

T.C.
YALOVA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

**TÜRK HUKUKUNDA BİLİŞİM SUÇLARI VE BİLİŞİM
YOLUYLA İŞLENEN SUÇLAR**

YÜKSEK LİSANS TEZİ
Muhammed Burak GÜNGÖR

Enstitü Anabilim Dalı: KAMU HUKUKU
Enstitü Bilim Dalı: KAMU HUKUKU

Tez Danışmanı: Dr. Öğr. Üyesi Can CANPOLAT

Ocak 2021

T.C.
YALOVA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

TÜRK HUKUKUNDA BİLİŞİM SUÇLARI VE BİLİŞİM
YOLUYLA İŞLENEN SUÇLAR

YÜKSEK LİSANS TEZİ
Muhammed Burak GÜNGÖR

Enstitü Anabilim Dalı: KAMU HUKUKU
Enstitü Bilim Dalı: KAMU HUKUKU

Bu tez 14/01/2021 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

	Adı SOYADI	Kanaati			İmza
Jüri Başkanı (Danışman)	Dr. Öğr. Üyesi Can CANPOLAT	☒ Kabul	☐ Düzeltme	☐ Ret	
Jüri Üyesi	Dr. Öğr. Üyesi İsmail DURSUN	☒ Kabul	☐ Düzeltme	☐ Ret	
Jüri Üyesi	Dr. Öğr. Üyesi Zafer İÇER	☒ Kabul	☐ Düzeltme	☐ Ret	

SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS İNTİHAL YAZILIM RAPORU
BEYAN BELGESİ

Tez Başlığı: Türk Hukukunda Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar

Yukarıda başlığı belirtilen tez çalışmamın toplam 137 sayfalık kısmına ilişkin aşağıda belirtilen filtrelemeler uygulanarak alınmış olan ve 06.01.2021 tarihinde aşağıda ismi yazılı araştırma görevlisi tarafından şahsıma iletilen Turnitin intihal tespit programı raporuna göre tezimin benzerlik oranı % 13'tür.

Uygulanan filtrelemeler:

1. Kaynakça hariç,
2. Alıntılar dâhil,
3. 5 kelimeden daha az örtüşme içeren metin kısımları hariç.

Bu bilgiler doğrultusunda tez çalışmamın herhangi bir intihal içermediğini; aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

İmza

Adı Soyadı : Muhammed Burak Güngör
Öğrenci Numarası : 177211006
Ana Bilim Dalı : Kamu Hukuku
Programı : Kamu Hukuku
Türü : () Proje (x) Yüksek Lisans Tezi () Doktora
Tezi

Can Canpolat
(Adı Soyadı, İmzası, Tarih)

ÖNSÖZ

Ülkemizde bilişim suçları üzerine oldukça çalışılmış olmasına rağmen uygulamada bir takım sıkıntıların yaşandığı hususunda gözlemim üzerine Türk Ceza Kanununun 243-246. maddeleri ile 142/2-e ve 158/1-f maddelerini konu alan bu tez çalışması tarafımda hazırlanmıştır.

Öncelikle tez hazırlama sürecinde değerli yardım ve bilgileriyle bana yol gösteren saygıdeğer tez danışmanım Dr. Öğr. Üyesi Can Canpolat’a teşekkürlerimi borç bilirim.

Jüri üyeleri olan Zafer İçer ve İsmail Dursun’a da eleştiri ve katkıları için teşekkürlerimi sunarım.

Bugünlere gelmeme vesile olan anneme ve babama, daima bana destek olan kardeşime, hayatımın her alanında yanımda olan ve desteğini benden esirgemeyen sevgili eşim ve meslektaşım Leyla Güngör’e, minnet ve teşekkürlerimi sunarım.

Muhammed Burak GÜNGÖR

15.01.2021

İçindekiler Tablosu

BEYAN BELGESİ.....	i
ÖNSÖZ.....	ii
KISALTMALAR LİSTESİ	xi
Giriş.....	1
BİRİNCİ BÖLÜM.....	5
Bilgisayarlar, İnternet ve Bilişim Sistemleri İle İlgili Temel Bilgiler	5
1.1.Bilişim Suçları ile İlgili Temel Kavramlar	5
1.1.1. Bilgisayar.....	5
1.1.1.1. Tanımı	5
1.1.1.2.Tarihi.....	5
1.1.1.3. Yapısı.....	8
1.1.2. Veri.....	9
1.1.3. İnternet.....	9
1.1.3.1. Genel Olarak.....	9
1.1.3.2 İnternet İle İlgili Kavramlar	10
1.1.3.2.1. TCP/IP	10
1.1.3.2.2. Domain ve DNS	10
1.1.3.2.3. WWW	11
1.1.3.2.4. URL.....	11
1.1.3.2.5. Yer Sağlayıcı	11
1.1.3.2.6. İçerik Sağlayıcı	12
1.1.3.2.7. Sunucu.....	12
1.1.3.2.8. Log Kaydı.....	12
1.1.3.2.9. Ağ (Network).....	12
1.1.3.2.10. ISS(Erişim Sağlayıcı)	12
1.1.3.2.11. İnternet Tarayıcısı.....	13
1.1.3.2.12. Sosyal Medya	13
1.1.3.2.13. Nesnelerin interneti.....	13

1.1.4. Bilişim ve Bilişim Sistemi.....	14
1.2. Bilişim Suçları İşlenirken Yaygın Olarak Kullanılan Yöntemler ve Araçlar	15
1.2.1. Bilişim Suçlarının İşlenmesi Amacıyla Kullanılan Programlar	15
1.2.1.1. <i>Virüsler (Viruses)</i>	15
1.2.1.2. <i>Solucanlar (Worms)</i>	16
1.2.1.3. <i>Truva Atı(Trojan Horses)</i>	17
1.2.1.4. <i>Kök Kitleri (Rootkits)</i>	18
1.2.1.5. <i>Casus Yazılımlar (Spyware)</i>	19
1.2.1.6. <i>Tavşanlar (Rabbits ya da Wabbits)</i>	20
1.2.1.7. <i>Bukalemunlar</i>	20
1.2.1.8. <i>Mantık Bombaları (Logic Bombs)</i>	21
1.2.1.9. <i>Fidye Yazılımları (Ransomware)</i>	22
1.2.1.10. <i>Bot Ağları (Botnet)</i>	23
1.2.1.11. <i>Arka Kapılar (Backdoors)</i>	24
1.2.2. Yemleme (Phishing).....	24
1.2.3. DoS Saldırıları	26
1.3. Doğrudan Bilişim Suçu ve Dolayısıyla Bilişim Suçu Kavramları	27
İKİNCİ BÖLÜM	28
Doğrudan Bilişim Suçları	28
2.1. Bilişim Sistemine Girme Suçu (TCK 243/1-3).....	28
2.1.1.Genel Olarak.....	28
2.1.2. Korunan Hukuki Yarar	31
2.1.3. Maddi Unsurlar.....	32
2.1.3.1. <i>Fiil</i>	32
2.1.3.2. <i>Fail</i>	35
2.1.3.3. <i>Mağdur</i>	35
2.1.3.4. <i>Suçun Konusu</i>	36
2.1.3.5. <i>Netice</i>	37
2.1.4. Manevi Unsurlar	37
2.1.5. Hukuka Aykırılık.....	39
2.1.6. Suçun Neticesi Sebebiyle Ağırlaşmış Hali.....	40
2.1.7. Suçun Nitelikli Hali	41

2.1.8. Neticesi Sebebiyle Ağırlaşmış Hal ile Nitelikli Halin Bir Arada Bulunması Durumu.....	43
2.1.9. Terör Amacı ile Bilişim Sistemine Girme veya Kalma.....	44
2.1.10. Suçun Özel Görünüş Biçimleri.....	44
2.1.10.1. Teşebbüs.....	44
2.1.10.2. İştirak.....	45
2.1.10.3. İçtima.....	45
2.1.11. Soruşturma Usulü ve Yaptırım.....	48
2.2. Veri Nakillerini Sisteme Girmeksizin Teknik Araçlarla İzleme Suçu (TCK 243/4)	50
2.2.1.Genel Olarak.....	50
2.2.2. Korunan Hukuki Yarar	51
2.2.3. Maddi Unsurlar.....	51
2.2.3.1. Fiil.....	51
2.2.3.2. Fail.....	52
2.2.3.3. Mağdur.....	52
2.2.3.4. Suçun Konusu.....	53
2.2.3.5. Netice	53
2.2.4. Manevi Unsurlar	53
2.2.5. Hukuka Aykırılık.....	54
2.2.6. Özel Görünüş Biçimleri.....	54
2.2.6.1. Teşebbüs.....	54
2.2.6.2. İştirak.....	54
2.2.6.3. İçtima	55
2.2.7. Yaptırım.....	55
2.3. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK 244/1-3)	55
2.3.1.Genel Olarak.....	55
2.3.2. Korunan Hukuki Yarar	57
2.3.3. Maddi Unsurlar.....	58
2.3.3.1. Fiil.....	58
2.3.3.1.1. Sistemin Engellenmesi ve Bozulması	58
2.3.3.1.1.1. Sistemin İşleyişinin Engellenmesi.....	58

2.3.3.1.1.2. Sistemin İşleyişinin Bozulması	59
2.3.3.1.2. Verilerin Bozulması, Yok Edilmesi, Değiştirilmesi, Erişilmez Kılınması, Sisteme Veri Yerleştirilmesi, Var Olan Verilerin Başka Yere Gönderilmesi	60
2.3.3.1.2.1. Verilerin Bozulması	60
2.3.3.1.2.2. Verilerin Yok Edilmesi.....	60
2.3.3.1.2.3. Verilerin Değiştirilmesi	61
2.3.3.1.2.4. Verilerin Erişilemez Kılınması	62
2.3.3.1.2.5. Sisteme Veri Yerleştirmek.....	62
2.3.3.1.2.6. Sistemde Var Olan Verileri Başka Bir Yere Göndermek	63
2.3.3.2. Fail.....	63
2.3.3.3. Mağdur.....	64
2.3.3.4. Suçun Konusu.....	64
2.3.3.5. Netice	65
2.3.4. Manevi Unsurlar	65
2.3.5. Hukuka Aykırılık.....	65
2.3.6. Suçun Nitelikli Hali.....	66
2.3.7. Suçun Özel Görünüş Biçimleri.....	67
2.3.7.1. Teşebbüs.....	67
2.3.7.2. İştirak	67
2.3.7.3. İçtima	68
2.3.7. Soruşturma Usulü ve Yaptırım.....	69
2.4. Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK 244/4)	70
2.4.1. Genel Olarak.....	70
2.4.2. Suçla Korunan Hukuksal Değer	72
2.4.3. Maddi Unsurlar.....	72
2.4.3.1. Fiil.....	72
2.4.3.2. Fail.....	73
2.4.3.3. Mağdur.....	74
2.4.3.4. Konu.....	74
2.4.3.5. Netice	75
2.4.4. Manevi Unsurlar	75

2.4.5. Hukuka Aykırılık.....	76
2.4.6. Özel Görünüş Biçimleri.....	76
2.4.6.1. Teşebbüs.....	76
2.4.6.2. İştirak.....	76
2.4.6.3. İçtima.....	76
2.4.7. Nitelikli Haller.....	77
2.4.8. Soruşturma Usulü ve Yaptırım.....	78
2.5. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK 245).....	78
2.5.1. Genel Olarak.....	78
2.5.2. Başkasına Ait Banka veya Kredi Kartlarını Kullanarak Yarar Sağlama Suçu.....	80
2.5.2.1. Korunan Hukuki Değer.....	80
2.5.2.2. Maddi Unsurlar.....	80
2.5.2.2.1. Fiil.....	80
2.5.2.2.2. Fail.....	83
2.5.2.2.3. Mağdur.....	84
2.5.2.2.4. Konu.....	85
2.5.2.2.5. Netice.....	86
2.5.2.3. Manevi Unsurlar.....	86
2.5.2.4. Hukuka Aykırılık.....	86
2.5.2.5. Suçun Özel Görünüş Biçimleri.....	86
2.5.2.5.1. Teşebbüs.....	86
2.5.2.5.2. İştirak.....	87
2.5.2.5.3. İçtima.....	87
2.5.2.6. Şahsi Cezasızlık Sebebi.....	90
2.5.2.7. Etkin Pişmanlık.....	91
2.5.2.8. Soruşturma Usulü ve Yaptırım.....	93
2.5.3. Sahte Banka Veya Kredi Kartı Üretmek, Satmak, Devretmek, Satın Almak veya Kabul Etmek Suçu.....	93
2.5.3.1. Korunan Hukuki Değer.....	93
2.5.3.2. Maddi Unsurlar.....	94
2.5.3.2.1. Fiil.....	94

2.5.3.2.2. Fail	96
2.5.3.2.3. Mağdur	96
2.5.3.2.4. Konu	96
2.5.3.2.5. Netice	97
2.5.3.3. Manevi Unsurlar	97
2.5.3.4. Hukuka Aykırılık	97
2.5.3.5. Suçun Özel Görünüş Biçimleri	97
2.5.3.5.1. Teşebbüs	97
2.5.3.5.2. İştirak	98
2.5.3.5.3. İçtima	98
2.5.3.6. Soruşturma Usulü ve Yaptırım	100
2.5.4. Sahte Banka ve Kredi Kartlarını Kullanarak Yarar Sağlama Suçu	100
2.5.4.1. Korunan Hukuki Değer	100
2.5.4.2. Maddi Unsurlar	100
2.5.4.2.1. Fiil	100
2.5.4.2.2. Fail	101
2.5.4.2.3. Mağdur	101
2.5.4.2.4. Suçun Konusu	102
2.5.4.2.5. Netice	102
2.5.4.3. Manevi Unsurlar	102
2.5.4.4. Hukuka Aykırılık	102
2.5.4.5. Suçun Özel Görünüş Biçimleri	102
2.5.4.5.1. Teşebbüs	102
2.5.4.5.2. İştirak	103
2.5.4.5.3. İçtima	103
2.5.4.6. Soruşturma Usulü ve Yaptırım	104
2.6. Yasak Cihaz ve Programlar (TCK 245/A)	105
2.6.1. Genel Olarak	105
2.6.2. Suçla Korunan Hukuki Yarar	107
2.6.3. Maddi Unsurlar	108
2.6.3.1. Fiil	108
2.6.3.2. Fail	110

2.6.3.3. <i>Mağdur</i>	110
2.6.3.4. <i>Konu</i>	110
2.6.3.5. <i>Netice</i>	112
2.6.4. Manevi Unsurlar.....	112
2.6.5. Hukuka Aykırılık.....	112
2.6.6. Suçun Özel Görünüş Biçimleri.....	113
2.6.6.1. <i>Teşebbüs</i>	113
2.6.6.2. <i>İştirak</i>	113
2.6.6.3. <i>İçtima</i>	113
2.6.7. Soruşturma Usulü ve Yaptırım.....	114
ÜÇÜNCÜ BÖLÜM	115
Dolayısıyla Bilişim Suçları	115
3.1. Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık Suçu (142/2-e)	115
3.1.1. Genel Olarak.....	115
3.1.2. Korunan Hukuki Yarar	115
3.1.3. Maddi Unsurlar.....	116
3.1.3.1. <i>Fiil</i>	116
3.1.3.2. <i>Fail</i>	116
3.1.3.3. <i>Mağdur</i>	116
3.1.3.4. <i>Konu</i>	117
3.1.3.5. <i>Netice</i>	117
3.1.4. Manevi Unsurlar	118
3.1.5. Hukuka Aykırılık.....	118
3.1.6. Suçun Özel Görünüş Biçimleri.....	118
3.1.6.1. <i>Teşebbüs</i>	118
3.1.6.2. <i>İştirak</i>	119
3.1.6.3. <i>İçtima</i>	119
3.1.7. Suçun Gece Vakti İşlenmesi.....	120
3.1.8. Daha Az Cezayı Gerektiren Haller.....	120
3.1.8.1. <i>Hırsızlık Suçunun, Paydaş veya Elbirliği İle Malik Olunan Mal Üzerinde İşlenmesi</i>	120

3.1.8.2. Hırsızlık Suçunun Bir Hukuki İlişkiye Dayanan Alacağı Tahsil Amacıyla İşlenmesi.....	121
3.1.8.3. Malın Değerinin Az Olması	121
3.1.9. Şahsi Cezasızlık Sebebi veya Cezada İndirim Yapılmasını Gerektiren Şahsi Sebep	121
3.1.10 Etkin Pişmanlık	121
3.1.11. Soruşturma Usulü ve Yaptırım.....	122
3.2. Bilişim Sistemlerinin Kullanılması Suretiyle Dolandırıcılık Suçu (158/1-f).....	122
3.2.1. Genel Olarak.....	122
3.2.2. Korunan Hukuki Yarar	123
3.2.3. Maddi Unsurlar.....	124
3.2.3.1. Fiil.....	124
3.2.3.2. Fail.....	125
3.2.3.3. Mağdur.....	125
3.2.3.4. Konu.....	126
3.2.4. Manevi Unsurlar	126
3.2.5. Hukuka Aykırılık.....	126
3.2.6. Suçun Özel Görünüş Biçimleri.....	126
3.2.6.1. Teşebbüs.....	126
3.2.6.2. İştirak	127
3.2.6.3. İçtima	127
3.2.7. Suçun Daha Az Cezayı Gerektiren Hali	128
3.2.8. Şahsi Cezasızlık Sebebi veya Cezada İndirim Yapılmasını Gerektiren Şahsi Sebep	129
3.2.9. Etkin Pişmanlık	129
3.2.10. Soruşturma Usulü ve Yaptırım.....	129
SONUÇ.....	131
KAYNAKÇA.....	138
ÖZGEÇMİŞ.....	144

KISALTMALAR LİSTESİ

CMK	: Ceza Muhakemesi Kanunu
ENIAC	: Electronic Numerical Integrator And Computer
SEGBİS	: Ses ve Görüntü Bilişim Sistemi
TCK	: Türk Ceza Kanunu
TÜVAKA	:Türkiye Üniversite ve Araştırma Kurumları Ağı
UYAP	:Ulusal Yargı Ağı Projesi
vb.	: ve benzeri

Giriş

İnsanoğlunun çağlar boyu süren gelişimi özellikle son yüzyılda büyük bir hız kazanmış ve teknoloji hayatımızın vazgeçilmez bir unsuru olarak yerini almıştır. Bilgisayarların İkinci Dünya Savaşı yıllarında üretilen ENIAC ile başlayan macerası kişisel bilgisayarların yaygınlaşması ile bambaşka bir noktaya taşınmıştır. Bilgisayarlar ve bilgisayarları da kapsayan bir unsur olan bilişim sistemleri bugün hayatın her alanında vazgeçilmez konumdadır. Kişiler arası iletişim artık büyük ölçüde bilişim sistemleri aracılığıyla gerçekleşmektedir. Elektronik postalar, sosyal ağlar ve benzeri sistemler günlük hayatın vazgeçilmezleri olmuştur. Benzer şekilde iş dünyası da bilişim sistemlerinden yararlanmaktadır. Ticaretin daha hızlı gelişmesi için bilişim sistemlerinin bir araç olarak kullanılmasıyla birlikte uzak konumlarda bulunan kişiler arasında da ticari ilişkiler kurulması kolaylaşmış, ekonomi küresel bir boyut kazanmıştır.

Teknoloji iş dünyası için bir iletişim aracı olmanın ötesine geçmiş, aynı zamanda doğrudan bir iş kolu da olmuştur. İnternet üzerinden yapılan alışverişler bugün ticaretin büyük bir kısmını oluşturmaktadır. Bunun yanı sıra pek çok firma da hizmetlerini bilişim sistemleri aracılığıyla sunmaktadır. Örneğin internet bankacılığı sistemleri günümüzde hemen hemen herkesin kullandığı sistemlerdir. Bu sistemler hem kullanıcıların işlemlerini daha kolay yapmasını sağlamakta hem de bankaların maliyetlerini düşürerek kâr oranlarını arttırmaktadır.

Bilişim sistemleri yalnızca ticaret için değil hayatın her alanı için önem arz etmektedir. Okullarda ve diğer eğitim kurumlarında bilişim sistemleri kullanılmakta ve bu sayede verimlilik arttırılmaktadır. İnternet üzerinden randevu alınması, hasta takibinin bu sistemler üzerinden yapılması, e-reçete gibi uygulamalar bilişim sistemlerinin sağlık sektöründeki katkılarından bazılarıdır. Hatta akıllı bileklik ve akıllı saat gibi cihazlar kullanıcılarının bazı sağlık verilerini anlık olarak tespit etmekte ve aktarımını yapmaktadır. Yine toplumun temel düzenini sağlayan adalet sisteminin işleyişinde de bilişim sistemlerinden istifade edilmektedir. UYAP, SEGBİS gibi uygulamalar yargılamanın hızlı olması açısından vazgeçilmez konumdadırlar.

Bilişim sistemleri, kullanıcıları için faydalı birer araç olmanın yanı sıra birer eğlence ve kültür aracı olarak da hayatın vazgeçilmezi konumundadır. Bu sistemler vasıtasıyla oyunlar oynamak, film ve dizi izlemek, eğlenceli içeriklere ulaşmak; kullanıcıların eğlence ve kültür ihtiyaçlarını karşılamaya yönelik aktivitelerin bir kısmıdır. Ayrıca kişiler sosyal medya sayesinde paylaşma ve kendini ifade etme ihtiyaçlarını da tatmin etmektedir.

Hiç şüphe yok ki bilişim sistemlerinin gelişmesinin en büyük faydası bilgiyi kolay ulaşılabilir hale getirmesidir. Normal şartlarda öğrenilmesi için çok uzun süreler araştırma yapılması gereken konular bile bu sistemler aracılığıyla kolaylıkla öğrenilebilmektedir. Oluşturulan akademik ve bilimsel ağlar dünyanın çeşitli yerlerindeki bilim insanlarının ortak çalışmalar yapmasına imkân tanımış ve bilginin hızlı aktarımını sağlamıştır.

Tüm bu gelişmeler bilişim sistemlerini toplum için vazgeçilmez kılmışlardır. Bilişim sistemlerinin insan yaşamının önemli bir parçası olması suç işleme amacı güden kişilerin de bu sistemlere ilgi duymasına ve bu sistemler aracı kılınarak işlenen yeni suçlar

doğmasına sebep olmuştur. Bilişim sistemlerinin gelişmesiyle birlikte hırsızlık, dolandırıcılık gibi pek çok suç bu sistemler üzerinden de işlenmeye başlanmış, bilişim sistemlerinin getirdiği hız ve cazibe kullanıcılar için aynı zamanda bir risk unsuru da yaratmıştır. Ayrıca yalnızca bilişim sistemleri kullanılarak işlenebilecek suçlar ve yalnızca bilişim sistemlerine yönelik işlenebilecek suçlar ortaya çıkmıştır.

Bilişim sistemlerinin, kişilerin ve toplumun zararına olacak şekilde kullanılması ulusal ve uluslararası boyutta düzenlemeler yapılması ihtiyacı doğurmuş, bu ihtiyaç da yasa koyucuyu harekete geçirmiş ve bu konudaki düzenlemeler mevzuattaki yerini almıştır. Ülkemizde 1991 yılında 3756 sayılı yasayla yapılan düzenlemeler bilişim suçlarıyla ilgili ilk yasal düzenleme yapılmıştır. Söz konusu Kanunun 20., 21., 22., 23. ve 24. maddeleri ile o dönem yürürlükte olan 765 sayılı TCK'ya "*Bilişim Alanında Suçlar*" başlıklı "*Onbirinci Bab*" eklenmiş ve bu başlık altında 525 a, 525 b, 525 c ve 525 d maddeleri düzenlenmiştir. Ancak bu düzenlemeler o dönem için dahi yeterli olmamış ve eleştirilmiştir.

