2014 tarihli ve E:2014/7245, K:2014/5492, https://www.lexpera.com.tr, erişim tarihi: 09.05.2023.

veya bilişim sistemine ait verileri tamamen veya kısmen çalışamaz hale getirmek mümkündür.[376]

Nitekim Yargıtay 8. Ceza Dairesi'nin 04.10.2017 tarihli kararına konu olayda sanığın daha önce çalıştığı bir firmada internet vasıtasıyla kullanılan bir programı bildiği tüm şifreleri programı çalışamaz, kullanılamaz hale geldiği tespit edilmiş olup ilk derece mahkemesi tarafından bilişim sisteminin işleyişini engelleme veya bozma suçuna sübut verdiği gerekçesiyle TCK m. 244/1 uyarınca cezalandırılmasına karar verilmiştir. Akabinde yapılan Yargıtay incelemesi neticesinde de mahkeme kararı hukuka uygun bulunarak onama kararı verilmiştir.[377]

Öte yandan gelişen ve değişen teknoloji kapsamında blok zincir kullanılmak suretiyle oluşturulan kripto varlıklara ilişkin madencilik faaliyetinin yapıldığı bilişim sistemlerinin çalışmasının engellenmesi de bu suçu oluşturacaktır. Yine sanal cüzdanın yer aldığı bilişim sistemin engellenmesi fiili de TCK m. 244/1 kapsamında değerlendirilebilecektir.[378]

2. Hukuka Aykırılık

Fiilin hukuka aykırı olması gerekmektedir. Bir başka deyişle, yalnızca ceza hukukunu ihlal eden yani ceza hukuku normu ile çatışan bir fiilin varlığı söz konusu olmalıdır. Bu halde suçun varlığından söz edilebilecektir. Hukuka aykırılığın ortadan kalktığı, fiilin hukuka uygun hallerde ise hukuka uygunluk nedenleri söz konusu olacaktır.[379] Ortada bir hukuka uygunluk nedeni olduğu takdirde ise fiil baştan itibaren suç olmak çıkacak, fail tarafından hukuka uygun hareket edilmiş olunacaktır.[380]

TCK'nin 244. maddesinin birinci fıkrasına göre de bir fiilin hukuka aykırılığından bahsedebilmek için bir bilişim sisteminin engellenmesi veya bozulması söz konusu olmalıdır. Dolayısıyla hukuka aykırı olarak çalışmamızın *"Bilişim Suçlarının İşlenme Şekilleri"* kısmında tahdidi olarak yer verdiğimiz hareketlerden biri ile bilişim sisteminin

[376] Dülger, s.346.
[377] Yargıtay 8. Ceza Dairesi'nin 04.10.2017 tarihli ve E:2016/8701, K:2017/10869 sayılı Kararı https://www.corpus.com.tr/, erişim tarihi:09.05.2023.
[378] Durdu, Erdal: Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku, Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018, s.170.
[379] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s.193.
[380] Eşitli Aygün, Ezgi: Kalkışma Suçları, Yetkin Yayınları, Ankara 2016, s.159.

bozulmasına veya engellenmesine sebebiyet verildiği takdirde hukuka aykırılık unsuru gerçekleşmiş olacaktır.

Söz konusu suçta izin (TCK m. 26/2) hukuka uygunluk hallerinden biridir.[381] İzin verildiği takdirde hukuka aykırılık söz konusu olmadığından suç sübut etmeyecektir.[382] Bu noktada hukuka uygunluk nedeninin varlığının bakımından geçerli rızanın tespiti önem arz etmektedir. Çalışmamızın ilgili kısmında da belirttiğimiz üzere, karma bir hukuki konu benimsememiz sebebiyle hukuki menfaat sahibi ilgili gerçek kişinin rızası, geçerli bir rızadır. Örneğin bilişim sistemlerine karşı yapılacak siber saldırılara karşı önlem almak için oluşturulan virüs programlarının kullanılması, hukuka uygundur.[383]

Bununla birlikte verilecek rızanın daha önceden verilmesi gerekmektedir. Müdahaleden sonra verilecek onay suçun soruşturmasını veya kovuşturmasını engellemeyecektir.[384]

Öte yandan kanun hükmünün icrası da bu suçta bir diğer hukuka uygunluk nedenlerinden biridir. Zira *"5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*un 8. maddesi ile idari yaptırım veya koruma tedbiri olarak internet erişiminin engellenmesi mümkündür.[385]

3. Kusurluluk

Kusurluluk fail ile fiil arasındaki psişik bir bağ olup failin fiilinden sorumlu tutulabilmesi için fiilin iradi ve şuurlu olması gerekmektedir. Kusurlu fiil ise kast ya da taksir ile işlenebilmektedir.[386]

Buna göre, bilişim sisteminin işleyişini engelleme ve bozma suçları ancak kasten işlenebilir. Dolayısıyla fail tarafından ancak bilerek ve istenerek bu suçların işlenmesi gerekmektedir. Bu doğrultuda kast dışında başkaca bir amaç aranmamaktadır.[387] Olası kast ile işlenebilmektedir. Zira söz konusu suç kanaatimizce neticeli suç olduğundan dolayısıyla netice kast belirlediğinden olası kastla işlenmesi mümkündür.

---

[381] Özbek ve diğ, s.1011.
[382] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453.
[383] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453.
[384] Malkoç, İsmail: Açıklamalı İçtihatlı Yeni Ceza Kanunu, Malkoç Kitabevi, Ankara 2007, s.1667.
[385] Özbek ve diğ, s.1010.
[386] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s.244-247.
[387] Kurt, s.75.;

Taksirle işlenemez.[388] Failin suçun kanuni tanımındaki tüm unsurları bilmesi gerekir. Kastın dışında başka bir manevi unsur (saik, amaç gibi) aranmamıştır.[389] Dolayısıyla failin bir bilişim sisteminin işleyişini bilerek ve isteyerek engelleme veya bozma iradesi bulunmalıdır.[390]

4. Kusurluluğu Kaldıran Nedenler

Fiilin iradiliğini ortadan kaldıran ve fiilin bilinmemesinden kaynaklanan nedenler kusurluluğu kaldıran nedenler olarak gösterilmektedir. Bir başka deyişle, bilmeme veyahut hata kusurluluğu ortadan kaldırmaktadır. Buna göre;

1. *"Fiille fail arasındaki psişik/manevi bağı ortadan kaldıran nedenler; kendinde olmama, mücbir sebep, maddi cebir,*
2. *Hata; hukuki hata, fiili hata, isabette hata,*
3. *Manevi cebir ve bu temelde kişiden beklenenin bulunduğu koşullarda kendisinden istenememesi (istenememezlik ilkesi)"* kusurluluğu kaldıran nedenlerdir.[391]

4.1.Fiille Fail Arasındaki Psişik/Manevi Bağı Ortadan Kaldıran Nedenler

Çalışmamızın üst başlıklarında da ifade edildiği üzere faili fiilinden sorumlu tutabilmek için fiilin iradi olması istisnası olmayan bir kuraldır. Fiilin iradi olması ise fiil ile fail arasında psişik bir bağın var olması demektir. Dolayısıyla fiil ile fail arasındaki bu psişik bağ bir başka deyişle manevi bağ ortadan kaldırıldığında fiilin iradiliği ortadan kalkacaktır ve suç oluşmayacaktır. Bu doğrultuda kendinde olmama, mücbir sebep ve maddi cebir fiilin iradiliğini etkileyen bir başka deyişe fiil ile fail arasındaki psişik bağı kaldıran hallerdendir.[392]

Kendinde olmama, bilinci kaybetme şeklinde ortaya çıkmakta iken mücbir sebebin ise genelde başa çıkmanın imkanı olmadığı bir güç nedeniyle kişinin zorlama yoluyla önlenemez bir icra veya ihmal hareketinde bulunması olarak tanımlanması mümkündür. Bu durumda bilişim sisteminin işleyişini bozmak veya engellemek neticelerine sebebiyet verecek fiillerde kendinde olmama veya mücbir sebebin varlığı nedeniyle fail ile fiil

[388] Özbek ve diğ, s.1011.
[389] Koca/Üzülmez, s.815.
[390] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.454.
[391] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s. 289-291.
[392] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s. 291.

arasındaki psişik bağın kesilmesi bir başka deyişle fiilin iradiliğinin ortadan kalkması mümkün değildir. Dolayısıyla bu suçta mücbir sebep ve kendinde olmama hallerinin kusurluluğu kaldıran neden olarak kabul edilmesi olası görünmemektedir.

Bir diğer faille fiil arasındaki manevi bağı kaldıran neden maddi cebirdir. TCK'nin 28. maddesinde *"...kurtulamayacağı cebir ve şiddet ... sonucu suç işleyen kimseye ceza verilmez"* denilmek suretiyle Kanun koyucu maddi cebri düzenlemiştir. Bu halde maddi cebir etkisinde kalan bir kişi suç oluşturan fiili işlediği takdirde suç oluşmayacaktır.[393] Buna karşın kişinin üzerinde maddi cebir uygulayan kişinin etkisinden kurtulma imkanı varsa bu halde ortada maddi cebir veya şiddet olmayacaktır.[394] Bu halde bilişim sisteminin işleyişini engelleme ve bozma suçunda maddi cebir vasıtasıyla suçun işlenmesi ihtimal dahilindedir. Bu halde maddi cebir etkisinde kalan kişi suç işlemiş olmayacak ancak suçu işleyen üzerinde maddi cebir uygulayan kişi fail olarak cezalandırılacaktır.

4.2.Hata

Gerçeğin bilinmemesi veyahut doğru bir şekilde bilinmemesi ya da sahte olarak bilinmesi halinde hatadan söz edilmektedir. Hata kastı ve taksiri ortadan kaldıran kusurluluğu kaldıran nedenlerden olup [395] TCK'nin 30. maddesinde düzenlenen hatayı, kural üzerinde hata, fiil üzerinde hata veya hukuka uygunluk nedenlerinde hata şeklinde üçe ayırmak mümkündür.[396]

Kural üzerinde hata, bir başka deyişle TCK'nin 4. maddesinde düzenlenen hukuki hatadır. Söz konusu hüküm *"ceza kanunlarını bilmemek mazeret sayılmaz"* kuralı koymuştur. Buna göre bilişim sisteminin işleyişini bozma veya engelleme suçunda kural olarak hukuki hata mümkün değildir. Zira failin hukuki hata yapabilmesi için fiilin antisosyal niteliğini bilmemesi ve bu fiilin suç olduğunu bilmemede beşeri imkansızlığı bulunması gerekmektedir. Oysa söz konusu suçta bir bilişim sisteminin işleyişine karşı müdahalede bulunan gerçek kişi failin bu fiilin suç olduğunu bilmediğini iddia edemez.

Fiil üzerinde hata bir başka deyişle fiili hata, fiile ilişkin hata olup suç teşkil eden fiilin unsurlarında hataya düşmek anlamına gelmektedir. Bilişim sisteminin işleyişini

[393] Artuk, Mehmet Emin/Gökcen, Ahmet/ Yenidünya, Ahmet Caner: Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara 2020, s.583-585.
[394] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s. 292.
[395] Soyaslan, Doğan: Ceza Hukuku Genel Hükümler, Yetkin Yayınları, Ankara 2018, s.466.
[396] Eşitli Aygün, s.176.

bozma veya engelleme suçunda fail şayet, kendisini yetkili sanarak bir bilişim sisteminin işleyişini engellemekte veya bozmaktaysa bu halde fiili hata söz konusu olacaktır. [397]

Hukuka uygunluk nedenlerinde hatada ise, fail tarafından hukuk uygunluk nedenlerinde hataya düşülmesi anlamına gelmektedir. Örneğin bilişim sistemi üzerinde menfaati olan kişinin rızası var olduğu düşünülerek fiili gerçekleştirdiği takdirde fail cezalandırılmayacaktır.

4.3.Manevi Cebir ve Bu Temelde Kişiden Beklenenin Bulunduğu Koşullarda Kendisinden İstenememesi (İstenememezlik İlkesi)

TCK'nin 28. maddesi *"muhakkak ve ağır bir korkutma veya tehdit sonucu suç işleyen kimseye ceza verilmez…korkutma ve tehdidi kullanan kişi suçun faili sayılır"* hükmü ile manevi cebir hüküm altına almıştır. Burada iradilik değil, kusurluluk üzerinde bir etki vardır. Zira fail korku veya tehdit ile fiili işlemişse de bir irade bulunmaktadır. [398] Bu halde bilişim sisteminin işleyişini engelleme veya bozma fiili fail tarafından manevi cebir altında işlenmekte ise fail söz konusu fiili nedeniyle cezalandırılmayacaktır.

İstenemezlik ilkesini ise kişiden beklenenin bulunduğu koşullarda kendisinden istenememesi veya başka bir davranışta bulunmasının beklenememesi olarak ifade etmek mümkündür. Bu halde failin içinde bulunduğu koşulda kendisinden daha farklı bir şekilde davranmasını insani olarak beklenmiyorsa bu halde fail kusurlu sayılmayacaktır.[399] Bu halde fail tarafından bilişim sisteminin işleyişini bozma veya engelleme neticesine sebebiyet verecek fiilin istenememezlik ilkesi kapsamında işlenmesi olası değildir. Dolayısıyla bu kapsamda söz konusu fiil bakımından istenememezlik hali, kusurluluğu kaldıran bir neden olarak uygulanamamaktadır.

[397] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s. 297.
[398] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s.297.
[399] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s.301-303.

B. BİR BİLİŞİM SİSTEMİNDEKİ VERİLERİ BOZMA, YOK ETME, DEĞİŞTİRME, ERİŞİLMEZ KILMA, SİSTEME VERİ YERLEŞTİRME VEYA VAR OLAN VERİLERİ BAŞKA BİR YERE GÖNDERME SUÇUNUN UNSURLARI

1. Fiil

TCK Türk Ceza Kanunu'nun 244. maddesinin ikinci fıkrasında suç *"verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi"* olarak tanımlamıştır.

Öğretide bazı yazarlar tarafından söz konusu suçun bir seçimlik hareketli[400] suç olduğu belirtilmektedir. Bu görüşe göre ilgili fıkra hükmünde belirtilen *"bozma"*, *"yok etme"*, *"değiştirme"* ya da *"verileri erişilmez kılma"*, *"sisteme veri yerleştirme"*, *"var olan verileri başka bir yere gönderme"* suçun hareket unsuru olarak kabul edilmektedir. Bu yazarlara göre ilgili hükümdeki hareketlerin birden fazlasının yapılması ile tek suç oluştuğunu, buna karşın hakimin temel cezayı belirlemesinde etkili olduğunu ifade etmişlerdir.[401] Başka bir görüşe göre maddede belirtilen hususların hareketin kendisi değil, neticeleri olduğu belirtilerek suçun serbest hareketli suç olduğu ileri sürülmüştür.[402]

Kanaatimizce daha önce çalışmamızda da belirtildiği edildiği üzere, TCK m. 244, TCK m. 151 hükmünde düzenlenen "*mala zarar verme suçu*" nun özel bir halidir. Böyle olunca söz konusu fıkrada da verilere karşı ızrarın düzenlendiği göz önüne alındığında TCK m. 244/2'de düzenlenen suç, serbest hareketli suçtur.

Bu suçta bilişim sistemine yönelik değil, sistemin içeriğine ilişkin bir müdahale bulunmaktadır.[403] Burada dikkat edilmesi gereken husus bu suçu oluşturacak fiillerin bilişim sisteminin işleyişini engellememesi veya bozmaması gerekliliğidir. Zira bu halde ilgili madde hükmünün birinci fıkrası oluşacaktır.[404]

---

[400] Ketizmen, s.138.; Erdoğan, s.217.; Gerçeker, Hasan: Yorumlu & Uygulamalı Türk Ceza Kanunu (2 Cilt), C:2, Seçkin Yayıncılık, Ankara 2022, s.2211. Aksi görüşte Dülger bu suçun serbest hareketli suç olduğunu ifade etmiştir. Dülger, s.353.
[401] Hafızoğulları/Özen, Topluma Karşı Suçlar, s. 455; Koca/Üzülmez, s.919.
[402] Erdoğan, s.217.
[403] Gül, Ahmet: Doğrudan-Dolaylı Bilişim Suçları, Seçkin Yayıncılık, Ankara 2021, s.135.
[404] Koca/Üzülmez, s.813.

İlgili maddede *"bir bilişim sistemi"* tabiri kullanılmaktadır. Buna göre *"bir"* ibaresinden kastın belli bir bilişim sistemi olduğu ifade edilmektedir. Bununla birlikte suç, icra hareketi ve ihmali hareket ile işlenebilmektedir ve ani suçtur[405].

Anılan suçun tehlike mi zarar suçu mu olduğu hususunda da öğretide tartışma bulunmaktadır. Bir görüşe göre, TCK'nin 244. maddesinin ikinci fıkrasında yer alan bu suç tipi, tipte ayrıca bir neticenin meydana gelmesi gerektiğine yönelik ibarenin bulunmadığı düşüncesinden hareketle tehlike suçu olarak nitelendirilmektedir.[406] Zarar suçu olduğunu savunan yazarlar ise hükümde yer verilen fiiller sonucu neticeler meydana geldiğini belirtmektedirler. Bu görüşe göre, suçta, hükümde belirtilen fiillerin gerçekleşmesi ile bir neticenin meydana gelmesi aranmaktadır. Dolayısıyla bir neticenin arandığını belirtmektedirler.[407] Bazı yazarlar ise *"sisteme veri yerleştirilmesi"* dışındaki fiiller açısından suçun zarar suçu olduğu, *"sisteme veri yerleştirilmesi"* fiili bakımından oluşan suçun ise tehlike suçu olduğunu belirtmektedirler.[408] Kanaatimizce çalışmamızın üst başlıklarında da ifade edildiği ve yargı kararlarında da açıkça ifade edildiği üzere, söz konusu suç bir zarar suçudur ve neticeli bir suçtur.[409]

Nitekim Yargıtay 8. Ceza Dairesi'nin bir kararında[410] *"TCK.nın 244. maddesinin bir ve ikinci fıkralarında klasik mala zarar verme suçunun özel bir şekli düzenlenmiş 3. fıkrada nitelikli haline, 4. fıkrada ise haksız çıkar sağlanmasına yer verilmiştir. Maddede yazılı suçun oluşması için, bir bilişim sisteminin işleyişine yönelik engelleyici ve zarar verici fiiller bulunmalıdır. Diğer bir anlatımla bilişim sistemine yapılan müdahalelerle sistemin; veri işleme fonksiyonu yerine getirmesi engellenmeli, fonksiyonunu tamamen veya kısmen kaybetmeli veya verilere zarar verilmelidir."* ibareleriyle suçun oluşması için verilerin zarar görmesi gerektiği açıkça hüküm altına alınmıştır.

Öğretide bu suçun icra hareketi ile işlendiği hususunda görüş birliği bulunmaktadır.[411] Dülger'in görüşü de bu yönde olsa da teknik ekibin bilişim sistemine karşı yapılan virüs saldırısını bilinçli olarak gerekli olan yazılımları eklemeyerek

[405] Aksi yönde Kurt, s.153.; Taşkın s.32.
[406] Özbek ve diğ, s.1001.
[407] Dülger, s.355.
[408] Yaşar, Osman/ Gökcan, Hasan Tahsin/ Artuç, Mustafa: Yorumlu Uygulamalı Türk Ceza Kanunu, Adalet Yayınevi, Ankara 2014, s.7314.
[409] Yılmaz, s.77.
[410] Yargıtay 8. Ceza Dairesi'nin 10.05.2022 tarihli ve E: 2019/26683, K: 2022/6848 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi: 18.08.2023.
[411] Aynı yönde Dülger, s.352.; Erdoğan, s.185.

önlememesi veya bilişim sistemini dışarıdan gelen zararlı müdahalelere karşı savunmasız bırakması hallerinde suçun istisnai olarak ihmal suretiyle işlenebileceğini de ifade etmiştir.[412]

Yargıtay'ın bu suç kapsamındaki kararlarında suçu oluşturan hareketlerin hiçbir şüpheye yer vermeyecek şekilde somut bir tespitle ortaya konması gerektiği buna karşın ilk derece mahkemelerince yetersiz inceleme ile mahkumiyet hükmü kurulduğundan bahisle bozma kararı verdiği görülmektedir. [413]

Nitekim bu hususa ilişkin olarak Yargıtay 8. Ceza Dairesi'nin bir kararına konu olayda sanık tarafından katılanın mail adresi ile facebook adresi irtibatlı olduğu ve sanık tarafından katılanın rızası ve bilgisi dışında erişilemez kılındığı iddia olunmuş ve ilk derece mahkemesi tarafından mahkumiyet hükmü kurulmuştur. Buna karşın Yargıtay tarafından yapılan incelemede eksik ve yetersiz inceleme ile mahkumiyet hükmü kurulmasında hukuka uyarlık görülmemiştir. Zira sanığın kendisine ait olduğu iddia olunan e-mail adresine dair dosyada hiçbir bilgi ve belge bulunmamaktadır. Yine sanığın başkaca kişilerin interneti kullanabilme ihtimali bulunduğuna ilişkin beyanı neticesinde başkalarının da interneti kullanıp kullanmadığı araştırılmamıştır. Ayrıca sanığın mail adresinin suç tarihinde faal olup olmadığı tespit edilememiştir. Mail adresine ilişkin şifre değiştirildi mi, değiştirildi ise hangi IP numarası ile hangi tarihte erişimin sağlanması suretiyle şifrenin değiştirildiği sorulmamıştır. Dolayısıyla eksik inceleme neticesinde katılanın beyanına itibar edilerek kurulan hükmün eksiklikler giderildikten sonra bilirkişiye gönderilmesi ve tüm delillerin birlikte incelenmesi gerektiği açıkça vurgulanmıştır.[414]

Yine bir başka Yargıtay Kararı'na konu olayda sanıkların suça konu bir ATM'de kart yuvasına bir aparat taktıkları, bu aparat sayesinde müştekinin kartının sıkışmasını sağladıkları, müştekiye yardım bahanesiyle kart şifresini öğrendikleri ve kartı ele geçiremeden yakalandıkları olayda, ilk derece mahkemesince banka ve kredi kartlarının kötüye kullanılması suçundan mahkumiyet hükmü kurulmuştur. Buna karşın Yargıtay, aparat takılı olduğu sürece ATM'nin kullanılamaz halde olduğundan sanığın fiilinin hiçbir kuşkuya ver vermeyecek şekilde ayrıntılı olarak tespitinin yapılması gerektiğini, bu

[412] Dülger, s.352.
[413] Gün, Nagihan: Türk Ceza Hukukunda Bilişim Suçları, Çankaya Üniversitesi Yüksek Lisans Tezi, Ankara 2020, s.230.
[414] Yargıtay 8. Ceza Dairesi'nin 03.02.2015 tarihli ve E:2014/19342, K:2015/2322 sayılı Kararı, https://www.corpus.com.tr/ (erişim tarihi:10.05.2021)

aparatın ATM'nin kısa sürede de olsa çalışmasını engelleyip engellemediği, bilişim sistemine zarar verip vermediği incelenerek bilirkişi raporu alınması gerektiği, bu halde bilişim sisteminin işleyişini engelleme veya bozma, hırsızlık suçu veya mala zarar verme suçu oluşup oluşmadığına karar verilmesi gerektiği belirtilerek Kanun'a aykırı kararın bozulmasına hükmetmiştir.[415]

1.1.Verileri Bozmak, Yok Etmek, Değiştirmek

Ketizmen'e göre verinin bozulması, verinin varlığının sona erdirilmesi, verinin yok edilmesi, kısmen veya tamamen güçlükle elde edilebilecek hale getirilerek tasarruftan çıkartılması anlamına gelmektedir.[416]

Koca/Üzülmez'e göre verinin bozulması ise verinin içeriği yahut yapısına karşı bir müdahalede bulunulmak suretiyle ilgili verinin kısmen veya tamamen kullanılmaz hale getirilmesidir.[417]

Bilişim sistemindeki verilerin bozulması esasen verilerin varlıklarını devam ettirmelerine karşın varlık sebeplerinin, işleyişlerinin kısmen veya tamamen gereği gibi yerine getirilememesi anlamına gelmektedir.[418]

Verinin bozulması ile verinin yok edilmesi arasındaki fark esasen budur. Zira verinin bozulmasında verinin tasarruf alanından çıkartılmaması olduğu gibi ortadan kaldırılmaması da mevzuubahistir. Bir başka deyişle bozma hususunda var olan verinin içeriğine olan zararlı müdahalenin verinin kullanılabilirliğine etki etmesi olarak da ifade edilebilir.[419]

Verilerin bozulması yani verilerin kullanılamaz hale gelmesi bakımından en elverişli yöntemler genellikle bilişim virüsü, kurtçuklar ve mantık bombaları olup Dülger tarafından veriyi içerek diskin fiziken parçalanması ya da veri taşıma aracının fiziki yolla kırılmasının da bu suçu oluşturacağı belirtilmiştir.[420]

---

[415] Yargıtay 11. Ceza Dairesi'nin 13.03.2013 tarihli ve E:2011/2816, K:2013/4065 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:10.05.2021.
[416] Ketizmen, s.139.
[417] Koca/Üzülmez, s.814
[418] Erdoğan, s.220.
[419] Ketizmen, s.139.
[420] Dülger, s.345.

Öte yandan Türk Dil Kurumu sözlüğünde yok etmek; *"varlığına son vermek, ortadan kaldırmak"* olarak tanımı yapılmıştır.[421]

Veriyi yok etmenin ne anlama geldiği öğretide yazarlarca tartışma konusudur.

Kurt, verinin yok edilmesinden maksadın tamamen yok olması, varlığının sona erdirilmesi, tamirinin mümkün olamaması, veriye bir daha ulaşılamaz hale gelmesi anlamına geldiğini belirtmiştir.[422]

Buna karşı Dülger bilişim sistemindeki verilerin tamamen ortadan kaldırılmasının ve varlığının sona erdirilmesinin mümkün olmadığını belirtmiştir. Yazara göre Kanun koyucunun buradaki iradesi bir mantıksal yok oluştur. Zira bilişim sistemi üzerinde *"sil"* komutu verildiğinde bilişim sisteminden o veri silinmiş olmamaktadır. Yalnızca o veri bütününün temsil ettiği veriye *"silindi"* ibaresi eklenmiştir. Verinin üzerine yazma işlemi bir başka deyişle wipe işlemi yapılmadan sistemdeki veriler silinmeyecektir. Yine bilgisayara format atılmasının da verileri silmeyeceğini ifade etmektedir. Dolayısıyla söz konusu hükümde verinin yok olmasından kastın verinin silinmesi olduğunu ifade etmiştir.[423]

Taşkın ise sil komutuyla geri dönüşüm kutusuna gönderilen veriler, tek tık ile geri alınabileceğini dolayısıyla verinin geri dönüşüm kutusuna göndermek suretiyle silinmesinin verileri yok etmek anlamına gelmeyeceğini belirtmiştir. Verilerin yok edilmesinin geri dönüşüm kutusuna gönderilen verinin oradan da silinmesi veyahut bilgisayara format atılması halinde mümkün olacağı belirtmiştir.[424]

Ketizmen ise verinin yok edilmesinden kastın verinin varlığının sona ermesi, ortadan kaldırılması, bir daha elde edilemeyecek veya güçlükle elde edebilecek şekilde ilgilinin tasarrufundan çıkartılması olduğunu verinin silinmesi ile verinin yok edilmesinin aynı anlamda olduğunu ifade etmiştir.[425]

Yazıcıoğlu da Kanunu'nun eski halinde yani TCK m. 525/b hükmünde *"silme"* ifadesi kullanıldığından silmeyi, mevcut kayıtların bulundukları yerde varlıklarının sona erdirilmesi yani yok edilmesi şeklinde tanımlamıştır. Ancak yazar tarafından silmenin

[421] http://www.tdk.gov.tr, erişim tarihi:11.05.2021.
[422] Kurt, s.168.
[423] Dülger, s.346.
[424] Taşkın, s.47.
[425] Ketizmen, s.139.

verinin maddi olarak yok olması anlamına gelmediği yalnızca silinen veriye normal yollarla ulaşılmasının mümkün olmadığı ifade edilmiştir. .[426] Yazara göre silme ve yok etmenin aynı anlama geldiği söylenebilir.

Değirmenci ise verilerin bozulmasının tanınamaz hale gelmesi ve verilerin bulunduğu yerdeki bağın koparılması anlamına geldiğini ve bu sayede veriye ulaşımın engellendiğini ifade etmiştir.[427]

Özbek-Doğan-Bacaksız ise söz konusu verinin bulunduğu yerden yani kayıtlı olduğu bellekten silinmesi suretiyle erişiminin engellenmesinin verilerin bozulması anlamına geldiğini ifade etmektedir. Bu anlamda yazarlar veriye erişiminin engellenmesinin de verinin yok edilmesi anlamı taşımadığını vurgularlar. Burada söz konusu olan erişimin engellenmesi, veriye verilen komutun sonuçsuz kalmasına sebebiyet verecek şekilde silinmesidir. Buna karşın bir verinin kayıtlı olduğu bellekten bir daha dönüşü olmayacak şekilde yok olmasının da mümkün olmadığı belirtilmektedir.[428]

Durdu, kripto paraları sanal cüzdanda tutulan bir kişinin, sanal cüzdanına ait gizli anahtarın değiştirilmesinin de verilerin değiştirilmesi olacağını belirtmiştir.[429]

Veriyi değiştirmek ise verinin asıl halinden kısmen veya tamamen başka bir hale gelmesi söz konusudur. Burada önemli olan verinin kullanılamaz hale gelmeyecek derecede bir değiştirmenin söz konusu olmasıdır. Zira veri kullanılmaz hale geldiğinde verinin bozulması söz konusu olacaktır. Veriyi değiştirmekten kasıt esasen verinin orijinalliğini kaybetmesidir.[430] Örneğin veriyi içinde barındıran programa virüs gibi kötü amaçlı kodların eklenmesi halinde de verinin önceki haliyle verinin değiştirilmesi söz konusu olmaktadır. Bu halde verinin tamamen veya kısmen değiştirilmesinde herhangi bir farklılık bulunmamaktadır.[431]

Verinin değiştirilmesi, ilgili veri grubuna fotoğraf veya not eklenmesi şeklinde olabileceği gibi uygulama yazılımının değiştirilmesi vasıtasıyla da olabilmektedir. Örneğin sistemdeki şifrenin başka bir şifre ile değiştirilmesi halinde de bu durum oluşabilecektir.

[426] Yazıcıoğlu, s.263.
[427] Değirmenci, s.190.
[428] Özbek ve diğ, s.1002.
[429] Durdu, s.171.
[430] Kurt, s.168.
[431] Ketizmen, s.140.

Nitekim Yargıtay bir kararında fail tarafından bir başkasının facebook hesabı kırılarak fotoğrafının değiştirilmesi olayında TCK m. 244/2'den hüküm kurmuştur.[432]

Öte yandan Durdu, kripto para hesabında işlem yapılmasını sağlayan sanal cüzdanın içindeki gizli şifrenin değiştirilmesi halinde de bu suçun oluşacağını ifade etmiştir.[433]

1.2.Veriyi Erişilmez Kılmak, Sisteme Veri Yerleştirmek, Var Olan Verileri Başka Bir Yere Göndermek

Verinin erişilmez kılınması, kişinin veriye istediği zaman ulaşmasının engellenmesi anlamına gelmektedir.[434] Bu halde esasen verinin içerdiği bilgiye müdahalede bulunulmaz, yalnızca veriye normal şekilde erişim engellenir. Böylece veri üzerinde herhangi bir bozma ve yok edilme durumu söz konusu olmamaktadır. Verinin içeriği bütün olarak korunmuş olmaktadır. Sadece verilere ulaşım noktasındaki işlem bağı kopmaktadır.[435]

Verinin erişilmez kılınması fiilini gerçekleştirmeye DDoS saldırıları[436], şifre koymak[437] ve virüs göndermek[438] elverişli olup veriye erişilmesinde erişim engelinin geçici veya kalıcı olmasının bir önemi bulunmamaktadır.[439]

Yargıtay kararları incelendiğinde mail ve sosyal medya hesapları üzerindeki şifrelerinin değiştirilmesi suretiyle ilgilinin hesabına erişiminin engellenmesini TCK'nin 244. maddesinin ikinci fıkrası uyarınca değerlendirildiği görülmektedir.[440]

Nitekim Yargıtay 8. Ceza Dairesi'nin bir kararına konu suça sürüklenen çocuğun mağdura ait facebook şifresini kırdığı ve bu hesabın yöneticisini değiştirdiği, bu suretle hesabı bir gün süre ile kendi hâkimiyetinde bulundurduğu olayda ilk derece mahkemesi

[432] Dülger, s.347.
[433] Durdu, s. 172.
[434] Dülger, s.347.
[435] Özbek ve diğ, s.1003.
[436] Ketizmen, s.140.
[437] Erdoğan, s.225.
[438] Özbek ve diğ, s.1003.
[439] Ketizmen, s.140.
[440]Yargıtay 15. Ceza Dairesi'nin 15.11.2016 tarihli ve E:2016/3871, K:2016/8608 sayılı Kararı, www.corpus.com.tr, erişim tarihi:11.05.2021.

tarafından beraat kararı verilmişse de Yargıtay TCK m. 244/2. fıkrası hükmü çerçevesinde sanığın mahkûmiyetine karar verilmesi gerektiği gerekçesiyle kararı bozmuştur.[441]

Yargıtay 4. Dairesi'nin kararına konu olayda ise sanığın katılana ait mail adresi ile facebook hesabına bağlantı kurduğu, bu suretle facebook şifresini katılanın rızası ve bilgisi dışında değiştirdiği ve sistemde kalmaya devam ederek katılanın hesaba erişimini engellediği olayda Yargıtay tarafından TCK'nin m. 244/2. fıkrası uyarınca suçun oluştuğu kabul edilmiştir.[442]

Öte yandan öğretide sanal cüzdanının oluşturulduğu dosyalar yalnızca okunabilir duruma getirildiğinde veya verilerin şifrelenmesi halinde erişimin engelleneceği belirtilmiştir.[443]

Bilişim sistemine veri yerleştirmek'ten fail tarafından birtakım verilerin sisteme kaydedilmesi ya da bu verilerin sisteme yüklenmesi yahut sisteme veri eklenmesi anlaşılmaktadır.[444] Sisteme doğrudan veri girişi yapılması ya da veri taşıma araçları (CD, flash disk, disket vb.) ile de sisteme veri yerleştirilmesi mümkündür.[445]

Yargıtay 11. Ceza Dairesinin bir kararında sanığın e-bildirge sistemi kullanarak şifre ve imza aracılılığıyla işe giriş bildirgesi düzenleme fiilinde, somut şekilde düzenlenmiş bir belge bulunmadığından Türk Ceza Kanunu'nun m. 244/2-3 hükmü gereğince *"Sisteme veri yerleştirme suçu"*nun oluştuğu dikkate alınmaksızın kamu görevlisinin resmi belgede sahtecilik suçundan mahkumiyet hükmü kurulmasının hukuka aykırı olduğuna karar verilmiştir.[446]

Sistem içerisindeki verinin başka bir yere gönderilmesi, verinin bir yerden başka bir yere kopyalanılarak transferi anlamına gelmektedir. Bu noktada verinin nereye transfer edildiğinin bir önemi bulunmamaktadır. Örneğin bir öğrencinin sınav sorularını alması, failin hiç işine yaramayacağı mağdura ait resim, fotoğraf ve videoların alınması, casusluk amacıyla askeri bilgilerin kopyalanması bu suçu oluşturacaktır.[447]

---

[441] Yargıtay 8. Ceza Dairesi'nin 23.12.2019 tarihli ve E:2018/3125, K:2019/15507 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:10.05.2023.
[442] Yargıtay 4. Ceza Dairesi'nin 10.06.2021 tarihli ve E:2021/6140, K:2021/18796 sayılı Kararı.
[443] Durdu, s.171.
[444] Dülger, s.350.
[445] Koca/Üzülmez, s.814
[446] https://barandogan.av.tr , erişim tarihi:25.05.2021.
[447] Kurt, s.170.

Burada verinin orijinalliği korunmaktadır. Bir başka deyişle bu halde verinin aslı yok olmaz veyahut ortadan kaldırılmaz. Aksi halde verinin yok olması söz konusu olacaktır.[448]

Bilişim sistemindeki mevcut verilerin başka bir yere gönderilmesi esas itibarıyla verilerin bir taşıma aracına veyahut başkaca bir bilişim sistemine kaydı, kopyalanması veya aktarılmasıdır.[449]

Nitekim Yargıtay 8. Ceza Dairesi'nin bir kararında[450] sanığın yetkisi ve katılanın rızası olmaksızın sanık tarafından katılan şirkete ait bilgisayara girilerek oradaki verilerin kendi kullandığı bilgisayara ve CD'ye aktarılması olayında TCK m. 244/2 hükmü gözetilmeksizin karar verilmesini hukuka aykırı bulmuştur.

Ketizmen ise *"verinin kopyalanması"* ibaresini verinin çoğaltılması olarak değerlendirmiş ve bu halde verinin kopyalanmasının verinin ulaşılabilirliğinde veya erişilebilirliğinde herhangi bir etkisi bulunmadığını ifade ederek verinin esasen halen sistemde kaldığını belirtmiştir. Böyle olunca da veriye karşı herhangi bir olumsuz müdahalenin gerçekleşmeyeceğini vurgulamış, bu halin maddenin konuluş amacına aykırı olduğunu belirtmiştir.[451] Yine kişinin bilgisayarında muhafaza ettiği sanal cüzdanına ait bilgilerin veya bu cüzdandaki gizli anahtar bilgilerinin bir diğer bilgisayara gönderilmesi de bu suça sebebiyet verecektir.[452]

Burada önemle bahsedilmesi gerekir ki fail tarafından şayet mağdurun kişisel verilerinin bir yerden başka bir yere aktarılması söz konusu olursa o halde TCK'nin 135. maddesinde hüküm altına alınan *"Kişisel verilerin kaydedilmesi suçu"* ya da TCK'nin 136. maddesinde düzenlenen *"Kişisel verilerin hukuka aykırı olarak verilmesi veya ele geçirilmesi suçu"* oluşacaktır.[453] Nitekim Yargıtay 8. Ceza Dairesinin 18.01.2023 tarihli ve E:2020/11243, K:2023/118 sayılı Kararı'nda TCK m. 244/2'den bahsedilebilmesi için mağdurun bir bilişim sistemi bulunması ve failin de oraya hukuka aykırı yolla girmek suretiyle verilere zararlı müdahaleler yapması gerektiği belirtilmiştir. Buna karşın karara konu olayda sanık tarafından mağdurun facebook hesabı bulunmaması, sanığın mağdurun

[448] Ketizmen, s.141.
[449] Özbek ve diğ, s.1003; Dülger, s.351.
[450] Yargıtay 8. Ceza Dairesi'nin 14.07.2014 tarihli ve E:2013/3173, K:2014/18506 sayılı Kararı, Gül, s.139.
[451] Ketizmen, s.141.; Aynı yönde Özbek ve diğ, s.1004.
[452] Durdu, s. 172.
[453] Dülger, s.351.

fotoğrafının, ad-soyadının kullanılması söz konusu olduğundan TCK m. 136'da düzenlenen *"Kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak suçu*" oluştuğu gözetilmeden TCK m. 244'ten kurulan hükmün hukuka aykırı olduğuna karar verilmiştir.[454]

Yine Yargıtay 12. Ceza Dairesi'nin bir kararında da sanığın somut olaydaki katılanın facebook hesabındaki şifresini ve hesabın ismini değiştirmesi fiillerinin TCK m. 136/1 ya da TCK m. 244/2'de belirtilen suçları oluşturduğu gözetilmeden yalnızca verileri hukuka aykırı olarak verme ve ele geçirmeden hüküm kurulmasının hukuka aykırı olduğuna karar verilmiştir.[455]

2. Hukuka Aykırılık

Fiilin hukuka aykırı olması gerekmektedir. Bir başka deyişle, fail *"bir bilişim sistemindeki veriyi bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka yere gönderme"* konusunda yapmasına izin verilmediği ya da herhangi bir hukuka uygunluk sebebi bulunmadığı yani yapmaya yetkili olmadığı bir davranışta bulunması hukuka aykırılıktır.[456]

Suçta ilgilinin rızası hukuka uygunluk nedenidir. Kişinin rızası olduğu takdirde suç oluşmayacaktır. Örneğin teknik destek ekibinin sisteme müdahale etmesi için yetki verilmesi ve bu yetkiye istinaden teknik ekibin sorunun çözümü için sisteme veri yerleştirmesinde suç oluşmayacaktır.[457] Ancak bu rıza ile teknik ekibe sistem içerisindeki tüm verilere zarar verme, veri yerleştirme, bozma veya verilerin yerinin değiştirmesi yetkisi verilmez. Dolayısıyla yetkili kişi tarafından zarar verme kastıyla sisteme veri yerleştirilmesi söz konusu olursa bu halde suç oluşacaktır.[458]

Yargıtay bir kararında eşlerden birinin evli oldukları dönemde diğer eşin facebook şifresini bildiği, daha sonra boşanma davası açtıkları ve davanın devam ettiği ve bu rızanın boşanma davası devam ettiği dönemde bulunmadığı olayda, mahkeme tarafından açık veya zımni rızanın boşanma davası aşamasında bulunmadığı, şifreyi bilse dahi bilişim sistemine

---

[454] Yargıtay 8. Ceza Dairesinin 18.01.2023 tarihli ve E:2020/11243, K:2023/118 sayılı Kararı, https://legalbank.net, erişim tarihi:17.05.2023

[455] Yargıtay 12. Ceza Dairesi'nin 05.10.2022 tarihli ve E:2022/5072, K:2022/6245 sayılı Kararı https://www.lexpera.com.tr, erişim tarihi: 18.05.2023.

[456] Taşkın, s.50.; Koca/Üzülmez, s.818.

[457] Taşkın, s.51.

[458] Dülger, s.358.

girmesi, orada kalması ve hatta veri yükleyerek değişiklik yapması ve facebook girişini engellemesi TCK'nin 244. maddesinin ikinci fıkrası uyarınca suç teşkil edeceği hükme bağlanmıştır.[459]

Öte yandan failin bu hükme göre yaptırıma tabi tutulabilmesi için sistem için güvenlik tedbiri alınmasının da bir önemi bulunmamaktadır. Örneğin bir kişi bilgisayara giriş şifresi koymadığı olayda failin bu durumdan yararlanarak sisteme kendi belirlediği bir şifreyi koyması da bu suç oluşacaktır.[460]

Bu suçta özellikle görevin ifası hukuka uygunluk nedeninin gerçekleşmesi mümkündür. Zira hakim sanığa ait bilgisayar loglarında arama yapılmasına ve burada bulunan verilerin kopyalanmasına karar verebilir. Bu halde suç oluşmayacaktır. Keza *"5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* kapsamında internet erişiminin engellenmesine yönelik kararın icrası halinde de fiil hukuka aykırılık teşkil etmez.[461]

Yine rızanın daha önceden verilmesi gerekmektedir. Müdahaleden sonra verilecek rıza suçun soruşturmasını veya kovuşturmasını engellemeyecektir.[462]

Bir diğer hukuka uygunluk nedeni olan kanun hükmünün icrasıdır. Bu halde *"5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu"* nun 8. maddesi ile idari yaptırım veya koruma tedbiri olarak internet erişiminin engellemesi örnek olarak gösterilebilir.[463] Yine CMK'nin 134. maddesi gereğince bilişim sistemlerinde yapılmış veya yapılacak el koyma,

---

[459] Yargıtay 12. Ceza Dairesi'nin 28.10.2013 tarihli ve E:2012/31601, K:2013/23586 sayılı Kararı *"sanığın, resmi nikahlı eşi olması nedeniyle daha önce bildiği katılan Evrim'e ait facebook adresinin internet şifresini, katılanla aralarında boşanma davası devam ettiği ve fiilen ayrı yaşadıkları dönemde, hakkı bulunmadığı halde kullanmak suretiyle bilişim sistemindeki katılana özel kısma girdiği ve buraya kendisine ait resmi koyacak kadar süreyle hukuka aykırı olarak sistemde kalmaya devam edip, katılana ait facebook internet şifresini değiştirerek, katılanın sistemdeki kendisine ait kısma erişememesine sebebiyet verdiği olayda, sanığın, eşi katılanın kişisel verilerini ele geçirme, kaydetme, yayma, onun başkasıyla gerçekleştirdiği haberleşme içeriğini öğrenme, kaydetme veya ifşa etme, özel hayatının gizliliğine müdahalede bulunma, huzur ve sükûnunu bozma kastıyla hareket ettiğine dair dosya kapsamında bir delil bulunmadığı anlaşılmakla, sanığın sübut bulan bilişim sistemindeki şifreyi değiştirip, katılanın sistemdeki kendisine ait kısma erişimini engellemekten ibaret eyleminin TCK'nın 244/2. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturacağı gözetilmeden, delillerin takdirinde ve suç vasfında yanılgıya düşülerek, dosya kapsamına uygun düşmeyen yetersiz gerekçelerle, sanık hakkında TCK'nın 136/1. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçundan mahkumiyet hükmü kurulması,"* (https://www.hukukturk.com, erişim tarihi:03.08.2023)

[460] Dülger, s.359.

[461] Koca/Üzülmez, s.815.

[462] Malkoç, İsmail: Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu, Malkoç Kitabevi, Ankara 2007, 2. Cilt, s.1667.

[463] Özbek ve diğ, s.1010.

kopyalama ve arama tedbirleri de TCK'nin 244. maddesinin ikinci fıkrasındaki suça vücut vermeyecektir.[464] Bununla birlikte "*çıkar amaçlı suç örgütleri"* hakkındaki yargılamalarda 4422 sayılı Kanun'un ikinci ve dördüncü maddelerinde usul ve esaslara uygun olmak suretiyle bilişim sistemindeki verileri veya programların ele geçirilmesi de TCK'nin 49. maddesinin birinci fıkrası uyarınca kanun emrini icra kapsamında değerlendirilmektedir. Bu halde de suçun oluşmayacağını belirtmek gerekmektedir.[465] Bir başka örnek ise belirli dönemlerde veya belirli şartların varlığı hallerinde devlet tarafından vergi borçlarının silinmesi halinde de veriyi silen kişi veriyi yok etme fiili bakımından cezalandırılmayacaktır.[466]

3. Kusurluluk

Kusurluluk bakımından ise suç kastla işlenebilmektedir. Dolayısıyla kast, failin belli bir bilişim sisteminde mevcut olan verileri bilerek ve isteyerek, yok etmesi, bozması, erişilmez kılması, değiştirmesi, var olan verileri başka bir yere göndermesi, sisteme veri yerleştirmesi iradesidir. [467] Dolayısıyla fail tarafından bu suçların ancak bilerek ve istenerek işlenmesi gerekmektedir. Bu doğrultuda kast dışında başkaca bir amaç aranmamaktadır.[468]

Ayrıca bilişim sisteminin işleyişini engelleme ve bozma suçlarının olası kastla da işlenebilmesi mümkün olacaktır.[469]

Suç, taksirle işlenemez.[470] Bu noktada bazı yazarlar teknik ekipteki görevlilerin özen yükümlülüklerinin üst düzey yerine getirmesi gerektiğini, aksi halde bilişim sistemindeki verilerin yok olması halinde ilgililerin, teknik ekipteki görevlinin bu fiili kasten işlediğini kanıtlaması gerekeceğini, dolayısıyla verileri yok olan ilgilinin, teknik personel karşısında mağduriyet yaşayabileceğini belirterek bu suçta taksirli halin de düzenlenmesi gerektiğini eleştirisinde bulunmuşlardır.[471]

---

[464] Taşkın, s.28.
[465] Yenidünya/Değirmenci, s.71-72.
[466] Akbulut, 2016, s.40
[467] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.456. Aynı yönde Dülger, s.357.
[468] Kurt, s.75.
[469] Artuk/ Gökcen /Yenidünya, s.1171.
[470] Koca/Üzülmez, s.815.
[471] Taşkın, s.53.

Failin suçun kanuni tanımındaki tüm unsurları bilmesi gerekir. Kastın dışında başka bir manevi unsur (saik, amaç gibi) aranmamıştır.[472] Dolayısıyla failin bir bilişim sisteminin işleyişini bilerek ve isteyerek engelleme veya bozma iradesi bulunmalıdır.[473]

Buna karşın söz konusu fıkrada belirtilen neticelere sebebiyet verecek fiiller ile sistemin işleyişinin engellenmesi veya bozulması da söz konusu olabilir. Böyle bir durumda failin fiilinin hangi fıkra hükmüne göre nasıl yaptırıma tabi tutulacağının belirlenmesinde faildeki amacın yorum aracı olarak belirlenmesi gerekmektedir.[474]

Nitekim TCK'nin 243. maddesinin üçüncü fıkrası ile 244. maddenin birinci ve ikinci fıkrasındaki suçların uygulanması bakımından da somut olayda failin kastı belirleyici olacaktır. Örneğin failin hukuka aykırı olarak sisteme girip orada kalma kastıyla hareket ettiği bir olayda, failin bu kast ile girdiği sistemde verilerin yok olması veyahut değişmesi nedeniyle faile hangi madde hükmü uygulanacaktır? Bu halde failin TCK m. 244 kapsamında kastı olmaması, fiilin hukuka aykırı olarak sisteme girmesi ve sistemde kalmak şeklinde olması ve failin girdiği sistemde verilerin yok olması veyahut değişmesi söz konusu olduğunda failin fiilinin TCK m. 243 kapsamında değerlendirilmesi gerekmektedir. Buna karşın sisteme girdikten sonra failin kastını değiştirerek veriyi kasten değiştirmek isterse bu durumda ne olacaktır? Bu halde bilişim sisteminin işleyişini bozmamakta ise TCK m. 244/2 hükmü uyarınca sorumlu tutulacaktır.[475]

Bazı yazarlar böyle bir durumda eklenen kast nedeniyle TCK m. 244/2'nin uygulanması gerektiğini belirtmektedirler.[476]

4. Kusurluluğu Kaldıran Nedenler

4.1.Fiille Fail Arasındaki Psişik/Manevi Bağı Ortadan Kaldıran Nedenler

TCK'nin 244. maddesinin ikinci fıkrasında düzenlenen *"Bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçu"* bakımından da kendinde olmama veya mücbir sebebin varlığı nedeniyle fail ile fiil arasındaki psişik bağın kesilmesi bir başka deyişle fiilin iradiliğinin ortadan kalkması mümkün değildir. Dolayısıyla bu suçta mücbir sebep ve

[472] Koca/Üzülmez, s.815.
[473] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.454.
[474] Kurt, s.175.
[475] Karagülmez, s.219.
[476] Gül, s.140.

kendinde olmama hallerinin kusurluluğu kaldıran neden olarak kabul edilmesi olası görünmemektedir.