1 Haziran 2005'te 765 sayılı TCK yürürlükten kalkmış, onun yerini 5237 sayılı TCK almıştır. Yeni TCK'da da bilişim suçlarına yer verilmiş, bu yapılırken de mülga TCK dönemindeki eleştiriler dikkate alınmıştır. Söz konusu suçlar 5237 sayılı TCK'nın üçüncü kısmında "Topluma Karşı Suçlar" başlığı altında ve bu kısmın onuncu bölümünde "Bilişim Alanında Suçlar" başlığı altında yer almaktadır. Bu suçlar TCK'nın 243 ila 246. maddelerinde yer almaktadır. 2016 yılında ise çıkarılan 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesi ile TCK'nın 244/4 ve 245/A maddeleri eklenmiştir. Bilişim suçları ile ilgili düzenlemeler bunlarla sınırlı olmayıp daha sonra çıkarılan 5070 sayılı Elektronik İmza Kanunu, 5846 sayılı Fikir ve Sanat Eserleri Kanunu gibi pek çok farklı kanunda da yerini almıştır.

Bilişim sistemleri kullanılarak işlenen suçlarda suç işlemek nispeten kolay, faili bulmak çoğu zaman zordur. Bu sebeple bu suçların soruşturulması da kendine özgü yöntemlere ihtiyaç duymaktadır. Bu yöntemlere 5271 sayılı CMK'nın 134. maddesinde düzenlenen Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma örnek verilebilir. CMK'nın 134. maddesinde düzenlenen bu koruma tedbiri ile bilişim suçu olsun olmasın, suçlara ilişkin olarak bütün dijital delillerin elde edilebilmesi amaçlanmıştır. TCK'nın 243 ila 246. maddelerinde düzenlenen suçların yanı sıra bilişim yoluyla işlenen hırsızlık ve dolandırıcılık suçları, şantaj, tehdit gibi suçlara ait deliller de bu yöntemle elde edilebilmektedir.

Teknoloji alanındaki ilerlemelerin bilişim sistemlerine de sirayet etmesiyle hukuk sisteminde meydana gelen değişim yeni suçlar ihdas edilmesiyle sınırlı kalmamış, mevcut düzenlemelerin de yeniden yorumlanmasına yol açmıştır. Benzer şekilde bu gelişmelerin neticesinde yalnızca münhasıran bilişim sistemleri kullanılarak işlenen yeni suçlar ortaya çıkmamış, var olan suçların da bilişim sistemleri vasıtasıyla işlenmesi mümkün hale gelmiştir. Günümüzde suçların önemli bir kısmı bilişim sistemleri vasıta kılınarak işlenebilmektedir. Bu suçlardan hırsızlık ve dolandırıcılık suçlarının bilişim yoluyla işlenmesi TCK'nın 142/2-e ve 158/1-f maddelerinde nitelikli hal olarak düzenlenmiştir. Çalışmamızda da yalnızca bilişim suçları değil bilişim yoluyla işlenen bu suçlar da inceleme konusu yapılmıştır.

Bilişim sistemleri ile işlenen suçlar diğer suç tiplerinden farklı olarak ülke sınırlarının çok ötesinde bir nitelik arz etmektedir. Fail bir ülkenin sınırları içinde bulunurken, farklı ülkelerde bulunan mağdurlara karşı bu suçları işleyebilmekte ve kimi zaman suçun neticesi de bambaşka bir ülkede doğabilmektedir. Bu durum bilişim suçlarının ulusal sınırları aşan, uluslararası nitelikte önem arz eden suçlar olduğunu ortaya koymaktadır. Bir devletin egemenlik sınırları içerisinde işlenmiş bulunan ve iç düzenlemelerine göre suç kabul ettiği bir eylemle ilgili olarak yargılama yapabilmesi ve bu yargılamanın neticesinde fail hakkında takdir edilen cezanın infaz edilebilmesi için failin o ülke içerisinde bulunması, ülke sınırlarının dışında olması durumunda ise iadesinin sağlanması gerekmektedir. Suçluların iadesinin sağlanabilmesi için de istisnai haller saklı olmak üzere¹ fiilin her iki devlet açısından suç oluşturması gerekmektedir. Bilişim sistemlerinin ulusal sınırları aşan niteliği de göz önünde bulundurulduğunda faillerin cezasız kalmasının önlenmesi açısından uluslararası düzenlemeler yapılması gerekmiştir. Bu amaçla Sanal Ortamda İşlenen Suçlar Sözleşmesi hazırlanmış, 23.11.2001 tarihinde imzaya açılan bu sözleşmeyi ülkemiz 10 Kasım 2010 tarihinde imzalamış, anlaşmanın onaylamasının uygun bulunması ise Türkiye Büyük Millet Meclisi tarafından 22.04.2014 tarihinde kabul edilen 6533 sayılı yasa ile olmuştur.

Bilişim suçlarının oldukça yeni suçlar olması ve bu suçlara ilişkin uygulamaların tam olarak oturmamış olması dolayısıyla ilgili suçlar arasındaki ayrım net olarak yapılamamakta; eylemlerin hukuki olarak nitelemesinde ve içtimasında karışıklıklar yaşanmaktadır. Uygulamada karşılaşılan bir diğer sorun ise bilişim suçlarının soruşturma ve kovuşturmasının hukuki bilginin yanı sıra teknik bilgi de gerektirmesi, ancak uygulayıcıların bu konuda yeterli bilgiye sahip olmamasıdır. Bu çalışmada hem bilişim suçlarına ilişkin birtakım teknik terimleri açıklayacak hem de bu uygulamada karşılaşılan birtakım problemlere yönelik çözüm önerileri sunacağız.

Çalışmamız üç bölümden oluşmaktadır. İlk bölümde bilgisayarlar ve bilişim sistemleri ile ilgili temel bilgilere yer verilecektir. Bu kapsamda öncelikle bilişim suçları ile ilgili temel kavramlar açıklanacaktır. Bu kavramların bir kısmı doğrudan doğruya inceleme konusu yapılmış olan suçların unsurlarını oluşturmaktadır. Öte yandan bilişim suçlarının birtakım teknik terimler içermesi, bu suçların doğru anlaşılabilmesi ve uygulanabilmesi için bu kavramların bilinmesini zorunlu kılmaktadır. Yine bu bölümde “bilişim suçu” ve “bilişim yoluyla işlenen suç” kavramları anlatılarak aralarındaki farklar ve ortak noktaları incelenecektir. Bilişim suçları ve bilişim yoluyla işlenen suçlar kendilerine özgü bazı yöntemlerle işlenebilmektedir. Çalışmamızın bu bölümünün üçüncü kısmında da bu yöntemler anlatılarak, bilişim suçlarının ne şekilde işlenebileceği ortaya konulmaya çalışılacaktır.

¹ İsveç, Norveç, Finlandiya ve Danimarka gibi ülkelerde çifte suçluluk bir iade şartı olarak kabul edilmediği gibi Avrupa Birliği üyesi ülkeler arasında da hakkında yakalama kararı çıkarılan bir kişinin çifte suçluluk şartı aranmaksızın iadesi yapılmaktadır. (Bkz.: Canpolat, Can. “YABANCILARIN İADESİ: ‘TÜRKİYE’DEN YABANCI DEVLETE İADENİN ŞARTLARI YÖNÜNDEN BİR İNCELEME”, Türkiye Adalet Akademisi Dergisi, 43, 2020, s. 315-350.)

Çalışmamızın ikinci ve üçüncü bölümlerinde ise TCK’da düzenlenen bilişim suçları ile bilişim yoluyla işlenen hırsızlık ve dolandırıcılık suçları incelenecek, bu suçlar incelenirken de 246. maddede yer alan tüzel kişiler hakkında güvenlik tedbirinin uygulanmasına da değinilecektir. Bu suç tiplerinin incelenmesi sırasında doktrindeki farklı görüşlere ve Yargıtay uygulamasına da yer verilecek ve bu suç tipleri tüm yönleriyle ortaya konulmaya çalışılacaktır.



BİRİNCİ BÖLÜM

Bilgisayarlar, İnternet ve Bilişim Sistemleri İle İlgili Temel Bilgiler

1.1.Bilişim Suçları ile İlgili Temel Kavramlar

1.1.1. Bilgisayar

1.1.1.1. Tanımı

Güncel Türkçe sözlükte bilgisayar sözcüğü yüksek miktarda mantıksal ya da aritmetiksel işlemlerden meydana gelen bir görevi, önceden tanımlanmış bir programa göre *göre* tamamlayıp sonuçlandıran elektronik araç, elektronik beyin anlamına gelmektedir². Bilgisayarlar bilgileri işleyen ve bunları kullanarak anlamlı çıktılar verebilen makinelerdir³.

Bu tanımdan hareketle bilgisayarlar verileri ve bilgileri elektronik ortamda saklayan, istenildiği takdirde kullanıcısının hizmetine sunan ve kullanıcıya bunlar üzerinde işlem yapabilme imkânı sağlayan cihazlar olarak tanımlanabilir.

Günümüzde iletişimin temeli sayılabilecek sistemler genellikle bilgisayar tabanlıdır. Bilişim suçlarının belirlenebilmesi açısından da bilgisayarın doğru bir tanımının yapılması elzemdir. Tarihsel anlamda bilgisayar denildiğinde akla gelen monitör, kasa ve diğer unsurlardan oluşan sistemdir ancak teknolojinin gelişmesiyle birlikte bilgisayarlar farklı şekillere evrilmiştir. Dizüstü bilgisayarlar, tablet bilgisayarlar, cep telefonları ve akıllı ev gereçleri de birer bilgisayardır.

Klasik anlamda bilgisayarlar; giriş birimleri(klavye, fare, kamera, tarayıcı), depolama birimleri(Hard disk, disket, cd-rom), bilgi işleme birimleri(CPU), çıkış birimleri(ekran, yazıcı) olmak üzere dört unsurdan oluşmaktadır.

1.1.1.2.Tarihi

Sayıların bulunuşunu, dört işlemler ve matematik izlemiş; insanlık, zamanının önemli bir kısmını hesaplamalar yapmaya ayırmıştır. Uzun ve zor olan hesaplama işlemlerini daha pratik hale getirmek de insanoğlunun tarih boyunca verdiği mücadelelerden birisi olmuştur. Bu hesaplamalarda kullanılan ilk yardımcı gereç M.Ö. 3000 yıllarından beri kullanılmakta olan abaküstür. Bilinen en ilkel bilgisayar örneği kabul edilebilecek olan abaküs günümüzde de kullanılmaya devam etmektedir⁴.

Logaritmanın 16. yüzyılda John Napier tarafından bulunmasından sonra William Oughtred tarafından geliştirilen ve ölçme yoluyla hesaplama yapabilen sürgülü cetvel bir çeşit analog bilgisayar örneğidir⁵.

² <https://sozluk.gov.tr/>, 01.04.2020.

³ BOZDOĞAN AKBULUT, Berrin. "Bilişim Suçları." Selçuk Üniversitesi Hukuk Fakültesi Dergisi 8.1-2 (Milenyum Armağanı) (2000), s.545.

⁴ KESER, Hafize. Bilgisayarın Evrimi. Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 24.2, s. 411.

⁵ KESER, s. 411-422.

İlk hesap makinesi Wilhelm Schickard tarafından 1623 yılında geliştirilmiştir⁶. Bunu 1642 yılında Pascal'ın geliştirdiği hesap makinesi izlemiştir. 1671 yılına gelindiğinde Gottfried Wilhelm Leibniz dört işlemi yapabilen bir makine geliştirmiştir⁷.

Hesap makinelerinden sonra bilgisayara doğru atılan ilk önemli adım Joseph Marie Jacquard'ın 1806 yılında geliştirdiği dokuma tezgâhıdır. Delikli kartlar yardımıyla çalışan bu sistemde tezgâh, üzerindeki kart sayesinde hangi ipin ne zaman atılacağını belirliyordu. Delikli kartlarda kullanılan bu sistem daha sonra geliştirilerek bilgisayarda kullanılan sistemin temelini oluşturdu⁸.

Jean-Baptiste Falcon tarafından bulunan ve Jakar Tezgâhında kullanılan delikli kart sistemi daha sonra Amerikalı istatistikçi Herman Hollerith tarafından da kullanılmıştır. Amerika Birleşik Devletleri'nde 1890 yılında yapılan Nüfus sayımının değerlendirmesinin 10 yıl kadar süreceği tahmin edilmekteyken Hollerith tarafından geliştirilen yöntem ile 2,5 yılda tamamlanabilmiştir⁹. Hollerith tarafından geliştirilen sistemde 240 değerlendirme kriterinin her biri için bir kare ayrılmıştı, söz konusu kare delikse evet, değilse hayır anlamına geliyordu. Bugün bilgisayarlarda da 1 ve 0'lar kullanılarak yapılan sistemle benzer nitelikte olan bu sistem mekanik hesaplama döneminin de başlangıcı olarak kabul edilmişti. Daha sonraları Herman Hollerith'in patentlerini işlemek ve geliştirmek amacıyla kurulan IBM dünyanın en büyük şirketlerinden biri olmayı başarmıştır¹⁰.

Karar alma yeteneğine sahip ilk makine 1912 yılında Leonardo Torres y Quevedo tarafından geliştirilmişti. Torres, bu makineden basit satranç problemlerinin çözümünde faydalanmıştır. Bu makinenin yapay zekâya sahip ilk makine olarak kabulü ise 1914 yılında University of Paris tarafından yapılmıştır¹¹.

Bilgisayara giden yolda gelişmeler 1930 ve 1940'lı yıllarda hız kazanmıştır. Bu dönemde elektronik devreler bulunmuş, Konrad Zuse'nin 1941 yılında tamamladığı Z3, ilk bilgisayar ünvanına sahip olmuştur¹². Onu ilk elektronik dijital bilgisayar Atanasoff-Berry izlemiştir. Colossus bilgisayarı 2. Dünya Savaşı'nda İngilizler tarafından Almanların yazışmalarını çözmek için kullanılmıştır. Harvard Üniversitesi'nde 1937-1944 yılları arasında geliştirilen Harvard Mark I, CPU(merkezi işlem birimi) kullanan ilk bilgisayar olmuştur. Bu aşamadan

⁶ UYSAL, Dudu. "Dijital ve Sanal Yansımalar Wolfgang Hohlbein'in "Im Netz der Spinnen" ve "Das Netz" Adlı Romanları" - İksad Uluslararası Yayınevi, Ankara, 2020, s. 23. <https://iksadyayinevi.com/wp-content/uploads/2020/04/D%C4%B0J%C4%B0TAL-VE-SANAL-YANSIMALAR-WOLFGANG-HOHLBEIN%E2%80%99IN-%E2%80%99CIM-NETZ-DER-SPINNEN%E2%80%9D-VE-%E2%80%9CDAS-NETZ%E2%80%9D-ADLI-ROMANLARI-.pdf>

⁷ DÖNMEZ, Ali. "Bilgisayarcı matematikçiler." Doğu Üniversitesi Dergisi, Cilt 2, Sayı 2, 2001, s.30. <http://journal.dogus.edu.tr/index.php/duj/article/view/214>

⁸ DÖNMEZ, s. 37.

⁹ AK, Bilal. Türkiye'de sağlık bilişimi, bir kişisel değerlendirme ve uluslararası bir başarı öyküsü: CorTTex. Akademik Bilişim, 2009, 11-13.

¹⁰ UYSAL, s. 25-26.

¹¹ GONZALEZ Redondo, Francisco A. The Contribution Of Leonardo Torres Quevedo To Lighter-Than-Air Science And Technology. The International Journal For The History Of Engineering & Technology, 2011,81.2:212-232.

¹² <https://dergi.bmo.org.tr/bilisim-tarihi/konrad-zuse-ve-makineleri>, 16.12.2020

sonra artık hesaplayıcılardan bilgisayarlara geçilmiştir.¹³. Amerikan ordusu tarafından geliştirilen ENIAC ilk genel amaçlı kullanılabilen bilgisayardır¹⁴. ENIAC birinci kuşak bilgisayarların ilki sayılmış ve bunu dört kuşak daha izlemiştir. Yani günümüzdeki bilgisayarların gelişimi beş farklı kuşakta gerçekleşmiştir.

Değişen her kuşakla birlikte bilgisayarların boyutları küçülmüş, performansları artmış ve çevre donanımları gelişmiştir.

1946-1959 yılları arasında bilgisayarlar birinci kuşaklarını yaşamıştır. Bu dönem bilgisayarları vakumlu tüp teknolojisi ile çalışıyorlardı. 30 ton ağırlığında olan ve 167 m² yer kaplayan ENIAC tam 18.000 vakumlu tüp ile çalışıyordu¹⁵.

Birinci kuşak bilgisayarların genel özellikleri şu şekilde sıralanabilir; işlemci olarak büyük vakumlu tüpler kullanmaları, çok yüksek enerji harcamaları, programların makine dilinde yazılmış olması, saklama aracı olarak manyetik tüplerin kullanılması, çevreye çok fazla ısı yaymaları ve soğutulmalarının uzun sürmesi, veri programlarını ana bellekte tutmaları ve yavaş çalışmaları. Birinci kuşak bilgisayarlar vakum tüplü bilgisayarlar olarak da anılırlar¹⁶.

1959-1964 yıllarında bilgisayarlar ikinci dönemlerini tamamlamıştır. Bu dönemki bilgisayarlar transistör teknolojisiyle üretildiği için Transistörlü Bilgisayarlar olarak da anılırlar. Birinci kuşaktaki bilgisayarlara nazaran daha hızlıdır ve daha az enerji harcarlar. Boyutları da birinci kuşak bilgisayarlara nazaran oldukça küçüktür. Bu kuşakta FORTRAN, CALGOL, ALGOL gibi bilgisayar dilleri kullanılmıştır. İkinci kuşak bilgisayarların genel özellikleri şu şekilde sıralanabilir; işlemci olarak transistör kullanmaları(Ortalama 10 bin civarı transistör ile çalışıyorlardı.), bellek kapasitelerinin birinci kuşak bilgisayarlara nazaran daha fazla olması, daha az enerji kullanmaları ve daha az ısı yaymaları, transistörlerin tabloların içine elle işlenmesi. Bu dönemde IBM serisi ve BURROUGHS serisi modeller üretilmiştir. Üretilen ilk model IBM 1401'dir¹⁷.

Entegre Devreli yani üçüncü kuşak bilgisayarlar dönemi 1964 yılında başlayıp 1970 yılına kadar sürmüştür. Bu dönemde bilgisayar boyutları çok daha önemli ölçüde azalmış ve performansları artmıştır. IBM 360 ve 370, RCA Spectra 70 ve HONEYWELL 2200 bilgisayarları bu dönemde üretilmiştir. IBM 360 bu dönemin ilk bilgisayarıdır. Bu dönemdeki bilgisayarların genel özellikleri şu şekildedir; işlemci olarak entegre devreler kullanmaları, manyetik diskler kullanmaları, aynı anda birden fazla program işleyebilmeleri, program ve verileri gerektiğinde depolayabilmeleri, maliyetlerinin düşük olması, daha güvenilir olmaları, daha hızlı ve daha yüksek kapasiteli olmaları¹⁸.

1970 yılına gelindiğinde ise bilgisayarlar için dördüncü kuşak başlamıştır. Bu dönemin en önemli özelliği bilgisayarlarda mikroişlemci kullanılmaya başlanmış olmasıdır. Bu teknoloji sayesinde bilgisayarlar oldukça küçülmüştür. Güç tüketimleri azalmış ve

¹³<https://www.milliyet.com.tr/teknoloji/bilgisayarlarin-tarihi-1362416>, 13.08.2020,

¹⁴<https://www.hurriyet.com.tr/gundem/eniac-nedir-ne-ise-yarar-40485962>, 14.08.2020.

¹⁵<https://www.hurriyet.com.tr/gundem/eniac-nedir-ne-ise-yarar-40485962>, 14.08.2020.

¹⁶<https://bembilgisayar.com/bilgisayar-kusaklari>, 02.04.2020.

¹⁷<https://bembilgisayar.com/bilgisayar-kusaklari>, 02.04.2020.

¹⁸<https://bembilgisayar.com/bilgisayar-kusaklari>, 02.04.2020.

performansları artmıştır. Bu dönemde geliştirilen ilk mikro işlemci İntel 4004'dir. Ayrıca bu dönemde yapay zekâ kavramı da ortaya çıkmıştır. Yine bu dönemde bilgisayarlar arasında ağlar vasıtasıyla iletişim sağlanmış, depolama konusunda da önemli gelişmeler yaşanmıştır¹⁹.

Beşinci kuşak bilgisayarlar dönemi ise 1990 yılında başlamıştır. Bu kuşak bilgisayarlar günümüzde de gelişmeye devam etmektedir. Bu dönemde yapay zekâ teknolojileri hız kazanmıştır. Bu dönemin bilgisayarları problem çözmede çok daha ileri boyutlardadır. Bu dönemin bilgisayarları insan ile eş zamanlı çalışmaya başlamıştır²⁰. Bu bilgisayarlar oldukça kabiliyetlidirler ve insan zekâsına yakın düzeyde işlem yapabilmektedirler. Günümüzde de gelişmeye devam ettikleri için bu bilgisayarların mevcut durumundan çok dönemin sonunda gelecekleri seviye önemlidir²¹.

1.1.1.3. Yapısı

Bilgisayarlar en basit düzeyde donanım ve yazılım olarak ikiye ayrılırlar. Bilgisayarın elektronik unsurlarına donanım, program kısmına ise yazılım ismi verilir.

Bilgisayarın fiziksel organları da kendi içerisinde ikiye ayrılır. Bunlar, giriş birimleri ve çıkış birimleridir. Tüm bu birimler merkezi işlem birimine (CPU) bağlı olarak çalışmaktadır. Ayrıca depolama ve bellek birimleri de donanım unsurlarına dâhildir. Tüm bu donanım unsurlarının üzerine yerleştirildiği donanım parçası ise anakarttır.

Merkezi işlem birimi bilgisayarın içindeki veri akımını yönetir. Hesaplamaları yapan ve komutları işleyen birim de budur.

Bilgisayar içindeki veriler sabit diskte tutulur. Bilgisayarlarda bir ya da daha fazla sabit disk bulunabilir. Sabit diskler özelliklerine göre farklı boyutlarda veri tutabilirler. Ayrıca her sabit diskin bir dönüş hızı vardır, bu dönüş hızı bilgisayar performansına doğrudan etki eder. Ayrıca bilgisayar içerisindeki verilerin harici disklerde tutulması da mümkündür.

Ana bellek (RAM), bilgisayar içerisindeki verilerin yalnızca kullanıldığı anda tutulduğu bir depolama birimidir. Kullanıcı herhangi bir işlem yapmak istediğinde, sabit diskte ya da harici depolama cihazı üzerinde yazılı olan program ve veriler ana belleğe alınır. Bu programlar çalıştırıldığı sürece ana bellek bu verileri saklar, bu programların yaptıkları işlemlerin neticesini toplar ve tüm bu verileri merkezi işlem birimine aktarır.

Ekran kartı, işlemci tarafından üretilen görüntü bilgilerini ekrana gönderen donanım unsurudur. Ekran, merkezi işlem biriminden aldığı sinyalleri gözle görünebilecek şekilde görüntüye dönüştürür.

Ses kartları, bilgisayarda dijital olarak var olan sesleri hoparlör gibi donanım unsurlarına aktararak kulağın algılayabileceği şekilde sese dönüşmesini sağlar.

¹⁹ GÖKBULUT, İlker, Bilgisayar Uygulamaları, İstanbul Üniversitesi Açık ve Uzaktan Eğitim Fakültesi, s. 14, http://auzefkitap.istanbul.edu.tr/kitap/sivilhava_ao/bilgisayaruygulamalari.pdf, adresinden alınmıştır.

²⁰ <https://bembilgisayar.com/bilgisayar-kusaklari/>, 02.04.2020.

²¹ GÖKBULUT, s. 14-15.

Klavye, bilgisayarda yazı yazılmasını sağlayan temel giriş birimidir. Fare ise kullanıcının sistem içerisinde hareket yoluyla işlem yapmasını sağlayan giriş aygıtıdır.

Yazılım ise kullanıcının işlevlerini yapmasını sağlayan programlardır.

İşletim sistemi yazılımları, bilgisayarın yapacağı bütün işleri yöneten programlardır. Windows, Linux, Android, iOS işletim sistemlerine örnek olarak verilebilir.

Bunun dışında her biri farklı bir işlem için yazılmış uygulama yazılımları vardır. Word, Excel gibi yazılımlar, oyun yazılımları, iletişim uygulamaları vb. yazılımlar bunlara örnek verilebilir.

1.1.2. Veri

Veri, temel anlamıyla bilgi demektir. Sözlükte olguların, komutların ya da kavramların, yoruma, iletişime ve işleme uygun biçimde gösterimi, data, bilgi olarak tanımlanmıştır²².

Sanal Ortamda İşlenen Suçlar Sözleşmesinin 1. maddesinin b bendinde “*Bir bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsili*” olarak tanımlanmıştır.

Veri, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun’un 2. maddesinin k bendinde ise “*Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*” olarak tanımlanmıştır.

Veriler, bilişim sistemlerinin soyut unsurlarıdır. Veri kavramı bilgilerin soyut bir şekle çevrilmiş hali olarak tanımlanmıştır²³. Bilgisayarda yer alan bilgilerin formatlanmış hali olması bakımından veri bilgisayar programlarını da kapsamaktadır²⁴.

Veriler bilgisayar sistemlerinin temelini oluşturur. Bilgisayarlar yaptıkları her işlemde verileri kullanır ve yeni veriler üreterek bunları depolar. Bu nedenle bilişim suçlarının incelenmesinde veri kavramı önemli bir yer tutmaktadır.

1.1.3. İnternet

1.1.3.1. Genel Olarak

İnternet, küresel çaptaki bilgisayar sistemlerinin birbiriyle iletişim kurmasını ve veri transferi yapmasını sağlayan ağıdır. Sözlükte “*genel ağ*” olarak tanımlanmıştır²⁵. İnternet kelimesi, interconnected (kendi arasında bağlı) ve network (ağ) kelimelerinin birleştirilmesinden oluşturulmuştur.

²² <https://sozluk.gov.tr/>, 03.04.2020.

²³ KARAKEHYA, Hakan, Türk Ceza Kanunu’nda Bilişim Sistemine Girme Suçu, TBB Dergisi, 2009, 81: 1-24, s. 10. (<http://tbbdergisi.barobirlik.org.tr/m2009-81-498> adresinden alınmıştır.)

²⁴ DEĞİRMENCI, Olgun, Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi, TBB Dergisi, 2004, 58: 195-208, s. 199 – 200.

²⁵ <https://sozluk.gov.tr/>, 03.04.2020.

İnternet kendi içerisinde pek çok farklı ağ barındırır. Bu ağların birleşmesiyle internet oluşmuştur. Örneğin ticari ağlar, akademik ağlar, kurum ağları gibi ağlar bir araya gelmiştir.

İnternet ile ilgili ilk önemli gelişme ARPANET'tir. ARPANET, ABD Savunma Bakanlığı tarafından kurulmuştur. 29 Ekim 1969 tarihinde ARPANET üzerinden ilk iletinin gönderimi gerçekleşmiştir. İlk ARPANET hattı ise 21 Kasım 1969'da Kaliforniya Üniversitesi ile SAE arasında oluşturulmuştur. 1 Ocak 1983'te TCP/IP'nin kullanılmaya başlanmasıyla internet bugünkü halini almıştır. İlerleyen dönemde ARPANET yerini uluslararası ağlara bırakmıştır²⁶.

Türkiye'de internet ile ilgili ilk gelişme 1987'de Ege Üniversitesi öncülüğünde kurulan TÜVAKA'dır. 12 Nisan 1993'te ise ODTÜ ile ABD'de arasında Türkiye'nin ilk internet bağlantısı yapılmıştır²⁷. İlerleyen yıllarda Bilkent, Boğaziçi, Ege ve İTÜ de bu ağa bağlanmıştır. 1994 yılında T.C. Merkez Bankası da bu ağa bağlanmıştır²⁸.

1.1.3.2 İnternet İle İlgili Kavramlar

1.1.3.2.1. TCP/IP

IP adresi, aynı ağa bağlı olan bilgisayarların birbirini tanımak ve veri iletişimi yapmak için kullandıkları adrestir²⁹.

TCP/IP Transmission Control Protokol(Aktarım Denetim Protokolü) ve Internet Protokol'ün (İnternet Protokolü) kısaltılmış şeklidir. Günümüzde en yaygın kullanılan protokol takımı TCP/IP'dir.

İnternete ile bağlı olan her bir cihaz IP adresine sahiptir. Bu adres o bilgisayarındır ve onu tanımlar. İnternet üzerinden veri alışverişi yapılırken gönderici ve alıcı bu adres vasıtasıyla tanınmaktadır.

İnternet üzerinden gönderilen veriler küçük paketlere bölünür. Bu paketler IP adresleri vasıtasıyla doğru hedefe iletilir. Düzenli ya da düzensiz olarak gelen bu küçük paketler TCP ile ilk düzenine getirilir³⁰.

1.1.3.2.2. Domain ve DNS

Domain kavramı, alan adı anlamına gelmektedir. Bir internet sitesine ulaşmak için kullanılan adresin tanımlar. google.com, yahoo.com, yalova.edu.tr, yok.gov.tr alan adlarına örnek olarak verilebilir. Türkiye'nin kendine özgü alan adı uzantısı “.tr”dir. 1991-2020 yılları arasında www.nic.tr adresi üzerinden dağıtımı yapılmıştır. Şu anda ise bu uzantı BTK tarafından sağlanmaktadır.

²⁶ <http://www.internetarsivi.metu.edu.tr/tarihce.php>, 03.04.2020.

²⁷ <http://www.internetarsivi.metu.edu.tr/tarihce.php>, 03.04.2020.

²⁸ <http://internet.org.tr/>, 03.04.2020.

²⁹ DÜLGER, Murat Volkan; MODOĞLU, Gözde. Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku Uygulama Rehberi (Cybercrimes, Investigations and Trials for Cybercrimes and Internet Telecommunication Law, s.25.

³⁰ <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html>, 03.04.2020.

DNS ise Türkçeye alan adları sistemi olarak çevrilebilecek Domain Name System'in kısaltmasıdır. İnternet sitelerinin içerikleri bir sunucu üzerinde tutulur. Her bilgisayarın olduğu gibi sunucuların da bir IP adresi vardır. Kullanıcı internet tarayıcısına bir web sitesinin adresini yazdığında söz konusu internet sitesinin bulunduğu sunucuya yani bu sunucunun IP adresine bağlanmasını sağlayan sistem DNS'tir.

Böyle bir sisteme ihtiyaç duyulmasının sebebi IP adreslerinin zor hatırlanabilir olmasıdır. Kullanıcı bu karmaşık rakamlar dizisini ezberlemek yerine çok daha kolay olan alan adını yazarak web sitelerine bu şekilde ulaşabilmektedir.

Her alan adının belirli bir kullanım alanı vardır; com uzantısı ticari kuruluşlar için, net internet hizmeti sağlayan ağlar için, org sivil toplum örgütü ve benzeri kurumlar için, edu eğitim kurumları için, gov hükümet kurumları içindir. Ancak günümüzde bu sisteme pek riayet edilmemektedir. Özellikle günümüzde bu uzantılara alternatif pek çok uzantının da gelmesiyle alan adları sistemi yeni bir hal almıştır. Yeni domain uzantılarına .name, .museum, .istanbul, .asia, .press vb örnekler verilebilir. Bu uzantılarla birlikte alan adları eskiye nazaran çok daha özelleştirilebilir olmuştur. Ülkemizde .ist ve .istanbul alan adları diğer alan adlarından farklı olarak nic.istanbul adresi üzerinden dağıtılmaktadır.

1.1.3.2.3. WWW

WWW, dünya çapında ağ(world wide web) anlamına gelmektedir. WWW, web sayfalarının internet üzerinden birleşmesiyle oluşan devasa ağı ifade eder.

1.1.3.2.4. URL

URL bir web sitesi üzerinde yer alan içeriğin, o site içerisindeki konumu olarak ifade edilebilir. Uniform Resource Locator sözcüklerinin kısaltmasıdır. Türkçeye değişmez kaynak bulucu olarak tercüme edilebilir. 5651 sayılı yasanın 2. maddesinde de bu kavramın bir içeriğin internet üzerinde yer aldığı tam adresi ifade ettiği belirtilmiştir.

Örneğin Yalova Üniversitesi Sosyal Bilimler Enstitüsü'nün tez yazım kılavuzunun bulunduğu URL <http://sbe.yalova.edu.tr/Page/Icerik/tez-proje-yazim-yonergesi> şeklindedir. Tarayıcıya bu adres yazıldığında doğrudan ilgili sayfa açılacaktır.

1.1.3.2.5. Yer Sağlayıcı

5651 sayılı yasanın 2. maddesinin k bendinde yer sağlayıcının hizmetlerin ve öğelerin içinde bulunduğu sistemlerin işletmecisi ya da sağlayıcısı olan gerçek veya tüzel kişileri ifade ettiği belirtilmiştir.

Yer sağlayıcılara örnek olarak forum siteleri, sosyal medya siteleri gibi siteler verilebilir. Bu siteler kullanıcılara içerik paylaşımları için gerekli ortamı sağlamakta ve bu paylaşılan içerikleri barındırmaktadır.

Öte yandan yer sağlayıcı terimi web sitelerinin barındığı sunucuları web site sahibine kiralayan host şirketlerini de ifade eder.

5651 sayılı yasanın 5. maddesinin ilk dört fıkrasında yer sağlayıcı olan gerçek ya da tüzel kişilerin yer sağladıkları içerikleri kontrol etmekle, hukuka aykırı bir işleğin bulunup bulunmadığını denetlemekle yükümlü olmadıkları düzenlenmiştir. Bununla birlikte yer

sağlayıcıların hukuka aykırı bir içeriğin varlığından haberdar edilmesi durumunda bu içeriği yayından kaldırmak yükümlülüğü vardır. Ayrıca yer sağlayıcılar hizmetlerine ilişkin trafik bilgilerini yönetmelikte belirlenecek süre boyunca depolamak ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdürler.

1.1.3.2.6. İçerik Sağlayıcı

5651 sayılı yasanın 2. maddesi f bendinde içerik sağlayıcının internet ağı aracılığıyla kullanıcılara ulaştırılan bilgileri ve içerikleri üreten, değiştiren, sağlayan gerçek veya tüzel kişileri ifade ettiği belirtilmiştir.

İçerik sağlayıcılar bir web sitesindeki içeriği oluşturan, paylaşan veya değiştiren kişilerdir. Bir forum sitesinde ya da bir sosyal medya sitesinde paylaşım yapan kullanıcı içerik sağlayıcı olduğu gibi kendisine ait bir web sitesi üzerinde içerik yayınlayan kişi de içerik sağlayıcıdır.

5651 sayılı yasanın 4. fıkrasına ile içerik sağlayıcılar internet üzerinden kullanıcıya açtıkları her türlü içerikten sorumlu tutulmuştur ancak içerik sağlayıcının bir başka içeriğe bağlantı sağlamış olması dolayısıyla bir sorumluluğu yoktur. Öte yandan bağlantı sağladığı içeriği benimsediğini ve kullanıcının bu içeriğe ulaşmasını amaç edindiğini açıkça belli etmiş ise genel hükümlere göre sorumluluğu devam edecektir.

1.1.3.2.7. Sunucu

İnternet üzerinden yapılan paylaşımların barındığı ve diğer kullanıcılara sunulduğu bilgisayarlardır. Günümüzde büyük hosting firmaları bulunmakta ve pek çok web sitesi, içeriklerini bu firmaların sunucularında barındırmaktadır. Başta büyük siteler olmak üzere bir kısım siteler ise kendilerine ait sunucuları kullanmaktadır. Ayrıca herhangi bir kullanıcının kendisine ait bir ev bilgisayarını dahi sunucu olarak kullanması mümkündür.

1.1.3.2.8. Log Kaydı

Log kaydı, yapılan işlemlerin kayıtlarına verilen isimdir.

5651 sayılı yasanın 5. maddesinin 3. fıkrası ile yer sağlayıcılara log kaydı tutulması zorunluluğu getirilmiştir. Log kayıtları sayesinde bir web sitesi üzerinden yapılan paylaşımın hangi gün hangi saatte hangi IP adresi üzerinden yapıldığı anlaşılabilmektedir.

1.1.3.2.9. Ağ (Network)

Ağ, iki veya daha fazla bilgisayarı birbirine bağlayan sistemdir. Bu bağlantı günümüzde kablolu ya da kablosuz olarak sağlanabilmektedir. En büyük bilgisayar ağı ise internettir.

1.1.3.2.10. ISS(Erişim Sağlayıcı)

5651 yasanın 2. maddesinin e bendinde erişim sağlayıcının kullanıcılara internete ağına ulaşım imkânı sunan gerçek ve tüzel kişileri ifade ettiği belirtilmiştir. Erişim sağlayıcılara örnek olarak TTNET, Turkcell, Vodafone gibi firmalar verilebilir. Kullanıcılar bu firmaların sundukları hizmetler vasıtasıyla internete erişim sağlamaktadır.

Bir suçun soruşturulması ya da kovuşturulması aşamasında IP adresleri hukuka aykırı erişimin yapıldığı yer sağlayıcıdan temin edilmektedir. Erişim sağlayıcılar bu durumlar IP

adresinin tahsis edildiği kullanıcının açık kimlik bilgilerini yetkili makamla paylaşmaktadır. Aynı şekilde Bilgi Teknolojileri Kurumu'ndan da bu bilgilerin temin edilmesi mümkündür.³¹

5651 sayılı yasanın 6. maddesine ile erişim sağlayıcılar kullanıcılarının yayınladığı hukuka aykırı içeriklerinden haberdar edildiği takdirde bu içeriğe erişimi engellemekle ve hizmet sağladığı işlere ilişkin trafik bilgilerini yönetmelikte belirtilen süre boyunca depolamakla ve bunları bütünlüğünü, doğruluğunu, gizliliğini temin etmekle yükümlüdür. ISS'in bu bilgileri kuruma teslim etme yükümlülüğü vardır. Etkinliğini sona erdirmeye karar veren erişim sağlayıcılar en az üç ay önceden durumu kuruma, içerik sağlayıcılara ve müşterilerine bildirmekle yükümlüdür. Ancak erişim sağlayıcı, kullanıcılarının eriştikleri içeriklerin hukuka uygunluklarını denetlemekle ya da bu kişilerin sorumluluklarını yerine getirip getirmediıklarını incelemekle yükümlü değildir.

1.1.3.2.11. İnternet Tarayıcısı

İnternet tarayıcısı, kullanıcıların internet üzerinde yer alan siteleri görüntülemelerini sağlayan yazılımlardır. En bilinen internet tarayıcıları, Google Chrome, Opera, Mozilla Firefox, Microsoft Edge ve Safari'dir.

1.1.3.2.12. Sosyal Medya

Sosyal medya, içeriklerini yer sağlayıcıların değil bir web sitesini kullanan kişilerin oluşturduğu sistemdir. Bu tür sitelerde içerik akışı tek yönlü değildir. Her bir kullanıcı içeriklerin hem üreticisi hem de hedefidir. İnternet forumları ve bloglar sosyal medyanın öncüsü olarak görülebilir. LinkedIn, Myspace, Facebook, Reddit, YouTube, Twitter, Tumblr, Foursquare, Instagram, Snapcht en bilinen sosyal medya platformlarıdır.

İlk blog sitesinin 1994'te kurulduğu yine 1990lı yılların başından itibaren pek çok sosyal iletişim sitesi ve hizmetinin bulunduğu göz önüne alındığında sosyal medyanın tarihinin yukarıda sayılan platformlardan çok daha eski olduğu görülecektir.

1.1.3.2.13. Nesnelerin interneti

Nesnelerin interneti, nesnelerin birbirleriyle ya da ağlarla bağlantılı oldukları ağa verilen isimdir.

Günümüzde nesneler internete bağlanabilmekte, veri gönderip alabilmektedir. Bir kimse evde değilken dahi evindeki ışıkları açabilmekte, kahve makinesini çalıştırabilmektedir. Otobüs durakları otobüs ile internet üzerinden iletişim kurarak otobüslerin yerini öğrenmekte ve kaç dakika içinde durağa varacağını hesaplamaktadır. Bunlar ve bunlar gibi sayısız örnek verilebilir nesnelerin interneti için.

Nesnelerin kendi ağlarını kullanıyor olmalarının insan yaşamını kolaylaştırdığı kuşkusuz olmakla birlikte bu durum kötü niyetli kimselerce güvenlik zafiyetlerine dönüştürülmesi imkânı da bulunmaktadır.

³¹ SEMİZ, Murat, İçtihatlar ve Uygulamadan Örnekleriyle Bilişim Suçları ve Soruşturma Yöntemleri, Adalet Yayınevi, Ankara, 2020, s. 25.

1.1.4. Bilişim ve Bilişim Sistemi

Bilişim sözlük anlamı ile insanlığın teknik, ekonomi ve sosyal alandaki haberleşmesinde yararlandığı ve bilimin temeli olan bilginin özellikle elektronik makineler aracılığıyla sistematik ve ussal bir biçimde işlenmesi bilimi, enformatik demektir³². Doktrinde bilişim kelimesinin hem bilgi işlemi hem de veri aktarımını ifade ettiği belirtilmiştir³³. Bilişim sisteminin ise çevre birimleri ile iletişim alt yapısı ve programların oluşturduğu, veri işleme ve saklama ve iletme sistemi olarak ifade edilmiştir³⁴. Bilişim sözcüğü enformasyon ve otomatik kelimelerinin bir araya getirilmesinden türetilmiş olan enformatik sözcüğünün Türkçe karşılığıdır. Enformasyonun makineler aracılığı ile işlenmesi anlamına gelmektedir³⁵.

TCK'nın 243. maddesinin gerekçesinde “*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.*” denilerek bilişim sisteminin tanımı yapılmıştır. Bu tanıma göre bilişim sisteminin özellikleri, manyetik bir sistem olması, verileri toplayıp yerleştirmesi ve verileri otomatik işlemlere tabi tutmasıdır³⁶. Bu tanım yetersiz olduğu gerekçesi ile eleştirilmiş, bilişim sisteminin veriyi saklayan, sakladığı bu verileri otomatik olarak işleyen, organize eden, değerlendiren ve aktaran yönünün tanımda yer alması gerektiği savunulmuştur³⁷. Bir görüşe göre TCK'nın gerekçesinde yapılan tanımın bilişim sisteminden ziyade bilgisayarı ifade ettiği belirtilmiştir³⁸.

Bilgisayar ile bilişim sistemi aynı şey değildir. Bilişim sistemi ifadesi bilgisayarı da içine alan çok daha geniş bir çerçeveyi ifade eder³⁹. Bilişim sistemini bilgisayarlardan farklı kılan en önemli unsur bilgileri otomatik olarak işleme tabi tutmasıdır⁴⁰.

Öte yandan TCK'nın üçüncü kısım onuncu bölümünün başlığı “Bilişim Alanında Suçlar”dır. Buna rağmen TCK'da, gerekçesinde ya da sair kanunlarda bilişim alanı kavramı tanımlanmamıştır. Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu'nda ise “*Bilişim alanından maksat verileri toplayıp yerleştirdikten sonra bunları otomatik*

³² <https://sozluk.gov.tr/>, 03.04.2020.

³³ BOZDOĞAN AKBULUT, s.546.

³⁴ DÜLGER, Murat Volkan; MODOĞLU, Gözde. "Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku Uygulama Rehberi (Cybercrimes, Investigations and Trials for Cybercrimes and Internet Telecommunication Law).

³⁵ KETİZMEN, Muammer, “Türk Ceza Hukukunda Bilişim Suçları”, Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 8.

³⁶ ÖZBEK, Veli, Özer, "Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)". Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 9 / 0 (July 2007): 1019-1063, s. 1024. (<https://dergipark.org.tr/en/pub/deuhfd/issue/46938/589018> adresinden alınmıştır.)

³⁷ DEĞİRMENCI, s. 199.

³⁸ ERDAĞ, Ali İhsan. Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). Gazi Üniversitesi Hukuk Fakültesi Dergisi, 2010, 14.2: 275-303. s. 278.

³⁹ KETİZMEN, s. 19.

⁴⁰ ÖZBEK, s. 1025.

işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.” ifadesine yer verilmiştir⁴¹. Bu tanım TCK’nın 243. maddesinin gerekçesinde bilişim sistemi için yapılan tanım ile benzerlik göstermektedir.

1.2. Bilişim Suçları İşlenirken Yaygın Olarak Kullanılan Yöntemler ve Araçlar

1.2.1. Bilişim Suçlarının İşlenmesi Amacıyla Kullanılan Programlar

TCK’nın 243 ila 246 maddeleri arasında düzenlenen suçlar başta olmak üzere bilişim yoluyla işlenebilen pek çok suç tipi belirli bir uzmanlık gerektirmekte ve genellikle uzman kişiler tarafından, özel yazılımlar kullanılarak işlenmektedir. Bu yazılımların oluşturulması, satılması, satın alınması, dağıtılması ve hatta bulundurulması dahi TCK’nın 245/A. maddesinde düzenlenen suçu oluşturacaktır. Bunun yanı sıra bu yazılımlar kullanılarak genellikle sistemlere ya da sistemdeki verilere zarar verilmesi amaçlandığından TCK’nın 244/1. ve 244/2. maddelerinde düzenlenen sistemi engelleme, bozma, verileri yok etme veya değiştirmek suçu bu yazılımlar kullanılarak en çok işlenen suçtur. Failin bu yolla menfaat temin etmesi halinde 244/4. fıkrasında düzenlenen suç da uygulama alanı bulacaktır. Bunun dışında TCK’nın 132. ila 140. maddeleri arasında düzenlenen Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar da yaygın olarak bu yazılımlar vasıtası ile işlenebilmektedir.

1.2.1.1. Virüsler (Viruses)

Siber saldırılar denildiğinde ilk akla gelen kavram genellikle virüslerdir. Bu durumun temelinde halk arasında virüs kavramının diğer kötü amaçlı yazılımların yerine, genel bir isim olarak kullanılması da yatmaktadır.