TCK'nin 28. maddesinde *"...kurtulamayacağı cebir ve şiddet ... sonucu suç işleyen kimseye ceza verilmez"* denilmek suretiyle düzenlenen maddi cebir, TCK'nin 244. maddesinin ikinci fıkrasında düzenlenen suçta uygulama alanı bulabilmektedir. Bu halde "*Bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçu"*nun maddi cebir vasıtasıyla suçun işlenmesi ihtimal dahilindedir. Zira maddi cebir etkisinde kalan kişi suç işlemiş olmayacak ancak suçu işleyen üzerinde maddi cebir uygulayan kişi fail olarak cezalandırılacaktır.

4.2.Hata

TCK'nin 4. maddesinde *"ceza kanunlarını bilmemek mazeret sayılmaz"* denilmek suretiyle kural üzerinde hata düzenlenmiş olup TCK m.244/2'de düzenlenen *Bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçu"* nda kural olarak hukuki hata mümkün değildir. Zira failin hukuki hata yapabilmesi için fiilin antisosyal niteliğini bilmemesi ve bu fiilin suç olduğunu bilmemede beşeri imkansızlığı bulunması gerekmektedir. Oysa söz konusu suçta bir bilişim sistemindeki verilere karşı müdahalede bulunan gerçek kişi failin bu fiilin suç olduğunu bilmediğini iddia edemez.

Fiil üzerinde hata bir başka deyişle fiili hata, suç teşkil eden fiilin unsurlarında meydana gelen hata olup söz konusu TCK m.244/2'de düzenlenen suçta fiil üzerinde hata mümkündür. Örneğin bir kimsenin esasen yetkisiz iken kendisini yetkili zannederek suça konu fiili işlemesi halinde verilerin bozulması, yok olması, değişmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi söz konusu olursa bu hata fail lehine değerlendirilecektir.[477]

Hukuka uygunluk nedenlerinde hatada da söz konusu suçta kusurluluğu kaldıran neden olarak gösterilebilmektedir. Örneğin bilişim sistemi üzerinde menfaati olan kişinin rızası var olduğu düşünülerek failin hareket etmesi ve bu hareketler neticesinde bilişim sistemindeki verilerin bozulması, yok olması, değişmesi veya erişilmez kılınması, sisteme

[477] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.458.

veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi söz konusu olduğu takdirde fail cezalandırılmayacaktır.

4.3.Manevi Cebir ve Bu Temelde Kişiden Beklenenin Bulunduğu Koşullarda Kendisinden İstenememesi (İstenememezlik İlkesi)

TCK'nin 28. maddesinde hüküm altına alınan manevi cebir, bu suç bakımından mümkündür. Buna göre bilişim sistemlerindeki verilerin bozulmasına, yok olmasına, değişmesine veya erişilmez kılınmasına, sisteme veri yerleştirilmesine, var olan verilerin başka bir yere gönderilmesine neden olacak fiiller fail tarafından manevi cebir altında işlenmekte ise fail söz konusu fiili nedeniyle cezalandırılmayacaktır. Örneğin bir kişinin, hacker olan diğer bir kişiyi (bilişim sistemleri üzerinde bilgi sahibi olması nedeniyle) tehdit ederek başka bir kişinin bilişim sistemindeki verileri bozmasını istediği olayda, hacker suça konu fiili nedeniyle cezalandırılmayacaktır.

VI. SUÇLARIN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

A. TEŞEBBÜS

TCK'nin 35. maddesinde *"Kişi, işlemeyi kastettiği bir suçu elverişli hareketlerle doğrudan doğruya icraya başlayıp da elinde olmayan nedenlerle tamamlayamaması*" hali teşebbüs olarak tanımlanmıştır. Teşebbüs halinin varlığı için icra hareketlerinin tamamlanamamış olması ya da icra hareketi tamamlanmış olsa da neticenin gerçekleşmemesi gerekmektedir. Bir başka deyişle fail tarafından bir suçun işlenmesi hususunda karar verilmesi, daha sonra bu kararın icrası için hazırlık hareketleri yapılması ancak elde olmayan nedenlerle suçun tamamlanmamış olmalıdır. Dolayısıyla icra hareketine başlanılmış ancak elde olmayan nedenlerle tamamlanmamış suçlara *"Teşebbüs halinde kalmış suçlar"* denilmektedir.[478]

TCK m. 244'ün ilk iki fıkrasında düzenlenen suçlara teşebbüsün mümkün olup olmadığı öğretide tartışmalıdır. Bazı yazarlara göre failin sistemi engellemeye veya bozmaya veya sistemdeki verileri bozmaya, yok etmeye, yer değiştirmeye, erişilmez kılmaya, veri yerleştirmeye yönelik herhangi bir fiili gerçekleştirmesine karşın elinde olmayan sebeplerle netice ortaya çıkmamışsa, suç teşebbüs aşamasında kalacaktır.[479] Buna

[478] Koca/Üzülmez, s.416; Özgenç, İzzet: Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara 2022, s.555.
[479] Dülger, s.359.; Aynı yönde Özbek ve diğ, s.1012.; Kurt, s.153.; Taşkın s.32.; Koca/Üzülmez, s.816.; Gül, s.141. Karşı yönde, Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453, 455,

karşın öğretideki bazı yazarlar bu suçlara teşebbüsün mümkün olmadığı kanaatindedirler.[480]

Biz teşebbüsün mümkün olmadığı görüşüne katılmamaktayız. Kanaatimizce söz konusu suçlar neticeli suçlar olduğundan suçun icrasına yönelik elverişli hareketler tamamlandıktan sonra failin elinde olmayan nedenlerle netice meydana gelmediği takdirde suç teşebbüs aşamasında kalacaktır. Zira örnek vermek gerekirse fail tarafından sisteme virüs gönderilmesi ancak bu durumun fark edilmesi üzerinde verilerde herhangi bir zarara sebebiyet vermeden virüsün yok edilmesi halinde de suça teşebbüs mümkün olacaktır.[481]

Bununla birlikte fail tarafından icra hareketlerine başlanmasının akabinde hareketin bölünebilmesi nedeniyle failin elinde olmayan sebeplerle bu hareketlerin yarıda kalmasıyla da suçlara teşebbüs mümkündür.[482] Örneğin, fail tarafından hukuka aykırı olarak TCK'nin 243. maddesi uyarınca bilişim sistemine girildikten sonra elektriklerin kesilmesi halinde fiil teşebbüs aşamasında kalacak TCK m. 244/1 veya m. 244/2 hükmü uyarınca teşebbüsten sorumlu tutulacaktır.[483]

Öte yandan söz konusu hükmün birinci ve ikinci fıkralarında belirtilen hususları netice olarak kabul ettiğimizden söz konusu neticelerden biri gerçekleşmiş bun karşı diğer netice teşebbüs aşamasında kalmış ise bu halde failin suçun tamamlanmış halinden ceza verilmesi gerektiği kanaatindeyiz.[484]

Ayrıca belirtmek gerekir ki bu suç bakımından da gönüllü vazgeçme müessesesi söz konusu olabilecektir. Örneğin fail elektrik kesildiği için değil de pişman olması sebebiyle netice gerçekleşmeden sistemden çıkarsa bu halde fail, TCK'nin 36. maddesi uyarınca gönüllü vazgeçme müessesesinden yararlanacaktır. Dolayısıyla yalnızca TCK m. 243 hükmünden cezalandırılacaktır.[485]

Öğretide bazı yazarlar tarafından fiil tamamlandıktan sonra eski hale getirilme söz konusu olursa yine gönüllü vazgeçme hükümlerinden yararlanılabileceği görüşü belirtilmiştir. Örneğin fail bilişim sisteminde mevcut verilere hasar vermek için mağdurun sisteme girse ve orada biraz kalsa, ardından verileri değiştirse ancak daha sonra pişman

[480] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.455
[481] Akbulut, s.43.
[482] Dülger, s. 359.
[483] Özbek ve diğ, s.1012.
[484] Erdoğan, s. 232.
[485] Özbek ve diğ, s.1011-1012.

olup düzeltse ya da verilere zarar vermekten vazgeçse bu halde TCK m. 244/2 hükmüne göre cezalandırılmayacaktır. Buna karşın fiil artık bilişim sistemine girme ve orada kalma olduğu için eylemine uyan TCK m. 243 gereği cezalandırılacaktır.[486]

Buna karşın bir başka görüşe göre fiil tamamlanmış ise suç oluşmuştur. Dolayısıyla suç tamamlandıktan sonra veriye veya bilişim sisteminin işleyişine yapılan müdahalenin geri alınmasında olsa olsa etkin pişmanlık hükümleri mümkün olacaktır. Buna karşın söz konusu suçlar bakımından kanunda etkin pişmanlık müessesesi açıkça düzenlenmediğinden sanığın eylemine uyan TCK m. 244/1 veya TCK m. 244/2 hükümlerinden cezalandırılması gerekecektir.[487] Biz de bu görüşe katılmaktayız.

B. İŞTİRAK

İştirak bakımından bu suçlar bir özellik göstermezler. İştirake ilişkin genel kurallar (faillik, azmettirme, yardım etme), TCK m. 224/1 ve TCK m. 244/2 hakkında da uygulanır.[488]

C. İÇTİMA

Bir kimsenin bir veya birden çok fiille, ceza kanunun aynı hükmünü veya farklı hükümlerini bir veya birden çok kez ihlal etmesi halinde, failin birden çok suçtan değil de tek bir suçtan sorumluluğunun söz konusu olmasına suçların içtimaı denir.[489] Suçların içtimaında, suçlardaki bağlantı sebebiyle failin suç sayılan fiillerine karşılık birden çok ceza ile karşılaşması gerekirken sorumluluğun tek bir ceza olarak belirlenmesi söz konusudur.[490]

Suçların içtimaı Türk Ceza Kanunu'nun ikinci kısmının beşinci bölümünde *"Suçların İçtimaı"* başlığı altında düzenlenmiştir. Bu başlık altında 42. maddede bileşik suç, 43. maddede zincirleme suç ve 44. maddede ise fikri içtima kurumları hükme bağlanmıştır

TCK 42. maddesinde düzenlenen bileşik suç, *"Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suç"* olarak tanımlanmıştır.

---

[486] Kurt, s.265-266.
[487] Erdoğan, s.233-234.
[488] Koca/Üzülmez, s.816.; Aynı yönde Hafızoğulları/Özen, Topluma Karşı Suçlar, s.453,455.
[489] Hafızoğulları/Özen, Türk Ceza Kanunu Genel Hükümler, s.354.
[490] Merki, Duygu: Bileşik Suç, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, Ankara 2009, s.7-8.

Buna göre bir suçun bileşik suç olabilmesi için; her biri birbirinden bağımsız suç oluşturan iki veya daha fazla fiilden oluşması gerekmektedir ve bileşik suçta tek başına suç oluşturan fiillerden her biri tek bir suçu oluşturmak için kurucu görev üstlenebilir (Yağma suçu gibi). Bileşik suçun oluştuğu bu iki durumda da kanunda belirlenen temel cezaya hükmedilmektedir.[491]

TCK'nin 43. maddesinde düzenlenen zincirleme suç, *"suç işleme kararında birlik"* düşüncesinden doğmuştur. İlgili madde metninde de *"Bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumunda, bir cezaya hükmedilir"* denilmek suretiyle tanımlanmıştır. Buna göre zincirleme suç aynı suçun bir kişiye değişik zamanlarda işlenmesi halinde söz konusu olacaktır. Burada önemli olan faildeki suç işleme kararında birlik olması gerekmektedir. Bir başka deyişle fail tarafından planlı ve programlı olarak aynı suçu bir kişiye değişik zamanlarda işleme iradesinin yani suçlar arasında sübjektif bir bağın bulunması gerekmektedir. Aynı maddenin 2. fıkrası ile ayrıca aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi halinde de zincirleme suç hükümlerinin uygulanacağı hükme bağlanmıştır. [492]

TCK'nin 44. maddesi ile hüküm altına alınan fikri içtima ise *"İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır."* olarak tanımlanmıştır. Bu halde söz konusu hükme göre, fail tarafından tek bir fiille birbirinden bağımsız iki ayrı suç işlenmesi halinde bu suçlardan en ağır olanıyla sorumlu tutulması gerekmektedir.

TCK'nin 244. maddesinin birinci ve ikinci fıkrasındaki suçlar, içtima hükümleri bakımından özellikli bir durum arz etmemekte[493] olup çalışmamızın devamında zincirleme suç, bileşik suç ve fikri içtima halleri incelenecektir.

Söz konusu suçlar, zincirleme suç hükümleri çerçevesinde incelendiğinde zincirleme suç hükümlerinin bu suçlar hakkında da uygulanması mümkündür. Örneğin failin aynı mağdurun bilişim sistemini değişik zamanlarda birden çok kez engellemesi

[491] Merki, s.86.
[492] Hafızoğulları/Özen, Türk Ceza Kanunu Genel Hükümler, s.361-363.
[493] Akarslan, s.50.

veyahut bozması halinde zincirleme suç hükümlerinin uygulanmasından söz edilebilir.[494] Burada önemli olan tek bir suç işleme kastının bulunması gerekliliğidir.[495]

Nitekim Yargıtay, fail tarafından ayrılmış olduğu kız arkadaşının kuzenine ait mail adresi değiştirilerek izinsiz şekilde mağdurun facebook hesabına girildiği ve bu hesap üzerinden eski kız arkadaşının annesi ile iletişim kurduğu olayda TCK m. 244/2 uyarınca *"sistemi engelleme, bozma, verileri yok etme veya değiştirme"* suçunu oluştuğu ayrıca mail hesabı ve facebook hesabı iki değişik bilişim sistemi olduğundan bir suç işleme kararı kapsamında değişik zamanlarda aynı kişiye aynı eylemi birden fazla kez işlemesi nedeniyle zincirleme suç hükümlerinin uygulanmasına karar verilmiştir. [496]

Yine Yargıtay'ın bir kararında sanık tarafından 10.10.2007-31.03.20088 tarihleri arasında bilgisayar ortamında birden çok sahte işe giriş bildirgesi düzenlendiği olayda, TCK m. 43 uyarınca zincirleme suç hükümlerinin uygulanması gerektiği belirtilmiştir.[497]

Ayrıca ifade etmek gerekir ki TCK m. 244/1 ve TCK m.244/2'nin serbest hareketli suçlar olmaları sebebiyle suçu oluşturan serbest hareketlerden birden fazla gerçekleştirmeleri halinde yine tek suç işlenmiş sayılacaktır. Ancak fail tarafından bu serbest hareketlerin aynı suç işleme kararıyla bir kişiye karşı, farklı zamanlarda gerçekleştirmesi halinde zincirleme suç hükümleri uygulanacaktır.[498]

Bu noktada TCK'nin 244. maddesinin birinci ve ikinci fıkrası arasındaki ilişkiyi öğretide farklı görüşler bulunması nedeniyle içtima kuralları bakımından ele almakta fayda bulunmaktadır. Zira bilişim sistemindeki verilerin değiştirilmesi nedeniyle bilişim sisteminin işleyişinin engellenmesi veya bozulması söz konusu olduğunda hangi madde kapsamında değerlendirileceğinin ortaya konulması gerekmektedir.

Bir görüşe göre, suçun mala zarar verme suçuna göre yalnızca yazılım unsurunu kapsayan özel bir norm olduğu düşüncesinden hareketle, TCK'nin 244. maddesinin birinci fıkrasında düzenlenen yazılım unsuruna yönelik hareketlerin verilerle gerçekleştirilmesi şeklinde olduğu, dolayısıyla ikinci fıkrasındaki verilere ilişkin müdahaleler ile sisteme

[494] Özbek ve diğ, s.1012.
[495] Taşkın s.32.
[496] Yargıtay 12. Ceza Dairesi'nin 01.03.2017 tarihli ve E:2015/10388, K:2017/1556 sayılı kararı, www.corpus.com.tr, erişim tarihi:10.05.2021.
[497] Yargıtay 8. Ceza Dairesi'nin 16.03.2020 tarihli ve E:2020/1338, K:2020/1154sayılı kararı, www.corpus.com.tr, erişim tarihi:10.05.2021.
[498] Özbek ve diğ, s.1012.

ilişkin müdahaleler arasında **geçitli suç** ilişkisi bulunduğu ifade edilmektedir.[499] Oysa geçitli suç, hedeflenen ağır suçu işlemek maksadıyla önce daha hafif bir suçtun işlenip daha sonra hedeflenen ağır suçun işlenmesi hali olup bu halde fail yalnızca hedeflenen ağır suçtan sorumlu tutulmamaktadır.[500] Geçitli suçun tanımından hareketle, birinci fıkra hükmünün daha ağır bir yaptırımı olması karşısında söz konusu görüşe katılmamız mümkün değildir.

Diğer bir görüşe göre, Kanun koyucunun birinci fıkrasındaki yaptırımı ikinci fıkradaki yaptırıma göre daha ağır düzenlediği dikkate alınarak, ikinci fıkradaki seçimlik hareketlerle bilişim sisteminin işleyişinin engellenmesi veya bozulması söz konusu olduğu takdirde birinci fıkra hükmünün uygulanması gerektiği belirtilmiştir.[501] Başka bir görüş ise bilişim sisteminin engellenmesi veya bozulması ikinci fıkradaki fiiller neticesinde gerçekleşmişse bu halde birinci fıkra hükmünün uygulanması gerektiğini belirtmiştir. Bu görüşün esası birinci fıkradaki suçun hangi hareketlerle gerçekleştiğinin açıkça ifade edilmemesine dayanmaktadır. Dolayısıyla bu görüşe göre ikinci fıkradaki hareketler bilişim sisteminin işleyişine müdahale boyutuna ulaştığı takdirde bu halde ikinci fıkra hükmü değil, birinci fıkra hükmünün uygulanması gerektiği belirtilmektedir.[502] Buna karşın biz bu görüşe katılmamaktayız. Zira bu düşünce suçun kusurluluk unsurunu göz ardı ederek netice üzerinden bir değerlendirme yapmaya sebebiyet vermektedir.

Bir diğer görüşe göre, bu sorun failin kastının belirlenmesiyle aşılacaktır. Buna karşın fail tarafından bilişim sistemindeki işletim yazılımındaki sistem dosyalarını sildiği olayda failin verileri bozma değil, sistemin işleyişini bozma kastının olduğu, zira failin sıradan verilere değil, sistemin işleyişini sağlayan dosyalara yöneldiği ifade edilmiştir.[503] Dolayısıyla bu görüşe göre failin kastı belirlenirken, somut olayın kendine has özellikleri ve fiilin yöneldiği verilerin de önemli olduğu belirtilmiştir. Bu görüşe katılmaktayız. Her ne kadar bazı durumlarda kastın belirlenmesi açısından zorluk bulunmaktaysa da suçun unsurlarının tam ve şüpheye mahal vermeyecek şekilde ortaya konulması bakımından bu görüşün desteklenmesi, suç genel teorisi çerçevesinde daha sağlıklı olacağı kanaatindeyiz.

---

[499] Ketizmen, s.137.
[500] Özen, Mustafa, Suçların İçtiması (Zincirleme Suç- Fikri İçtiması- Bileşik Suç), Ankara Üniversitesi Sosyal Bilimler Enstitisü Kamu Hukuku Ana Bilim Dalı Doktora Tezi, Ankara 2008, s.352.
[501] Karagülmez, s.217-218. Aynı görüşte, Dülger, s.319.
[502] Koca/Üzülmez, s.917.
[503] Kurt, s.167.

TCK'nin 244. maddesinin birinci ve ikinci fıkrası ile TCK'nin 243. maddesi arasındaki ilişkinin de içtima kuralları kapsamında incelenmesi önem arz etmektedir.

Öğretide bir görüşe göre, TCK'nin 243. maddesinde[504] düzenlenen *"Bilişim sistemine hukuka aykırı olarak girme ve sistemde kalmaya devam etme suçu"* ile TCK'nin 244. maddesinin birini ve ikinci fıkrasında düzenlenen suçlar arasında **geçitli suç** ilişkisi olduğu ifade edilmektedir. Bu halde TCK m. 244/1-2'deki suçların TCK m. 243'te belirtilen bilişim sistemine hukuka aykırı olarak girmek veya orada kalmayan devam etmek suretiyle gerçekleşebileceği, dolayısıyla yalnızca TCK m. 244'ten cezalandırması gerektiği ifade edilmektedir.[505]

Buna karşın katıldığımız diğer bir görüşe göre bu iki suç arasında geçit suçunun söz konusu olması mümkün değildir. Zira geçit suçundan bahsedebilmek için cezası hafif olan suçun önce işlenmesi, daha sonra diğerinin gerçekleşmesi gerekmektedir. Bu halde sonraki ağır suçun ilk suçla aynı hukuki değeri koruması gerekmektedir. Oysa TCK m. 243 ile bilişim güvenliği korunduğu, TCK m. 244/2 ile de mağdurun malvarlığı korunduğundan farklı hukuksal değeri koruyan bu iki hüküm arasında geçit suçunun söz konusu olması mümkün olmadığı belirtilmiştir.[506]

Bir görüşe göre tek fiille TCK m. 243 ve TCK m. 244 ihlal edildiği takdirde **fikri içtima** uygulanması gerekir. Zira fail bilişim sistemindeki verileri değiştirmek isterken bilişim sistemine hukuka aykırı olarak girmektedir. Böylece TCK m. 243'ü de ihlal etmektedir.[507] Buna karşın burada failin tek bir fiilinden söz edilmesi mümkün değildir. Zira failin TCK'nin 244. maddesinin birinci ve ikinci fıkralarındaki suçu TCK'nin 243. maddesindeki bilişim sistemine girmek veya orada kalmak fiilleri ile gerçekleştirdiğinde farklı fiiller gerçekleştirmekte olduğundan fikri içtima da uygulanamayacaktır. Bir diğer

---

[504] ***Bilişim sistemine girme***
*"**Madde 243:** (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.*
(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.
(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.
(4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır"

[505] Soyaslan, 676.; Aynı görüşte Akarslan, s.50.; Taşkın s.55; Gül, s.140.

[506] Dülger, s.316-318.

[507] Koca/Üzülmez, s.817.; Aynı görüşte, Apaydın, Cengiz: Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, Seçkin Yayıncılık, Ankara 2023, s.182.; Erdoğan, s.236.

görüşe göre, fiiller arasında zamansal yakınlık bulunduğu takdirde TCK m. 244'ten, yakınlık bulunmadığı takdirde gerçek içtima uygulanmalı yani TCK m. 244 ve TCK m. 243'ten ayrı ayrı cezalandırılmalıdır. [508]

Bizim de katıldığımız görüşe göre bu iki fıkranın uygulaması **failin kastına** göre belirlenmelidir. TCK m. 243 kapsamında bilişim sistemine girildikten sonra failin kastı verilere müdahale kastına dönüşmüş olsa da fail iki ayrı suçtan cezalandırılmayacaktır. Zira bu halde TCK m. 243'te belirtilen bilişim sistemine hukuka aykırı olarak girmek veya orada kalmak fiili artık TCK m. 244/2'de belirtilen suçun unsuru haline gelecektir. [509] Yani fail tarafından bir bilişim sisteminin içindeki verilerin yok edilmesi veya değiştirilmesi kastıyla hareket edildiğinde bu halde TCK m. 244/2'den sorumluluk söz konusu olacaktır.[510]

TCK'nin 151. maddesinde düzenlenen mala zarar verme suçu ile 244. maddesinde düzenlenen suçlar arasındaki ilişki de öğretide tartışmalıdır. Zira bilişim sistemine ilişkin fiziksel saldırıda bulunulduğunda faile hangi hüküm uygulanacaktır? Bu sorunun çözümü için öncelikle bu fıkranın yazılım ve donanıma ilişkin fiillerin bir bütün olarak ele alınıp alınmayacağının belirlenmesi gerekmektedir. Bu hususa ilişkin çalışmamızda bilişim sisteminin yazılım ve donanımıyla bir bütün olduğu ifade edilmiştir. Bir görüşe göre Kanun koyucu tarafından bilişim sisteminin *"işleyişi"* kavramının kullanılması bilinçlidir. Zira bu görüşteki yazarlar, Kanun koyucunun asıl amacının, sisteme yönelik fiziki müdahalelerde bulunarak sistemin işleyişinin engellenmesi veya bozulması değil, veriye müdahale yoluyla ya da yazılımlarda değişiklik yapılması suretiyle işleyişin engellenmesi ve bozulması olduğunu belirtirler. Dolayısıyla bilişim sistemine fiziksel müdahaleler neticesinde bilişim sisteminin bozulması veya engellenmesi halinde faile mala zarar verme suçu hükümleri uygulanacağı ifade edilmektedir.[511]

Bir görüşe göre bilişim sistemine karşı fiziksel saldırılarda bulunulduğunda akla mala zarar verme suçunun uygulanması gerektiği gelse de bunun yanında bilişim sisteminin işleyişine de zarar verildiğinden faile fikri içtima hükümleri uyarınca en ağır cezayı gerektiren suçun uygulanması gerektiği belirtilmiştir.