Virüsler en basit tanımıyla uzman yazılımcılar tarafından birden fazla bilgisayara kopyalanmak amacıyla yazılan, farklı türleri bulunan yazılımlardır. Temel anlamda sıradan bir bilgisayar programı olan virüsler girdiği sistemlerde kendilerini kopyalayabiliyor olmaları dolayısıyla ayrışır. Virüsler bu sayede sistemin kapanmasına, çalışmaz hale gelmesine sebep olabilir ya da sistemdeki bazı veri ya da programları çalışamaz hale getirebilir.

Bir virüsün çalışma sistemi temelde 3 ana evreden oluşur. Bunlar çoğalma, programın tetiklenmesi ve önceden amaçlanan zararın verilmesidir⁴². Virüslerin en belirgin özelliği insan etkileşimi ile tetiklenmeleridir⁴³. Örneğin kullanıcının bir linke tıklaması ve virüslü dosyayı indirmesi, virüs içeren bir flaş diskin kullanılması ya da virüslü bir elektronik posta eklentisinin açılması gibi işlemler sonucunda virüs kullanıcı tarafından yayılır.

⁴¹ Türk Ceza Kanunu Tasarısı ve Adalet Komisyonu Raporu (1/593), <https://www.tbmm.gov.tr/sirasayi/donem22/yil01/ss664m.htm>.

⁴² SAMET, Refik. "BÖLÜM 8: KÖTÜ AMAÇLI YAZILIMLAR VE ANALİZİ." in SAĞIROĞLU, Şeref, ALKAN, Mustafa, Siber Güvenlik ve Savunma Farkındalık Ve Caydırıcılık, Grafiker Yayınları, Ankara, 2018, s. 228. <https://acikerisim.siiir.edu.tr/xmlui/handle/20.500.12604/883>

⁴³ CANBEK, Gürol; SAĞIROĞLU, Şeref. Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. Gazi Üniversitesi, Mühendislik Mimarlık Dergisi, 2007.

Bir fikir olarak bilgisayar virüsleri yani kendi kendini kopyalayarak çoğalabilen yazılım fikri 1949 yılında matematikçi John von Neumann tarafından ortaya atılmıştır⁴⁴. Bilinen ilk bilgisayar virüsleri ise 1980’li yılların başlarında geliştirilmiştir.

Dünyanın ilk bilgisayar virüsü olarak kabul edilen Elk Cloner 1982 yılında 15 yaşında bir lise öğrencisi olan Rich Skrenta tarafından yazılmıştır. Bu virüs bilgisayar hafızasına yerleştikten sonra, bilgisayara takılan her diske kendisini kopyalayabilme becerisine sahiptir. Virüsün yaptığı tek şey ise bilgisayarın her 50. açılışında ekrana bir şiir getirmesidir.⁴⁵

Bir terim olarak bilgisayar virüsü ise 1983 yılında Fred Cohen tarafından tanımlanmıştır⁴⁶. Cohen, bu virüsü bilgisayar güvenliği konulu bir seminerde sunulacak bir deney için tasarlamış ve virüs ismi kendisine Len Adleman tarafından önerilmiştir⁴⁷.

Yaygın olarak bilinen bilgisayar virüslerine “Chernobly (CIH)” “Melissa” ve “ILOVEYOU” örnek olarak verilebilir. Bu virüslerden ILOVEYOU yalnızca bir gece içinde milyonlarca bilgisayara bulaşmayı başarmış ve tahmini olarak 10 milyar dolar civarında maddi zarara sebep olmuştur⁴⁸.

Virüsler temel olarak dört grupta incelenirler. Bunlar; dosya sistemi virüsleri, önyükleme bölümü virüsleri, makro yazılım virüsleri ve komut dosyası virüsleridir⁴⁹. Dosya sistemi virüsleri bir programa ya da dosyaya yapışırlar ve konakladıkları bu program çalıştırıldığında etkin hale gelirler. Önyükleme bölümü virüsleri ise disklerin ön yükleme bölümlerine yerleşerek bilgisayar her açıldığında aktif hale gelen virüslerdir. Makro yazılım virüsleri MS Office gibi makro yazılımların içerisinde gizlenen ve bu yazılımlar vasıtasıyla yayılabilen virüslerdir. Komut dosyası virüsleri ise internet sayfalarının kaynak kodu dosyaları aracılığıyla yayılan virüslerdir.

Bilgisayar virüsleri ile pek çok bilişim suçu işlenebilir de bilgisayar virüslerinin en sık kullandığı suç tipleri TCK’nın 244/1. ve 244/2. maddelerinde düzenlenen suç tipleridir.

1.2.1.2. Solucanlar (Worms)

Solucanlar bilgisayarlara saldıran ve ağ vasıtasıyla yayılan kötü amaçlı kod bilgisayar programdır⁵⁰. Solucanlar da virüsler gibi kendilerini kopyalayabilirler ancak virüslerden farklı olarak kendilerini başka makinelere ve ağlara kullanıcının müdahalesi olmadan

⁴⁴ <https://history-computer.com/Internet/Maturing/Thomas.html>, 23.03.2020.

⁴⁵ ÖZTÜRK, Cumali, TEKEREK, Mehmet, YILMAZ, Ahmet Serdar, “Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırması” in SAĞIROĞLU, Şeref, ALKAN, Mustafa, AKYILDIZ, Ersan, AKLEYLEK, Sedat, Bilgi Güvenliği ve Kriptoloji Konferansı Bildiri Kitabı, 25-26 EKİM 2016, s. 236., <https://www.iscturkey.org/assets/files/isc-BildiriKitabi2016.pdf>

⁴⁶ BASSHAM, Lawrence E., ve William T. Polk. Threat Assessment of Malicious Code and External Attacks. No. NISTIR-4939. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD, 1992, <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4939.pdf>

⁴⁷ <https://web.eecs.umich.edu/~aparaksh/eecs588/handouts/cohen-viruses.html>, 23.03.2020.

⁴⁸ <http://www.yeniduzen.com/viruslerin-tarihcesi-104990h.htm>, 25.03.2020.

⁴⁹ <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-Truva-at%C4%B1>, 23.03.2020

⁵⁰ https://help.eset.com/ecs/6/tr-TR/ud_glossary_virustypes_worms.html, 23.03.2020.

gönderebilirler. Herhangi bir kullanıcı etkileşimine ihtiyaç duymaksızın, bağımsız şekilde çalışırlar.

Bilinen ilk solucan 1970 yılında mühendis Robert (Bob) H. Thomas tarafından yazılmıştır. Bazı kimseler tarafından ilk bilgisayar virüsü olarak anılsa da Creeper adlı bu yazılım aslında bir solucandır. Creeper'in yaptığı şey ise bulaştığı bilgisayarlara "*I'M THE CREEPER : CATCH ME IF YOU CAN*(*BENİM ADIM CREEPER: BECERE BİLİRSEN BENİ YAKALA*)" yazmaktır. Bunun dışında bilgisayarlara hiçbir zarar vermeyen yazılım akademik bir araştırmanın parçası olarak yazılmıştır⁵¹. Solucanlar isimlerini ise John Brunner tarafından 1975 yılında yazılmış olan "Shockwave Rider" adlı bir bilim kurgu romanından almaktadır.

Solucanlar sistemlere çok çeşitli etkilerde bulunabilecek şekilde tasarlanabilirler. En yaygın örnekler bilgisayarın kontrolünü ele geçirmek, dosyaları silmek ya da dosya içeriklerini değiştirmek, bilgisayarları çökertmek, bilgisayarlara istenmeyen dosyalar indirmek, veri hırsızlığı yapmak, bilgisayardaki dosyaları kripto-viral gasp saldırısının bir parçası olarak şifrelemektir⁵². Bu sebeple soluncanların en çok kullandığı suç tipi TCK'nın 244/1. ve 244/2. maddelerinde düzenlenen suçlardır.

1.2.1.3. Truva Atı(Trojan Horses)

Truva atı ismini Truva efsanesinden almaktadır. Efsaneye göre İthika Kralı Odysseus Truva surlarını aşmak için tahtadan bir at maketi yaptırmış ve içine bir grup askerini gizlemiştir. Truvalılar ise bu atı içeriye almışlardır ve gece sızmış haldelerken atın içinde bekleyen askerler çıkarak şehri ele geçirmişlerdir. Truva atı normal bir bilgisayar programı gibi görünen ancak içinde zararlı kodlar barındıran yazılımlardır. Görünüşte gayet normal olan bu program kullanıcı tarafından çalıştırıldıktan sonra programın içinde bulunan kötü amaçlı yazılım da harekete geçer.

Programı kodlayan kişi sıfırdan bir program kodlayarak içine kötü amaçlı kodlar ekleyebileceği gibi var olan bir programın içine de bu kodları yerleştirebilir. Yaygın örneklerinden birisi ücretli olarak sunulan oyun ya da programların bir cracker(kırıcı) tarafından "crack(kırma ya da ilaç)" işlemi yapılır, daha sonra bu yazılımın içine zararlı kodları da ekleyerek yayınlar. Söz konusu yazılımı ücretsiz olarak elde etmek isteyen kullanıcı da ilaçlı dosyayı indirerek bilgisayarına yükler ve çalıştırır. Söz konusu programın çalışmasıyla birlikte program içine yerleştirilmiş Truva atı da harekete geçerek kendisini kodlayan kişi tarafından önceden verilmiş olan emri yerine getirir.

Truva atları virüsler ya da solucanlar gibi kendisini çoğaltamaz. Yine solucanlardan farklı olarak kendiliğinden harekete geçmez, içine gizlendiği yazılımın çalıştırılması yoluyla harekete geçer.

Truva atları 7 ana gruba ayrılır. Bunlar; uzaktan erişim sağlayan Truva atları, e-posta bilgilerini toplayan Truva atları, veri yıkımına sebep olan Truva atları, proxy Truva atları,

⁵¹ <https://www.kaspersky.com.tr/blog/faydali-virus-bir-sekilde-faydali-ilk-5-zararli-yazilim/1050/>, 23.03.2020

⁵² JOHNSON, Mark ,Cyber Crime, Security and Digital Intelligence, Gower, 2013, s. 48-49.

dosya gönderip alan Truva atları, güvenlik yazılımını devre dışı bırakan Truva atları, DoS saldırıları yapan Truva atları ve url Truva atlarıdır.

Arka kapı Truva atları, kendisini kodlayan kişinin hedef bilgisayardaki kontrolü ele almasını sağlar. Bu kişi hedef sistemde; dosya gönderebilir, dosya alabilir, bir programı başlayabilir, verileri silebilir ya da açabilir ve bilgisayarı yeniden başlatabilir. Sistem kullanıcısı pek çok zaman bunun farkına varmaz. Bu yazılımın amacı çoğu zaman botnet ya da zombi ağı kurmaktır⁵³.

PSW Truva atları, hedef bilgisayarda bulunan şifreleri, Trojan-GameThief online oyun hesaplarını, Trojan-Banker banka ve hesap bilgilerini, Trojan-IM mesajlaşma uygulamalarında kullanılan şifreleri çalmak için kullanılan Truva atlarıdır. Trojan-Downloader ve Trojan-Dropper bilgisayara zararlı yazılımlar yükleyen Truva atlarıdır. Proxy Truva atları, bilgisayarı saldırganın vekil sunucu olarak kullanmasına imkân sağlar. Trojan-Spy kullanıcının ekran, klavye ve fare gibi faaliyetlerini saldırgana gönderir. Trojan-FakeAV kullanıcıya bilgisayarda bir tehdit olduğu hissiyatı vererek para sızdırmayı amaçlar. Trojan-ArcBomb ya da arşiv bombaları arşiv dosyalarını açan programları sabote ederek bilgisayarın alakasız dosyalarla dolmasına ya da çökmesine neden olur⁵⁴.

Bilinen ilk Truva atı ANIMAL ismini taşımaktadır ve 1975 yılında John Walker tarafından geliştirilmiştir⁵⁵. Program 20 soruda kullanıcının düşündüğü hayvanı tahmin etmeye çalışan bir oyundan ibarettir. Oyun ön planda çalışırken arka planda sisteme güncel bir kopyasını yerleştiriyordu. ANIMAL ve arka planda çalıştırdığı PERVADE sistemde bulunan hiçbir şeyi silmemeye özen göstermiş olsa da kullanıcı ANIMAL’I çalıştırdığında PERVADE’nin de kendiliğinden harekete geçerek çalışması ve kullanıcıdan habersiz işlem yapması dolayısıyla bilinen ilk Truva atı örneği olarak kabul edilmiştir. Bilinen bir hasara yol açmamış ve kullanıcıların işlemlerini etkilememiştir. Bu bakımdan kötü amaçlı bir yazılım olarak tasarladığı söylenilemez.

ANIMAL, Walker tarafından San Francisco’da çalıştırıldıktan sonra bir hafta içinde Washington DC’ye kadar ulaşmıştır⁵⁶.

Truva atları kullanılarak genellikle sistemdeki verilere zarar verilmekte ya da sisteme veri yerleştirilmektedir. Bu sebeple Truva atlarının en çok kullanıldığı suç tipi 244/2. maddede düzenlenen suçtur.

1.2.1.4. Kök Kitleri (Rootkits)

Kök kitlerinin iki belirgin özelliği vardır; bunlar saldırgana bilgisayar sisteminde yönetici düzeyinde sınırsız erişim hakkı vermek ve işletim sisteminden gizlenmektir. Kök kitleri, bilgisayara yerleştikten sonra anti virüs yazılımı tarafından algılanmamak için işlemleri ve

⁵³<https://www.kaspersky.com.tr/resource-center/threats/trojans>, 24.03.2020.

⁵⁴<https://www.kaspersky.com.tr/resource-center/threats/trojans>, 24.03.2020.

⁵⁵ <https://www.kaspersky.com.tr/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>, 24.03.2020.

⁵⁶ <http://virus.wikidot.com/animal>, 24.03.2020.

dosyaları gizler ve kendisini normal yöntemlerle tespit edilemez hale getirir⁵⁷. Bu yazılımların çoğalma amacı yoktur, önceliği varlığını gizlemektir.

Kök kitleri tek başlarına çok zararlı olmasalar da virüs, solucan ve Truva atlarıyla birlikte çok etkili saldırılar yapmaktadırlar⁵⁸. Kök Kitleri de tıpkı diğer kötü amaçlı yazılımlar gibi genellikle TCK'nın 244/1. ve 244/22. maddelerinde düzenlenen suçlarda kullanılmaktadır.

1.2.1.5. Casus Yazılımlar (Spyware)

Yerleştiği bilgisayarda kullanıcılara ait bilgileri ve kullanıcı işlemlerini, kullanıcının kendisine hissettirmeden toplayan ve bu bilgileri saldırgana gönderen yazılımlara casus yazılım denilmektedir.

Sıklıkla virüs olarak adlandırılırsalar da casus yazılımlar virüs değildir. Bu yazılımlar virüs ve solucanlar gibi kendi kopyalarını oluşturmaz, sisteme yayılmazlar. Öte yandan kimi zaman casus yazılımlar virüslerle birlikte de sisteme gelebilmektedir.

Casus yazılımın amacı kullanıcıya ait belirli bilgileri toplamaktır. Bu bilgiler; kullanıcının klavye hareketleri, görüntülediği internet siteleri, arama geçmişi, elektronik postaları, banka ve kredi kartı bilgileri gibi kişisel güvenlik açısından önem arz eden bilgilerdir. Casus yazılımlar ayrıca kişinin sesini kaydedebilir, ekran görüntüsü yakalayabilir, cihazın uzaktan kontrolünü sağlayabilir, mesajlaşma uygulamalarının içeriklerini takip edilebilmektedir.

Casus yazılımların pek çok çeşidi vardır. Bunlar; adware, cookies, keylogger, infostealerlar ve Red Shell'dir.

Adware, kullanıcı geçmişini izleyerek kullanıcıya ilgi alanına yönelik reklamlar sunmayı hedefleyen köyü amaçlı yazılımdır. Bu yazılımın kötü amaçlı kabul edilmesindeki en önemli etken kullanıcının bilgisi dışında çalışması ve bilgi toplamasıdır⁵⁹. Ayrıca bu yazılım sistemde yavaşlamalara da sebep olabilmektedir.

Cookies ya da Türkçe adıyla çerezler kullanıcının ziyaret ettiği web sitelerinin kullanıcının bilgisayarında depoladığı bilgilerdir⁶⁰. Çerezler aslında kullanıcının web deneyimini daha iyi hale getirmeyi amaçlayan, faydalı bilgilerdir fakat kötü niyetli kimseler tarafından kullanıcı etkinliklerini izlemek için de kullanılabilirler. Tracking Cookie olarak anılan bu durum kullanıcının gezdiği tüm internet sitelerinin bilgilerini aktarabilir. Bu bilgiler arasında kullanıcıya ait oturum bilgilerinin yanı sıra banka ve kredi kartı bilgileri de bulunabilir.

Keyloggerlar, kullanıcının klavye hareketlerini izleyen ve kaydeden yazılımlardır. Keylogger yazılımları bu sayede kullanıcıya ait kullanıcı adı ve şifreleri, mesaj içeriklerini ve buna benzer önemli bilgileri kaydedebilmektedir.

⁵⁷

https://help.eset.com/ecs/6/tr-TR/ud_glossary_virustypes_rootkits.html?zoom_highlightsub=rootkit, 24.03.2020.

⁵⁸ SAMET, s. 231.

⁵⁹ <https://www.kaspersky.com.tr/resource-center/threats/adware>, 24.03.2020.

⁶⁰ <https://support.mozilla.org/tr/kb/cerezler-web-sitelerinin-bilgisayarinizda-depoladi>, 24.03.2020.

Infostealerlar, kullanıcıya ait bilgileri toplar. Keylogger da aslında bir tür bilgi toplayıcıdır ancak diğer tür bilgi toplayıcılar keyloggerlara nazaran çok daha fazla bilgiyi toplayabilmektedir. Bu bilgilere; tarama geçmişi, belgeler, mesajlaşmalar örnek olarak verilebilir⁶¹.

Red Shell, kullanıcıların oyun etkinliklerinin izlenmesi ve bu verilerin oyun firmalarına aktarılması amacı taşıyan bir casus yazılım türüdür. Bilinen pek çok oyun bir dönem bu yazılımla birlikte gelmiştir. Konunun sosyal paylaşım sitesi Reddit'te gündem olmasının ardından kimi oyun yapımcıları güncellemeler yayınlayarak Red Shell'i oyunlarından kaldırmıştır⁶².

Casus yazılımların kişisel verileri toplayan özellikleri göz önüne alındığında en çok kullanıldığı suç tiplerinin TCK'nın 135. ila 138. maddelerinde düzenlenen suçlar olduğu görülecektir.

1.2.1.6. Tavşanlar (Rabbits ya da Wabbits)

Tavşanlar da tıpkı virüsler ve solucanlar gibi kendilerini kopyalayan yazılım bir türüdür. Tavşanların virüslerden farkı herhangi bir program veya belgeye bulaşmamaları, solucanlardan farkı ise yayılmak için ağa ihtiyaç duymamalarıdır⁶³. Bu yazılım tıpkı tavşanlar gibi hızlıca çoğalmakta ve bir süre sonra sistem hafızasını tamamen doldurmakta, sistemi işleyemez hale getirmektedir. Virüsün ismi de çoğalma hızından gelmektedir.

Bir tavşan yazılımı hazırlamak oldukça basittir, genellikle birkaç satırlık bir kod ile dahi bir tavşan yazılımı oluşturulabilir. Bu sebeple tavşanlar bazen kasıtlı olarak yazıldığı gibi bazen de bir yazılım hatası sonucu sonsuz kopya oluştururlar⁶⁴. Kasıtlı olarak oluşturulan tavşanlar ise daha çok hizmet engelleme saldırılarında (DoS) kullanılırlar.

Bilinen ilk tavşan yazılımı 1974 yılında geliştirilen Fork yazılımıdır⁶⁵. Bu yazılım bulaştığı bilgisayarların çökmesine neden olmuştur. Fork yazılımından önce de benzer yazılımların bulunduğu söylenmektedir⁶⁶.

Tavşanlar da tıpkı virüsler ve solucanlar gibi genellikle TCK'nın 244/1. ve 244/2. maddelerinde düzenlenen suçların işlenmesinde kullanılmaktadır.

1.2.1.7. Bukalemunlar

Bukalemunlar, bilinen ilk polimorfik kötü amaçlı yazılımlardır. İlk bukalemun Mark Washburn tarafından yazılmıştır⁶⁷. Bu yazılım kendi kodunu yazabilen Cascade virüsüne benzese de her bulaştığı sistemde farklı kodlara bürünmesi yoluyla ondan ayrılmış ve çok daha ötesine geçmiştir⁶⁸. Bu yazılım ilk çıktığında o güne dek tek yaptıkları sistemde belirli

⁶¹ <https://www.avast.com/c-spyware>, 24.03.2020.

⁶² https://www.reddit.com/r/Steam/comments/8pud8b/psa_red_shell_spyware_holy_potatoes_were_in_space, 24.03.2020

⁶³ CANBEK, SAĞIROĞLU, s. 132.

⁶⁴ <https://encyclopedia.kaspersky.com/glossary/fork-bomb/>, 25.03.2020.

⁶⁵ <https://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain/>, 20.03.2020.

⁶⁶ <http://virus.wikidot.com/fork-bomb>, 25.03.2020.

⁶⁷ <http://virus.wikidot.com/chameleon>, 25.03.2020.

⁶⁸ <https://encyclopedia.kaspersky.com/knowledge/year-1990/>, 25.03.2020.

bir kod parçacığını aramak olan anti virüs programları çaresiz kalmış ancak bu durum fazla uzun sürmemiştir.

Bukalemunlar sistem içerisinde bulunan güvenilir programları taklit ederler. Bu aldatmaca ile sistemi ve kullanıcıyı kandıran bukalemun, sistem içerisinde pek çok zararlı işlem gerçekleştirebilir.

Bukalemunlara güncel bir örnek olarak Google Chrome web tarayıcısını silerek yerine geçen ve bu web tarayıcısını taklit eden eFast Browser adlı yazılım gösterilebilir. Söz konusu yazılım bilgisayara yerleştikten sonra kullanıcıya reklam gösterme, çeşitli sitelere yönlendirme ve kullanıcı hareketlerini takip etme gibi işlemler yürütmektedir⁶⁹.

Bukalemunlar da TCK'nın 244/1. ve 244/2. maddelerinde düzenlenen suçların işlenmesinde kullanılabilirler. Öte yandan bukalemunları kullanan bir bilgisayar saldırganı genellikle bu işten maddi bir menfaat de temin edecektir. Bu halde failin eylemi TCK'nın 244/4. maddesinde tanımlanan suçu oluşturacaktır.

1.2.1.8. Mantık Bombaları (Logic Bombs)

Mantık bombaları, aktif hale gelmeleri için belirli bir işlemin önceden yapılmasına ihtiyaç duyan yazılımlardır, bu özellikleri ile mayına basmaya benzerler⁷⁰. Bir programın içerisine zararlı bir kod yerleştirilerek oluşturulurlar.⁷¹ Örneğin kullanıcı bilgisayara flaş disk taktığında ya da belirli bir web sayfasını ziyaret ettiğinde harekete geçerek belirli bir işlemi yapan bir yazılım mantık bombasıdır. Kullanıcı belirli web sayfasını ziyaret ettiğinde bu sayfadaki hareketlerini izleyip saldırgana bildirir, bir flaş disk taktığında bu diskin içindeki verileri saldırgana gönderir. Kendisine tanımlanan koşul gerçekleşinceye kadar hiçbir işlem yapmadan bekler.