---

[508] Dülger, s.319.
[509] Karagülmez, s.219.
[510] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.450.; Aynı yönde Özbek ve diğ, s.992.
[511] Ketizmen, s.135-137.

Dolayısıyla TCK m. 151 uyarınca suçun cezası "*dört aydan üç yıla*" iken TCK m. 244 uyarınca suçun cezası "*bir yıldan beş yıla*" kadar olduğundan fail TCK m. 244 uyarınca fiilinden sorumlu olacağı ifade edilmektedir. Failin kastını da bilişim sistemini bozmak olması gerektiği de vurgulanmıştır.[512]

Bir başka görüşe göre bilişim sisteminin soyut veya somut unsurlarına bilişim sisteminin işleyişini engelleme veya bozma kastıyla bir harekette bulunulduğunda TCK m. 244/1 hükmü uygulanacaktır. Ancak bu görüşe göre önemli olan husus fiilin sistemi engelleyecek ya da bozacak nitelikte olması olup eğer sistemin işleyişini bozmuyor ya da engellemiyorsa suç tamamlanmamış olacak ve teşebbüs aşamasında kalacaktır. Dolayısıyla sistemin yanında olan veya sisteme bağlı olup da işleyişe etkisi olmayan unsurlara zarar vermenin TCK m. 244/1 hükmü ile değil, TCK m. 151 hükmü uyarınca *"Mala zarar verme suçu"* ndan sorumlu tutulması gerektiği belirtilmektedir.[513] Biz de bu görüşe katılıyoruz. Dolayısıyla fail tarafından bilişim sisteminin donanım unsuruna yapılan fiziki müdahaleler TCK m.244'te belirtilen neticelerin oluşumuna sebebiyet verdiği ve kastının da bu yönde olduğu takdirde TCK m. 151 değil, TCK m. 244 hükmü uygulanmalıdır.

Öte yandan fail tarafından bilişim sistemindeki verilere karşı fiziksel bir müdahalede bulunularak zarar verilmişse bu halde yine TCK m. 151 hükmü değil, TCK m. 244 hükmü uygulanacaktır. Zira TCK m. 151 hükmü uygulanabilmesi için ortada bir "*mal*" söz konusu olması gerekmektedir. Veriler, mal olarak değerlendirilemediğinden TCK m. 244 uygulanma alanı bulacaktır.[514]

TCK m. 244 ile belgede sahtecilik suçları arasındaki içtima ilişkisi de öğretide tartışmalı olduğundan bu konuya da değinmekte fayda görmekteyiz. Öğretideki bazı yazarlar, fail tarafından bilişim sistemine veri eklenmek veya bu veriler değiştirilerek sahte belge düzenlenmesi veyahut değiştirilmesi sağlanmış ise gerçek içtima gereği iki suçtan ayrı ayrı cezalandırılması gerektiğini belirtmişlerdir.[515] Bir diğer görüşteki yazarlar ise Yargıtay Ceza Genel Kurulu'nun 29.09.2020 tarihli ve E:2017/1122, K:2020/381 sayılı Kararı'nda da belirtilen TCK m. 244 hükmün elektronik belgelerdeki sahtecilik fiillerine

[512] Kurt, s.165.; Karagülmez, s.215.
[513] Soyaslan, Doğan: Ceza Hukuku Özel Hükümler, Yetkin Yayıncılık, Ankara 2020, s.668. Erdoğan, s.206.; Pallı, s.207.
[514] Erdoğan, s.237.
[515] Mahmutoğlu, Fatihlg Selami: *"Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi",* İÜHFM, C. 71, S.1, Y. 2013, s.870.

ilişkin özel norm niteliğinde bulunduğu, dolayısıyla özel normun önceliği ilkesi gereğince elektronik belgede sahteciliğin TCK m. 244 kapsamında olduğunu ifade etmişlerdir.[516]

Katıldığımız bir diğer görüşe göre bu durum somut olaya göre değişkenlik gösterebilmektedir.

Örneğin sahte belge, verilerin tahribatı için kullanılmaktaysa bu halde TCK m. 212'nin *"Sahte resmi veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması halinde, hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunur."* şeklindeki hükmü uyarınca iki ayrı suçtan cezalandırılmalı iken verilerde tahribat yapılarak sahte belge düzenlenmesinde fikri içtima hükümleri uygulanmalıdır.[517]

Yine TCK'nin "*Özel hayatın gizliliğini ihlal"* başlıklı 134, *"Kişisel verilerin kaydedilmesi"* başlıklı 135 ve *"Verileri hukuka aykırı olarak verme veya ele geçirme"* başlıklı 136. maddeleri uyarınca TCK m. 244 hükmü arasındaki içtima ilişkisinin de değerlendirilmesi önem arz etmektedir. Zira somut olaya göre kişisel verilerin kaydedilmesi fiili, sisteme veri yerleştirilmesi fiili ile aynı anlamda olabilir. Yine verilerin hukuka aykırı olarak ele geçirilmesi fiili ile özel hayatın gizliliğinin ihlal edilmesi ya da bilişim sistemine hukuka aykırı olarak girmek suretiyle kişisel verilerin hukuka aykırı olarak ele geçirilmesi söz konusu olabilir. Bu hallerde öğretide fikri içtima hükümlerinin uygulanması gerektiği belirtilmiştir.[518] Buna karşın diğer bir görüşe göre fail, iki ayrı suçtan da ayrı ayrı sorumlu tutulabilecektir.[519]

Gerçekten Yargıtay 12. Ceza Dairesi kararında sanık tarafından şikayetçinin e posta adresinin ele geçirildiği ve bu adrese erişiminin engellendiği olayda *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu"* nun yanı sıra şikayetçinin e-posta adresindeki kişisel veri niteliğinde olan arkadaşlarına ait bilgilerin de ele geçirildiğinden TCK m. 44 hükmü gereğince fikri içtima olarak değerlendirilemeyeceği, her iki fiil için ayrı ayrı sorumlu tutulması gerektiği belirtilmiştir.[520]

Yine Yargıtay 12. Ceza Dairesi'nin bir kararında sanığın tamir için kendisine bırakılan bilgisayardaki fotoğrafları ve Messenger programında kullanılan e posta adres ve

[516] Dülger, 362.
[517] Erdoğan, s.237.
[518] Dülger, s.360.
[519] Erdoğan, s.237.; Koca/Üzülmez, s.907.
[520] Yargıtay 12. Ceza Dairesi'nin 08.09.2014 tarihli ve E:2014/11398, K:2014/17253 sayılı Kararı, https://www.lexpera.com.tr/, erişim tarihi: 14.08.2023.

şifreleri mesleğinin sağladığı kolaylıktan yararlanarak bir flash diske aktardığı, bu e-posta ve şifreyi kullanarak katılanın Messenger hesabını açtığı ve kendisini arkadaş olarak eklediği olayda TCK m. 136/1 ve TCK m.244/2'den ayrı ayrı cezalandırılması gerektiğine karar verilmiştir.[521]

Fikri içtima bakımından incelendiğinde ise TCK m.244/1 ve TCK m.244/2 düzenlenen suçlarda fikri içtima da mümkündür. Örneğin bir kişi başka bir kişi ile internet vasıtasıyla görüştüğü sırada birden üçüncü kişi tarafından bilgisayara virüs atağı gerçekleştirilirse ve bilgisayar devre dışı hale geçerse bu TCK m. 124 hüküm altına alınan haberleşmenin engellenmesi suçu ile TCK m. 244/1'de düzenlenen suç arasında fikri içtima ilişkisi kurulabilir.[522]

TCK m. 244/1 ve 244/2, dördüncü fıkranın bir unsuru olup bileşik suç oluşturmaktadır. Zira bir bilişim sistemindeki verileri başka bir yere göndererek veya verileri değiştirerek yahut bozarak haksız çıkar sağlandığında TCK m. 244/4 hükmündeki suç işlenmiş olacaktır.[523] Nitekim Yargıtay 8. Dairesi'nin bir kararında da TCK m. 244/4 hükmünün bileşik suç olduğu ifade edilmiştir.[524]

VII. SUÇLARIN NİTELİKLİ HALİ

TCK m. 244/3'e göre aynı maddenin birinci ve ikinci fıkralarında düzenlenen suçların banka veya kredi kurumu ya da kamu kurum veya kuruluşuna ait bilişim sistemleri üzerinde işlenmesi halinde verilecek ceza yarı oranında arttırılmaktadır.[525]

Söz konusu nitelikli halin düzenlenmesinin sebebi bu kurumları bilişim sistemleri vasıtasıyla yürüttükleri kamu hizmeti nedeniyle toplumu oluşturan bireylerin mağdur edilmesinin daha ağır bir yaptırıma bağlanması hassasiyetinden kaynaklanmaktadır.[526]

Buna karşın öğretide bazı yazarlar söz konusu nitelikli halin yalnızca kamu kurum veya kuruluşları ile banka veya kredi kurumuna indirgenmesini eleştirmiştir. Zira bir şirket veya işletme için de sistemin işleyişinin engellenmesinin önemli olduğu, dolayısıyla

[521] Yargıtay 12. Ceza Dairesi'nin 07.04.2014 tarihli ve E:2013/15899, K:2014/8411 sayılı Kararı, https://www.lexpera.com.tr/, erişim tarihi:14.08.2023.
[522] Özbek ve diğ, s.1012.
[523] Koca/Üzülmez, s.826.; Aynı görüşte Özbek ve diğ, s.1012,. Karşı görüşte Taşkın, s.33.
[524] Yargıtay 8. Ceza Dairesi'nin 11.06.2020 tarihli ve E:2017/21566, K:2020/13171 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:08.08.2023.
[525] Erdoğan, s.229.
[526] Koca/Üzülmez, s. 816.

hükmün yalnızca kamu kurum ve kuruluşlar ile banka ve kredi kuruluşları ile sınırlı olmaması gerektiğini vurgulamışlardır. Öte yandan birinci ve ikinci fıkrada belirtilen suçların tamamına aynı artırım oranın uygulanmaması gerektiğini de belirtmişlerdir.[527]

Yargıtay 8.Ceza Dairesi'nin 29.04.2014 tarihli ve E:2013/9376, K:2014/10958 sayılı Kararına konu olayda sanık, katılana ait eczane şifresi ile Sosyal Güvenlik Kurumunun sistemine girmiş ve katılanın eczanesine kayıtlarındaki reçete bilgilerini silmiştir. Yargıtay ise TCK'nın 244. maddesinin üçüncü fıkrası uyarınca cezanın arttırılması gerektiği gözetilmemesini hukuka aykırı bulmuştur.[528]

VIII. YAPTIRIM, SORUŞTURMA VE KOVUŞTURMA

TCK'nin 244. maddesinin birinci fıkrasındaki fiilleri gerçekleştiren fail, *"bir yıldan beş yıla kadar hapis cezası"* ile cezalandırılır. TCK'nin 244. maddesinin ikinci fıkrasındaki fiilleri gerçekleştiren fail ise *"altı aydan üç yıla kadar hapis cezası ile cezalandırılır"*. Bu suçlar, şikayete tabi olmayıp re 'sen soruşturulur ve kovuşturulur.[529]

Burada önemle belirtmek gerekir ki TCK'nin 244. maddesinin birinci fıkrasındaki yaptırımın daha ağır nitelikte oluşudur. Esasen bu durum bilişim sisteminin, içindeki veriye nazaran daha önemli olduğu fikrine dayanmaktadır. Buna karşın verinin bilişim sisteminden daha değerli olabilme ihtimali değerlendirilmemiştir. Böyle bir halde cezanın arttırılmasının mümkün olması gerekmektedir.[530] Bu suçlar için görevli mahkeme asliye ceza mahkemesidir.

Bu suçlarda asliye ceza mahkemesi görevlidir. Bununla birlikte 1229 sayılı Hakimler Savcılar Kurulu Kararı nedeniyle 15.12.2021 tarihi itibarıyla bu suçlar hakkında gelen dosyalar ihtisas mahkemelerinde görülecektir. [531]

Öte yandan bu suçlar hakkında yetkili mahkeme belirlenirken suçun işlendiği yer mahkemesinin tespiti zordur. Bu noktada bilişim sisteminin bulunduğu yer ile suçun işlendiği yer aynı ise bir sıkıntı olmasa da farklı yerler olduğunda hangi mahkeme yetkili

[527] Akbulut, 2016, s.41.
[528] Yargıtay 8.Ceza Dairesi'nin 29.04.2014 tarihli ve E:2013/9376, K:2014/10958 sayılı Kararı, www.corpus.com.tr, erişim tarihi:11.05.2021. Aynı yönde Yargıtay 8. Ceza Dairesi'nin 02.06.2015 tarihli ve E:2014/36596, K:2015/18100 sayılı Kararı. (Gül, s.138.)
[529] Özbek ve diğ, s.1012.; Koca/Üzülmez, s.827.
[530] Karagülmez, s.224.
[531]30.11.2021 tarihli ve 31675 sayılı Resmi Gazete, https://www.resmigazete.gov.tr, erişim tarihi: 20.12.2021.

olacaktır? Bu durumda özellikle hareketin gerçekleştiği yer ve neticenin gerçekleştiği yer farklı olduğunda yetkili mahkemenin tespiti zorlaşmaktadır. Bu halde bilişim sisteminin bulunduğu yerin mahkemesinin mi yoksa neticenin meydana geldiği yerin mahkemesinin mi yetkili olacağı sorunu ile karşılaşılmaktadır. Bir görüş fail tarafından suça konu fiilin gerçekleştiği yer belli ise o yer mahkemesi değil ise fiil sebebiyle neticenin meydana geldiği yer mahkemesi yetki mahkeme olacağı yönündedir.[532] Bir diğer görüş ise suçun işlenmesinde araç olarak kullanılan bilişim sisteminin bulunduğu yer mahkemesi ile üzerinde hedef bilişim sisteminin bulunduğu yer mahkemesinin de yetki olması gerektiği yönündedir. Bu görüş farklılıkları 7331 sayılı Kanun ile 08.07.2021 tarihinde Ceza Muhakemesi Kanunu'nun 12. maddesine eklenen altıncı fıkra uyarınca *"Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir."* denilmek suretiyle çözüme kavuşturulmuştur. Böylece hem suçun işlendiği yer mahkemesi hem de mağdurun yerleşim yerindeki yer mahkemesi yetkili kılınmıştır. [533]

Tüzel kişiler bakımından ise TCK'nin 20. maddesi uyarınca suçun faili olamayacakları yalnızca güvenlik tedbirleri uygulanabileceği açıkça belirtilmiştir. TCK'nin 60. maddesinin altıncı fıkrası uyarınca da güvenlik tedbirlerinin uygulanabilmesi için "*kanunun ayrıca belirttiği hallerde"* uygulanacağı belirtilmiştir. Türk Ceza Kanunu'nun bilişim alanında suçlar başlıklı bölümünde *"Tüzel kişiler hakkında güvenlik tedbiri uygulanması"* başlıklı 246. maddesi düzenlenmiş olup TCK m. 243, 244, 245 ve 245/A' da belirtilen suçlar, tüzel kişiler tarafından işlendiği takdirde ilgili güvenlik tedbirlerinin uygulanacağı anılan maddede hüküm altına alınmıştır. Bu halde tüzel kişiler hakkında kendilerine özgü güvenlik tedbirlerinden olan iznin iptali ve müsadere uygulanabilecektir. [534]

[532] Özbek ve diğ, s.1013.; Akbulut, Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme, s.50.
[533] Dülger, s.381-382.
[534] Erdoğan, s.174-176.

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SİSTEMLERİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU

I. GENEL OLARAK

TCK'nin 244. maddesinin dördüncü fıkrasında *"Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur"* demek suretiyle *"Bilişim sistemi aracılığıyla haksız çıkar sağlamak suçu"* düzenlenmiştir.[535] Her ne kadar öğretide bazı yazarlar [536] bu fıkrada düzenlenen hükmün birinci ve ikinci fıkralarında yer alan suç tiplerinin nitelikli hali olduğunu belirtmekteyseler de bazı yazarlar da bizim de katıldığımız görüşe göre bu maddeyle bağımsız bir suç düzenlenmiştir.[537] Nitekim Yargıtay da söz konusu fıkranın ayrı bir suç olduğu kanaatindedir.[538]

5237 sayılı Kanun'da madde gerekçesi *"Bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet*

[535] Bu suç için öğretide genellikle "Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu" ibaresi veya bu ibareye benzer nitelikte tanımlamalar yapılmıştır. Bkz. Gül, s.143, Koçoğlu, s.164. Koca/Üzülmez *"Bilişim sistemi aracılığıyla haksız yarar sağlama suçu"* s.921, Tezcan/Erdem/Önok *"Haksız yarar sağlama suçu",* Erdoğan *"Bilişim sistemi aracılığıyla kendisinin ya da başkasının yararına haksız bir çıkar sağlama suçu",* Karagülmez *"244. Madde kapsamındaki suçlar nedeniyle haksız çıkar sağlama suçu"* s.221, Ketizmen *"Bilişim sistemleri aracılığıyla yarar sağlama suçu"* s.144, Gürler "*Bilişim sistemini kullanarak haksız yarar sağlama suçu"* s.153.

[536] Pallı, s.167. Özbek ve diğ, s.993.

[537] Hafızoğulları/Özen, s.457., Akbulut, 2016, s.6., Dülger, s.364., Erdoğan s.244.Karşı görüşte Ketizmen s.156.

[538] Nitekim Yargıtay Ceza Genel Kurulu'nun 25.11.2014 tarihli ve E:2013/448, K:2014/524 tarihli Kararı'nda *"Uyuşmazlığa esas dördüncü fıkrada ise, birinci ve ikinci fıkralardaki fiillerin gerçekleştirilmesi suretiyle kişinin haksız çıkar sağlaması eyleminin, başka bir suçu oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasını gerektiren bir suç olarak cezalandırılacağı yaptırıma bağlanmıştır."* denilmek suretiyle ayrı bir suç olarak değerlendirildiği görülmektedir. Yine Yargıtay 11. Ceza Dairesi'nin 22.01.2008 tarihli ve E:2007/8423, K:2008/117 sayılı Kararı'nda da *"... eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan M.Ç.'ye yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle 5237 SY. TCK.nun 244/4 maddesine uyan suçu oluşturduğu gözetilmeden...,"* denilmek suretiyle ayrı bir suç olarak ele alınmıştır. Yargıtay 11. Ceza Dairesi'nin 26.05.2011 tarihli ve E:2010/11811, K:2011/2564 sayılı Kararı da aynı yöndedir. https://www.corpus.com.tr, erişim tarihi:21.08.2023.

suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir."[539] şeklindedir.

Dülger'e göre söz konusu hüküm ile gerekçesi arasında çelişki bulunmaktadır. Zira dördüncü fıkrada *"başka bir suç oluşturması halinde"* denildiği halde, madde gerekçesinde *"fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir"* denilmesi çelişki oluşturmaktadır. [540]

Hafızoğulları/Özen ise bu hususta *"tamamlayıcı bir hüküm"* olduğunu ve hükmün gerekçesinde belirtilen biçimde anlaşılması gerektiğini ifade etmiştir.[541]

Koca-Üzülmez ise, bu suçun TCK m. 244/1 ve 2. fıkralarından bağımsız ayrı bir suç olduğuna katılmakla beraber, yapısı itibarıyla bileşik ve dolayısıyla çok hareketli suç olduğunu belirtmiştir. Öte yandan diğer bir özelliğinin ise tali norm niteliğinde olduğunu ifade ederek somut olayda bilişim sistemleri vasıtasıyla haksız çıkar sağlama fiili gerçekleştiği takdirde, öncelikle fiilin hırsızlık, dolandırıcılık, güveni kötüye kullanma veya zimmet suçları gibi başkaca bir suça sübut verip vermediği araştırılması gerektiğini, gerçekleştirilen fiil bahsi geçen suçlardan birisinin tanımına uymuyorsa 244. maddenin dördüncü fıkra hükmünün uygulanabileceğini belirtmiştir.[542]

II. SUÇUN HUKUKİ KONUSU

Öğretide TCK'nin 244. maddesinin dördüncü fıkrasındaki suçun hukuki konusu bakımından da farklı görüşler bulunmaktadır.

Özbek-Doğan-Bacaksız ise önceki başlıklarda da belirttiğimiz üzere TCK'nin 244. maddesindeki suçların karma hukuki niteliği haiz olduğunu belirtmişlerdir. Bu hukuki değerlerden birincisinin sistemin ve verinin güvenilirliği, ikincisinin ise TCK m.244/4 gereği mülkiyet hakkı olduğunu ifade etmiştir. Zira söz konusu maddenin ilk iki fıkrasındaki fiillerin gerçekleştirilmesi ile haksız çıkarın oluştuğu gözetildiğinde söz konusu suç ile bir bütün halinde mülkiyet hakkı da suçun hukuki konusu olarak gösterilmesinin gerekliliği vurgulanmıştır. [543]

[539] Karagülmez, s.221-222.
[540] Dülger, s.364-365. Aynı görüşte Ketizmen, s.177.
[541] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.458.
[542] Koca/Üzülmez, s.818-819.
[543] Özbek ve diğ, s.995-996.

Yenidünya-Değirmenci, bu maddede düzenlenen suçların hukuki konusu bakımından karma bir nitelikte olduğunu, anılan maddedeki suçun genel anlamda bir maddi zarar ya da faydaya yol açtığı, bu nedenle de korunan hukuki değerin ekonomik çıkarla ilintili olduğunu belirtmiştir. Bununla birlikte, suça ilişkin fiilin özel hayatın gizliliği, kişi ve haberleşme hürriyetini etkilediğinden bahisle bu çıkarları zedeleme tehlikesi barındırdığından Kanun koyucunun bu tehlikeyi önlemek istediğini belirtmiştir.[544]

Dülger de söz konusu suç ile korunan hukuki değer bakımından kanun maddesinin tanımına göre bir değerlendirme yaparak karma niteliği bulunduğunu ifade etmiştir. Buna göre maddede belirtilen suçlarda ceza yaptırımı ile korunan hukuki değerin bilişim sistemi, bilişim sistemindeki veriler ve diğer unsurların güvenli bir şekilde çalışabilmesi olduğunu ifade etmiştir.[545] Dördüncü fıkrasında ise birinci ve ikinci fıkrasında belirtilen fiiller nedeniyle haksız bir çıkar sağlanması gerektiğinin altını çizerek söz konusu çıkarın nasıl bir çıkar olduğunun açıkça ifade edilmediği belirtmiştir. Yazara göre çıkarın tanımı belirtilmediğinden fail tarafından sağlanan tüm maddi ve manevi yararın bu kapsama girmektedir.[546]

Koca-Üzülmez ise madde hükmünde belirtilen haksız çıkarın doğrudan kişilerin malvarlığına yönelik olduğunu ifade etmiştir. Zaten maddenin amacının da bu yönde olduğunu belirtmiştir. Dolayısıyla yazarlar tarafından söz konusu maddeni ilk iki fıkrasındaki fiillerin işlenmesi suretiyle sağlanan haksız çıkar söz konusu olduğundan ilgili fıkralardaki suçların koruduğu hukuki değer ile birlikte malvarlığı hukuki değerinin de korunduğu ifade edilmektedir.[547]

Artuk-Gökcen-Yenidünya ise bu suç tipiyle korunan değeri, özel hayatın gizliliğinden malvarlığı haklarına kadar geniş bir kapsamda değerlendirmiştir. Öte yandan kişilerin maddi ve manevi haklarının da korunduğu ifade edilmiştir.[548]

Erdoğan ise gerekçe de dikkate alındığında esasen birinci ve ikinci fıkradaki neticelere sebebiyet verecek fiillerin gerçekleştirilmesiyle haksız bir çıkar sağlanması halinde verilerin kişi veya mal statüsünde olmayacağından hırsızlık ve dolandırıcılık suçunun oluşamayacağı, dolayısıyla Kanun koyucu tarafından hem bir tali norm olarak

[544] Yenidünya/Değirmenci, s.93.
[545] Dülger, s.335.
[546] Dülger, s.365.
[547] Koca/Üzülmez, s.926.
[548] Artuk/Gökcen/Yenidünya, s.4671. Aynı görüşte Soyaslan, s.678.

hem de boşluğun doldurulması için TCK m.244/4'ü tatbik edildiğini belirtmiştir. Böyle olunca bu suç ile ilk ilki fıkra ile korunan hukuki değerin yanında yarar sağlanabilecek her türlü değer koruma altına alınmıştır. Bu noktada sağlanılan yararın miktarı ve seviyesinin hiçbir önemi bulunmamaktadır.[549]

Buna karşın ilgili madde hükmü ve gerekçesinde de açıkça ifade edildiği üzere *"dolandırıcılık, hırsızlık, güveni kötüye kullanma ve zimmet"* gibi suçlar olduğu takdirde TCK m.244/4 hükmü uygulanamayacaktır. Özellikle dolandırıcılık ve hırsızlık malvarlığına karşı suçlar olup malvarlığı değeri korunduğu gibi bu suçlar fail tarafından mağdurun malvarlığında bir azalma meydana getirilmektedir. Bu halde dolandırıcılık ve hırsızlık suçu oluşmadığı halde TCK m. 244'ün devreye girmesi mümkündür. Bununla birlikte haksız çıkarın maddi bir yarar olmaması halinde TCK m. 244/4 uygulama alanı bulabilecektir. Dolayısıyla mağdurun manevi yararının da korunduğu söylenebilmektedir.[550]

Nitekim Yargıtay 8. Ceza Dairesi'nin bir kararında madde hükmünde düzenlenen *"haksız çıkarın"* kavramının maddi yararların yanında herhangi bir başkaca menfaatin elde edilmesi hallerini de kapsadığını açıkça belirtmiştir. Buradaki önemli olan husus fail tarafından elde edilen menfaatin haksız olduğunun bilinmesi gerekliliğidir. [551]

Bu noktada öğretide söz konusu fıkranın farklı bir hukuki değeri koruması nedeniyle başka bir maddede düzenlenmesi gerektiği de belirtilmiştir.[552]

Biz TCK'nin 244. maddesinde suçla korunmak istenen hukuki değerin bir başka deyişle suçun hukuki konusunun çalışmamızın önceki başlıklarında da ifade edildiği üzere karma nitelikli olduğu kanaatindeyiz. Zira bu maddenin *"Topluma Karşı Suçlar"* başlığı altında düzenlenmesinin sebebi esasen bilişim sisteminin güvenilirliği sağlanarak toplum düzeni ve kamu barışını sağlanılması olduğu gibi özel hayatın ve sırların gizliliğinin, mülkiyet hakkının korunmasının ve haberleşme özgürlüğünün sağlanılmasının da istenmesidir.