Mantık bombaları virüs, solucan ya da truva atı formunda olabilir. Ayırt edici özelliği işlem yapmak için belirli bir koşulun oluşmasını beklemesidir. Elbette bir yazılımın mantık bombası olarak kabul edilmesi için diğer koşul da bu yazılımın kullanıcı tarafından bilinmemesidir. Belirli bir koşul gerçekleştiğinde belirli bir işlemi yapacağı kullanıcı tarafından bilinen, bu özelliğini gizlemeyen bir program mantık bombası olarak kabul edilemez. Örneğin sınırlı sürüm olarak indirilen ve kullanıcıya yalnızca belirli bir süre için ya da belirli bir adet kullanım için izin veren bir yazılım da teknik anlamda bir mantık bombası gibi çalışmaktadır çünkü sürenin dolmasıyla kendisini devre dışı bırakacaktır. Ancak bu durum kullanıcı tarafından zaten önceden bilinmektedir, üstelik bu yazılım kullanıcıya ayrıca bir zarar da vermemektedir.

Bir Siemens Corporation çalışanı olan David Tinley, şirketin bilgisayarlarına mantık bombaları yerleştirilerek belirli bir süre sonra arızalanmalarını sağlamış ve şirket adına bu

⁶⁹DEMİRCAN, Kozan, "Chrome Taklidi Yapan Bilgisayar Virüsüne Dikkat >> Efast Virüsü Chrome'u Silip Yerine Geçiyor", <https://khosann.com/chrome-taklidi-yapan-bilgisayar-virusune-dikkat-efast-virusu-chromeu-silip-yerine-geciyor/>, 25.03.2020; <https://shiftdelete.net/chrome-silen-zararli-yazilim-efast-browser-64976>, 25.03.2020.

⁷⁰ AKARSLAN, Hüseyin, Bilişim Suçları, Ankara, 2015, s. 96.

⁷¹ ASLAY, F. "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi". International Journal of Multidisciplinary Studies and Innovative Technologies 1 (2017): 24-28, <https://dergipark.org.tr/tr/pub/ijmsit/issue/32341/359378>

arızaları düzeltmek için ücret almıştır. Bu durum iki yıl boyunca fark edilmemiş ancak Tinley'in şehir dışında olduğu bir dönemde anlaşılabilmiştir⁷².

Zaman tabanlı mantık bombaları ise, belirli bir tarih ve saatte kodun belirli eylemleri gerçekleştirdiği bir tür mantık bombasıdır⁷³. Bu tür mantık bombalarına örnek olarak Çernobil verilebilir. Bu yazılım Çernobil faciasının yıldönümü olan 26 Nisan tarihinde aktif hale gelerek bulunduğu bilgisayarın sabit diskindeki tüm verileri silmektedir. Bu yazılımın farklı versiyonları da mevcuttur⁷⁴. Söz konusu virüs 1999 yılında dünya genelinde 4 milyar doları bulan zarara sebep olurken Türkiye'de de 30 milyon dolar civarında bir zarara sebep olmuştur⁷⁵.

Mantık bombalarının virüs, solucan ya da truva atı gibi formlarda olabildiği düşünüldüğünde bu yazılımların da en çok kullandığı suç tipinin TCK'nın 244/1. ve 244/2. maddelerinde düzenlenen suç tipleri olduğu görülecektir.

1.2.1.9. Fidy Yazılımları (Ransomware)

Fidy yazılımı (ransomware), mağdurun bilgisayarındaki verilerin şifreleme yoluyla kilitlendiği ve bu şifrelerin çözülmesi için mağdurdan para istendiği yazılım türüdür. Fidy yazılımları, sosyal mühendislik, zararlı reklamlar, exploitler ve truva atları gibi vasıtalarla bilgisayarlara sızabilmektedir.

Fidy yazılımları bir virüs çeşidi değildir⁷⁶. Çünkü bu yazılım kendisini kopyalamaz. Verilere bir kez bulaşarak bunları şifreler ve sonrasında kullanıcıdan para talep edilir. Takibin zorlaşması açısından saldırganlar söz konusu fidyeleri genellikle kripto para olarak istemektedirler.

Mağdurun dosyalara belirli bir süre erişememesinin yanı sıra sistemin temizlenmesi ve yeniden yüklenmesi de zaman ve emek kaybına yol açar. Ayrıca mağdur, saldırganın istediği ödemeyi yapsa dahi verilerine ulaşabileceğinin garantisi yoktur.

Bilinen ilk fidye yazılımı AIDS Truva Atıdır. Bu yazılım 1989 yılında yapılmıştır.⁷⁷ Bu yazılımı geliştiren kişi Joseph Popp olarak belirlenmiş ancak akıl sağlığının uygun olmaması dolayısıyla duruşmaya katılmamıştır. Kendisi de bir aids araştırmacısı olan Popp, saldırıyı gerçekleştirmek için diğer aids araştırmacılarına 20.000 disket dağıtmıştır. Disketler 90. çalıştırılmalarından sonra bilgisayardaki dosyaları şifrelemiştir. Popp, mağdurlardan 189 dolar talep etmiştir⁷⁸.

⁷² <https://www.justice.gov/usao-wdpa/pr/siemens-contract-employee-intentionally-damaged-computers-planting-logic-bombs-programs>, 25.03.2020.

⁷³ ER, Yasin, Logic (Mantık) Bombası Nedir?, 2019, <https://teknodestek.com.tr/logicmantik-bombasi-nedir>, 25.03.2020.

⁷⁴ <https://answers.microsoft.com/tr-tr/protect/forum/all/cih-%C3%A7ernobil-vir%C3%BCs%C3%BC/a1de04f7-d8eb-4d94-9e70-60c5b775affb>, 25.03.2020.

⁷⁵ <https://www.hurriyet.com.tr/ekonomi/cernobil-virusu-4-milyar-dolar-yedi-39076290>, 25.03.2020.

⁷⁶ <https://www.isnet.net.tr/BlogIcerik/Fidy-Yazl%C4%B1m%C4%B1-Ransomware-Nedir-isnet-blog>, 24.03.2020.

⁷⁷ Kılıç, Çiğdem. Düünden bugüne fidye yazılımların (Ransomware) gelişimi ve geleceği, Yayınlanmış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi, 2019, s. 6.

⁷⁸ <https://www.eset.com/tr/ransomware/>, 24.03.2020, <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html>, 24.03.2020.

ABD İç Güvenlik Bakanlığına bağlı bir kuruluş olan CERT fidye yazılımlarına karşı sistemlerin güncel tutulmasını, istenmeyen elektronik postalardaki bağlantı ve eklere karşı temkinli olunmasını, veri yedeklerinin düzenli olarak ve ayrı bir cihaza tutulmasını, internette güvenli yöntemlerle erişimin sağlanmasını önermektedir⁷⁹. Bilinen diğer büyük fidye yazılımları GpCode, WinLock, Reveton, CryptoLocker, Locky , WannaCry ve Sodinokibi'dir. Bu yazılımlardan CryptoLocker dünya genelinde 600.000'den fazla bilgisayarı etkilemiş ve 5 milyarın üzerinde dosyayı şifrelemiştir. Yazılım etkinliğinin %3'lük kısmının Türkiye'de gerçekleştiği bilinmektedir⁸⁰. CryptoLocker toplamda 3 milyon dolar toplamayı başarmıştır⁸¹. Bir diğer yazılım olan WannaCry ise İngiltere ve İskoçya'da sağlık sisteminin çökmesine sebep olmuştur⁸².

Fidye yazılımlarını kullanan bir kullanıcı öncelikle bilişim sistemindeki verileri kitlemekte, ardından da kullanıcıdan para istemektedir. Böyle bir durumda failin eylemi TCK'nın 244/2. ve 244/4. maddelerinde düzenlenen suçları oluşturacaktır.

1.2.1.10. Bot Ağları (Botnet)

Bot, ağları tarayan ve tehditlere açık bilgisayarları tespit ederek bunlar üzerinde etkiye bulunan programdır. Robot olarak da anılan botlar, işlemlerini otomatik olarak gerçekleştirirler⁸³. Botlar yüklü oldukları bilgisayarların kontrolünün saldırganlar tarafından ele geçirilmesini sağlarlar. Bu tür bilgisayarlara zombi bilgisayarlar da denilmektedir. Çok sayıda bilgisayarın bu şekilde etkilenmesi sonucu bu botlar bir bot ağı oluşturur. Botnet, zombi ağı olarak da bilinmektedir.

Botnet, "robot" ve "network" sözcüklerinin birleştirilmesi ile oluşmuş bir sözcüktür⁸⁴.

Botnetler yasadışı ve zararlı olarak kullanılabilirler gibi yasal şekilde de kullanılabilirler. Örneğin IRC(İnternet Aktarmalı Sohbet) de bir botnet örneğidir⁸⁵. Benzer şekilde arama motorlarının web sitelerini dizinlerine ekleyebilmek için kullandıkları botlar (Örneğin Google Spider ya da GoogleBot) da birer botnet örneğidirler⁸⁶.

Kötü amaçlı botnetler; DDoS saldırıları için kullanılabilir, internet kullanıcılarına istenmeyen e-postalar göndermek için kullanılabilir, kimi internet sitelerine yönelik bir internet trafiği oluşturmak için kullanılabilir. Bunların dışında da pek çok saldırı botnetler ile gerçekleştirilmektedir.

⁷⁹ <https://www.us-cert.gov/Ransomware>, 24.03.2020.

⁸⁰ <https://www.uab.gov.tr/uploads/pages/cryptolocker-virusu-hakkinda-bilgilendirme/74bc0128f065b41.pdf>, 24.03.2020.

⁸¹ Johansen, Alison Grace, What is ransomware and how to help prevent ransomware attacks, 2019, <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html>, 4.03.2020.

⁸² <https://www.bbc.com/turkce/39899848>, 24.03.2020.

⁸³ <https://help.eset.com/eis/10/tr-TR/botnet.html>, 24.03.2020

⁸⁴ <https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks>, 24.03.2020.

⁸⁵ <https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html>, 24.03.2020.

⁸⁶ CANBEK, SAĞIROĞLU, s.127-128.

Kimi zaman, bazı kişiler saldırganlardan bu botnetleri kiralayabilmekte ya da satın alabilmektedir⁸⁷. Botnetleri kiralayan ya da satın alan kişiler genellikle istenmeyen e-posta göndermek isteyen kişilerdir.

Botnetlerin de en çok kullandığı suç tipi TCK'nın 244/1. ve 244/2. maddelerinde düzenlenen suçlardır.

1.2.1.11. Arka Kapılar (Backdoors)

Arka kapılar, bir bilgisayar sisteminde güvenlik mekanizmalarını ve kimlik kanıtlama süreçlerini atlatarak, sistemi kullanıcının bilgisi dışında uzaktan erişime açan programlardır. Bir sistemde arka kapı bulunduğunu yalnızca saldırgan bilir ve sisteme yerleştirdiği arka kapıyı daha sonra kullanır.

Arka kapılar pek çok zaman Truva atları gibi yöntemler vasıtasıyla sisteme yüklenirler. Sisteme yüklenen bu arka kapılar daha sonra virüs ve solucanslar vasıtasıyla kullanılırlar⁸⁸.

Truva atları ile arka kapılar arasındaki fark Truva atının bilgisayar tarafından faydalı olarak gözükmesi, arka kapının ise sistemde varlığı fark edilememesi ancak yine de bu sisteme erişim sağlamasıdır⁸⁹.

Arka kapılar kimi zaman yazılım hataları sonucu oluşurken kimi zaman da üreticiler tarafından bilinçli olarak açılmaktadır. Bilinçli olarak bırakılan arka kapılar çoğu zaman yazılımcı tarafından kullanıcılara destek sunma amacıyla bırakılmış olsa da kimi zaman çeşitli devletlerin casusluk faaliyetleri için de böyle arka kapılara izin verildiği iddia edilmektedir. Bu konudaki en yaygın iddialardan birisi Microsoft şirketinin, Windows işletim sisteminde Amerikan Ulusal Güvenlik Ajansı(NSA) için bilinçli olarak bir arka kapı bırakmış olduğudur⁹⁰. 2016 yılında FBI, Apple'dan da iPhone telefonlar için bir arka kapı açmasını istemiş ve Apple'ın bu talebi reddetmesi ile konu dünya gündemine gelmiştir. Söz konusu olayda Facebook ve Google da Apple'a destek olurken Microsoft kurucusu ve o dönemki başkasını Bill Gates FBI'ın talebini haklı bulmuştur⁹¹. Benzer bir talebin Linux için de yapıldığı iddia edilmişse⁹² de Linux yazılımının açık kaynak kodlu olması dolayısıyla bu durum pek mümkün görünmemektedir.

Arka kapılar vasıtasıyla en çok işlenen suç tipleri 243/1. maddesinde düzenlenen suçtur.

1.2.2. Yemleme (Phishing)

Oltalama ya da sazan avı olarak da bilinir. Phishing sözcüğü, Password ve fishing sözcüklerinin birleştirilmesiyle oluşmuştur.

Yemleme; saldırganın, kendi hazırladığı sistemi güvenilir bir kurum ya da işletmeye aitmiş gibi göstererek kullanıcının bilgilerini elde etmesi şeklinde olmaktadır. Bu bilgiler,

⁸⁷ <https://www.kaspersky.com.tr/resource-center/threats/botnet-attacks>, 24.03.2020.

⁸⁸ SAMET, s. 230.

⁸⁹ CANBEK, SAĞIROĞLU s. 126.

⁹⁰ CANBEK, SAĞIROĞLU, s. 126.

⁹¹ <https://www.dw.com/tr/iphonedede-arke-kap%C4%B1-talebine-kar%C5%9F%C4%B1-direni%C5%9F/a-19067503>, 24.03.2020.

⁹² <https://www.donanimhaber.com/NSA-Torvaldsdan-Linuxa-yazilimsal-acik-koymasini-istedi--52657>, 24.03.2020.

kullanıcıya ait kredi kartı bilgileri ya da kullanıcı adı ve şifreler gibi önemli bilgilerdir. En sık karşılaşılan örnekler bir banka ya da kamu kurumunun internet sitesinin bir benzerini yaparak kullanıcının aldatılması şeklinde olmaktadır. Bu siteyi işlem yapmak istediği banka ya da kuruma ait gerçek bir site zanneden mağdur, kişisel bilgilerini hiç çekinmeden sisteme girmekte ve bu bilgileri kendi elleri ile saldırganla teslim etmektedir. Kimi zaman bu kurumlardan geliyormuş gibi gönderilen sahte elektronik postalarla da kullanıcılar bu tarz sahte platformlara yönlendirilebilmekte ve kişisel bilgilerini sisteme girmektedirler.

Yemleme sonucunda elde edilen bilgiler bilişim sistemlerinin kullanılması suretiyle hırsızlık faaliyetlerinde kullanılabilir. Yine bu yöntemle banka ve kredi kartlarının kötüye kullanılması suçu işlenebilmektedir. Yine çalınan bilgilerin satılması da mümkündür. Daha pek çok suçun bu yöntemle işlenmesi mümkündür. Öte yandan bu yöntemle kişisel verilerin ele geçirilmesi de başlı başına bir suç teşkil etmektedir.

Yemleme, sistemleri değil insanları kullanan bir yöntemdir. Bu yöntemin başarıya ulaşması insan hatasına bağlıdır. Dolayısıyla bu yöntem bir sosyal mühendislik yöntemidir. Yemleme faaliyeti kapsamında, mağdurları kandırmak için e-posta, telefon görüşmeleri, kısa mesajlar ve sosyal medya uygulamaları da kullanılmaktadır.

Yemleme faaliyetleri genellikle birden fazla kişiyi etkilemeyi amaçlayan faaliyetlerdir. Bu sebeple kullanıcılara gönderilen içeriklerde isme özel hitaplar yerine genel hitaplar kullanılır. Kimin bu faaliyetin kurbanı olacağı saldırgan açısından önemsizdir. Önemli olan birilerinin bu sahteciliklere aldanarak işlem yapmasıdır. Spearphishing ise daha gelişmiş bir yemleme yöntemidir⁹³. Bu yöntemde mağdurlar hakkında önceden araştırma yapılarak, kişiye ya da belirli bir gruba özel sahte platformlar ya da mailler hazırlanır. Bu yöntemin hedefi genellikle daha varlıklı kimselerdir. Üst düzey yöneticileri ya da hükümet yetkililerini hedef alan saldırılara balina avı (Whaling) da denmektedir⁹⁴.

Kopya yemleme (Clone Phishing) tekniğinde saldırgan gerçek elektronik posta formatını kullanmaktadır. Gerçek bir fatura dekontu, borç bilgileri ya da düzenli olarak bildirim alınan bir kaynaktan gelen e-postaları kopyalayıp gönderirler. Kullanıcı bu gerçek bilgilere aldanarak kendisine gönderilen e-posta içindeki linke tıklar⁹⁵.

Kullanıcının bir web sitesine girerken adres yazımında küçük bir hata yapması sonucu sahte olarak oluşturulmuş bir web sitesine gitmesi olasıdır. Söz konusu web siteleri orijinalinin benzeri olacağı için kullanıcı farkı anlamayacak ve siteye güvenecektir⁹⁶. Bu yöntem Typosquatting denilmektedir.

Su deliği(Watering Hole) yönteminde saldırgan hedefindeki kişi ya da grubu önceden araştırarak bu kimselerin sıklıkla ziyaret ettiği sitelere saldırılar düzenler. Bu saldırılardan

⁹³ <https://www.eset.com/tr/phishing/>, 25.03.2020.

⁹⁴ <https://www.kaspersky.com/resource-center/definitions/what-is-a-whaling-attack>, 25.03.2020.

⁹⁵ GÜRYUVA, Yasemin. Uluslararası siber güvenlik ve siber ortamdaki tehditlerin fiziksel bir savaşa dönüşme olasılığı. Yüksek Lisans Tezi, Çankaya Üniversitesi, Sosyal Bilimler Enstitüsü. 2019, s. 48.

⁹⁶ <https://www.mcafee.com/blogs/consumer/what-is-typosquatting/>, 25.03.2020.

sonra, söz konusu siteleri tekrar ziyaret eden mağdurlar saldırganın hedefi olurlar. Bu yöntemle son yıllarda pek çok büyük saldırı gerçekleştirilmiştir⁹⁷.

Pharming, ise phishing(balıkçılık) ve farming(çiftçilik) kelimelerinin birleşmesiyle üretilmiş bir kelimedir. Bu yöntemde DNS sunucuları etkilenerek kullanıcı sahte bir web sayfasına yönlendirilir. Bu kullanıcının bilgisayarına virüs ya da truva atı yerleştirilerek yapılabileceği gibi web sayfasının DNS sunucuları üzerinden de yapılabilir⁹⁸. Diğer yöntemler kullanıcı hatasına dayanmakta iken pharming yönteminde kullanıcı hiçbir hata yapmamasına rağmen mağdur olmaktadır. Pharming, bu yönüyle diğer yemleme yöntemlerinden ayrılır. Bu yöntemle kullanıcı adres çubuğuna doğru web sayfası adresini yazmış olmasına rağmen sahte bir siteye yönlendirilmiştir. Dolayısıyla en tehlikeli yöntemlerden bir tanesidir.

Kullanıcılara sahte e-postalar gönderilerek belirli linklere tıklamaya ya da e-posta üzerindeki formu doldurmaya teşvik edilmesi yöntemi elektronik posta sahteciliği (Email Spoofing) olarak anılır.

İnternet sitelerinde ya da uygulamalarda gösterilen sahte reklamlar vasıtasıyla kullanıcıların sahte platformlara yönlendirilerek mağdur edilmeleri de sıklıkla başvurulmuş bir yöntemdir. Ayrıca ünlü kişilerin hesaplarını ele geçiren saldırganların bu hesaplar üzerinden sosyal mühendislik yoluyla ya da hediye çekilişi ve benzeri yöntemlerle kullanıcıların bilgilerini toplaması da mümkündür.

İlk kez 1995 yılında saldırganların AOL Instant Messenger (AIM) kullanarak mağdurlarla iletişime geçmesi ve kendilerini AOL çalışanı gibi göstererek bilgi toplamaları sonrasında kullanılmaya başlayan phishing terimi daha sonra benzer saldırılar için kalıcı olarak kullanılmıştır⁹⁹. 2014 yılında FIFA resmi sitesini taklit eden saldırganlar, kullanıcıları Uruguay milli takımı oyuncusu Albert Suarez'in savunma dilekçesini imzalamaya çağırmış ve bu yöntemle pek çok kişinin bilgilerini ele geçirmiştir¹⁰⁰.

Phishing genellikle dolandırıcılık ve kişisel verilerin hukuka aykırı olarak ele geçirilmesi suçlarının işlenmesi esnasında kullanılan bir yöntemdir.

1.2.3. DoS Saldırıları

Bir web sitesinin, sunucunun ya da benzer şekilde çevrimiçi hizmet sunan bir uygulananın hizmetlerinin süreli ya da süresiz aksamasına yol açarak kullanıcıların buraya erişmesini engelleyen saldırılara DoS saldırıları denir. Hizmet engelleme ya da hizmet reddi saldırıları olarak da bilinir. Bu saldırılar için kullanılan yöntem hedefe eş zamanlı olarak çok fazla sayıda istek gönderilmesi ve aşırı yükleme yapılarak söz konusu hedefin yavaşlatılması ya da erişilemez hale getirilmesi ve gerçek kullanıcıların erişimin bu yolla engellenmesidir.

⁹⁷ KÜÇÜKSİLLE, E. U., M. A. Yalçinkaya, and O. Uçar, "Siber saldırılarda istismar kitlerinin kullanımı üzerine bir analiz ve savunma önerileri. 7." Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 2014. <https://isc-turkey.org/assets/files/2016/03/isc2014-29.pdf>

⁹⁸ <https://www.kaspersky.com.tr/resource-center/definitions/pharming>, 25.03.2020.

⁹⁹ <https://www.eset.com/tr/phishing/>, 25.03.2020.

¹⁰⁰ <https://www.kaspersky.com.tr/blog/oltalama-neden-ise-yarar-ve-nasil-korunursunuz/1826/>, 25.03.2020.

DoS saldırılarının çeşitli şekillerde işlenmesi mümkündür. En bilinen DoS saldırısı türü DDoS saldırılarıdır. DDoS saldırıları dağınık hizmet engelleme ya da dağınık hizmet reddi saldırıları olarak da bilinir. DDos saldırılarının DoS saldırılarından farkı, DoS saldırılarının tek kaynaktan yapılmasına karşın DDoS saldırılarının birden fazla farklı kaynaktan yapılmasıdır. Bu saldırılarda, saldırı pek çok farklı noktadan geldiği için engellenmesi daha zordur. Bu saldırılarda genellikle zombi ağları kullanılır.

En sık başvurulanan DoS saldırısı türü ise arabellek aşımı saldırısıdır. Bu saldırı türünde hedefe karşılayamayacağı kadar çok trafik yollanır. Bu saldırı türünde sistemin zayıf noktası önceden tespit edilerek bu noktaya yükleme yapılabileceği gibi böyle bir tespit yapılmadan da saldırının yapılması mümkündür¹⁰¹.

SYN saldırılarında ise sunucuya gerçek bir IP adresinden geliyormuş gibi istekler yollanır. Makine bu istek için bir kaynak ayırır ve istediği yanıtlar ancak söz konusu IP adresi gerçek bir adres olmadığı için işlemi doğrulayamaz ve her seferinde işlemi tekrarlar. Bu yöntemin belirli bir sayıda uygulanmasıyla söz konusu sistem çökmeye zorlanır¹⁰².

Smurf saldırılarında saldırgan bir ağın directed broadcast adresinden ping isteğinde bulunur ve istekte bulunurken isteği hedef makinenin IP adresinden geliyormuş gibi görünecek şekilde ayarlar. Ağ üzerinde bulunan bütün bilgisayarlar da hedef bilgisayara yanıt verirler. Hedef makine ise bu trafiği karşılayamayarak devre dışı kalır. Bu yöntem adını Şirinler adlı çizgi filminden almıştır¹⁰³.

Bilinen ilk DoS saldırısı 1974 yılında, lise öğrencisi David Dennis tarafından tarafından yapılmıştır¹⁰⁴. İlk DDoS saldırısı ise 1999 yılında Minnesota Üniversitesine karşı yapılmıştır¹⁰⁵. İlerleyen yıllarda DoS ve DDos saldırıları oldukça yaygınlaşmıştır. Aralık 2016'da Ukrayna'daki bir elektrik şirketine yapılan DDoS saldırı nedeniyle 225.000 kişinin elektrikleri kesilmiş ve telefon hatları da kullanılamaz hale gelmiştir¹⁰⁶.

DDoS yöntemi ile genellikle TCK'nın 244/1. ve 244/2. maddelerinde düzenlenen suçlar işlenmektedir.

1.3. Doğrudan Bilişim Suçu ve Dolayısıyla Bilişim Suçu Kavramları

5237 sayılı TCK'nın İkinci Kitabının "Topluma Karşı Suçlar" Başlıklı üçüncü bölümünde yer alan onuncu bölüm "Bilişim Alanında Suçlar" başlığını taşımaktadır. Bu bölümde

¹⁰¹ [https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/denial-of-service-\(dos\)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri](https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri), 26.03.2020.

¹⁰² <https://www.binance.vision/tr/security/what-is-a-dos-attack>, 25.03.2020.

¹⁰³ https://en.wikipedia.org/wiki/Smurf_attack, 26.03.2020; [https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/denial-of-service-\(dos\)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri](https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri), 26.03.2020, https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html, 26.03.2020.

¹⁰⁴ Weisman, Steve, What are Denial of Service (DoS) attacks? DoS attacks explained, 2020. <https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html>, 25.03.2020.

¹⁰⁵ https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html, 26.03.2020.

¹⁰⁶ YALMAN, Yıldırım. Siber Terör, Terörizm ve Mücadele, "BÖLÜM 8: KÖTÜ AMAÇLI YAZILIMLAR VE ANALİZİ." in SAĞIROĞLU, Şeref, ALKAN, Mustafa, Siber Güvenlik ve Savunma Farkındalık Ve Caydırıcılık, Grafiker Yayınları, Ankara, 2018, s. 267. <https://acikerisim.siiir.edu.tr/xmlui/handle/20.500.12604/883>

düzenlenen maddeler sırasıyla “Bilişim sistemine girme”, “Sistemi engelleme, bozma, verileri yok etme veya değiştirme”, “Banka veya kredi kartlarının kötüye kullanılması” ve “Yasak cihaz veya programlar” programlar başlıklarını taşımaktadır. Bu maddelerin bir kısmı tek bir suç düzenlerken bir kısmı birden fazla, farklı suça yer vermektedir. Ayrıca “Tüzel kişiler hakkında güvenlik tedbiri uygulanması” durumunu düzenleyen son bir madde de bulunmaktadır.

Her ne kadar Türk Ceza Kanun’un 243 ila 246. maddeleri yukarıdaki şekilde belirlenen suç tiplerini düzenlemişse de bilişim sistemlerinin kullanılması suretiyle işlenebilen suçlar bunlarla sınırlı değildir. Bu suçların yanı sıra Türk Ceza Kanun’un 142/2-e maddesinde hırsızlık suçunun bilişim yoluyla işlenebilen nitelikli haline ve 158/1-f maddesinde ise dolandırıcılık suçunun bilişim sistemlerinin kullanılması suretiyle işlenebilen nitelikli şekline yer verilmiştir. Ayrıca TCK’da özel bir düzenleme bulunmamakla birlikte “Eğitim ve öğretim hakkının engellenmesi”, “Kamu hizmetlerinden yararlanma hakkının engellenmesi”, “Hakaret”, “Haberleşmenin gizliliğini ihlal”, “Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”, “Özel hayatın gizliliğini ihlal”, “Kişisel verilerin kaydedilmesi”, “Verileri hukuka aykırı olarak verme veya ele geçirme”, “Verileri yok etmeme”, “Halk arasında korku ve panik yaratmak amacıyla tehdit”, “Suç işlemeye tahrik”, “Suçu ve suçluyu övme”, “Halkı kin ve düşmanlığa tahrik veya aşağılama”, “Kanunlara uymamaya tahrik”, “Müstehcenlik” ve “Kumar oynanması için yer ve imkân sağlama” gibi suçların da bilişim sistemlerinin kullanılması yoluyla işlenmesi mümkündür. Görüldüğü gibi bu suçlar ağırlıklı olarak “Kamu Barışına Karşı Suçlar” ve “Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar” başlıklı bölümlerde düzenlenmiş olmakla birlikte diğer bölümlerde yer alan düzenlemeler de vardır. Hatta TCK dışında düzenlenen suçların da bilişim sistemleri kullanılarak işlenmesi mümkündür. Bu suçlara örnek olarak 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu’nun 37. maddesi ya da 5846 sayılı Fikir ve Sanat Eserleri Kanun’un 71 ve 72. maddelerinde düzenlenen suçlar ve 5070 sayılı Elektronik İmza Kanunu’nun 16. ve 17. maddeleri örnek verilebilir.

Yargıtay uygulamasında TCK’nın 243., 244., 245., 245/A ve 246. maddelerinde düzenlenen suçlar doğrudan bilişim suçları ya da gerçek bilişim suçları; bu suçların dışında kalan diğer suçlar ise dolayısıyla bilişim suçları ya da bilişim bağlantılı suçlar olarak adlandırılmaktadır¹⁰⁷. Bu suçların ayıran en önemli unsur doğrudan bilişim suçlarının yalnızca bilişim sistemleri kullanılarak işlenmesi mümkün iken diğer suçların bilişim sistemleri kullanılarak ya da kullanılmadan işlenmesinin mümkün olmasıdır.

İKİNCİ BÖLÜM

Doğrudan Bilişim Suçları

2.1. Bilişim Sistemine Girme Suçu (TCK 243/1-3)

2.1.1.Genel Olarak

TCK’nın “Bilişim Alanında Suçlar” başlıklı onuncu bölümünde düzenlenen ilk suç bilişim sistemine girme veya kalma suçudur. Bu suçun düzenlendiği 243. maddenin ilk fıkrasında

¹⁰⁷ ALTUĞ, Şahin, Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri (CMK – TCK – Özel Yasalar), Yargıtay Cumhuriyet Başsavcılığı, Ankara, 2018, s. 829.

bilişim sistemine girme veya orada kalma şeklindeki temel suç tipi düzenlenmiş, ikinci fıkrasında bu fiillerin bedeli karşılığında yararlanılabilen bir sistem hakkında işlenmesi durumunda cezanın indirileceği şeklinde bir nitelikli hal düzenlenmiş, üçüncü fıkrada ise verilerin kaybolması veya değişmesi durumunu içeren suçun neticesi sebebiyle ağırlaşmış şekli düzenlenmiştir.

Bilişim sistemine girme veya kalma suçunu düzenleyen TCK'nın 243. maddesi 3 fıkradan oluşmakta iken 24.03.2016 tarihli 6698 Sayılı Kişisel Verileri Koruma Kanunu'nun 30. maddesi ile TCK'nın 243. maddesine yeni bir fıkra daha eklemiştir. Ancak 243. maddenin 4. fıkrası tarafımızca ayrı bir suç olarak değerlendirildiğinden bu fıkra ile ilgili açıklamalar çalışmamızın bir sonraki bölümünde yer alacaktır.

TCK'nın 243. maddesinin ilk üç fıkrası şu şekildedir:

“(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkroda 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.”

Ülkemiz tarafından da imzalanan ve 22.04.2014 tarih ve 6533 sayılı “Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun” ile onaylanarak yürürlüğe giren Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin *Ulusal Düzeyde Alınacak Önlemler* başlıklı ikinci bölümünün Yasadışı Erişim başlıklı ikinci maddesi ise şu şekildedir: “Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız bir şekilde erişim fiilinin, kasıtlı olarak yapıldığında kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Taraflar söz konusu suçu, bilgisayar verilerinin elde edilmesi amacıyla veya sahtekârlığa yönelik baska bir amaçla güvenlik sisteminin ihlal edilmesi şeklinde veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemini esas alarak tanımlayabilirler.”

Bu maddenin ilk fıkrası önceden “Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.” şeklindeydi. 07/04/2016 tarih ve 29677 Sayılı Resmi Gazete’de yayımlanan 24.03.2016 tarihli 6698 Sayılı Kişisel Verileri Koruma Kanunu'nun 30. maddesi ile bu fıkroda yer alan “ve” bağlacı “veya” olarak değiştirilmek suretiyle suç, seçimlik hareketli bir suç tipi haline getirildi.

243. maddenin ilk fıkrasında 2016 yılında yapılan bu değişiklikten önce bir bilişim sistemine girmek tek başına yeterli sayılmıyor ayrıca bu sistemde kalmaya devam edilmesi şartı da aranıyordu. Oysa görüldüğü gibi Sanal Ortamda İşlenen Suçlar Sözleşmesinin taraf devletlere bir bilişim sisteminin tamamına yahut bir kısmına haksız erişimin suç olarak düzenlenmesi yükümlülüğü yüklüyordu. 6698 sayılı yasanın 30. maddesinde yapılan değişikikten sonra Sanal Ortamda İşlenen Suçlar Sözleşmesinde aranan bu şart yerine

getirilmiş olduğu gibi bu sözleşme ile öngörülmemiş olan “sistemde kalmaya devam etmek” şeklinde bir suç tipi daha getirilmiş oldu.

Bilişim Sistemine Girme veya Kalma Suçu ilk kez 5237 sayılı TCK ile mevzuatımızda yer aldı. 765 sayılı Mülga TCK’da böyle bir suç tipi bulunmuyordu. Söz konusu 765 sayılı yasada Bilişim Alanında Suçlar; 525/a maddesinde düzenlenen “*Verilerin Ele Geçirilmesi Suçu*”, 525/b maddesinde düzenlenen “*Bir Sistemi Veya Verileri Veya Diğer Herhangi Bir Unsuru Kısmen Veya Tamamen Tahrip Etmek, Değiştirmek, Silmek Veya Sistemin İşlemesine Engel Olmak yada Yanlış Biçimde İşlemesini Sağlamak Suçu*”, 525/c maddesinde yer alan “*Hukuk Alanında Delil Olarak Kullanılmak Maksadıyla Sahte Belge Oluşturmak İçin Sisteme Veri Yerleştirmek Veya Verileri Tahrip Etmek Suçu*” şeklindeydi. Oysa tüm bu fiiller işlenirse dahi yalnızca bir bilişim sistemine girilmesi dahi kullanıcılar açısından büyük olumsuzluklar yaratmaktaydı. 5237 sayılı yasanın 243. maddesinde düzenlenen bu suç ile bu alandaki büyük bir sorun giderilerek veri güvenliği anlamında önemli bir adım atılmış oldu. Gerçekten de bilişim alanında en sık karşılaşılan suçlardan birisi Bilişim Sistemine Girme suçudur.

Bilişim Sistemine Girme veya Kalma suçu kimi zaman tek başına işlenebileceği gibi kimi zamanlarda ise başka bir suçun işlenmesi için “araç suç” niteliğindedir. Bu yönüyle bu suç tipi konut dokunulmazlığını ihlal suçuna benzetilmektedir¹⁰⁸ Amaç suç – araç suç ilişkisinin bulunduğu durumlarda amaçlanan suçun işlenmesi durumunda gerçek gerçek içtima kuralları uygulanacaktır¹⁰⁹. Başka bir deyişle amaçlanan suçun gerçekleştiği durumda her iki suçtan da ceza verilecekken amaç suç gerçekleşirse dahi araç suçtan dolayı fail cezalandırılacaktır. Dolayısıyla bilişim sistemine girme veya kalma suçunun amaç suç olarak işlendiği durumlarda yalnızca bu ihlal dahi suç kabul edildiğinden caydırıcılık artacak, araç suç olarak işlendiği durumlarda ise amaçlanan diğer fiiller gerçekleştirmemiş olsa dahi sadece sisteme girilmiş olması dahi cezalandırılmış olacaktır. Günümüzde neredeyse bütün kurum ve kuruluşların, işletmelerin ve hatta kişilerin verilerinin bilişim sistemleri aracılığıyla saklandığı düşünüldüğünde bu suç tipinin düzenlenmesinin ne denli önemli olduğu da ortaya çıkacaktır.

TCK 243. maddesinin ilk fıkrasında “bilişim sistemine girmek” ve “sistemde kalmaya devam etmek” şeklinde iki farklı suç tipi düzenlenmiş olmasına rağmen madde başlığında yalnızca “bilişim sistemine girme” ifadesi geçmektedir. Bu durum madde başlığının madde içeriğinde tanımlanan suçları anlatmada yetersiz kalmasına yol açmaktadır. Benzer şekilde dördüncü fıkra da yer alan Sisteme Girmeksizin Veri Nakillerini Teknik Araçlarla İzlemek Suçu madde başlığı ile tamamen alakasız olduğu gibi bu suç tipi ile 243. maddenin ilk fıkrasında düzenlenen Bilişim sistemine girme veya kalma suçuyla da bir ilgisi bulunmamaktadır. Madde başlığı ile içeriğin uyumsuz olması ve birbiriyle bağlantılı olmayan iki farklı suçun tek bir maddede düzenlenmiş olması tutarsızlığa yol açmakta ve uygulamada da birtakım karışıklıklara neden olmaktadır. Madde başlığı ile ilgili karışıklığın giderilmesi için doktrinde farklı öneriler sunulmuştur. Örneğin Soyaslan bu suç

¹⁰⁸ DÜLGER, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, 2018, s. 238; AKBULUT, Berrin, Bilişim Alanında Suçlar, Ankara, 2017, s. 115.

¹⁰⁹ ÖZGENÇ, İzzet, Türk Ceza Hukuku Genel Hükümler, Ankara, 2020, s. 612.

için “Başkasının bilişim sistemine girme suçu”, *Tezcan/Erdem/Önok* “Bilişim Sistemine Girme veya Orada Kalma Suçu”, *Karakehya*¹¹⁰ “izinsiz bilişim sistemine girme”, demektedir. Bu suçun başlığının “Bilişim Sistemine Girme veya Kalma Suçu” olarak değiştirilmesi ve maddenin son fıkrasının ayrı bir madde olarak düzenlenmesi ile bu karışıklıkların giderilebileceği kanaatindeyiz.

2.1.2. Korunan Hukuki Yarar

Günümüzde neredeyse bütün kurum ve kuruluşların işleyişinde bilişim sistemleri kilit rol oynamaktadır. Ayrıca bilişim sistemlerinin kişisel kullanımdaki yeri ve önemi de oldukça büyüktür. Gelişen teknoloji ile birlikte kişiler ve kurumlar kendilerine ait her türlü bilgiyi, fotoğraf ve videoyu, dokümanı ve bunun gibi pek çok veriyi bilişim sistemleri aracılığıyla muhafaza etmekte ve işlemektedirler. Bilişim sistemlerinin önemi bu denli büyükken bu sistemlere yönelik saldırıların cezasız bırakılması düşünülemez. Bir bilişim sistemine girilmesi ile daha sonra başka bir suç işlenmemiş olsa dahi verilerin gizliliği zedelenecektir. Ayrıca bu sistemlere yönelik güven duygusu da zarar görecektir.

Yaygın görüşe göre bilişim sistemine girme ve kalma suçuyla korunan hukuki yarar bilişim sisteminin güvenliğidir. Bu görüşe göre bilişim sistemlerine yapılacak hukuka aykırı erişimlerin engellenmesiyle verilerin gizlilikleri korunacak, özel hayatın dokunulmazlığı ya da kişi ve kurumların ihtiyaç duyduğu güvenlik duygusu sağlanacaktır. *Dülger’e* göre tüm bunları kapsayacak olan hukuksal değer bilişim sisteminin güvenliğidir.¹¹¹ *Akbulut* da bu suçla korunan hukuki değer bilişim sisteminin güvenliği ve dokunulmazlığı olduğu görüşündedir. Kanun koyucu bu suç tipini düzenleyerek kişilerin her türlü müdahaleden uzak ve rahatsız edilmeden güven içinde bilişim sistemlerini kullanmasını korumaktadır¹¹². *Parlar*, korunan hukuki yararın bilişim sisteminin güvenliğinin sağlanması ve kullanıcıların çıkarlarının zedelenmemesi olduğunu belirtmektedir¹¹³. *Koca/Üzülmez* de bu suçla korunan hukuki yararın bilişim sistemlerinin güvenliği olduğu görüşündedir¹¹⁴. Biz de bu suçla korunan hukuki yararın bilişim sisteminin güvenliğinin sağlanması olduğu yönündeki görüşe katılmaktayız.

Bir başka görüşe göre ise bu suçla korunan hukuki yarar karma niteliktedir. *Gül*, öncelikli olarak bilişim sisteminin güvenliğinin korunduğunu bunun yanı sıra özel hayatın gizliliği, haberleşme özgürlüğü, kişilerin ya da kurumların duyduğu güvenlik duygusu gibi konularda da hak ihlallerinin önlenmek istendiğini benimsemektedir¹¹⁵. *Soyaslan* da bu suç tipi ile birden fazla hukuki yararın korunduğu görüşündedir. *Soyaslan’a* göre bu değerler sistem maliki ya da kullanıcısının özel yaşamının gizliliği ve verilerin güvenlik içinde

¹¹⁰ Karakehya, Hakan, “TCK’da Bilişim Sistemine Girme Suçu”, TBBD, Sayı 81, 2009 s.6.

¹¹¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 243.

¹¹² AKBULUT, s. 118.

¹¹³ PARLAR, Ali, Türk Ceza Hukukunda Bilişim Suçları, Bilge Yayınevi, Ankara, 2015, s. 17.

¹¹⁴ KOCA, Mahmut ve ÜZÜLMEZ, İlhan, Türk Ceza Hukuku Özel Hükümler, Adalet Yayınları, Ankara 2018, s. 849.

¹¹⁵ GÜL, Ahmet, Doğrudan/Dolaylı Bilişim Suçları, Seçkin Yayıncılık, Ankara, 2018, s. 59.

muhafazasıdır¹¹⁶. *Tezcan/Erdem/Önok* da sistem güvenliğinin yanı sıra özel yaşamın gizliliğinin ve haberleşme özgürlüğünün ihlalinin de korunduğu görüşündedir¹¹⁷.

Bazı yazarlar bu suçla korunan hukuki değerlerin bilişim sisteminin güvenliği ve güvenilirliği olduğunu, yasa koyucunun bu suçla güvence altına alınan bir bilişim sistemine yetkisiz erişimi engellemeyi amaçladığı görüşündedirler¹¹⁸.

2.1.3. Maddi Unsurlar

2.1.3.1. Fiil

23.03.2016 tarihinde 6698 sayılı kanunla madde metninde değişiklik yapılmadan önce TCK m.243/1’de yer alan suç çok hareketli bir suçtu. Zira madde metninde geçen “girmek” ve “kalmak” fiilleri “ve” bağlacı ile bağlanmıştı. Dolayısıyla suçun oluşması için girmek ve kalmak fiillerinin her ikisinin de yapılması gerekiyordu. O dönem TCK 243. maddesindeki suç birleşik hareketli bir suçtu¹¹⁹.

Bu dönemde özellikle kalma eyleminin ne zaman meydana geleceği konusunda tartışmalar bulunuyordu. Kalma eyleminin süresinin çok kısa olduğu durumlarda suçun oluşup oluşmayacağı yönündeki tartışmalar bir yana, sisteme giriş yapar yapmaz sistemi terk eden failin eyleminin cezasız kalması gibi önemli problemler mevcuttu.

Madde metninde yapılan değişiklik sonrasında bilişim sistemine girme veya kalma suçları artık seçimlik hareketli hale gelmiştir. Madde metninde bulunan “ve” bağlacı “veya” olarak değiştirilmiş, failin girmek ya da kalmak eylemlerinden herhangi birisini yapması yeterli hale getirilmiştir.

Sisteme girme veya sistemde kalma fiillerinin nasıl gerçekleşeceği hususunda ise bir sınırlama yoktur. Bu itibarla suç aynı zamanda serbest hareketli suçtur¹²⁰. Sisteme bir ağ vasıtasıyla bağlanması, sistemin yakınında bulunarak yahut uzaktan erişim yoluyla bağlanması, herhangi bir yazılım kullanılması yahut kullanılmaması gibi durumlar suçun oluşumunu etkilemez¹²¹. Sistemle fiziki temasa geçerek sisteme girilmesi de mümkündür¹²².

Fail yalnızca sisteme girerek ya da yalnızca sistemde kalarak bu suçun oluşmasına sebebiyet verebileceği gibi bu fiillerden her ikisini de yapabilir. Bu eylemlerin ikisinin de yapılmış olması suçun tekliğini etkilemez, fail hukuka aykırı olarak girdiği bilişim sisteminde kalmaya devam etse de tek suç oluşur.

Bilişim sistemine girmeksizin yalnızca sisteme bir elektronik posta yahut dosya gönderilmesi bu suçun oluşması için yeterli değildir¹²³. Ancak e-posta içerisinde gönderilen

¹¹⁶ SOYASLAN, Doğan, Ceza Hukuku Özel Hükümler, Yetkin Yayınları, Ankara, 2018, s. 654.

¹¹⁷ TEZCAN, Durmuş, ERDEM, Ruhan, ve ÖNOK, Murat, Teorik ve Pratik Ceza özel Hukuku, Seçkin Yayıncılık, Ankara, 2019, s. 1054-1055.

¹¹⁸ ÖZBEK, Veli Özer, KANBUR, Mehmet Nihan, DOĞAN, Koray, BACAĞIZ, Pınar ve TEPE, İlker, Türk Ceza Hukuku Özel Hükümler, Seçkin Yayıncılık, Ankara, 2018, s. 966.

¹¹⁹ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 258; ERDOĞAN, 125.

¹²⁰ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 258.

¹²¹ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 258. ERDOĞAN, 131.

¹²² TEZCAN/ERDEM/ÖNOK, s. 1057.

¹²³ AKBULUT, s. 131.

bir casus program vasıtasıyla sisteme erişim sağlanırsa TCK 243'teki suç oluşmuş olacaktır¹²⁴.

Gül ve Tezcan/Erдем/Önok'a göre bir başkasının hukuka aykırı olarak eriştiği sistem içerisinde kalmaya devam eden kişi de bu suç işlemiş olacaktır¹²⁵.