---

[549] Erdoğan, s.251.
[550] Dülger, s.366.
[551] Yargıtay 8. Ceza Dairesi'nin 11.06.2020 tarihli ve E:2017/21566, K:2020/1371 sayılı Kararı, Yeldan, s.97.
[552] Yazıcıoğlu, Recep Yılmaz: *"Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi",* Yeditepe Üniversitesi Hukuk Dergisi, İstanbul 2005, C: II, S:2, s.410.

III. SUÇUN MADDİ KONUSU

Öğretide bu suçun maddi konusu hakkında yazarların farklı görüşleri bulunmaktadır. Bir başka görüş ise suçun konusunu yalnızca bilişim sistemi veya bu sistemdeki verilerin oluşturduğunu belirtmiştir.[553] Buna karşın biz bu görüşe katılmamaktayız. Zira söz konusu suçun maddi konusunun *"haksız çıkar"* oluşturduğu kanaatindeyiz.

Nitekim öğretide de yazarlar tarafından da söz konusu suçun maddi konusunu "*hukuka aykırı yarar"* oluşturduğu ifade edilmektedir. [554] Bu hususta failin hukuka aykırı yararı elde etme kastının da bulunması gerektiği de belirtilmiştir.[555]

Yazarlar tarafından bu yarar, genellikle malvarlığı değerlerinin suçun konusunu oluşturduğu belirtilmişse de ekonomik getirisi olan veya manevi yararların bu kapsama girip girmediği hakkında öğretide tartışma bulunmaktadır.

Bir görüşe göre suçun maddi konusunun yalnızca çıkar oluşturduğu ifade edilmektedir. Çıkarın sözlük anlamı olan *"dolaylı bir biçimde elde edilen kazanç"* tanımından hareketle failin ya da başkasının malvarlığında elde edilecek artış veya borçlarında bir azalışa sebebiyet veren her türlü çıkarın suçun maddi konusunu oluşturduğunu ifade etmektedirler. Bir başka deyişle bu görüşü savunanlara göre suçun maddi konusu maddi bir kazanç olabileceği gibi ekonomik durumunu iyileştirecek bir menfaat de olabilecektir. Buna karşın haz veya manevi yararın bu suçu oluşturmayacağı ifade edilmektedir.[556]

Katıldığımız bir diğer görüşe göre ise söz konusu haksız çıkarın mali, ekonomik getirisi olan veya manevi bir çıkar da olabileceği vurgulanmıştır.[557] Nitekim Yargıtay 11. Ceza Dairesi tarafından verilen bir kararda sanığın alkol muayenesine itiraz neticesinde hastaneye götürülmesi ve ceza almamasını sağlamak adına hastanedeki bilişim sistemlerine müdahale etmek suretiyle verileri değiştirdiği olayda fail TCK m.244/4 hükmünden sorumlu tutulmuştur.[558] Bu itibarla, her ne kadar uygulamada genellikle suçun konusunu

[553] Artuk/Gökcen/Yenidünya, s.4673.
[554] Dülger, s.368.; Koca/Üzülmez, s.927.
[555] Dülger, s.368.
[556] Koca/Üzülmez, s.927.; Tezcan/Erdem/Önok, s.1170.
[557] Özbek ve diğ, s.1010.; Dülger, s.368.; Gerçeker, s.2210.
[558] Yargıtay 11. Ceza Dairesi'nin 15.01.2013 tarihli ve E:2010/12162, K:2013/658 sayılı Kararı, Akbulut, s.253.

malvarlığı değerlerinin oluşturduğu görülmekte ise de bizce manevi çıkarların da bu madde kapsamında değerlendirilmesi gerekmektedir. Manevi çıkardan kasıt hukuka aykırı çıkardır.

IV. FAİL VE MAĞDUR

Dolayısıyla fail bakımından hükümde *"kişi"* ibaresi kullanıldığından fail, bilişim sistemine müdahalede bulunan herkestir.[559] Buradaki herkesten kasıt gerçek kişidir. Zira tüzel kişiler fail olamayacaktır. TCK m. 244'ün ilk iki fıkrasında belirtilen açıklamalar bu suç için de geçerlidir.

Kanun koyucunun bu suçları Kanun'un *"Topluma Karşı Suçlar"* kısmında ele alması nedeniyle kamu idaresinin suçun mağduru olması haklı bir görüş olmakla birlikte gelişen ve değişen teknoloji nedeniyle kanaatimizce söz konusu suçların mağdurunun karma nitelikte olduğunu söylemek mümkündür. [560] Bu nedenle bilişim sistemleri aracılığıyla haksız çıkar sağlanmak adına müdahalede bulunulan "*Bilişim sistemi veya veriler üzerinde hak sahibi"* suçun mağdurudur. Tarafımızca hak sahibi, kavramının kullanılması bilinçlidir. Zira bilişim sisteminin veya verinin sahibinin sahibi kavramının kullanılması, bunlar üzerinde sadece hak sahibi olanlar açısından yetersiz kalacaktır.[561] Örneğin bilişim sistemindeki verilere zarar verilerek verinin maliki veya veri taşıma aracının ya da bilişim sisteminin maliki aynı kişi olmayabilir. Bu halde suçun mağdurunu yalnızca malik veya zilyet olarak sınırlandırmak suçun mağdurunun belirlenmesinde sorun yaratabilecektir. Dolayısıyla suçun mağduru olmak için bilişim sisteminin veya verinin ilgilisi olmak yeterlidir.[562] Bununla birlikte TCK'nin 244. maddesinin ilk iki fıkrasında belirtilen hususlara sebebiyet veren fiillerle kişinin üzerinden haksız çıkar sağlanan ve bilişim sistemindeki işleyişi veya verileri zarar gören kişiler farklı olduğu durumda bilişim sistemindeki işleyişi veya verileri zarara gören kişiler de suçun mağduru olacaktır.[563]

Bu noktada bazı yazarlar, bilişim sisteminin kullanılmasından zarar gören kimseler bu suçun mağduru olduğu gibi bilişim sisteminin güvenilirliğinin sağlamakla yükümlü

[559] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.451.
[560] Nitekim Yargıtay 8. Ceza Dairesi'nin 15.05.2014 tarihli ve E:2013/2959, K:2014/12412 sayılı Kararı'nda *"Sanığın, müştekilere karşı TCK'nın 244/2 maddesi kapsamında kalan eylemlerinin birbirinden bağımsız ayrı suçları oluşturduğu halde tek suç kabul edilerek mahkumiyet hükmü kurulması bozmayı gerektirmiştir"* olarak hükmedilmiştir. Görüldüğü üzere söz konusu kararda her bir mağdura karşı fiilin farklı bir suça vücut verdiği, suç sabit ise ayrı ayrı mahkumiyet kararı verilmesi gerektiği vurgulanmıştır.
[561] Erdoğan, s.253.
[562] Dülger, s.367.
[563] Koca/Üzülmez, s.823.

kamu idarelerinin de bu suçun mağduru olduğunu belirmektedirler. Bu görüşü savunanlara göre, suçun doğrudan zarar verdiği kimseler suçtan zarar gören olarak kabul edilmektedir.[564] Biz suçun mağdurunun yalnızca kamu idareleri olduğu görüşüne suçun karma hukuki niteliği olduğundan katılmıyoruz.

V. SUÇUN UNSURLARI

A. FİİL

TCK m. 244/4'te kanunun bahsettiği *"yukarıda tanımlanan fiiller"* denilmek suretiyle ilgili maddenin birinci ve ikinci fıkrasına atıf yapılmıştır. Bu doğrultuda söz konusu suçun seçimlik hareketli suç mu yoksa serbest hareketli bir suç mu olduğu hususu tartışmalıdır. Bazı yazarlara göre bu suç, seçimlik hareketli suçtur. Zira bu görüşe göre, TCK m. 244/4 hükmünün de fiil unsuru, birinci ve ikinci fıkrada düzenlenen fiillerdir. Dolayısıyla bu suçun sübut etmesi için *"bir bilişim sisteminin işleyişini engellemek veya bozmak, bilişim sistemindeki verileri yok etmek, değiştirmek veya erişilmez kılmak, sisteme ver yerleştirmek, var olan verileri başka yere göndermek"* fiillerinden herhangi birinin veya birkaçının gerçekleştirilmesinin gerekliliğini vurgulamışlardır.[565]

Buna karşın bazı yazarlar ise Kanun koyucu tarafından fıkrada *"tanımlanan fiillerin işlenmesi suretiyle"* ibaresine yer verilmesi ve bu suretle söz konusu fillerden birinin ya da birkaçının yapılarak failin kendisine veya başkasına haksız çıkar sağlaması fiiliyle sübut eden suçun seçimlik hareketli suç olmasının yanında bağlı hareketli bir suç olduğunu belirtmektedir. Zira bu görüşe göre, fail tarafından bilişim sistemine veya veriye karşı bir fiil gerçekleştirilmekte ve söz konusu fiil neticesinde haksız bir çıkar söz konusu olmaktadır. Bir başka deyişle bağlı bir hareket yapıldıktan sonra neticenin gerçekleşmesi halinde suç işlenmiş olacaktır.[566]

Bizim de katıldığımız bir başka görüşteki yazarlar ise söz konusu maddenin birinci ve ikinci fıkrasında düzenlenen hususların netice olarak kabul etmeleri nedeniyle TCK m. 244/4'te belirtilen suçu serbest hareketli suç olarak değerlendirmektedir. Bu görüşe göre ilgili maddenin dördüncü fıkrası, birinci ve ikinci fıkraya atıf yapması nedeniyle suç serbest hareketli suç olmaktadır. Zira bu görüşe göre fail, serbest bir harekette bulunarak sistemin işleyişini bozmak veya engellemek veyahut sistemdeki verileri bozmak,

[564] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.457.
[565] Dülger, s.368. Artuk/Gökcen/Yenidünya, s.4673.
[566] Hafızoğulları/Özen, s.458.

değiştirmek, erişilmez kılmak, yok etmek, verileri başka yere göndermek veya sisteme veri yerleştirmek suretiyle kendisine veya başkasına haksız çıkar sağlarsa bu suç oluşacaktır. Meğerki başka bir suçu oluştursun…[567]

Söz konusu suçun zarar suçu mu yoksa tehlike suçu mu niteliğinde olduğu hususu da tartışmalıdır. Bazı yazarlar kanun maddesi incelendiğinde birinci ve ikinci fıkradaki fiiller neticesinde bir haksız çıkar elde edilmesi düzenlenmişse de aynı zamanda bu fiil nedeniyle bir zarar meydana gelmesi gerektiği belirtilmediğinden bir tehlike suçu olduğunu ifade etmişlerdir. Bu görüşü savunanlar esasen fail tarafından bu filler gerçekleştirildiğinde bir zararın oluşacağı açıktır ancak suçun oluşması için ortada bir zararın var olup olmadığının araştırılmayacağını belirtmişlerdir.[568]

Bazı yazarlar ise hukuka aykırı olarak elde edilen yararın söz konusu fillerin işlenmesi neticesinde mağdurun zarar görmesi sonucunu doğurduğunu ifade etmektedirler.[569] Bazı yazarlar ise bu suçun oluşması için failin kendisine veya bir başkasına haksız çıkar sağlamasının yeterli olduğunu, ayrıca mağdurun zarara uğramasının aranmadığını vurgulamışlardır. Buna karşın aynı yazarlar bu durumun suçun zarar suçu olmadığı anlamına gelmeyeceğini de belirtmektedir.[570]

Kanaatimizce, bu maddede düzenlenen suçun tehlike suçu olduğu görüşüne katılmak mümkün değildir. Bizce söz konusu maddede düzenlenen suçta, failin gerçekleştirdiği fiiller neticesinde haksız bir çıkar sağlanması aranmıştır. Dolayısıyla suçun oluşması için öncelikle TCK'nin 244. maddesinin birinci veya ikinci fıkralarındaki neticeleri gerçekleştirecek fiillerin işlenmesi gerekmekte, akabinde bu fiiller neticesinde suçun konusunu oluşturan maddi veya manevi çıkar meydana gelmesi gerekmektedir. Dolayısıyla suç, zarar suçu olup neticelidir. Manevi çıkardan kastedilen hukuka aykırı çıkardır.

Öte yandan elde edilen çıkarın haksız olması gerekmektedir. Gerçekten Kanun koyucu suçun oluşması için *"haksız bir çıkar sağlanmasını"* aramaktadır. Buradaki haksız çıkardan kastedilen "*hukuka aykırı yarardır".* Yarar elde edilmemesi durumunda TCK m. 244/4 oluşmayacaktır, bu halde TCK m. 244/1 veya TCK m. 244/2. fıkradaki suçlar söz

[567] Erdoğan, s.252-253. Bu hususa ilişkin değerlendirmelerimiz çalışmamızın ilgili maddenin birinci ve ikinci fıkralarında düzenlenen suçların fiil unsuru başlıklarında ayrıntılı olarak izah edilmiştir.
[568] Dülger, s.374.
[569] Taşkın, s.58.; Aynı yönde Hafızoğulları/Özen, Topluma Karşı Suçlar, s.458.
[570] Koca/Üzülmez, s.373.

konusu olabilecektir.[571] Bu nokta failin bu hukuka aykırı çıkarı kendisine veya başkasına sağlamasının bir önemi bulunmamaktadır. Suçun oluşumu için her halde hukuka aykırı bir çıkar sağlanması yeterli olacaktır.[572]

Gerçekten somut olaydaki hukuka aykırı yararın somut olarak *tespiti* önemlidir. Yargıtay 8. Ceza Dairesi'nin kararına[573] konu olayda sanıklar tarafından okuldaki ders notlarını ve devamsızlıklarını değiştirmek maksadıyla Milli Eğitim Bakanlığına tabi okullarda kullanılan e-okul sistemine ait şifreleri ele geçirerek girilmiştir. Temyize konu kararda failler tarafından bilişim sitemine karşı yapılan fiillerin devamsızlık durumlarının ve notlarının düzeltilmesi dışında başkaca yarar elde edildiği ifade edilmişse de Yargıtay tarafından söz konusu menfaatlerin ne olduğu ve kim tarafından sağlandığı tartışılmadan yetersiz gerekçe ile 244. maddenin dördüncü fıkrası gereğince cezalandırılmasının kanuna aykırı olduğu belirtilmiştir.

Yine Yargıtay 8. Ceza Dairesi'nin kararına konu olayda sanık ile katılan şirket arasındaki sözleşmeye dayanılarak katılan şirketin hesabından düzenlemeler yapılmış ve bu düzenlemeler uygulamaya geçirilmiştir. Buna karşın katılan şirket ile sanık arasında yaşanan mali sıkıntı nedeniyle sanık, yayını askıya alıp durdurduğu gibi şifreleri de değiştirerek katılan şirket tarafından banka hesaplarına girişi engellenmiştir. Bu halde Yargıtay tarafından sanığın hukuki menfaat elde ettiğinin ispatlanamaması nedeniyle TCK m. 244/2'deki suçun oluştuğu belirtilmiştir.[574]

Aynı Daire'nin başka bir kararında da sanık tarafından uydu alıcısı satılmakta olup satış yaptığı kişilere cardsharing fiili ile şifreli olan Lig TV kanalının şifresini kırmak suretiyle satış yaptığı olayda, Yargıtay tarafından sanığın eyleminin TCK m. 244/4'ü değil, haksız yararlanma suçunu oluşturduğuna hükmedilmiştir.[575]

İlgili suçtaki bir diğer önemli unsur ise suça konu fiil, *"başka bir suç oluşturmaması"* gerekmektedir. Bu hükme göre fiil, TCK veya diğer özel kanunlardaki başkaca bir suçu oluşturmaması aranmaktadır. Fiil, başka bir suçu örneğin zimmet,

[571] Dülger, s.373.
[572] Soyaslan, s. 679.
[573] Yargıtay 8. Ceza Dairesi'nin 15.02.2017 tarihli ve E:2016/3794, K:2017/1405 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi: 17.05.2023.
[574] Yargıtay 8. Ceza Dairesi'nin 14.02.2023 tarihli ve E:2020/11290, K:2023/520 sayılı Kararı, https://legalbank.net, erişim tarihi: 17.05.2023.
[575] Yargıtay 8. Ceza Dairesi'nin 04.03.2020 tarihli ve E:2018/12677, K:2020/10872 sayılı Kararı, Yeldan, s.99.

dolandırıcılık, güveni kötüye kullanma ve hırsızlık suçlarından birini oluşturmaktaysa bu halde ilgili madde hükmü uygulanacak, 244/4 hükmü uygulama alanı bulamayacaktır.[576] Dolayısıyla bu suç diğer suçun içinde eritilmiş olacaktır.[577]

Bu noktada önemle belirtmek gerekir ki söz konusu hükmün gerekçesinde "*bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, filin daha ağır cezayı gerektiren başka bir suçu oluşturmaması gerekmektedir"* ibareleri bulunmaktadır. Burada önemle belirtmek gerekir ki Kanun koyucu tarafından *"daha ağır ceza"* kavramı kullanılmıştır. Oysa Kanun koyucu tarafından söz konusu madde hükmünde böyle bir ibare kullanılmamıştır. Böyle olunca kanun ile gerekçe arasındaki uyumsuzluk bulunsa da gerekçenin bağlayıcı olmaması karşısında suçta ve cezada kanunilik ilkesi çerçevesinde fiil başka bir suçu oluşturmakta ise kuşkusuz diğer hükmün uygulanması gerekmektedir. Buna karşın söz konusu madde bakımından "*daha ağır başka bir suç oluşturmaması"* olarak revize edilmesi maddenin getiriliş amacına uygun olacağı gibi gerekçe ile arasındaki uyumsuzluğun giderilmesini de sağlayacaktır.[578]

B. HUKUKA AYKIRILIK

Suçun hukuka aykırılık unsuru bakımından ilk iki fıkra hakkında ifade ettiğimiz hususlar bu suç için de geçerlidir. Zira TCK m. 244/4 hükmünde 1. ve 2. fıkraya atıf yapılmaktadır. Dolayısıyla söz konusu iki fıkra bakımından hukuka uygunluk nedeni sayılan haller bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu için de geçerlidir.[579] Dolayısıyla bu suçta da ilgilinin rızası, kanun hükmünün icrası ve görevin ifası hukuka uygunluk nedenleridir.[580]

Bu noktada ilgilinin rızası bakımından rızayı verecek kişi bakımından "*ilgili*" nin kim olduğunun belirlenmesi gerekmektedir. Burada kanaatimizce bilişim sistemi veya veri üzerinde hak sahibi[581] olan kişinin rızası gerekmektedir. Eğer hak sahibinin sağlanacak çıkara yönelik olarak rızası varsa fiil suç teşkil etmeyecektir.

---

[576] Özbek ve diğ, s.1006.
[577] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.458.
[578] Soyaslan, s. 680.; Erdoğan, s.264.
[579] Erdoğan, s.258.
[580] Koca/Üzülmez ilgilinin rızası ve kanun hükmünün icrasının bu suç bakımından mümkün olmadığını ifade etmektedir. Koca/Üzülmez, s.825.
[581] Hak sahipliği kavramından yalnızca malikin anlaşılmaması gerektiği, bilişim sistemi ve bilişim sistemindeki veriler üzerinde hak sahibi olan kişi olarak değerlendirilmesi gerektiği *"Fail ve Mağdur"* başlığı altında ayrıntılı olarak izah edilmiştir.

Buna karşın her zaman bilişim sisteminin veya verinin maliki ile çıkarın gerçek sahibi aynı kişi olmayabilir. Bu halde bilişim sistemin veya verinin malikinin rızası failin fiilini hukuka uygun hale getirmeyecektir. Dolayısıyla hukuka uygunluk nedenlerinden biri olan ilgilinin rızası hakkında somut olaya göre değerlendirme yapılarak karar verilmesi gerekmektedir.

C. KUSURLULUK

Suç ancak doğrudan kastla işlenebilmektedir. Taksirle işlenememektedir. Fail ilgili maddenin birinci ve ikinci fıkrasındaki neticelere sebebiyet verecek fiilleri işleyerek kendisine veyahut bir başkasına hukuka aykırı bir fayda sağladığını bilmelidir. Dolayısıyla haksız bir fayda olduğunu bilmediği takdirde suç oluşmayacaktır. Bu nedenle fiilin haksız olduğunu bilmesi gerekliliği bu suçun olası kastla işlenebilmesini engelleyecektir.[582]

Öğretide bazı yazarlar tarafından suçun oluşması için failde yalnızca suç işleme kastının varlığı gerektiğini[583], bazı yazarlar[584] tarafından ise kanun hükmünde *"kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlanması"* ibareleriyle yalnızca suç işleme kastının değil, haksız bir çıkar sağlama kastının da yani özel bir saikin bulunması gerektiği ifade edilmektedir. Bizce bu suçta özel bir saikin aranması gerekmez. Zira kanun metninde açıkça bu amaca yönelik bir ibare bulunmamaktadır. Dolayısıyla fail tarafından hükmün ilk iki fıkrasında düzenlenen hususları meydana getirecek elverişli hareketlerin haksız çıkar sağlayacak şekilde bilerek ve isteyerek işlenmesi suçun oluşumu için yeterlidir.

D. KUSURLULUĞU KALDIRAN NEDENLER

Çalışmamızın önceki bölümlerinde de ifade edildiği üzere, "*fiille fail arasındaki psişik/manevi bağı ortadan kaldıran nedenler, hata ve manevi cebir ve (istenememezlik ilkesi)"* kusurluluğu kaldıran nedenlerdendir. Bu nedenler fiilin iradiliğini ortadan kaldırmakta ve fiilin bilinmemesinden kaynaklanmaktadır.

TCK'nin 244. maddesinin dördüncü fıkrasında düzenlenen söz konusu suçun birinci ve ikinci fıkraya atıf yapması nedeniyle ilgili kısımda tarafımızca yapılan

[582] Koca/Üzülmez, s. 825; Erdoğan, s.258.; Aksi görüşte, Tezcan/Erdem/Önok, s.1171.
[583] Erdoğan, s.256.; Dülger, s.376.
[584] Kurt, s.175.; Karagülmez, s.218.; Yılmaz, s.89.

açıklamalar geçerlidir. Bununla birlikte çalışmamızın bu bölümünde TCK m. 244/4 hükmü uyarınca kusurluluğu kaldıran nedenler özetle incelenecektir.

1. Fiille Fail Arasındaki Psişik/Manevi Bağı Ortadan Kaldıran Nedenler

TCK m. 244/4 hükmündeki suça sebebiyet verecek fiillerde kendinde olmama veya mücbir sebebin varlığı nedeniyle fail ile fiil arasındaki psişik bağın kesilmesi bir başka deyişle fiilin iradiliğinin ortadan kalkması mümkün değildir. Dolayısıyla bu suçta mücbir sebep ve kendinde olmama hallerinin kusurluluğu kaldıran neden olarak kabul edilmesi olası görünmemektedir.