Failin hareketi olmadan neticenin gerçekleşemediği durumda suç olumlu hareketle işlenmiştir. Fakat failin bir harekette bulunsaydı netice gerçekleşmeyecekti diyebiliyorsak bu durumda suç olumsuz hareketle işlenmiştir¹²⁶. Olumlu hareketle işlenen suçlara hırsızlık örnek verilebilir. Burada failin eylemi neticeyi meydana getirmiştir. Fail söz konusu harekette bulunmazsa netice de gerçekleşmeyecektir. Olumsuz hareketle işlenen suçlara ise suçu bildirmeme örnek verilebilir. Kasten öldürme suçu gibi bazı suçlar ise olumlu hareketle işlenebileceği gibi olumsuz hareketle de işlenebilen suçlardır. Sistemde kalmaya devam etmek suçu olumlu hareketle işlenebileceği gibi olumsuz hareketle de işlenebilir. Örneğin, bir internet sitesinin kullanıcılarına erişim sağladıkları ilk tarihten itibaren bir ay boyunca ücretsiz erişim imkânı sunduğu, sürenin bitiminde kullanıcının siteye olan ücretsiz erişimini durdurduğu ve bunun denetimini de kullanıcının sistemine yerleştirdiği bir çerez dosyası ile yaptığı bir durumda kendi bilgisayarında kayıtlı bulunan çerez dosyasının içeriğini değiştirerek sistemde kalma süresini uzatan ve bu şekilde sistemde kalmaya devam eden failin eylemi olumlu hareketle işlenmiştir. Yine aynı sitenin bu kontrolü kendisinin yapmadığı, bir aylık sürenin sonunda sistemden çıkmak konusunda yükümlülüğü kullanıcıya yüklediği durumda sistemden çıkmayan kullanıcı olumsuz hareketle suçu işlemiş olacaktır. Olumlu veya olumsuz hareketle işlenen suç ayrımı ile ihmalî ve icrai hareketle işlenen suç ayrımını ise karıştırmamak gerekir. İcrai suçlar bir yasağın ihlali şeklinde gerçekleşen suçlar iken ihmalî suçlar bir emrin yerine getirilmemesi durumunda söz konusu olacaktır¹²⁷. Örneğin kanunlarımıza göre bir taşınır malın zilyedinin rızası olmaksızın alınması yasaktır. Bu yasağın delinmesi ile TCK'nın 141 vd. maddelerinde düzenlenen hırsızlık suçu oluşacaktır. Burada failin eylemi icrai niteliktedir. Burada kanun kişilerden bir şeyi yapmamasını istemiştir ve fail kanunun yapmamasını istediği bir şeyi yapmıştır. Kimi zaman ise fail kanunun kendisine yapmasını emrettiği bir davranışı yerine getirmekten imtina eder. Örneğin kanun bir hukukî ilişkiye dayalı olarak elde ettiği eşyanın, esasında suç işlemek suretiyle veya suç işlemek dolayısıyla elde edildiğini öğrenen kişinin bunu yetkili makamlara vakit geçirmeksizin bildirilmesini istemiştir. Bu bildirim bulunmayan failin eylemi TCK'nın 166. maddesinde düzenlenen bilgi vermeme suçunu oluşturacaktır. Burada failin eylemi ihmalî niteliktedir. Kanun kişilerden bir şeyi yapmasını istemiş, bunu emretmiştir ancak fail bu emrin gereklerini yerine getirmemiştir. İhmalî suçlar da kendi içinde gerçek ihmalî suçlar ve görünüşte ihmalî suçlar olarak ikiye ayrılır. Gerçek ihmalî suçlar yalnızca ihmalî bir davranışla işlenebilen

¹²⁴ TEZCAN/ERDEM/ÖNOK, s. 1057.

¹²⁵ TEZCAN/ERDEM/ÖNOK, s.1057, GÜL, s. 67.

¹²⁶ KUNTER, Nurullah, Suçun Maddi Unsurları Nazariyesi, İsmail Akgün Matbaası, İstanbul, 1954, s. 50-51.

¹²⁷ KUNTER, s. 54, HAKERİ, Hakan, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara, 2014, s. 157-161, ARTUK/GÖKCEN/YENİDUNYA, Ceza Hukuku Genel Hükümler, Adalet Yayınevi, Ankara, 2014, s. 235-242.

suçlardır. Örneğin denetim görevinin ihmali suçu böyledir. Bu suçun icrai olarak işlenmesi mümkün değildir. Yasa bu suçlarda faile bir şeyi yapmasını emreder, örneğin kişiye öğrendiği suçu bildirmesi emredilmiştir, bu emre aykırı davranan kişi gerçek ihmali bir suç olan suçu bildirmeme suçunu işlemiştir. Oysa görünüşte ihmali suçlar ise icrai bir hareketle de işlenebilecek suçun ihmali bir hareketle işlenmesi durumunda oluşur. Örneğin PVSK gereği insanların can ve mal güvenliklerini korumak amacıyla gerekli tedbirleri almakla yükümlü olan bir emniyet mensubunun kendisine kanunen yüklenmiş olan bu yükümlülüğe aykırı davranması ya da bir bebek bakıcısının kendisine sözleşme ile yüklenen çocuğa bakma görevine aykırı davranması durumlarında görünüşte ihmali suç oluşacaktır¹²⁸. Burada failin kendisine kanunen ya da sözleşme ile yahut ön gelen tehlikeli hareketi nedeniyle yüklenmiş olduğu yükümlülüğü ihmal etmesi neticesinde kişilerin ölümüne sebep olması durumunda görünüşte ihmali suç oluşacaktır. Zira öldürmek eylemi doğası gereği icrai nitelikte bir eylem olmasına rağmen burada fail ihmali olarak bu suçu işlemiştir. Bilişim sistemine girme suçu ile benzer nitelikte olduğu dile getirilen konut dokunulmazlığının ihlali suçunda ise bir kimsenin konutuna rızası hilafına girmek eylemi icrai, rıza ile girdikten sonra buradan çıkmamak ise ihmalidir. Burada kanun koyucu başkasının konutuna rızası olmaksızın girmeyi yasaklamıştır. Rıza ile girilen konuttan ise rıza sona erdikten sonra çıkmayı emretmiştir. İnceleme konumuz olan suçlardan bilişim sisteminde kalma suçu ise icrai olarak işlenebilen suçlardandır. Burada kanun faile sistemden çıkmasını emretmez ancak failin sistemde kalmaya devam etmesini yasaklar. Yukarıda vermiş olduğumuz örnekte de kanun faile sistemde kalmaya devam etmesini yasaklamıştır, fail bir aylık sürenin sonunda sistemde kalmaya devam ederek bu yasağa aykırı davranmıştır. Elbette failin sistemden çıkmak konusunda sözleşme ile ya da başka bir şekilde özel olarak yükümlü tutulduğu ancak bu yükümlülüğünün gereklerine uygun davranmayarak sistemde kaldığı durumda görünüşte ihmali suç oluşacaktır. Doktrinde sisteme girmek şeklindeki fiilin icrai, sistemde kalmak şeklindeki fiilin ise ihmali olduğu yönünde görüş mevcuttur¹²⁹. Sisteme girmek fiilinin yalnızca icrai olarak işlenebileceği hususunda bir tartışma yoktur ancak sistemde kalmaya devam etmek eyleminin ihmali olduğu görüşüne yukarıda da açıkladığımız gerekçe ile katılmıyoruz. Öte yandan bu suçların icrai ya da ihmali olarak işlenmesinin mevcut ceza yasalarımız açısından pratik bir faydası yoktur.

Doktrinde ayrıca “girmek” kavramı da eleştirilmekte, bunun yerine “erişim” kavramının kullanılmasının daha doğru olduğu savunulmaktadır¹³⁰. Bu görüşü savunan yazarlara göre girmek sözcüğü sisteme fiziki olarak girmeyi çağrıştırmaktadır. Aksi görüşteki yazarlar ise “erişim” sözcüğünün sisteme ilişkin soyut unsurlara yani bilişim sisteminin yazılım ile ilgili kısmına ulaşmak anlamına gelebileceğini ya da sisteme internet üzerinden yapılan

¹²⁸ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, Ceza Hukuku Genel Hükümler, s. 292-301.

¹²⁹ AKBULUT, 128;

¹³⁰ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 259; ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s.970;

eriřimleri ifade edeceđini belirterek “girmek” sözcüđünün kullanılmasının daha yerinde bir tercih olduđunu belirtmiřlerdir¹³¹.

Fiilin iki seřimlik hareketinden birisi “orada kalmaya devam etmektir.” Bu hareket devamlılık göstermektedir. Bu hareket bakımından bu suç tipi mütemadi bir suçtur¹³².

Fail sistemin tamamına yahut bir kısmına girerek bu suçu işleyebilir. Zira madde metninde “sistemin bütününe veya bir kısmına” ibaresi bulunmaktadır. Sistemin büyük bir kısmına erişim izni bulunmakla birlikte belirli bir kısmına erişimi sınırlandırılmış kimsenin bu kısma girmesiyle suç oluşur

2.1.3.2. Fail

TCK’nın 243. maddesinde suçu işleyecek kiři bir biliřim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden “kimse” olarak belirtilmiřtir. Dolayısıyla inceleme konumuz olan bu suç fail bakımından özel bir nitelik arz etmez. Herkes bu suçun faili olabilir.

İncelediđimiz suçun işlenmesi açısından failin biliřim sistemlerini kullanma becerileri yüksek kimseler olması beklense de böyle bir zorunluluk söz konusu deđildir. Bu konudaki becerileri ancak temel düzeyde olan kimseler dahi bu suçu işleyebilir. Örneđin bir biliřim sistemindeki ağıřı tesadüfen fark eden bir kimse bu sisteme hukuka aykırı olarak kasten girer yahut orada kalırsa bu suçu işlemiř olur. Bu ağıřı tesadüfen fark etmiř olması ile özel beceri kullanarak sistemsal açıkları keřfetmiř olması açısından bu suç tipinde bir fark yoktur. Yine de bu suçun ağıřlıklı olarak belirli düzeyde bilgi sahibi kimseler tarafından işlendiđi görölmektedir.

2.1.3.3. Mađdur

Bu suç tipinde mađdurun kim olabileceđi ile alakalı özel bir belirme bulunmamaktadır. Dolayısıyla suçun mađduru herkes olabilir. Kanaatimizce hukuka uygun olmayan řekilde bir biliřim sistemine girilmesi yahut orada kalınması sonucu menfaati zarara uğratan kimse söz konusu suçun mađdurudur.

İnceleme konusu suçun mađduru biliřim sisteminin maliki ya da kullanıcısı olabilir. Önemli olan söz konusu biliřim sistemi üzerinde hak sahibi olmasıdır¹³³.

Doktrinde bazı yazarlar tüzel kiřilere ait biliřim sistemlerine girilmesi durumunda tüzel kiřilerin de bu suçun mađduru olabileceđi görüşündedirler¹³⁴. Ancak bu görüşe katılmak mümkün deđildir. Zira Türk Ceza Hukuku sistematide tüzel kiřiler ancak suçtan zarar gören konumunda olabilirler.

Birden fazla kimseye ait verilerin tutulduđu bir biliřim sistemine girildiğinde veri sahiplerinin de bu suçun mađduru olabileceđi yönünde görüşler de mevcuttur¹³⁵. Söz gelimi bir kamu kurumuna ait sisteme hukuka aykırı olarak giriş yapıldığında bu sistemde verileri

¹³¹ AKBULUT, s.129; KOCA, ÜZÜLMEZ s. 853-855.

¹³² DÜLGER, Biliřim Suçları ve İnternet İletişim Hukuku, s. 264;

¹³³ AKBULUT, s. 121

¹³⁴ ERDOĐAN, 145.

¹³⁵ GÜL, 60-61.

bulunan tüm vatandaşların bu suçun mağduru olabileceği düşünülmektedir. Ancak böyle bir durumda TCK'nın 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme söz konusu olacaktır ve bu kimseler ancak bu suçun mağduru olacaklardır. Daha açık bir ifade ile bir sisteme hukuka aykırı olarak giriş yapılarak sistemde yer alan verilerin öğrenilmesi halinde hem TCK 243/1'de düzenlenen suç hem de TCK 136'da düzenlenen suç oluşacak, giriş yapılarak bir sistemde yer alan verilerin öğrenilmesi dolayısıyla sistemde verisi bulunan kişiler TCK'nın 136. maddesinde tanımlanan suçun mağduru olacak, sisteme giriş yapılmış olması dolayısıyla da sistem üzerinde hak sahibi olan kişi TCK'nın 243/1. maddesindeki suçun mağduru olacaktır.

Sisteme hukuka aykırı olarak girilmesi suçunun mağduru ancak bilişim sistemi üzerinde hak sahibi olan kişidir. Bir kimseye ait verilerin bir sistemde tutuluyor olması bu kimseyi o sistem üzerinde hak sahibi yapmayacaktır¹³⁶. Aksi yönde bir değerlendirme yapılması durumunda TCK'nın 136. maddesinde düzenlenen suç tipi de 243. maddeye dâhil edilecek ve bu suç tiplerinin ayrımının yapılması imkânsız hale gelecektir.

Tezcan/Erdem/Önok'a göre bu suçla korunan hukuki yarar bilişim sisteminin güvenliğidir, bu sebeple söz konusu suçun bir mağduru olduğu söylenemez¹³⁷. Gerçekten de çevrenin kasten kirletilmesi, halkı kin ve düşmanlığa tahrik veya aşağılama, suç uydurma, anayasayı ihlal gibi bazı suçların belirli bir mağdura karşı işlendiğinden söz edilemez. Bu gibi suçlarda suçun mağdurunun devlet olduğunu kabul edenler olduğu gibi¹³⁸ tüzel kişilerin suçun mağduru olamayacağını, bu suçların mağdurunun bütün toplum olduğunu¹³⁹ savunan görüşler de vardır. Mağdur bir suçla korunmak istenen hukuki yararın sahibi olan kişi ya da kişilerdir.¹⁴⁰ Mağdur, işlenen suç dolayısıyla haksızlığa uğrayan kimsedir.¹⁴¹ Dolayısıyla belirli bir mağduru olmayan bu suçlarda dahi kimi zaman menfaati suç dolayısıyla zarara uğratılan bir kimse bulunmakta ve bu kimse suçun mağduru kabul edilmektedir.¹⁴² TCK'nın 243/1. maddesinde düzenlenen bu suç dolayısıyla da menfaati zarara uğratılan bir kişi bulunmaktadır. Dolayısıyla biz bu suçun mağduru olarak yukarıda da açıkladığımız üzere bilişim sistemine girilmesi yahut orada kalınması sonucu menfaati zarara uğratılan kişiyi kabul ediyoruz.

2.1.3.4. Suçun Konusu

TCK'nın 243. maddesinde bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek suç olarak düzenlenmiştir. Dolayısıyla bu

¹³⁶ Aynı görüşte: AKBULUT, 122;

¹³⁷ TEZCAN/ERDEM/ÖNOK, s. 1055.

¹³⁸ DÖNMEZER/ERMAN, Nazari ve Tatbiki Ceza Hukuku, Der Yayınları, İstanbul, 2019 s. 693

¹³⁹ ÖZGENÇ, s. 226.

¹⁴⁰ ÖZBEK/DOĞAN/BACAKSIZ, Türk Ceza Hukuku Genel Hükümler, Seçkin Yayıncılık, Ankara, 2020, s. 213.

¹⁴¹ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, Ceza Hukuku Genel Hükümler, s. 378.

¹⁴² ÖZGENÇ, s. 226, DÜLGER, Murat Volkan, Ceza Hukuku Genel Hükümler, İstanbul, 2021., s. 381.

suçun konusunu hukuka aykırı olarak girilen ya da orada kalınan “bilgişim sistemi” oluřturur.

Bilişim sistemi kavramı ile ilgili detaylı açıklamayı yukarıda yapmıřtık. Madde gerekçesinde de “*bilgişim sisteminden maksat, verileri toplayıp yerleřtirdikten sonra bunları otomatik iřlemlere tâbi tutma olanađını veren manyetik sistemlerdir.*” denilmek suretiyle bilgişim sisteminin tanımı yapılmıřtır. Dolayısıyla ancak madde gerekçesinde de belirtilen özelliklere sahip olan bir sistem bilgişim sistemi olarak kabul edilecek ve suçun konusunu oluřturacaktır. Bu suçun konusunu oluřturan bilgişim sistemi ev ya da iř yerinde bulunan herhangi bir bilgisayar olabileceđi gibi bir cep telefonu ya da evde bulunan akıllı ampul ve bu ampulü kontrol etmeye yarayan sistem olabilir. Failin sistemin tamamına ya da bir kısmına girmesi de bu suçu oluřturacaktır. Dolayısıyla fail mađdurun cep telefonunun tamamına eriřim sađlayabileceđi gibi bir kısmına, örneđin cep telefonunda bulunan iletiřim uygulamasına giriř sađlarsa da suç oluřacaktır.

Ancak bu maddede belirtilen suçun oluřabilmesi için girilen ya da kalınan sistemin herkese açık bir sistem olmaması gerekir. Herkesin eriřime açık olan bir sisteme eriřilmesi durumunda eriřim haksızlık oluřturmayacađından TCK 243. maddesindeki suç oluřmayacaktır¹⁴³.

Maddenin ikinci fıkrasında ise konu bakımından bir sınırlama söz konusudur. Söz konusu fıkranın konusu yalnızca “bedeli karřılıđı yararlanılabilen sistemler” olarak düzenlenmiřtir.

Söz konusu maddenin üçüncü fıkrasında düzenlenen nitelikli halinde ise, suçun konusu bu kez bilgişim sistemleri deđil “sistemin içerdieđi veriler” olarak kabul edilmektedir.

2.1.3.5. Netice

TCK’nın 243. maddesinde düzenlenen suçun oluřması için bilgişim sisteminin bütününe yahut bir bölümüne girilmesi yeterli olup ayrıca bir neticenin gerçekteřmesi aranmamıřtır. Herhangi bir neticenin aranmadıđı bu suç tipi sırf hareket suçudur.

Bilişim sistemine girme suçunun oluřması için yalnızca sisteme girilmesi yeterlidir; sistemde bulunan verilere de ulařılması, bu verilerin ele geçirilmesi, verilere zarar verilmesi gibi durumlara gerek yoktur. Dolayısıyla bu suç soyut tehlike suçudur. Öte yandan verilerin öđrenilmesi ya da bu verilere zarar verilmesi durumunda TCK. 244 ya da 136. maddelerinde düzenlenen suçlar oluřabileceđi gibi 243/3 maddesi de uygulama alanı bulabilecektir.

2.1.4. Manevi Unsurlar

Bilişim sistemine girme veya sistemde kalmaya devam etme suçu kasten iřlenebilen bir suç tipidir. Bu suçun taksir ile iřlenmesi ise olası deđildir. Fail sisteme girmeye yahut kalmaya hakkının olmadıđını, dolayısıyla eyleminin hukuka aykırı olduđunu bilerek ve isteyerek hareket etmelidir.

Suç tipinde fiilin hukuka aykırı icra edilmesi gerektiđine iřaret edildiđi için failin kastı, hukuka aykırılıđı da kapsamalı, diđer bir deyiřle fail eriřimin hukuka aykırı olduđunu

¹⁴³ AKBULUT, s.134.

bilerek hareket etmelidir. Fail sisteme girişinin hukuka uygunluğu hususunda hataya düştüyse TCK'nın 30/1 maddesi uygulama alanı bulacak ve bu hatasından yararlanacaktır. Hukuka aykırı olan fiil ile bütün hukuk sistemine aykırı olan bir fiil kastedilmektedir. Yani failin eylemi ceza hukukunun yanı sıra örneğin medeni hukuk, idare hukuku gibi hukukun diğer alanlarında da hukuka aykırı olmalıdır¹⁴⁴.

Doktrinde bir görüşe göre hukuka aykırılığın suç tipinin bir unsuru olarak yer alması durumunda failin doğrudan kastla hareket etmesi gerekmektedir¹⁴⁵. Bir başka görüşe göre hukuka aykırılık ifadesi suçun maddi bir unsurunu niteliyorsa failin kastının bunu da kapsaması gerekir. Örneğin TCK'nın 91/5. maddesinde düzenlenen suç açısından suç konusunun hukuka uyum olmayan şekillerde elde edilmiş bir organ veya doku olması gerekmektedir. Burada hukuka aykırılık tipikliğe ait bir unsur olduğundan failin kastının bunu da kapsaması gerekmektedir¹⁴⁶. Doktrinde bazı yazarlara göre TCK'nın 243/1. maddesinde düzenlenen suç yalnızca doğrudan kast ile işlenebilir¹⁴⁷. Ancak doktrinde bazı görüşler bu suçun olası kastla da işlenebileceği şeklindedir¹⁴⁸. Kanaatimizce de failin sisteme erişiminin hukuka aykırı olduğunu kesin olarak bilmesi gerekmez. Fail sisteme erişimin hukuka aykırı olduğu konusunda kuşkuya düşmesine rağmen, bu durumu önemsemeyerek sisteme erişim sağlarsa da bilişim sistemine girme veya kalma suçu oluşacaktır. TCK'nın 21/2. maddesinde suçun kanuni tanımında yer alan unsurların meydana gelebileceğini fark etmesine rağmen fiili işleyen kişinin hareketini olası kast olarak düzenlemiştir, bu halde suçun oluşması için failin kanuni tanımında yer alan unsurların gerçekleşeceğini mutlak olarak bilmesinin gerekmediği, bunu öngörmesine rağmen fiili işlemesi durumunda da suç oluşacağı düzenlenmiştir. Bu açıklamalar ışığında failin sisteme erişiminin mutlak suretle hukuka aykırı olduğunu bilmesi gerekmediği, failin bunu öngörmesine rağmen fiili işlemesi durumunda olası kastla da bilişim sistemine girme veya kalma suçunun işlenebileceği kanaatindeyiz. Bu bakımdan TCK'nın 243/1. maddesinde yer alan bu suç bakımından hukuka aykırılığın madde metninde yer alması özel bir anlam ifade etmemektedir. Hukuka aykırılık özel olarak madde metninde yer almasaydı dahi failin yalnızca bir bilişim sistemine girmesi ya da orada kalması suç olmayacak aynı zamanda bu eylemin hukuka aykırı olması gerekecekti¹⁴⁹.

TCK'nın 243. maddesinde tanımlanan suç seçimlik hareketlidir. Fail sisteme taksirle girmiş olmasına rağmen, kasten sistemde kalmaya devam ettiyse yine suç oluşacaktır.

Söz konusu suçun işlenmesi için failin güttüğü saik önemli değildir. Fail kasten hareket ettiği suretle her ne maksatla sisteme girmiş olursa olsun suç oluşacaktır.

¹⁴⁴ ÖZGENÇ, s. 314.

¹⁴⁵ ÖZGENÇ, s. 321.

¹⁴⁶ DÜLGER, Ceza Hukuku Genel Hükümler, s. 479-485.

¹⁴⁷ AKBULUT, s.139.

¹⁴⁸ TEZCAN/ERDEM/ÖNOK, s. 1058

¹⁴⁹ DÜLGER, Ceza Hukuku Genel Hükümler, s. 483.

Ancak söz konusu maddenin üçüncü fıkrasının gerçekleşmesi için failin taksirle hareket etmesi gerekmektedir.

2.1.5. Hukuka Aykırılık

TCK m. 243'te düzenlenen suçun oluşması için failin bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmesi veya orada kalmaya devam etmesi gerekir. Madde metninde hukuka aykırılık vurgulanarak, hukuka aykırılığın suçun tipikliğine ilişkin bir unsur olduğu vurgulanmıştır¹⁵⁰.