TCK'nin 28. maddesinde düzenlenen maddi cebir de söz konusu suç bakımından bir kusurluluğu kaldıran nedendir. Bu halde maddi cebir etkisinde kalan bir kişi suç oluşturan fiili işlediği takdirde suç oluşmayacaktır.[585] Buna karşın kişinin üzerinde maddi cebir uygulayan kişinin etkisinden kurtulma imkanı varsa bu halde ortada maddi cebir veya şiddet olmayacaktır.[586] Bu halde "*Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu"* nda maddi cebir vasıtasıyla suçun işlenmesi ihtimal dahilindedir. Bu halde maddi cebir etkisinde kalan kişi suç işlemiş olmayacak ancak suçu işleyen üzerinde maddi cebir uygulayan kişi fail olarak cezalandırılacaktır.

2. Hata

TCK m. 4 hükmünde *"ceza kanunlarını bilmemek mazeret sayılmaz"* denilmek suretiyle kural üzerinde hata düzenlenmiştir. Bu doğrultuda bilişim sistemi aracılığıyla haksız çıkar sağlama suçunda hukuki hata yapılması mümkün değildir. Dolayısıyla suçta bir bilişim sisteminin işleyişine veya verilerine karşı müdahalede bulunan ve bu suretle haksız çıkar sağlayan gerçek kişi failin bu fiilin suç olduğunu bilmediğini iddia edemez.

Fiil üzerinde hata bir başka deyişle fiili hata, suç teşkil eden fiilin unsurlarında meydana gelen hata olup söz konusu suçta fiil üzerinde hata mümkündür. Örneğin bir kimsenin esasen yetkisiz iken kendisini yetkili zannederek suça konu fiili işlemesi halinde bu hata fail lehine değerlendirilecektir.[587]

---

[585] Artuk, Mehmet Emin/Gökcen, Ahmet/ Yenidünya, Ahmet Caner: Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara 2020, s.583-585.
[586] Hafızoğulları/Özen, Türk Ceza Hukuku Genel Hükümler, s. 292.
[587] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.458.

Hukuka uygunluk nedenlerinde hatada da söz konusu suçta kusurluluğu kaldıran neden olarak gösterilebilmektedir. Örneğin bilişim sistemi üzerinde menfaati olan kişinin rızası var olduğu düşünülerek TCK m. 244'ün ilk iki fıkrasındaki suçlara sebebiyet verecek fiilleri gerçekleştirerek failin kendisine veya başkasına haksız çıkar sağladığı takdirde fail cezalandırılmayacaktır.

3. Manevi Cebir ve Bu Temelde Kişiden Beklenenin Bulunduğu Koşullarda Kendisinden İstenememesi (İstenememezlik İlkesi)

TCK'nin 28. maddesinde hüküm altına alınan manevi cebir, bu suç bakımından da mümkündür. Buna göre, bilişim sistemleri aracılığıyla haksız çıkar sağlama suçuna ilişkin fiiller fail tarafından manevi cebir altında işlenmekte ise fail söz konusu fiili nedeniyle cezalandırılmayacaktır.

VI. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

A. TEŞEBBÜS

Teşebbüs açısından, bazı yazarlar suça teşebbüsün mümkün olmadığını belirtirken[588] bazı yazarlar da teşebbüsün mümkün olduğunu belirtmişlerdir.[589]

Erdoğan ilk iki fıkradaki neticeleri meydana getirecek fiillerin gerçekleştirilmesiyle haksız bir yarar sağlandığı takdirde suçun tamamlanmış olduğunu ifade etmektedir. Bu sebeple neticesi harekete bağlı bir suç olduğunu ve ancak fiil parçalara bölünebiliyor ise teşebbüsün mümkün olacağını belirtmektedir.[590]

Burada 244. maddenin birinci ve ikinci fıkralarında belirtilen fiillerin gerçekleşmesi ancak *"hukuka aykırı yarar"* sağlanmaması halinin üzerinde durulması gerekmektedir. Öğretide bu durum da tartışma konusudur. Bazı yazarlar tarafından haksız çıkar sağlanamamışsa teşebbüsten söz edilmesinin mümkün olmayacağı kanaatinde[591] iken bazı

[588] Hafızoğulları/Özen, s.458.
[589] Koca/Üzülmez, s.825.; Dülger, s.378.
[590] Erdoğan, s.260. Aynı yönde Doğan, Koray: *"Bilişim Suçları ve Yeni Türk Ceza Kanunu"*, Hukuk ve Adalet Eleştirel Hukuk Dergisi, Ekim 2002, Yıl:2, S:6-7. s.305.
[591] Yargıtay 11. Ceza Dairesi'nin 26.03.2009 tarihli ve E:2008/18190, K:2009/3058 sayılı Kararı'nı belirterek Özbek, Veli Özer/ Kanbur, Nihat/ Doğan, Koray/ Bacaksız, Pınar/ Tepe, İlker, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara 2010, s.925.

yazarlar, haksız çıkarın sağlanamaması halinde suçun teşebbüs aşamasında kaldığı iddia olunmaktadır.[592]

Teşebbüs aşamasında kaldığı görüşüne göre haksız çıkar sağlanamaması halinde failin kastının ne olduğu önem arz etmektedir. Zira bu görüşe göre, fail haksız çıkar sağlamak amacıyla 244. maddenin birinci ve ikinci fıkralarında belirtilen fiillerini işlemekte ise bu halde failin dördüncü fıkrasına teşebbüsten sorumlu tutulması gerekmektedir. Buna karşın failde haksız çıkar sağlamak amacı yok ise bu halde 244. maddenin birinci ve ikinci fıkralarına göre cezalandırılması gerektiği ifade edilmektedir.[593] Failin kastına göre cezalandırılması gerektiği görüşüne katılmaktayız. Zira suçun unsurlarından biri de "*kusurluluk*" tur. Bu unsur dikkate alınmaksızın faili yalnızca TCK m. 244'ün birinci veya ikinci fıkralarından sorumlu tutmak suç genel teorisi kapsamında hatalı olacaktır.

Yargıtay 11. Ceza Dairesi'nin bir kararında söz konusu maddenin dördüncü fıkrasında belirtilen suçun hukuka aykırı bir yarar elde edildiği takdirde oluşacağı dolayısıyla sanığın amaçladığı yarara henüz ulaşamadan yakalandığı olayda Yargıtay, fiilin teşebbüs aşamasında kaldığı gözetilmeden suçun tamamlandığı gerekçesiyle fazla ceza tayinini kanuna aykırı bulmuştur.[594]

B. İŞTİRAK

Suça iştirak açısından birinci ve ikinci fıkralarda düzenlenen suçlardaki olduğu gibi bir özellik bulunmamaktadır.[595]

C. İÇTİMA

Bilindiği üzere, Türk Ceza Kanunu'nun ikinci kısmının beşinci bölümünde *"Suçların İçtimaı"* başlığı altında 42. maddede bileşik suç, 43. maddede zincirleme suç ve 44. maddede ise fikri içtima kurumları hükme bağlanmıştır. Söz konusu suçların içtimaı kurumlarına ilişkin detaylı açıklamalar, çalışmamızın TCK'nin 244. maddesinin ilk iki fıkrasına ilişkin *"İçtima"* başlığı altında detaylıca izah edilmiştir.

---

[592] Koca/Üzülmez, s.825; Erdoğan, s.260-261.
[593] Koca/Üzülmez, s.826.
[594] Yargıtay 11. Ceza Dairesi'nin 15.01.2013 tarihli ve E:2010/12162, K:2013/658, https://www.corpus.com.tr, erişim tarihi:12.05.2023.
[595] Erdoğan, s.262.; Koca/Üzülmez, s.826.; Özbek ve diğ, s.1012.

Çalışmamızın devamında *"Bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu"* bakımından zincirleme suç , bileşik suç ve fikri içtima kurumları incelenecektir.

"*Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu"* na ilişkin hüküm incelendiğinde, ilgili maddenin birinci ve ikinci fıkralarına atıf bulunmaktadır. Bu halde TCK m. 244/4'te hüküm altına alınan suçun gerçekleşmesiyle TCK'nin 244. maddesinin birinci ve ikinci fıkrasında hüküm altına alınan suçlar, söz konusu suçun unsuru olduğundan TCK m. 244/4'teki suç bileşik suçtur.[596]

Dolayısıyla TCK m. 42' de belirtilen *"Bu tür suçlarda içtima hükümleri uygulanmaz"* hükmü uyarınca birinci ve ikinci fıkralardaki suçlarla dördüncü fıkradaki suç arasında gerçek içtima hükümleri uygulanmayacaktır.[597]

Fail tarafından değişik zamanlarda bir kişiye karşı aynı suç işleme kararının icrasıyla TCK m. 244/4'teki suçu oluşturacak fiilleri yapması halinde TCK m. 43'te düzenlenen zincirleme suç hükümleri uygulanabilecektir.[598] Örneğin sistemin çalışmasını engellemek veya sisteme veri yerleştirmek için aynı suç işleme kararının icrası ile belirli zaman aralıklarında bilişim sistemine birçok harekette bulunulabilir.[599]

Nitekim Yargıtay'ın bir kararında sanık üniversite öğrenci işlerinde şef olup gıda mühendisliğinde okuyup yan dal olarak bir başka mühendislik dalından ders alan üç öğrencinin bir dersten aldığı notları bir başka derse işlenmesi fiilinde, Yargıtay tarafından YCGK'nin 09.12.2007 tarihli ve E:2007/11-40, K:2007/200 sayılı Kararı'nda belirtilen bilişim sistemine girilerek bazı notların değiştirildiği olayda bilişim suçunun oluşacağı vurgulanmıştır. Kararda sanığın fiilinin görevi kötüye kullanma suçu oluşturup oluşturmayacağı hususunun gözetilmediği ifade edilse de nihayetinde not değişikliğinin aynı günde ve aynı anda yapılması nedeniyle zincirleme suç hükümlerinin uygulanmasının gözetilmemesi gerekçesiyle kararı bozmuştur.[600]

Bununla birlikte TCK'nin 243. maddesinde düzenlenen *"Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma"* suçu ile TCK'nin 244. maddesinde düzenlenen "*Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu"* arasında da içtima

[596] Özbek ve diğ, s.1012.; Koca/Üzülmez, s.992.
[597] Erdoğan, s. 262.
[598] Hafızoğulları/Özen, Topluma Karşı Suçlar, s.458.
[599] Dülger, s.380-381.
[600] Yargıtay 11. Ceza Dairesi'nin 10.01.2013 tarihli ve E:2010/5864, K:2013/8389 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:12.05.2023.

hükümleri bakımından önemi haizdir. Bu kısmı TCK'nin 244. maddesinin ilk iki fıkrasında hüküm altına alınan suçların fikri içtima hükümlerini incelerken detaylıca izah ettiğimizden tekrardan imtina etmekteyiz.

TCK'nin 244. maddesinde *"başka bir suçu oluşturmaması halinde"* ibaresi bulunmaktadır. Bu düzenleme ile asli norm-tali norm ilişkisi kurulmaktadır. Kanun koyucunun bu maddeyi ihdas etmesinin sebebi oluşabilecek boşluğu tamamlamaktır.[601] Dolayısıyla failin fiili bir başka suçu oluşturmaktaysa TCK m. 244/4 hükmü uyarınca sorumlu tutulamayacaktır. Böyle bir durumda fiil hem TCK m. 244/4 hükmünü hem de başka bir suçu oluşturuyorsa fikri içtima hükümleri uygulanamayacaktır.[602]

V. BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇUNUN BENZER SUÇLAR İLE FARKI

Kanun koyucu tarafından bir tali norm olarak düzenlendiği ve dolayısıyla kapsamının daraltıldığı "*Bilişim sistemleri aracılığıyla haksız çıkar sağlama suçu*"yla uygulamada sıkça görülen *"Bilişim sistemleri kullanılmak suretiyle nitelikli hırsızlık suçu"* (TCK m.142/2-e) ve "*Bilişim sistemlerinin banka ve yayın araçlarının sağladığı kolaylıktan faydalanmak suretiyle dolandırıcılık suçu"* (TCK m.158/1-f) arasındaki ilişkide uygulama alanının belirlenmesi önem arz etmektedir.[603] Dolayısıyla "*bilişim sistemi aracılığıyla haksız çıkar sağlama suçu"* ile nitelikli hırsızlık ve nitelikli dolandırıcılık suçlarının yargı kararlarındaki uygulaması öğretideki görüşlerle birlikte izah edilecektir.

A. HIRSIZLIK SUÇU İLE BİLİŞİM SİSTEMİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU

TCK m. 244/4 hükmünde belirtilen "*Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu*"nda çıkarın konusunu taşınır mal oluşturmakta ise madde hükmündeki *"başka bir suçu oluşturmaması"* hali bakımından hırsızlık suçu ile asli norm- tali norm ilişkisinin tartışılması gerekmektedir.[604] Aşağıdaki başlıklarda yargı kararları çerçevesinde bilişim sistemi aracılığıyla haksız çıkar sağlama suçu ile bilişim sistemleri kullanılmak suretiyle nitelikli hırsızlık suçunun uygulaması detaylıca izah edilecektir.

---

[601] Özbek ve diğ, s.1006.
[602] Erdoğan, s.262. Dolayısıyla "*Bilişim sistemi aracılığıyla haksız çıkar sağlama suçu"* ile nitelikli hırsızlık (TCK m. 142/2-e) ve nitelikli dolandırıcılık suçları (158/1-f) arasındaki ilişki de çalışmamızın ilgili kısmında detaylıca izah edilmiştir.
[603] Ketizmen, s.179.
[604] Ketizmen, s.180.

1. Bir Başkasının İnternet Bankacılığında Bulunan Paranın Başka Bir Hesaba Transfer Edilmesi

Bir başkasının internet bankacılığında bulunan paranın bir başka hesaba transfer edilmesi olayında failin TCK m. 142/2-e uyarınca "*bilişim sistemleri kullanılmak suretiyle nitelikli hırsızlık suçu*"ndan mı yoksa TCK m. 244/4 uyarınca "*bilişim sistemleri kullanılmak suretiyle haksız çıkar sağlanması suçu*"ndan mı sorumlu tutulacağı hususunda yargı kararlarında birlik bulunmamaktaydı. Önceden failin başkasına ait banka hesabına internet vasıtasıyla girilerek failin evvelden açtığı sahte hesabına haksız yollarla belirli bir para transfer etmesi, akabinde bu parayı çekmesi olayında Yargıtay 11. Ceza Dairesi'nin bir kararında TCK m. 142/2-e hükmünde düzenlenen hırsızlık suçundan değil, TCK m. 244/4 hükmü uyarınca "*bilişim sistemi aracılığıyla çıkar sağlama suçu"*ndan hüküm kurulması gerektiği belirtilmiştir. [605] Buna karşın Yargıtay 6. Ceza Dairesi o dönemde Yargıtay 11. Ceza Dairesi'nden farklı bir tutum benimsemiştir. Örneğin Yargıtay 6. Ceza Dairesi'nin 02.06.2008 tarihli 555/12249 sayılı kararında sanığın internet bankacılığı kullanan yakınının internet bankacılığına ilişkin şifreyi elde ederek hesap bilgilerine ulaştığı ve yakınının hesabındaki parayı sahte kimlikle açtığı hesaba gönderilmesi olayında, Yargıtay sanığın fiilini hırsızlık suçu olarak nitelendirmiştir. [606]

Buna karşın Yargıtay 11. Ceza Dairesi, 17.11.2009 tarihli YCGK kararı sonrası bu konuda içtihat değiştirmiştir. Yargıtay Ceza Genel Kurul Kararı'nın 17.11.2009 tarihli ve E:2009/11-193, K:2009/268 sayılı Kararı'nda farklı görüşteki daire kararlarına ve uygulamaya açıklık getirmiştir. Söz konusu karara konu olayda faillerin daha önce katılan şirketin internet bankacılığı şifresini hukuka aykırı bir şekilde elde etmeleri ve katılanın internet bankacılığı kullanılarak belirli bir tutarı, sanıklardan birinin hesabına göndermeleri ve aynı gün sanıkların bu parayı çekmeleri söz konusudur. Yargıtay Ceza Genel Kurulu Kararı'nda suçun işlendiği tarihi itibarıyla 765 sayılı Kanuna tabi olduğu, söz konusu fiil ile esasen katılanın malvarlığında azalmaya neden olma bir başka deyişle bilişim sistemindeki verinin bir yerden başka bir yere gönderilmesinin değil, bu verinin temsil ettiği meblağın elde edilmesinin, bir mal edinilmesinin söz konusu olduğunu belirtilmiştir. Ayrıca sanığın katılana ait banka hesabındaki paraya ulaşabilmek için bilişimin bir araç olarak kullanılmasının mecburi olduğu da vurgulanmıştır. Dolayısıyla somut olaydaki fiilin TCK m. 244/4'te belirtilen "*bilişim sistemi aracılığıyla haksız çıkar sağlama suçu*"nu değil

[605] Yargıtay 11. Ceza Dairesi'nin 16.09.2007 tarihli ve 6122/5897 sayılı Kararı, Karagülmez, s.228.
[606] Yargıtay 6. Ceza Dairesi'nin 02.06.2008 tarihli 555/12249 sayılı Kararı, Karagülmez, s.229.

de TCK m. 142/2-e hükmü uyarınca *"bilişim sistemi kullanılmak suretiyle hırsızlık"* suçunu oluşturduğu belirtilmiştir.[607]

Bu karara istinaden Yargıtay bu konuya ilişkin yeni tarihli verdiği kararlarında TCK m. 142/2-e hükmü uyarınca *"bilişim sistemi kullanılmak suretiyle hırsızlık suçunun"* oluştuğuna hükmetmiştir.

Nitekim Yargıtay 8. Ceza Dairesi'nin bir kararında sanık tarafından katılanın banka hesabına hukuka aykırı bir şekilde internet bankacılığı vasıtasıyla girilerek bankada bulunan paranın kendisi tarafından oluşturulan banka hesabına aktarılıp bu paranın çekilmesi olayında TCK m. 142/2-e hükmünde düzenlenen suçun oluştuğuna hükmedilmiştir. Buna karşın Yargıtay Cumhuriyet Başsavcılığı tarafından yapılan itiraz üzerine YCGK tarafından itiraz haklı görülerek bilişim sistemleri kullanılmak suretiyle hırsızlık suçundan hüküm kurulması gerektiğini kararında belirtmiştir.[608]

Öğretide bazı yazarlar fail tarafından mağdura ait internet bankacılığına hukuka aykırı bir şekilde girilerek kendisinin veya bir başkasının yararına olacak şekilde mağdurun parasının başka bir hesaba transfer edilmesi ve bu paranın çekilmesi halinde YCGK kararında da belirtildiği şekilde TCK m. 142/2-e hükmünde düzenlenen suçunun oluştuğuna katılmaktadır. [609]

Nitekim Karagülmez bu konuda TCK m. 244 hükmünün bir tali norm olduğunu ve karara konu olayda yani başkasının internet bankacılığı hesabındaki paranın bilişim sistemi vasıtasıyla bir başka transfer edilmesi olayında bilişim sistemi içerisindeki verinin, para olduğu ve hırsızlık suçu kapsamında bu verinin *"taşınır mal"* statüsü kapsamında değerlendirilmesi gerektiğini belirtmiştir. Dolayısıyla YCGK kararını isabetli bulmuştur.[610]

Yine Koca-Üzülmez de karara katılmaktadır. Yazarlara göre mevcut durumda suçun konusu paradır ve dolayısıyla fail, bilişim sistemini o parayı alabilmek için kullanmıştır.[611]

---

[607] Yargıtay Ceza Genel Kurul Kararı'nın 17.11.2009 tarihli ve E:2009/11-193, K:2009/268 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:11.04.2023.
[608] Yargıtay 8. Ceza Dairesi'nin 28.09.2020 tarihli ve E:2019/19845, K:2020/16153 sayılı Kararı, Yeldan, s.96.
[609] Koca/Üzülmez, s.820.; Şen, Ersan: *"Bitcoin Çalınır mı?"* https://www.haber7.com, erişim tarihi: 13.05.2023.
[610] Karagülmez, s.250.
[611] Koca/Üzülmez, s.821.

Buna karşın bazı yazarlar ise aksi görüştedir.

Nitekim Özbek-Doğan-Bacaksız'a göre TCK m. 244 hükmü, dolandırıcılık ve hırsızlık suçlarına kıyasla daha özel bir normdur. Normun önceliği ilkesi gereğince özel norm bulunmakta iken genel norma gidilmeyecektir. TCK m. 244'te belirtilen suçların ortak özellikleri bilişim sistemi içerisinde işleniyor oluşları ve maddi konularının veri olmasıdır. Dolayısıyla transfer edilen para, malvarlığı değeri olarak kabul edildiği takdirde TCK m. 244 düzenlemesinin hiçbir anlam ifade etmeyeceği dolayısıyla bu durumda *"bilişim sistemi aracılığıyla hırsızlık suçu"* ndan değil de bilişim sistemi aracılığıyla haksız çıkar sağlama suçunun oluşacağını ifade etmektedirler. Yazarlara göre zaten Kanun koyucu bu durumu göz önüne alarak bir nitelikli hal olan banka ve kredi kurumuna ait bilişim sistemlerinde bu suçun işlenmesi halini nitelikli hal olarak düzenlemiştir. [612]

Erdoğan ise YCGK'nın kararını suçun tipiklik unsurunun dışına çıktığı gerekçesiyle eleştirmiştir. Zira verinin bilişim sisteminde bulunan her türlü soyut değer olarak tanımını yaptıktan sonra hırsızlık suçunun oluşabilmesi için ortada bir taşınır malın bulunması gerektiğini ifade etmiştir. Dolayısıyla soyut bir kavram olan verinin hırsızlık suçunu oluşturamayacağını belirtmiştir. Öte yandan hesapta bulunan paranın bir başka hesaba transferi sağlandıktan sonra suçun tamamlanması nedeniyle paranın nakit olarak çekilip çekilmemesinin bir öneminin bulunmadığı da vurgulamıştır.[613]

YCGK kararına karşı azınlık oyu kullanan üye ise öncelikle verinin tanımını "*bilgisayar üzerinde işlem yapılan her türlü şey"* olarak yaptıktan sonra internet bankacılığında parayı temsil eden verinin bir taşınır mal olup olmadığını değerlendirmiştir. Bu hususta "*suçta ve cezada kanunilik ilkesini ve kıyas yasağını"* öngören TCK m. 2 hükmü gerekçe gösterilerek TCK'de verinin bir taşınır mal olarak tanımlanmadığı belirtilmiştir. Bu nedenle var olan verileri başka bir hesaba göndermek suretiyle eylemine uyan TCK m. 244/4 hükmü uyarınca cezalandırılması gerektiğini belirtmiştir.[614]

Gerçekten veri, taşınır mal olarak TCK'de tanımlanmamış olup söz konusu başkasına ait banka hesabındaki paranın bilişim vasıtasıyla bir başka hesaba aktarılması olayında YCGK'nın kararına katılmamaktayız. Zira azınlık oyunda da belirtildiği üzere

[612] Özbek ve diğ, s.1004.
[613] Erdoğan, s.289.
[614] Yargıtay Ceza Genel Kurul Kararı'nın 17.11.2009 tarihli ve E:2009/11-193, K:2009/268 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:11.05.2023.

suçta ve cezada kanunilik ilkesi, kanun ve Anayasa ile koruma altındadır. *"Veri"* çalışmamızın birinci bölümünde de ayrıntılı olarak tanımlanmış olup bilişim sistemi içerisinde bulunan soyut bir kavramdır. Para transferi olayında da *"veri"* esasen bir parayı temsil ediyor ise de bu durum o veriyi hırsızlık suçunun maddi konusu olan *"taşınır mal"* haline getirmeyecektir. Eğer ki her somut olayda verinin temsil ettiği değer dikkate alınarak sanığın eylemine uyan suç tipine karar verilir ise gelişen teknoloji nedeniyle örneğin kripto varlıkların çalınması gibi hallerde suçun kapsamı genişletilerek suçta ve cezada kanunilik ilkesine aykırı uygulamalara sebebiyet verilecektir.[615] Buna karşın kanımızca fiilin ağırlığı nedeniyle TCK'nin 244. maddesinin dördüncü fıkrası ile cezalandırılması da adil olmayacaktır. Dolayısıyla Kanun koyucu tarafından nitelikli hal veya yeni bir suç tipi olarak bu hususun düzenlenmesi gerekmektedir.

2. İnternet Vasıtasıyla Mağdura Ait Kontörlerin Bir Telefondan Diğer Bir Telefona Aktarılması

Bu konuda yukarıda belirtilen YCGK'ye rağmen Yargıtay 13. Ceza Dairesi sanık tarafından internet vasıtasıyla girilen şifre ile mağdurun telefon numarasından bir başka telefon numarasına oradan da şifre aracılığıyla kendi numarasına hukuka aykırı bir şekilde kontör gönderilmesi eyleminin, TCK'nin 244. maddesinin dördüncü fıkrasına göre cezalandırılması gerektiğini belirmiştir. YCGK'nin 25.11.2014 tarihli kararı ile bilişim sistemi kullanılmak suretiyle hırsızlık suçunun oluştuğunu ifade edilmiştir.[616]

Nitekim Yargıtay 8. Ceza Dairesi'nin kararına konu kontör işiyle uğraşan sanığın şikayetçinin internet sayfasındaki şifresini ele geçirerek başka bir hesaba bu kontörlerin gönderilmesi olayında bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun oluştuğu belirtilmiştir. Gerekçede öncelikle kontörü, telefonun kullanılması için gerekli olan, bedeli karşılığında alınan, ekonomik bir değeri olan ve sistemde veri ile temsil edilen şey olarak tanımlanmıştır. Akabinde kontörün başka bir telefona aktarılması fiilinin, işlem nedeniyle bilişim sistemi olan telefonunun sağlıklı ve fonksiyonuna uygun bir şekilde çalışmasında herhangi bir engel olmadığı özellikle belirtilmiştir. Dolayısıyla malvarlığında azalma meydana gelen katılanın rızasının bulunmadığı olayda hırsızlık suçunun oluştuğu

[615] Çalışmamızın devamında bu hususa değinilecektir.
[616] Yargıtay Ceza Genel Kurulu'nun 25.11.2014 tarihli ve E:2013/448, K:2014/524, https://www.corpus.com.tr erişim tarihi: 05.03.2023.

belirtilmiştir. Zira failin burada verinin temsil ettiği kontörü alarak mal edinmek istediği belirtilmiştir.[617]

Yine Yargıtay 8. Ceza Dairesi'nin çok yeni tarihli bir Kararı'nda sanık tarafından katılanın internet sitesine rıza ve bilgi dışı erişim sağlanarak birden çok GSM hattına kontör transfer edilmesi olayında da zincirleme şekilde bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun oluştuğu, dolayısıyla TCK m. 244/4'ten kurulan hükmün hukuka aykırı olduğuna karar verilmiştir.[618],

Görüldüğü üzere Yargıtay şu şekilde önüne gelen bir olayda şu soruların cevaplarını aramakta ve failin fiiline uyan suç tipini belirlemektedir:

- Kontör telefonun kullanılması için gerekli mi?
- Ekonomik bir değer ifade eder mi?
- Veri tanımına uymakta mıdır?
- Failin fiili nedir?
- Failin bu fiilinin sistemin çalışmasına herhangi bir etkisi bulunmakta mıdır?

Bu noktada öğretideki bazı yazarlar aksine banka hesabındaki paranın internet vasıtasıyla transfer edilmesi hukuka aykırı şekilde mal varlığında azalma meydana getirdiğinden kontörün temsil ettiği paranın alınması ile mal edinimi söz konusu olduğunu ifade ederek m. 142/2-e hükmü uyarınca *"bilişim sistemi kullanılmak suretiyle hırsızlık"* suçunun oluştuğunu belirtmektedirler.[619]

Buna karşın katıldığımız bir diğer görüşe göre bazı yazarlar, dış dünyada maddeden var olmayan ancak değeri parayla ölçülebilen kontörün internet vasıtasıyla başka bir yere gönderilmesinin hırsızlık suçu bağlamında değerlendirilmemesi gerektiğini belirtmektedirler. Zira suçun basit hali dahi oluşmamış iken nitelikli halin sübut etmesinden söz etmek mümkün olmadığı ifade edilmektedir. Dolayısıyla bu görüşe göre fail, TCK'nin 244. maddesinin dördüncü fıkrasına göre yaptırıma tabi tutulmalıdır.[620]

[617] Yargıtay 8. Ceza Dairesi'nin 23.09.2020 tarihli ve E:2019/9478, K:2020/15892 sayılı Kararı, Yeldan, s.97.
[618] Yargıtay 8. Ceza Dairesi'nin 15.03.2023 tarihli ve E:2019/25433, K:2022/4436, https://legalbank.net , erişim tarihi:17.05.2023.
[619] Dülger, s.518-519.
[620] Koca/Üzülmez, s.821-822.

3. Oyun Karakterinin Ele Geçirilmesi

Yargıtay kararları, oyun karakterlerinin ele geçirilmesi konusunda TCK m. 244/4 uyarınca "*bilişim sistemi aracılığıyla haksız çıkar sağlama suçu*"nun oluşacağı konusunda istikrar kazanmıştır. Nitekim kanaatimizce de oyun karakterlerinin taşınır bir mal olmaması nedeniyle hırsızlık suçunun maddi konusunu oluşturmayacaktır. Oyun karakterleri, ekonomik bir değer ifade eden, maddi bir varlığı olmayan, alınıp satılabilen bir veri olması nedeniyle bilişim sistemi aracılığıyla haksız çıkar sağlama suçunun maddi konusunu oluşturacaktır.

Nitekim Yargıtay 8. Ceza Dairesi'nin bir gazetede *"Yargıtay'dan oyun karakteri hırsızlığı kararı"* başlığıyla yayımlanan 19.01.2022 tarihli kararında katılanın KNİGHT ONLİNE WORD isimli oyunu Arhaus isimli oyun karakteri ile oynadığı, bu oyunu mail adresi ile bağladığı, sanık tarafından da mail adresine erişilerek katılanın bu mail adresi şifresini değiştirdiği ve oyun karakterine ulaşımının engellendiği olayda TCK'nin 244/4. maddesindeki suçun oluşacağı gözetilmeden karar verilmesini hukuka aykırı bulmuştur.[621]

Yargıtay bir kararında[622] bu fiili hırsızlık suçu bakımından da inceleyerek oyun karakteri ekonomik bir değer ifade ediyor ise de taşınır bir mal olmadığını belirtmiştir. Bununla birlikte oyun karakterlerinin bilgisayar ortamından elde edilen alınıp satılabilen, maddi bir değeri olan veri olduğu da vurgulanmıştır. Ayrıca bulunduğu yerden fiziken de alınmadığı hükme bağlanmıştır. Dolayısıyla hırsızlık suçunun unsurlarının oluşmadığı belirtilmiştir.

Yargıtay 2. C.D'nin 2020 tarihli kararına konu *"Katılanın ...@outlook.com isimli e-posta adresine bağlı... isimli oyuna 29/12/2013 günü kullanıcı adı ve şifresiyle giriş yaparak oyun oynarken saat 15:30 sıraları oyundan atılması sonrasında saat 15:45 sıraları oyuna yeniden giriş yapabilmesi, katılanın e-posta ve oyun hesabına izinsiz girilerek oyun karakteri üzerindeki 2.000 TL'lik 11 adet itemi ile oyun hesabında bulunan 100 TL'lik 5 GB'lık oyun parasının çalınması,"* olayında item[623] ve oyun parasının çalınması bakımından da *"Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar*

[621] Yargıtay 8. Ceza Dairesi'nin 19.01.2022 tarihli ve E:2019/23602, K: 2022/912 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:12.07.2022.
[622] Yargıtay 13. Ceza Dairesi'nin *"20.11.2020 tarihinde www.sgkrehberi.com'da "Oyun karakterlerinin çalınması hırsızlık sayılır mı? İşte Yargıtay'ın kararı..."* başlığıyla yayınlanan 08.01.2020 tarihli ve E:2019/9265, K:2020/258 sayılı Kararı, https://www.corpus.com.tr, erişim tarihi:12.05.2023.
[623] Online oyunlar içerisindeki eşyalara verilen genel bir isimdir. https://wmaraci.com/nedir/item, erişim tarihi:13.04.2023.

sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği" gerekçesiyle TCK m. 244/4 suçu oluştuğu gözetilmeksizin nitelikli hırsızlık suçundan hüküm kurulması hukuka aykırı bulunmuştur.[624]

4. Kripto Paraların Çalınması

Kripto paraların tanımı ve veri kapsamında değerlendirildiğine ilişkin çalışmamızın *"Kripto Paralar"* başlığı altında yapılmıştır. O halde örneğin bir bitcoinin çalınması halinde TCK m. 244'ten mi yoksa hırsızlık suçundan mı cezalandırılacaktır?

Bitcoinin şifrelenmiş bir data oluşu nedeniyle çalınamayacağı iddia edilmekte ise de kişiye ait bilgisayara girilmek suretiyle çalınması mümkün olabilecektir.[625] Bu konuda halihazırda herhangi bir yargı kararı bulunmamaktadır. Dolayısıyla başka kişinin internet bankacılığı hesabındaki paranın bir başka hesaba transfer edilmesi olayı hakkındaki 2009 tarihli Yargıtay Ceza Genel Kurulu'nun verdiği kararı doğrultusunda inceleme yapılması, her ne kadar üst başlıklarda karara katılmadığımızı ifade etmiş isek de bu konudaki Yargıtay kararlarına öncü olabileceğinden söz konusu doğrultusunda inceleme yapılması yerinde olacaktır.[626]

Çalışmamızın üst başlıklarında da ifade edildiği üzere Yargıtay Ceza Genel Kurulu 2009 tarihli kararında, suçun bilişim sistemindeki verilere karşı işlenmediğini, suçun maddi konusunun verinin temsil ettiği para olduğu, bu nedenle failin eylemine uyan nitelikli hırsızlık suçu uyarınca cezalandırılması gerektiği belirtilmişti. Bu gerekçe çerçevesinde kripto varlıkların çalınması halinde, failin nitelikli hırsızlık suçu ile cezalandırılması mümkün olmayacaktır. Dolayısıyla burada TCK m. 244/4 hükmünün uygulama alanı bulduğu söylenebilir.

Buna karşın öğretide de bazı görüşlere göre ekonomik bir değeri olan ve sanal dünyada para olarak nitelendirildiğinden malvarlığı değerinin bulunduğu ve *"bilişim hırsızlığı"* olarak yeni bir suç düzenlenmesi gerektiği ifade edilmekte[627] ise de

---

[624] Yargıtay 2. Ceza Dairesi'nin 13.01.2020 tarihli ve E:2019/11010, K:2020/568 sayılı Kararı, https://www.lexpera.com.tr, erişim tarihi: 13.04.2023.
[625] Şen, *"Bitcoin Çalınır mı?"*
[626] Bkz: Şen, *"Bitcoin Çalınır mı?";* Tarakçıoğlu, Zeynep: *"Kripto Varlıklar ve Ceza Hukuku Sorumluluğu"*, Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, Aralık 2021, C:11, S:2, s.329.
[627] Dülger, Murat Volkan/ Özkan, Onur: *"Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi"* In Prof. Dr. Mehmet Emin Artuk'a Armağan, ed. Mahmut Koca, 963-994, Seçkin Yayınevi Ankara 2020, s.985-986, akt. Tarakçı, s.330-331.; Durdu, s.101-102.

mevzuatımız bu varlıkları para olarak nitelendirmemektedir. Buna karşın başka bir görüşse taşınır mal kavramının esasen iletilebilir, aktarılabilir, transfer edilebilir mal olarak anlaşılması gerektiği, bu halde de kripto varlıkların çalınması fiilinin hırsızlık suçunun nitelikli hali olacağını belirtmektedir.[628]

Bizim görüşümüze göre mevzuatımızın mevcut haliyle kripto varlıklar, bir ödeme aracı olmadığı gibi mahiyeti itibarıyla gayri maddi varlıklardır. Bu noktada kripto varlıkların bir veri olduğunda tartışma bulunmamaktadır.[629] Hırsızlık suçunun konusunun *"taşınır mal"* olduğu ve kripto varlığı parayı temsil etmediği gerçeği karşısında TCK da eyleme en uygun olacak suçun TCK m. 244/4 olacağı kanaatindeyiz. Buna karşın tarafımızca internet bankacılığındaki paranın transferi olayında da ifade edildiği üzere fiilin ağırlığı nedeniyle 244/4'ten cezalandırılması adaletli olmayacağından bu konuda bir düzenleme getirilmesi gerekmektedir.[630]

B. DOLANDIRICILIK SUÇU İLE BİLİŞİM SİSTEMLERİ ARACILIĞIYLA HAKSIZ ÇIKAR SAĞLAMA SUÇU

TCK'nin 244. maddesinin dördüncü fıkrasında belirtilen bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçundaki madde hükmünde *"başka bir suçu oluşturmaması"* hali bakımından dolandırıcılık suçu ile asli norm-tali norm ilişkisinin de tartışılması gerekmektedir.

Yargıtay'ın yakın tarihli kararlarında, TCK m. 158/1-f maddesine düzenlenen *"Bilişim sistemlerinin banka ve yayın araçlarının sağladığı kolaylıktan faydalanmak suretiyle"* dolandırıcılık suçu ile TCK m. 244/4'teki *"Bilişim sistemi aracılığıyla haksız*

---

[628] Şen, *"Bitcoin Çalınır mı?"*

[629] Retornaz Aksoy, E. Eylem: *"Ceza Hukuku Perspektifinden Blokzincir",* (ed. RETORNAZ AKSOY, E. Eylem/GÜÇLÜTÜRK), Orhan Gazi, Gelişen Teknolojiler ve Hukuk I:Blokzincir, Oniki Levha Yayıncılık, İstanbul 2020, s.308.

[630] Şen YCGK kararını isabetli bulmaktadır. Dolayısıyla esasen kripto varlıkların çalınmasının da nitelikli hırsızlık kapsamında olması gerektiğini belirtmiştir. Buna karşı mevcut mevzuatımızda bitcoinin bir dijital veri olduğu gerçeği karşısında eyleme uygun olan suçun TCK m. 244/4 olduğunu, ancak bu konuda bir düzenleme yapılması gerektiğini zira fiilin ağırlığına göre mevcut ceza normlarının yetersiz kalacağını şu şekilde ifade etmiştir: *""bitcoin" türü bir sanal malvarlığının çalınmasının kapsamına girebileceği yegane ceza hükmü, bizce TCK m. 244/3 değil, m. 142/2-e'dir. Çünkü bu son hüküm, bilişim sisteminin kullanılması suretiyle bir başkasına ait malvarlığının çalınmasını suç olarak düzenlemiştir. Bu fikre karşı, hırsızlık suçunu tanımlayan TCK m. 141'in "bitcoin" türü sanal paraların çalınması eylemini suç saymaya yeterli olmadığı, ayrıca TCK m. 244/3'ün bilişim sisteminde var olan verilerin başka yere gönderilmesi eylemini özel olarak saydığı, bu hükmün "bitcoin" türü sanal paraların çalınması eylemine daha uygun düştüğü, çünkü "bitcoin" türü sanal değerlerin birer djital veri olduğu, ancak bu konuda hırsızlık suçu kapsamında "kanunilik" ilkesine uygun düşecek bir suç tanımının yapılmasının vaktinin geldiği, aksi halde gelişen bilim ve teknik ile internet karşısında ceza normlarının yetersiz kalacağı söylenebilir."* (Şen, *"Bitcoin Çalınır mı?")*

çıkar sağlama suçu" arasındaki farkı, fiilin *"KİME"* veya *"NEYE"* karşı işlendiğine göre değerlendirilmektedir. Buna göre ortada bir kişiye karşı, *"hile ve desise içerikli fiil"*, bilişim sistemi kullanılarak işlenmekte ve bunun sonucunda haksız bir yarar elde edilmekte ise bu halde TCK 158/1-f maddesinde düzenlenen suç oluşacaktır.[631]

Örnek vermek gerekirse fail tarafından bir başkasının MSN şifresi ele geçirilmesinin akabinde mağdurun arkadaş listesindeki kişiler ile internet vasıtasıyla kurduğu iletişimde, hesap sahibiymiş gibi kendisine para havalesi yapılmasını istemiş ve bu sayede haksız bir yarar elde etmişse bu halde nitelikli dolandırıcılık suçundan bahsedilmesi mümkündür.[632]

Yargıtay 8. Ceza Dairesi'nin yeni tarihli bir kararına konu olayda sanık tarafından katılan firmaya ait internet sitesindeki ürünleri, sitenin kaynak kodlarına değişiklik yapmak suretiyle hileli hareketlerle 0.01 TL bedel ile almıştır. Firma bu durumu fark etmeyerek söz konusu ürünleri sanığa göndermiştir. Bu olayda Yargıtay tarafından satış bedelinin çok altında olan ürünleri satın alarak menfaat sağlayan sanığın *"bilişim sistemlerinin banka ve kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçunu*" işlediği, dolayısıyla TCK m. 244/4 hükmünden cezalandırılmaması gerektiği belirtilmiştir.[633]

Yargıtay 11. Ceza Dairesi, sanık tarafından önceden kurulan bir düzenekle ATM cihazının içinde mağdurun kartının kalmasının sağlandığı, sanığın ATM kulübesine yerleştirilen çağrı merkezinin telefon numarasını aratarak banka görevlisi izlenimi veren kişi tarafından birden çok kez şifrenin girilmesi, bu sırada sanığın şifreyi öğrenmesi, sonrasında kartı yuttuğunun bilgisiyle şikayetçinin ATM'den ayrılmasının sağlandığı ve sanığın elde ettiği bilgilerle şikayetçiye ait parayı çektiği olayda nitelikli dolandırıcılık suçunun işlendiği sonucuna varılmıştır.[634]

Dolayısıyla TCK m. 244/4 hükmünde açıkça *"başka bir suçu oluşturmaması"* şartı getirildiğinden Yargıtay'ın yukarıda belirtilen kararlarında da görüldüğü üzere hileli davranışlarla bilişim sistemleri kullanılarak haksız yarar elde edilmiş ise bu halde nitelikli

[631] Özbek ve diğ, s.1007-1008.
[632] Özbek ve diğ, s.1008.
[633] Yargıtay 8. Ceza Dairesi'nin 10.05.2022 tarihli ve E:2019/26683, K:2022/6848 sayılı Kararı, https://legalbank.net, erişim tarihi:17.05.2023.
[634] Yargıtay 11. Ceza Dairesi'nin 24.04.2012 tarihli ve E:2012/7571, K:6376 sayılı Kararı. (Karagülmez, s.262.)

dolandırıcılık suçundan hüküm kurulmaktadır. Zira bu halde nitelikli dolandırıcılık suçu sübut etmektedir.

VI. YAPTIRIM, SORUŞTURMA VE KOVUŞTURMA

TCK'nin 244. maddesinin dördüncü fıkrası uyarınca faile *"iki yıldan altı yıla kadar hapis cezası ve beşbin güne kadar adli para cezası"* uygulanacaktır. Bununla birlikte bu suç da birinci ve ikinci fıkradaki suçlar gibi şikayete tabi olmayıp re 'sen soruşturulur ve kovuşturulur.[635]

Bu suçta asliye ceza mahkemesi görevlidir. Bununla birlikte 1229 sayılı Hakimler Savcılar Kurulu Kararı nedeniyle 15.12.2021 tarihi itibarıyla bu suç hakkında gelen dosyalar ihtisas mahkemelerinde görülecektir. [636]

Öte yandan bu suçlar hakkında yetkili mahkeme belirlenirken suçun işlendiği yer mahkemesinin tespiti zordur. Bu noktada bilişim sisteminin bulunduğu yer ile suçun işlendiği yer aynı ise bir sıkıntı olmasa da farklı yerler olduğunda hangi mahkeme yetkili olacaktır? Bu durumda özellikle hareketin gerçekleştiği yer ve neticenin gerçekleştiği yer farklı olduğunda yetkili mahkemenin tespiti zorlaşmaktadır. Bu halde bilişim sisteminin bulunduğu yerin mahkemesinin mi yoksa neticenin meydana geldiği yerin mahkemesinin mi yetkili olacağı sorunu ile karşılaşılmaktadır. Bir görüş fail tarafından suça konu fiilin gerçekleştiği yer belli ise o yer mahkemesi değil ise fiil sebebiyle neticenin meydana geldiği yer mahkemesi yetki mahkeme olacağı yönündedir.[637]

Bir diğer görüş ise suçun işlenmesinde araç olarak kullanılan bilişim sisteminin bulunduğu yer mahkemesi ile üzerinde hedef bilişim sisteminin bulunduğu yer mahkemesinin de yetki olması gerektiği yönündedir. Bu görüş farklılıkları 7331 sayılı Kanun ile 08.07.2021 tarihinde Ceza Muhakemesi Kanunu'nun 12. maddesine altıncı fıkra eklenerek çözüme kavuşturulmuştur. Buna göre *"Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir."* denilmek suretiyle suçun

[635] Özbek ve diğ, s.1012-1013.; Koca/Üzülmez, s.827.
[636] 30.11.2021 tarihli ve 31675 sayılı Resmi Gazete, https://www.resmigazete.gov.tr, erişim tarihi: 20.12.2021.
[637] Özbek ve diğ, s.1013.; Akbulut, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s.50.

işlendiği yer mahkemesi ile birlikte mağdurun yerleşim yerindeki yer mahkemesi de yetkili kılınmıştır. [638]

Tüzel kişiler bakımından ise TCK'nin 20. maddesi uyarınca suçun faili olamayacakları yalnızca güvenlik tedbirleri uygulanabileceği açıkça belirtilmiştir. TCK m. 60/6 hükmü uyarınca da güvenlik tedbirleri uygulanabilmesi için "*kanunun ayrıca belirttiği hallerde"* uygulanacağı belirtilmiştir. Türk Ceza Kanunu'nun bilişim alanında suçlar başlıklı bölümünde *"Tüzel kişiler hakkında güvenlik tedbiri uygulanması"* başlığı altında 246. madde düzenlenmiş olup TCK m. 243, 244, 245 ve 245/A' da belirtilen suçlar, tüzel kişiler bünyesinde işlendiği takdirde ilgili güvenlik tedbirlerine hükmedileceği anılan maddede belirtilmiştir. Bu halde söz konusu tüzel kişiler hakkında kendilerine özgü güvenlik tedbirlerinden olan iznin iptali ve müsadere uygulanabilecektir. [639]

[638] Dülger, s.398-383.
[639] Erdoğan, s.174-176.

SONUÇ

Bilgi Çağı olarak adlandırılan dönem, çağımızın en önemli dönemlerinden biridir. Teknolojinin gelişmesi diğer alanlarda olduğu gibi hukuk alanında da önemli gelişmelere sebebiyet vermiştir. Özellikle Bilgi Çağı'nın getirdiği avantajların yanında ceza hukukundaki suçların işlenişinde kolaylıklar sağlanması ve yeni suç türlerinin de ortaya çıkması söz konusudur. Bilişim suçları, günümüzde sıklıkla karşılaşılan suç türleri arasında yer almaktadır. Gelişen teknoloji ve değişen dünya nedeniyle bilişim suçlarının işlenme şekilleri, konuları ve yargı kararları bakımından yeni değişiklikler olmaktadır. Bu nedenle çalışmamızda bilişim suçlarından biri olan Türk Ceza Kanunu'nun *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"* başlıklı 244. maddesinde düzenlenen suçlar incelenmiş ve ilgili suçlara ilişkin değerlendirmeler ve önerilerde bulunulmuştur.

Bilişim suçları sayesinde uluslararası ve ulusal düzeyde çalışmalar yapılmış olup gelişen teknoloji ve değişen dünya düzeninde mevzuatta her geçen gün geliştirilmesi gereken hususlar bulunduğu kanaatine varılmıştır.

Çalışmamızın ilk bölümünde bilişim, bilişim sistemlerine ilişkin temel kavramlar, bilişim suçu tanımlanmıştır. Bu bilgiler çerçevesinde bilişim suçuna ilişkin genel esaslar üzerinde durulmuştur. *Bilişim* kavramı bakımından öğretide birçok tanımlama yapıldığı görülmektedir. Bu hususta yazarlar tanımlama yaparken verilerin saklanabilmesi, işlenebilmesi ve aktarılabilmesi unsurlarında ortak paydada buluşmaktadır. Birçok yazar tarafından bilgisayarın bilişimi kapsadığı ifade edilse de kanımızca bilişimin bilgisayarı da kapsayıcı bir özelliği bulunmaktadır. *Bilişim sistemi ve bilişim alanı* bakımından ise her ne kadar madde başlığında *"Bilişim Alanı"* kavramının kullanımına katılmasak da Türk Ceza Kanunu'nda yerinde bir tercih olarak *"Bilişim sistemi"* kavramının kullanımı tarafımızca olumlu değerlendirilmiştir.

Bilişim sistemi kavramlarında ise bilgisayar, veri ve internet incelenmiştir. *Bilgisayarlar* bakımından öğretide birçok tanımlama yapılmış olup mevzuatımızda herhangi bir tanımlama bulunmamaktadır. Bu noktada TCK'de kıyas yasağı ve suçta ve cezada kanunilik ilkesi gereğince boşluk bırakılmaması gerektiği için bir tanımlama yapılması ihtiyacı bulunmaktadır. Ancak bu tanımlama yapılırken gelişen ve değişen dünya düzeninde mümkün olduğunca daraltıcı bir yorumdan kaçınılması gerekmektedir. *Verinin,* uluslararası ve ulusal mevzuatta *"bilgisayar verisi"* olarak sınırlandırıldığı

görülmektedir Oysa Kanun koyucunun ilgili kanun maddesindeki amacının *"bilişim sistemi verileri"* olduğu kanaatindeyiz. *İnternet* ise bir bilgisayar ağı olup ağlar arasında en bilinendir. İnternet vasıtasıyla bilişim suçlarının işlenişlerinin kolaylaştığı söylenebilir.

Çalışmamızın ilgili bölümün devamında ise *"Bilişim Suçu Kavramı ve Bilişim Suçlarına İlişkin Genel Özellikler"* belirtilmiştir. Öğretide bu alanlardaki tanımlamalarda *"siber suç", "sanal suç", "bilgisayar suçu"* gibi birçok kavram kullanılmışsa da TCK'de *"bilişim suçu"* kavramının kullanılması bizce de yerinde olmuştur. Bu doğrultuda öğretide birçok sınıflandırma yapılmıştır. Ancak biz Kanun sistematiğine göre bu suçları, bilişim alanında suçlar, bilişim yoluyla işlenmesi suçun nitelikli hali olan suçlar, bilişim yoluyla işlenen diğer suçlar olarak ayırmakta fayda görmekteyiz.

Bilişim suçlarının artması, bu suçların önlenmesi ve cezalandırılması konusunda birçok ülkenin hukuk sistemini değiştirmesine neden olduğu görülmektedir. Ülkemiz mevzuatında da bu süreç 765 sayılı Kanun ile başlamış olup 5237 sayılı TCK'de ve diğer başkaca kanunlarda yapılan düzenlemelerle devam etmiştir.

Bu doğrultuda çalışmamızın devamında ise TCK'nin *"Bilişim Alanında Suçlar"* başlıklı onuncu bölümünde düzenlenen suçlar belirtilmiş olup çalışmamız bilişim suçları arasında en sık görülen suç tiplerini barındıran *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* başlıklı 244. maddesiyle sınırlandırılmıştır.

Söz konusu TCK m. 244 hükmü ile bizce esasen üç suç tipi düzenlenmiştir. İlgili maddenin birinci fıkrasında bilişim sisteminin işleyişine müdahalenin, ikinci fıkrasında bilişim sistemindeki verilere müdahalenin, dördüncü fıkrasında da birinci ve ikinci fıkradaki neticelere sebebiyet verecek fiillerle failin kendisine veya başkasına haksız çıkar sağlaması halinin suç olarak düzenlendiği kanaatindeyiz. Bir başka deyişle söz konusu madde hükmü ile bilişim sistemlerinin ve bilişim verilerinin çeşitli yollarla bozulması, engellenmesi ve değiştirilmesi neticesinde haksız bir çıkar elde edilmesini yaptırıma bağlanmıştır.

Bu kanaat doğrultusunda tarafımızca ikinci fıkrada düzenlenen hususlara dikkat edildiğinde maddenin başlığı ile uyum sağlamamaktadır. Zira madde başlığında yalnızca verileri *"yok etme veya değiştirme"* ibarelerine yer verilirken ikinci fıkrada bunların yanı sıra *"erişilmez kılma, sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme"* ibareleri de bulunmaktadır. Yine ilgili maddenin dördüncü fıkrası

incelendiğinde birinci ve ikinci fıkralardaki suçların işlenmesi nedeniyle failin kendisine veya bir başkasına haksız çıkar durumu da madde başlığında yer verilmemiştir. Dolayısıyla kanaatimizce TCK'nin 244. maddesi "*Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"* başlığı ile madde başlığı altında düzenlenen suçları tanımlamak noktasında yetersiz kalmaktadır.

Bu bilgiler çerçevesinde tarafımızca TCK'nin 244ç maddesinin birinci, ikinci ve dördüncü fıkrası Kanun koyucu tarafından ayrı suçlar şeklinde ele alınmış olup çalışmamızın ikinci bölümünde aralarında benzerlik bulunması sebebiyle TCK'nin 244. maddesinin birinci ve ikinci fıkralarında düzenlenen suçlar birlikte incelenmiştir.

TCK'nin 244. maddesinin birinci ikinci ve dördüncü fıkrasındaki suçun hukuki konusunun karma nitelikli olduğu kanaatindeyiz. Zira "*Sistemi engelleme, bozma verileri yok etme veya değiştirme"* başlıklı TCK'nin 244. maddesi *"Topluma Karşı Suçlar"* başlığı altında düzenlenmesi sebebiyle esasen bilişim sisteminin güvenilirliği sağlanarak toplum düzeni ve kamu barışını sağlanılması ile birlikte bizce özel hayatın ve sırların gizliliğinin, mülkiyet hakkının korunmasının ve haberleşme özgürlüğünün sağlanılması da istenilmektedir.

Konusu bakımından ise özellikle *"bilişim sistemi"* ve *"bilişim verileri"* bakımından suçta ve cezada kanunilik ilkesi ile kıyas yasağı uyarınca değişen ve gelişen teknoloji nedeniyle bir tanımlama ihtiyacı bulunmaktadır. Kanun koyucu tarafından bir tanımlama yapılmalıdır. Ancak bu tanımlamanın da sınırlandırıcı olmaması gerektiği kanaatindeyiz. Bu durum yargı makamlarının daha sağlıklı karar vermesi açısından da önem arz etmektedir.

Gerçekten bu nedenle verinin, taşınır mal olarak TCK'de tanımlanmaması nedeniyle başkasına ait banka hesabındaki paranın bilişim vasıtasıyla bir başka hesaba aktarılması olayında verinin temsil ettiği şeyin para olması nedeniyle TCK m.142/2-e hükmü uyarınca faili nitelikli hırsızlıktan sorumlu tutan YCGK'nın kararına katılamamaktayız. Zira kararın azınlık oyunda da belirtildiği üzere suçta ve cezada kanunilik ilkesi de göz önünde bulundurulduğunda *"veri"* esasen bir parayı temsil ediyor ise de bu durum o veriyi hırsızlık suçunun maddi konusu olan *"taşınır mal"* haline getirmeyecektir. Eğer ki her somut olayda verinin temsil ettiği değer dikkate alınarak sanığın eylemine uyan suç tipine karar verilir ise gelişen teknoloji nedeniyle örneğin kripto

varlıkların çalınması gibi hallerde suçun kapsamı genişletilerek suçta ve cezada kanunilik ilkesine aykırı uygulamalara sebebiyet verilecektir. Dolayısıyla hırsızlık suçunun konusunun *"taşınır mal"* olduğu, bankadaki paranın her ne kadar parayı temsil etmesi ve kripto varlıkların parayı temsil etmediği gerçeği karşısında TCK da eyleme en uygun olacak suçun TCK m. 244 hükmü olacağı kanaatindeyiz.

Buna karşın her ne kadar TCK m. 244 hükmü uyarınca sorumlu tutulması gerektiği kanaatindeysek de kanımızca fiilin ağırlığı nedeniyle TCK'nin 244. maddesi ile cezalandırılması da adil olmayacaktır. Dolayısıyla Kanun koyucu tarafından nitelikli hal veya yeni bir suç tipi olarak bu hususun düzenlenmesi gerekmektedir.

Tüm bu açıklamalar neticesinde açıkça görülmektedir ki bilişim hukuku ve ceza hukuku olarak bu tür suçların önlenmesi ve cezalandırılması için multidisipliner bir yaklaşım ile hareket edilmelidir. Söz konusu suçlarla mücadele kapsamında etkili önlemler alınması gerekmektedir. Bu çerçevede ulusal yasal düzenlemelerin yanı sıra uluslararası iş birliği de suçların önlenmesi ve cezalandırılması için önemlidir.

"Bilişim mahkemeleri" adı altında bu konuda uzman kişileri barındıran özel mahkemeler kurulmalıdır. Bilişim suçları hakkında mevcut mevzuatın yetersizliği, kavram kargaşası ve uygulama farklılıkları gibi sorunlar nedeniyle özel bir kanun çıkarılmalıdır. Ayrıca hukuk alanında uzmanlaşmış bireylerin varlığı oldukça önemlidir. Bu kişiler, bilişim suçları ile mücadelede aktif bir rol üstlenebilirler ve bu suçların önlenmesine katkı sağlayabilirler. Böylece bilişim suçlarıyla mücadele daha etkin, verimli ve sağlıklı olacaktır.

KAYNAKÇA

AKBULUT, Berrin: Bilişim Alanında Suçlar, Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Adalet Yayınevi, Ankara 2017.

AKBULUT, Berrin: Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Konya 2016, C. 24, S. 2, s.1-55.

AKARSLAN, Hüseyin: Bilişim Suçları, Seçkin Yayıncılık, Ankara 2012.

AKINCI, Hatice/ ALIÇ, A. Emre/ ER, Cüneyt*: "Türk Ceza Kanunu ve Bilişim Suçları"*, İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, s.156-275.

ALTUNOK, Ebru/ VURAL, Ali Fatih: *"Bilişim Suçları"*, Denetişim, C. 8, Y. 2016, s. 74-84.

APAYDIN, Cengiz: Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, Seçkin Yayıncılık, Ankara 2023.

ARTUK, Mehmet Emin/GÖKCEN, Ahmet/ YENİDÜNYA, Ahmet Caner: Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara 2020.

AYDIN, Emin Doğan: Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınları, Ankara 1992.

BAŞLAR, Yusuf: "Elektronik İmza Kanunu'nda Düzenlenen Bilişim Suçları", Antalya Bilim Üniversitesi Hukuk Fakültesi Dergisi, C.4, S.7, Y.2016, s.41-64.

BENSGHİR, Türksel Kaya: *"Türkiye'de Yönetim Bilişim Sistemleri Disiplinin Gelişimi Üzerine Düşünceler", Amme İdaresi Dergisi,* C.35, S.1, Y. 2002, s. 77-103.

BEYGU, Şahin: Yayıncılıkta Bilgisayar El Kitabı, Yalçın Ofset Matbaası, İstanbul 1990.

BOZDOĞAN AKBULUT, Berrin: *"Bilişim Suçları"*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, C.8, S.1-2, Y.2000, s.545-555.

BÜK, Alaattin: Bilişim Alanında Kişisel Verilerin Korunması, Seçkin Yayıncılık, Anlara 2018.

ÇAKICI, Mert: *"Türk Ceza Kanunu m. 243 ve m. 244'te Düzenlenen Bilişim Suçları"*, Ceza Hukuku Dergisi, C. 9, S. 24 Y. 2014, s. 307-349.

ÇAKIR, Hüseyin/ KILIÇ, Mehmet Serkan: Güncel Tehdit: Siber Suçlar, Seçkin Yayıncılık, Ankara 2014, 7. Bölüm, (AYTEKİN, Akın/ KILIÇ, Mehmet Serkan/ AYTEKİN, Akın: Karşılaştırmalı Hukuk Açısından Siber Suçlar).

ÇANKAYA, Ayhan: *"Bilişim Suçlarının Dünü, Bugünü ve Türkiye'deki Durumu"*, Polis Dergisi, S. 30, Y. 2002, s. 5-10.

CLOUGH, Bryan /MUNGO, Paul: Sıfıra Doğru: Veri Suçları ve Bilgisayar Yeraltı Dünyası, Çev. Emel Kurma, İletişim Yayınları, İstanbul 1999.

DEĞİRMENCİ, Olgun: Bilişim Suçları, Marmara Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, İstanbul 2002. (Yayınlanmamış)

DEĞİRMENCİ, Olgun: *"Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi"*, Türkiye Barolar Birliği Dergisi, C.18, S. 58, s. 195-208.

DEMİR, Önder: *"İnternet Servis Sağlayıcısının Hukuki Sorumluluğu",* Uluslararası İnternet Hukuku Sempozyumu, Dokuz Eylül Üniversitesi Yayınları, 21-22 Mayıs 2001, İzmir 2022.

DOĞAN, Koray: *"Bilişim Suçları ve Yeni Türk Ceza Kanunu"*, Hukuk ve Adalet Eleştirel Hukuk Dergisi, Ekim 2002, S.6-7, s.305.

DOĞAN, Ramazan: 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Adalet Yayınevi, Ankara 2014.

SOYASLAN, Doğan: Ceza Hukuku Genel Hükümler, Yetkin Yayınları, Ankara 2018.

DÖNMEZER, Sulhi: *"Ekonomik Suçlar",* Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, S.7, Y.1985, s.19-30.

DÖNMEZER, Sulhi: Kişilere ve Mala Karşı Cürümler, Beta Yayıncılık, Tıpkı 17.B, İstanbul 2004.

DURDU, Erdal: Kripto Para Birimi Olarak Bitcoin ve Ceza Hukuku, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018.

DURSUN, Hasan: *"Bilgisayar ile İlgili Suçlar",* Yargıtay Dergisi, C. 24, S. 3, Y. 1998, s.334-339.

DÜLGER, Murat Volkan: Bilişim Suçları ve İnternet İletişim Hukuku, 10. Baskı, Seçkin Yayıncılık, Ankara 2023.

DÜLGER, Murat Volkan/ Özkan, Onur: *"Kripto Para Suçları: Kripto Para Birimlerinin Hukuki Boyutu ve Türk Ceza Kanunu Bakımından Değerlendirilmesi"* In Prof. Dr. Mehmet Emin Artuk'a Armağan, ed. Mahmut Koca, s.963-994, Seçkin Yayınevi, Ankara 2020.

EKİCİ, Şerafettin: Bilişim ve Teknoloji Hukuku, Seçkin Yayıncılık, Nisan 2022.

EKİNCİ, Mustafa/ ESEN, Sinan: Anlatımlı ve Gerekçeli Yeni Türk Ceza Kanununda Yer Alan Hırsızlık, Yağma, Güveni Kötüye Kullanma, Dolandırıcılık, Hileli ve Taksirli İflas, Karşılıksız Yararlanma, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, Adalet Yayınevi, Ankara 2005.

ERCAN, Tuncay/ KUTAY, Mahir: *"Endüstride Nesnelerin İnterneti (IoT) Uygulamaları",* Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, Y. 2016, s.509-607.

ERDOĞAN, Yavuz: Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri, Legal Yayıncılık, İstanbul 2018.

ERDOĞAN, Yavuz: Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile), Legal Yayıncılık, İstanbul 2013.

ERMAN, Barış: *"Alman Hukukunda İnternetten Kaynaklanan Ceza Sorumluluğu"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul 2001, C. LIX, S. 1-2.

ERSOY, Yüksel: *"Genel Hukuki Koruma Çerçevesinde Bilişim Suçları",* Prof. Dr. Yılmaz GÜNAL'a Armağan, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Yayını, C. 49, S. 3-4, Y. 1994.

ERGÜN, İsmail: Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008.

EŞİTLİ AYGÜN, Ezgi: Kalkışma Suçları, Yetkin Yayınları, Ankara 2016.

GERÇEKER, Hasan: Yorumlu & Uygulamalı Türk Ceza Kanunu (2 Cilt), C:2, Seçkin Yayıncılık, Ankara 2022.

GÜL, Ahmet: Doğrudan-Dolaylı Bilişim Suçları, Seçkin Yayıncılık, Ankara 2021.

GÜRLER, Fazıl: Yargıtay Kararları Işığında Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar. Yetkin Yayınevi, Ankara 2015.

GÜN, Nagihan: Türk Ceza Hukukunda Bilişim Suçları, Çankaya Üniversitesi Yüksek Lisans Tezi, Ankara 2020.

Grolier International Americana Encylopedia: Sabah Yayınları, İstanbul 1993, C.3, İstanbul.

HELVACIOĞLU, Aslı Deniz: *"Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi"* İnternet ve Hukuk, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2004.

HAFIZOĞULLARI, Zeki/ÖZEN, Muharrem: Türk Ceza Hukuku Özel Hükümler Kişilere Karşı Suçlar, US-A Yayıncılık, Ankara 2016.

HAFIZOĞULLARI, Zeki/ ÖZEN, Muharrem: Türk Ceza Hukuku Özel Hükümler-Topluma Karşı Suçlar, Ankara 2017.

IŞIKLI, Şevki/KÜÇÜKVARDAR, Mert: Bilişim Devrimi Teknolojinin Felsefi ve Sosyolojik Analizi, Birleşik Yayınevi, Ankara 2016.

İÇEL, Kayıhan: *"Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 59, S. 1-2, Y. 2001, s.3-10.

İÇEL, Kayıhan/ÜNVER, Yener/ ÖZ, Kerem: Kripto Para ve Ceza Hukuku, HOCHMAN, Nathan J.: *"Kripto Paranın Vahşi Batı Görünümünü Düzenlemek"* (Çev. BOULANGER, Özge Didem), Seçkin Yayıncılık, Ankara 2022.

KANGAL, Zeynel T.: *"Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul 2001, C. LIX, S. 1-2.

KARAGÖZ, Mehmet Can: Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, On İki Levha Yayıncılık, 2020.

KARAGÜLMEZ, Ali: Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, 5. Baskı, Seçkin Yayıncılık, Ankara 2013.

KETİZMEN, Muammer: Türk Ceza Hukukunda Bilişim Suçları, Adalet Yayınevi, Ankara 2008.

KOCA, Mahmut/ ÜZÜLMEZ, İlhan: Türk Ceza Hukuku Özel Hükümler, Adalet Yayınevi, Ankara 2022.

KOÇOĞLU, Seda: Bilişim Sistemine ve Sistemdeki Verilere Müdahale ile Bilişim Sistemi Aracılığıyla Haksız Çıkar Sağlama Suçları (TCK m. 244), İstanbul Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, İstanbul 2019.

KÜÇÜKTAŞDEMİR, Özgür: Ekonomik Suçlar Bağlamında Türk Ticaret Kanununda Düzenlenen Suçlar ve Cezalar, Ankara 2018.

KÖKSAL, Aydın: Bilişim Terimleri Sözlüğü, Türk Dil Kurumu Yayınları, Ankara 1981.

KURT, Levent: Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, Seçkin Yayıncılık, Ankara 2005.

LEVİN, Richard B.: Bilgisayarda Virüs-Antivirüs, (Çev. Ferhat Okan Sezer), Doruk Yayınları, Ankara 1992.

MAHMUTOĞLU, Fatih Selami: *"Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu"*, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. LIX, S. 1-2, İstanbul 2001.

MAHMUTOĞLU, Fatih Selami: *"Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi",* İÜHFM, C. 71, S.1, 2013, s.855-889.

MALKOÇ, İsmail: Açıklamalı İçtihatlı Yeni Türk Ceza Kanunu, Malkoç Kitabevi, Ankara 2007.

MERKİ, Duygu: Bileşik Suç, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Yüksek Lisans Tezi, Ankara 2009.

MUCUK, Melike Hafsa: Bilişim Sistemine Girme (TCK 243) ve Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK 244) Suçları, Ankara Üniversitesi Sosyal Bilimler Üniversitesi Kamu Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara 2022.

ÖNDER, Ayhan: Şahıslara ve Mala karşı Cürümler ve Bilişim Alanında Suçlar, Filiz Kitapevi, İstanbul 1994.

ÖZBEK, Veli Özer: *"Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245)",* Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C.9, Özel Sayı, İzmir 2007, s.1019-1063. (Özbek, Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu)

ÖZBEK, Veli Özer: Ekonomi Ceza Hukuku Birinci Kitap Genel Hükümler, Seçkin Yayıncılık, Ankara 2020.

ÖZBEK, Veli Özer/ KANBUR, Nihat/ DOĞAN, Koray/ BACAKSIZ: Pınar, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara 2022.

ÖZBEK, Veli Özer/ KANBUR, Nihat/ DOĞAN, Koray/ BACAKSIZ, Pınar/ TEPE, İlker, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara 2010.

ÖZEN, Muharrem/BAŞTÜRK, İhsan: Bilişim-İnternet ve Ceza Hukuku, Adalet Yayınevi, Ankara 2011.

ÖZEN, Mustafa, Suçların İçtimaı (Zincirleme Suç- Fikri İçtimaı- Bileşik Suç), Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Doktora Tezi, Ankara 2008.

ÖZDİLEK, Ali Osman: İnternet ve Hukuk, Papatya Yayıncılık, İstanbul 2002.

ÖZGENÇ, İzzet: Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara 2022.

SAĞIROĞLU, Şeref/ŞENOL, Mustafa: BGD Siber Güvenlik ve Savunma Kitap Serisi 2, 1. Basım, Grafiker Yayınları, Ankara, s.25-58.

PALLI, Hayati: Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri 2008.

PARLAR, Ali: Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara 2011

RETORNAZ AKSOY, E. Eylem: *"Ceza Hukuku Perspektifinden Blokzincir",* (ed. RETORNAZ AKSOY, E. Eylem/GÜÇLÜTÜRK), Orhan Gazi, Gelişen Teknolojiler ve Hukuk I: Blokzincir, Oniki Levha Yayıncılık, İstanbul 2020.

SINAR, Hasan: İnternet ve Ceza Hukuku, Beta Yayınları, İstanbul 2001.

SIRABAŞI, Volkan: İnternet ve Radyo – TV Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi), Adalet Yayınevi, Ankara 2003.

SIRIMCIYAN, Alis: *"Tehlikeli Alışveriş Turları",* CHIP Dergisi, S.12, s.153-166.

SOYASLAN, Doğan: Ceza Hukuku Özel Hükümler, Yetkin Yayıncılık, Ankara 2020.

SUN, Frank: Canavarın İnternetteki Sayısı: 666 (Kutsal Kitap Gözüyle İnternet), (Çev. Özgül Erman) Cep Kitapları, İstanbul 2001.

ŞAHİN, Muhammet: *"Kripto Para Yeni Bir Vergi Sığınağı mı? Bilişim Teknolojilerindeki Gelişmeler Temelinde Bir Değerlendirme,"* Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, S.34, Y.2019, s.169-181.

ŞİŞMAN, Burak: Bilim Kurgudan Gerçeğe: Artırılmış Gerçeklik, Sanal Gerçeklik ve Karma Gerçeklik, Bilim ve Teknik, Mart 2021, s.59-65.

TARAKÇIOĞLU, Zeynep: *"Kripto Varlıklar ve Ceza Hukuku Sorumluluğu",* Akdeniz Üniversitesi Hukuk Fakültesi Dergisi, Aralık 2021, C.11, S.2, s.295-352.

TAŞKIN, Şaban Cankat, Bilişim Suçları, Beta Yayıncılık, Bursa 2008.

TAVUKÇUOĞLU, Cengiz: Bilişim Terimleri Sözcüğü, Asil Yayın Dağıtım, Ankara 2004.

TEZCAN, Durmuş/ ERDEM, Mustafa Ruhan/ ÖNOK, Murat: Teorik ve Pratik Ceza Özel Hukuku, Seçkin Yayıncılık, Ankara 2021.

TİEDEMANN, Klaus: *"Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi",* Çev. Yenisey, Feridun: İÜHFM, C. XLI, S. 1-4, Y. 1975.

TUNÇ, Demircan: Bilişim Alanında Suçlar, Selçuk Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, Konya 2007.

TURAN, Metin: Alman Bilişim Hukuku, Adalet Yayınevi, Ankara 2017.

TÜRKOĞLU, Süleyman: Bilgisayar ve İnternet Medya ve İletişim Ön Lisans Programı.

UÇAR, Hüdaverdi: 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Çankaya Üniversitesi Kamu Hukuku Yüksek Lisans Tezi, Ankara 2014.

ÜNVER, Yener: *"Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi",* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul 2001, C. LIX, S. 1-2.

YANAR, Yasin: Ceza Hukuku ve Bilişim Hukuku Bağlamında TCK md.245/A Yasak Cihaz veya Programlar Suçu, İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul 2019.

YAŞAR, Osman/ GÖKCAN, Hasan Tahsin/ ARTUÇ, Mustafa: Yorumlu Uygulamalı Türk Ceza Kanunu, Adalet Yayınevi, Ankara 2014.

YAZICIOĞLU, Yılmaz: *"Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı",* Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001, İzmir Dokuz Eylül Üniversitesi Yayını, Y.2002.

YAZICIOĞLU, Yılmaz: Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile, Alfa Yayınevi, İstanbul 1997.

YAZICIOĞLU, Recep Yılmaz: *"Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi"* 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara 2009.

YAZICIOĞLU, Recep Yılmaz: *"Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Genel Değerlendirmesi"*, Yeditepe Üniversitesi Hukuk Dergisi, İstanbul 2005, C. II, S.2.

YELDAN, Didem: Siber Suçlar, Seçkin Yayıncılık, Ankara 2022.

YENİDÜNYA, A. Caner: "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m. 243*)" Legal Fikri ve Sınai Haklar Dergisi, S.4, Y.2005, s.1018-1042.

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

YENİSEY, Feridun: *"İnternet Suçlarının Yeni İşleniş Biçimleri"*, Uluslararası İnternet Sempozyumu, İzmir Dokuz Eylül Üniversitesi Yayını, İzmir 2002.

YILDIZ, Sevil: Suçta Teknik Bir Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi, Nobel Yayınevi, Ankara 2007.

YILMAZ, Davut: Hacking Bilişim Korsanlığı ve Koruma Yöntemleri, Hayat Yayınları, İstanbul 2004.

Çevrimiçi Kaynaklar

http://archiv.jura.uni-saarland.de

https://bilimgenc.tubitak.gov.tr

https://cahitcengizhan.com

https://dergipark.org.tr

https://fenbildergi.aku.edu.tr

https://madran.net

http://ozocak.com

https://polis.osce.org

https://sozluk.gov.tr

https://tr.wikipedia.org

https://wmaraci.com

https://www.corpus.com.tr

https://www.crime-research.org

https://www.bbc.com

http://www.jura.uni-sb.de

https://www.haber7.com

http://www.hukukcu.com

https://www.hukukturk.com

https://www.kaspersky.com.tr

https://www.kvkk.gov.tr

https://www.mfa.gov.tr

https://www.resmigazete.gov.tr

https://www.sozcu.com.tr

http://www.tdk.gov.tr