Yasa koyucu TCK'nın 30/1. maddesi ile failin fiilini icra ederken suçun kanuni tanımında yer alan maddi unsurlara bilmemesi durumunda kasten hareket etmiş olamayacağını ancak taksirine dayanan bir sorumluluğu varsa bundan sorumlu olacağını düzenlemiştir. Fail, sisteme hukuka aykırı olarak girdiğini yahut sistemde hukuka aykırı olarak kaldığını bilmiyor; eyleminin hukuka uygun olduğunu zannediyorsa bu hatasından yararlanır. Örneğin failin bir dönem girmeye yetkili olduğu bir bilişim sistemine giriş yetkisi daha sonradan kaldırılmış ancak fail bir sebepten ötürü bu durumu öğrenememiş, sisteme girmeye yetkili olduğunu düşünerek sisteme girmişse bu hatasından yararlanacaktır. Burada failin sisteme hukuka aykırı olarak girme kastı yoktur, TCK'nın 243/1. maddesinde düzenlenen suçun taksirle işlenmesi ise mümkün değildir.

Bir diğer hukuka uygunluk nedeni ise rızadır. Sistem üzerinde hak sahibi bulunan kişinin rızası dâhilinde yapılan erişimler hukuka uygundur, dolayısıyla suç oluşmayacaktır. Bu rızanın açık ya da örtülü bir rıza olması arasında fark yoktur. Öte yandan mağdur, kısa süreli olarak sisteme girilmesine rıza göstermesine rağmen fail mağdurun rıza gösterdiği süreyi aşkın bir süre sistemde kalmaya devam ederse sistemde kalmaya devam etme bakımından suç oluşacaktır. Hiç şüphe yok ki bu rızanın geçerli olabilmesi için rıza gösteren mağdurun rıza göstermeye yetkili olması gerekir. Sistemin yalnızca kullanıcısı durumunda olup, sisteme girme hakkı bulunmakla birlikte üçüncü kişilerin sisteme girmesine rıza göstermeye yetkisi bulunmayan bir kişi tarafından verilecek rızaya dayanarak yapılan girişler hukuka aykırı olacaktır.

Mağdur, failin sisteme girdiğinden veya orada kaldığından sonradan haberdar olarak bu duruma rıza gösterdiğini beyan etse de artık suç oluşmuştur. Sonradan verilmiş olan rıza bu durumda suçun varlığını ortadan kaldırmayacaktır¹⁵¹. Ancak *Özbek/Doğan/Bacaksız/Tepe*'ye göre sisteme sahibinin rızası hilafına girmiş kişi henüz sistemdeyken sahibi tarafından sistemde kalmasına rıza gösterilirse eylem hukuka uygun hale gelecektir. Yazarlara göre bu suçun kesintisiz bir suç tipi olmasının ve temadi sona erinceye kadar hareketin devam etmesinin bir sonucudur. Kanaatimizce 2016 yılında yapılan değişiklikten önce eylemin sisteme girme ve orada kalma şeklinde olması sebebiyle, fail sisteme girdikten sonra sistemde kalmaya devam ederken verilen bir rıza suçun henüz tamamlanmamış olması dolayısıyla eylemi hukuka uygun hale getirdiğinden söz edilebilirdi. Ancak özellikle 2016 değişikliğinden sonra failin sisteme girmesiyle suç tamamlanacağından yazarların bu görüşüne katılmak mümkün değildir. Gerçekten de bu

¹⁵⁰ AKBULUT, s. 136.

¹⁵¹ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.284.

değişiklikle birlikte sisteme girme ve sistemde kalma fiillerinin suçun seçimlik hareketleri olarak düzenlenmiş olması karşısında failin bir anlığına bile olsa sisteme girmesiyle suç tamamlanmış sayılacaktır. Suç tamamlandıktan sonra verilen rıza fiili hukuka uygun hale getirmeyecek, mağdur şikâyetçi olmasa bile suçun soruşturma ve kovuşturması devam edecektir. Ancak mağdurun şikâyetçi olmaması durumunda adli makamların suçtan haberdar olması oldukça güçtür. Bilişim suçlarında genellikle mağdurun ihbarı üzerine soruşturma yürütülür. Kalma fiiline rıza gösteren mağdur bu yönde bir bildirimde bulunmayacaktır. Gerçekte işlenmiş olmasına rağmen bilinmeyen, suç istatistiklerine yansımayan suçlara suçta siyah sayılar ya da karanlık alan denir.¹⁵² Kalma fiiline sonradan rıza gösteren mağdurun bu yönde bildirimde bulunmaması dolayısıyla bu suçlar da siyah sayı olarak kalacaktır.

Bir kimseye bir bilişim sistemine bir kerelik erişim için izin verilmiş olması kişinin daha sonra da sisteme girebileceği anlamına gelmeyecektir. Aynı şekilde bir kimseye sosyal medya hesabının şifresinin verilmiş olması da bu kimsenin hesap sahibinin bilgisi dışında dilediği zaman sisteme girebileceği anlamına gelmez¹⁵³.

Rızayı gösteren iradenin sakatlanmamış olması gerekir.

Görevin ifası dolayısıyla hareket edilmesi de hukuka uygunluk sebebidir. Örneğin CMK 134. maddesi gereği hâkim kararı üzerine sisteme yapılacak bir erişim halinde, bu erişimi yapan kişinin eylemi TCK 243'te düzenlenen suçu oluşturmayacaktır.

2.1.6. Suçun Neticesi Sebebiyle Ağırlaşmış Hali

TCK'nın 243. maddesinin 3. fıkrasında failin eylemi neticesinde sistemde yer alan verilerin yok olması ya da değişmesi durumunda altı aydan iki yıla kadar hapis cezasına mahkum edileceği ifadesine yer verilerek suçun neticesi sebebiyle ağırlaşmış hali düzenlenmiştir. Söz konusu maddenin gerekçesinde de maddenin üçüncü fıkrası ile suçun neticesi sebebiyle ağırlaşmış hâlinin düzenlendiği belirtilmiştir. Gerekçede birinci fıkra tanımlanan suçun işlenmesi dolayısıyla sistemde yer alan verilerin yok olması yahut değişmesi durumunda failin, suçun temel şekline göre daha ağır ceza ile cezalandırılmasının düzenlenmiş olduğu belirtilerek 3. fıkranın birinci fıkra tanımlanan suçun neticesi sebebiyle ağırlaşmış hali olduğu vurgulanmıştır. Bazı yazarlar ise bu fıkranın, birinci fıkra yer alan suçun nitelikli hali olduğunu ifade etmektedirler¹⁵⁴. Ancak

¹⁵² ARTUK, M. Emin, ALŞAHİN, M. Emin, Kriminoloji, Adalet Yayınevi, Ankara, 2021, s. 134-136.

¹⁵³ “mağdur Ebru'ya ait elektronik posta adresinin ve bu adresle bağlantı kurulan facebook hesabının önceden bildiği internet şifrelerini, mağdurun bilgisi ve rızası dışında değiştirerek, hakkı bulunmadığı halde giriş yaptığı mağdurun facebook hesabı üzerinden eski kız arkadaşının üvey annesi ile iletişim kurup, hukuka aykırı olarak sistemde kalmaya devam ederek, mağdurun hesaplarına erişimini engellemesi eylemlerinin TCK'nın 244/2. maddesinde tanımlanan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunu oluşturduğu”. Yargıtay 12. Ceza Dairesi, 01.03.2017 tarih, 2015/10388 E - 2017/1556 K –UYAP'tan alınmıştır.

¹⁵⁴ GÜL, s. 68; TEZCAN, ERDEM, ÖNOK, s. 1058.

genel görüş, 3. fıkranın madde gerekçesinde de belirtildiği üzere neticesi sebebiyle ağırlaşmış hal olduğudur¹⁵⁵.

Burada önem arz eden nokta failin hareketi neticesinde veriler yok olduğu yahut değiştiği halde failin kastının bu yönde olmamasıdır. Madde gerekçesinde de bu halin söz konusu olabilmesi için, failin kasten verileri yok etmek veya değiştirmek amacıyla hareket etmemesi gerektiği hususuna yer verilmiştir. Zira failin kasten sistemdeki verileri yok ettiği yahut değiştirdiği durumda TCK'nın 244. maddesinde düzenlenen suç uygulama imkanı bulacaktır. Ancak bu nitelikli halin uygulama alanı bulabilmesi için failin ağırlaşmış neticeye ilişkin taksirle hareket etmiş olması gerekir. Gerçekten de TCK'nın 23. maddesinde “Bir failin, kastedilenden daha ağır veya başka bir neticenin oluşumuna sebebiyet vermesi halinde, kişinin bundan dolayı sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekir.” denilmiştir. Fail bu sonucu istemese de meydana gelen zarar ile failin fiili arasında nedensellik bağı bulunmalıdır.

Söz konusu fıkra neticeler seçimlik olarak düzenlenmiştir. Failin taksirli hareketi sonucunda sistemde bulunan verilerin değişmesi veya yok olması sonuçlarından birisinin gerçekleşmesi yeterlidir, her ikisinin de bir arada bulunması gerekmez. Ancak her ikisinin de gerçekleşmiş olması suçun tekliğine etki etmeyecektir.

Öte yandan doktrinde madde metninde suçun taksirle işlenebileceğinin düzenlenmediği, dolayısıyla üçüncü fıkranın da taksirle işlenmesinin imkânsız olduğu yönünde eleştiriler mevcuttur¹⁵⁶. Yazarlara göre TCK m. 244/3 de ancak kastla işlenebilir. Fakat bu durumda da TCK m. 244/2 ile TCK m. 243/3 arasında çatışma yaşanmaktadır. Ancak ceza hukukumuzda failin meydana gelen netice bakımından en azından taksirle hareket etmesi gerektiği¹⁵⁷ hususu göz önüne alındığında bu görüşe katılmak bizim açımızdan mümkün değildir. Çünkü TCK'nın 243/3. maddesinde yer alan düzenleme de bir neticesi sebebiyle ağırlaşmış haldir. Failin dikkat ve özen yükümlülüğüne aykırı davranışı sonucu madde metninde yer alan neticenin meydana gelmesi bu hal açısından yeterlidir.

2.1.7. Suçun Nitelikli Hali

TCK'nın 243. maddesinin ikinci fıkrasında birinci fıkra da yer alan fiillerin bedeli karşılığında faydalanılabilen sistemler hakkına işlenmesi durumuna cezanın yarı oranına kadar indirileceği hükme bağlanarak suçun daha az cezayı gerektiren nitelikli hali düzenlenmiştir.

Söz konusu fıkra da “bedeli karşılığında yararlanılabilen sistemler” ifadesi geçmekte ancak ne madde metninde ne de gerekçesinde bu kavramın ne anlama geldiği ifade edilmemektedir. Bedeli karşılığında yararlanılabilen sistemlerin ne olduğunun anlaşılabilmesi için evvela “bedel” kavramı ile neyin kastedildiği belirlenmelidir. Bedel

¹⁵⁵ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 969; DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.264; AKBULUT, s. 149; PARLAR, s. 22; Karakehya, s. 18; ARTUK, M.Emin, GÖKCEN, Ahmet, YENİDÜNYA, A. Caner, Adalet Yayınları, Ankara, 2014, s. 760; SOYASLAN, Ceza Hukuku Özel Hükümler, s. 659; KOCA/ÜZÜLMEZ, s. 859;

¹⁵⁶ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s.975.

¹⁵⁷ ÖZBEK/DOĞAN/BACAKSIZ, s. 498.

sözcüğü, “değer, fiyat, kıymet, bir şeyin yerini tutabilen karşılık” anlamına gelmektedir¹⁵⁸. Burada bedel sözcüğü ile ifade edilen şey yalnızca para değildir. Para dışındaki herhangi bir karşılık da söz konusu fıkra kapsamında bedel olarak değerlendirilebilecektir. Örneğin grafikerlerin yararlanmasına sunulmuş bir veri tabanı içerir internet sitesi, abone olma koşulu olarak belirli sayıda grafiğin site veri tabanına yüklenmesini şart koşmuş olabilir. Aynı şekilde birtakım özelliklere erişim için özel üyelik şartı koşan bir internet sitesi, bu özel üyeliğin alınabilmesi koşulu olarak sistemde belirli sayıda içerik paylaşılmasını yahut sisteme belirli sayıda abone getirilmesini şart koşmuş olabilir. Bu tarz durumlarda da söz konusu sistemler bedeli karşılığında yararlanılabilen sistemler olarak kabul edilecektir.

Bedeli karşılığında yararlanılabilen sistemlere örnek olarak sanal kütüphaneler, yalnızca ücret karşılığı oynanabilen oyunlar sunan sistemler, bedel karşılığında üye olunarak müzik dinlenen yahut dizi ve film izlenen siteler verilebilir.

Bazı yazarlar internet kafelerin bilgisayarlarından ücretsiz yararlanılması durumunu da TCK 243/2 kapsamında değerlendirmektedir¹⁵⁹. Bazı yazarlar ise bilişim sisteminin kullanıldığı mekânın değil, bizzat bu sistemin ücretli olması gerektiğini dolayısıyla bu durumun TCK 243/2 kapsamında değerlendirilemeyeceğini ifade etmektedirler¹⁶⁰.

TCK 243/2 maddesi uygulanırken dikkat edilmesi gereken hususlardan birisi de TCK 163. maddesinde düzenlenen karşılıksız yararlanma suçu ile arasındaki ayrımın iyi yapılmasıdır. Zira söz konusu maddenin ikinci fıkrasında telefon hatları ve frekanslarından yahut elektromanyetik dalgalarla yapılan şifreli ya da şifresiz yayınlardan sahibinin ya da zilyet olan kişinin rızası bulunmaksızın faydalanan kişinin altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılacağı düzenlenerek TCK 243/2. maddesi ile ortak uygulama alanı bulabilecek bir düzenlemeye yer verilmiştir. Burada dikkat edilmesi gereken husus TCK 163. maddesinde “telefon hatları ile frekanslarından veya elektromanyetik dalgalarla” denilerek bir sınırlamaya gidilmiş olduğudur. Dolayısıyla bu kapsamda yer alan sistemlere girilmesi durumunda TCK 163. maddesi uygulama alanı bulacak, bu kapsamında dışında kalan sistemler için ise TCK 243/2. maddesi uygulanacaktır. Yine de doktrinde bu konuda farklı görüşler mevcuttur. Örneğin bazı yazarlar internet üzerinden verilerin hizmetlerden yararlanılması durumunda TCK m. 163/2’nin oluşacağını savunmaktadırlar¹⁶¹. Bir başka grup yazarlar ise söz konusu ağın kablolu ya da kablosuz olması durumuna göre ayrım yapmaktadır. Bu grupta bulunan yazarlara göre kablosuz bir ağın kullanılması durumunda TCK 243/1-2 maddeleri uygulama alanı bulacak, kablolu bir ağın kullanılması durumunda ise TCK 162/2. maddesi uygulanacaktır¹⁶². Bazı yazarlar ise ücretli yayınların internet aracılığıyla şifrelerinin

¹⁵⁸ <https://sozluk.gov.tr>, Erişim Tarihi: 20.10.2019.

¹⁵⁹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 268; AKBULUT, s. 144; MAHMUTOĞLU, Fatih, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi". İstanbul Üniversitesi Hukuk Fakültesi Dergisi, 71, 2013, s.863.

¹⁶⁰ TEZCAN/ERDEM/ÖNOK, s. 1058; ERDOĞAN, 149-150.

¹⁶¹ ARTUK/GÖKCEN/YENİDÜNYA, s. 758/759.

¹⁶² TEZCAN, ERDEM, ÖNOK, s.856.

kırılarak izlenmesi durumunda TCK 243/2 maddesinin uygulanması gerektiğini belirtmektedir¹⁶³.

Bazı yazarlar, fiilin bedeli karşılığında yararlanılabilen sistemlere karşı işlenmesi durumunda cezanın indirilmesi durumunu eleştirerek bu halin cezayı ağırlaştırıcı bir hal olarak düzenlenmesi gerektiğini belirtmektedirler¹⁶⁴. Bu yazarlara göre suçun bedeli karşılığında yararlanılan bir sisteme karşı işlenmesi durumunda hem sistemin güvenliği ihlal edilmiş olacak hem de malvarlığına yönelik bir zarar oluşacaktır. Dolayısıyla iki farklı değer ihlal edilmiş olduğundan ceza ağırlaştırılmalıdır. Bazı yazarlar ise sisteme girme ve kalma fiilleri açısından bir ayırım yapılması gerektiğini, sisteme girme açısından söz konusu düzenleme bir sorun arz etmese de sistemde kalma açısından düzenlemenin yersiz olduğunu savunmaktadır¹⁶⁵.

“Bedeli Karşılığında Yararlanılabilen Bilişim Sistemlerine Girme veya Kalma” şeklindeki kendisine ait yaptırımı bulunan ayrı bir suç olarak düzenlenmesi gerekmektedir. İhdas edilecek bu yeni suç tipinin alt sınırı TCK’nın 243/1. maddesinde düzenlenen suça ilişkin yaptırımdan düşük, üst sınırı ise bu suça ilişkin yaptırımdan fazla olmalıdır. Hâkim, eylemin işleniş tarzı ve meydana gelen tehlikenin ağırlığına göre bu sınırlar arasından bir ceza tayin edecektir. Böyle bir düzenleme yapılmasının sebebi hiç şüphesiz bu şekildeki bir eylemin çok çeşitli şekillerde işlenebiliyor olmasıdır. Örneğin bilgisayar bilgisine ancak temel düzeyde olan bir kimse dahi internet üzerinden yaptığı küçük bir araştırma ile bedeli karşılığında yararlanılabilen bir bilişim sistemine giriş yapabilmektedir. Failin internet üzerinden basitçe ulaşabileceği bir yöntem ile ücreti karşılığında film izleyebileceği, müzik dinleyebileceği ya da oyun oynayabileceği bir sisteme girmiş olması durumunda hâkim alt sınırdan ceza tayin edebilecekken failin özel bilgi ve beceri gerektiren birtakım yöntemler kullanarak böylesi bir sisteme girmesi ya da giriş yaptığı sistemde malvarlığı bakımından büyük bir tehlike yaratması durumunda ise üst sınırdan ceza tayinini tercih edebilecektir.

2.1.8. Neticesi Sebebiyle Ağırlaşmış Hal ile Nitelikli Halin Bir Arada Bulunması Durumu

TCK 243/2 maddesinde birinci fıkrada düzenlenen suçun konusunun bedeli karşılığında yararlanılan bir sistem olması halinde cezada indirim yapılacağı düzenlenirken, üçüncü fıkrada ise eylem sonucunda sistemdeki verilerin yok olması veya değişmesi durumunu içerir neticesi sebebiyle ağırlaşmış hali düzenlenmiştir. Bedeli karşılığında yararlanılan bir sisteme karşı TCK 243/1 maddesinde düzenlenen suçun işlendiği ve bu fiil neticesinde sistemde bulunan verilerin yok olduğu yahut değiştiği durumda ise yine neticesi sebebiyle ağırlaşmış hal uygulama alanı bulacaktır. Zira söz konusu üçüncü fıkranın düzenlenmesinde ikinci fıkra ile ilişkili bir istisna söz konusu değildir¹⁶⁶.

¹⁶³ AKBULUT, s.145.

¹⁶⁴ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 269-272.

¹⁶⁵ AKBULUT, s.142-143.

¹⁶⁶ AKBULUT, s. 149; KOCA/ÜZÜLMEZ, s. 859; DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 273-274.

2.1.9. Terör Amacı ile Bilişim Sistemine Girme veya Kalma

3713 sayılı Terörle Mücadele Kanunu'nun 4. maddesinde katalog olarak belirlen suçların ilgili yasanın 1 inci maddesinde ifade edilen hedefler doğrultusunda suç işlemek amacıyla kurulmuş bir terör örgütünün eylemleri çerçevesinde işlenmesi durumunda terör suçu sayılacağı düzenlenmiş ve TCK 243. maddesi de bu kapsamda sayılmıştır.

İlgili yasanın 5. maddesinde ise yasanın 3.ile 4. maddelerinde belirtilen suçları işleyenler hakkında ilgili yasalar uyarınca belirlenecek hapis cezalarının ve adli para cezalarının yarı oranında arttırılacağına yer verilmiştir. Maddeye göre bu şekilde belirlenecek cezalarda, gerek o fiil için, gerek her türden yaptırım için belirlen cezanın yukarı sınırının aşılabileceği belirtilmiştir. Öte yandan müebbet hapis cezası yerine, ağırlaştırılmış müebbet hapis cezasına hükmolunur denilmiştir. Bu sebeple bilişim sistemine girme veya kalma suçunun terör faaliyeti çerçevesinde işlenmesi durumunda cezasının yarı oranında arttırılacağı da hükme bağlanmıştır.

2.1.10. Suçun Özel Görünüş Biçimleri

2.1.10.1. Teşebbüs

Bilişim sistemine girme veya sistemde kalma suçu sırf hareket suçudur, bu suçun gerçekleşmesi için netice aranmaz. Failin sisteme girmesiyle ya da hukuka aykırı olarak sistemde kalmaya devam etmesiyle suç oluşur.

TCK 243'te düzenlenen suç seçimlik hareketli bir suç olduğu için bu suça teşebbüsün mümkün olup olmadığını her iki hareket bakımından ayrı ayrı değerlendirmek icap etmektedir.

Fail hukuka aykırı olarak sisteme girmeye çalışırken elinde olmayan herhangi bir sebep dolayısıyla sisteme giriş yapamazsa bilişim sistemine girme suçu teşebbüs aşamasında kalmış olacaktır. Burada failin eyleminin yarıda kalmasına sebep olan durumun ne olduğu engel teşkil etmez. Örneğin failin sistemin güvenlik mekanizmalarını aşamaması sebebiyle eyleminin tamamlanamaması durumunda suç teşebbüs aşamasında kalmış olacaktır.

Bir bilişim sistemine girmeye çalışan failin bu fiilinde başarısız olması ancak mağdurun da sisteme erişimini engellemesi durumunda TCK 244/2. maddesinin de değerlendirilmesi gerekecektir¹⁶⁷.

Bir diğer seçimlik hareket olan sistemde kalmaya devam etme açısından ise teşebbüs mümkün değildir. Zira failin iradesi sistemde kalmak dahi olsa sisteme giriş yapmasıyla birlikte suç tamamlanmıştır, sistemde kalma hareketinin tamamlanmaması suçun oluşmasını etkilemeyecektir. Yine sisteme hukuka uygun olarak girmiş olan failin, sistemde

¹⁶⁷ “... sanık tarafından adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığı Microsoft şirketinden sorulup, sonucuna göre katılana ait mail adresinin erişilmez kılındığı takdirde Türk Ceza Kanunu'nun 244/2., mail adresine girildiği ancak; bu adrese erişimin engellenmemesi ve katılanın mail adresinde kalmaya devam ettiğinin tespiti halinde aynı yasanın 243/1. maddesi kapsamındaki suçun oluşacağı dikkate alınarak tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması...” (8. CD. 11.12.2015 gün ve 2015/9842 E – 25682 K – UYAP'tan alınmıştır.)

kalmasının hukuka aykırı hale geldiği anda sistemden çıkmaması durumunda suç tamamlanır. Burada sistemde kalma hareketinin çok kısa sürmüş olması önemli değildir.

2.1.10.2. İştirak

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme veya sistemde kalma suçu iştirak açısından özel bir nitelik arz etmez. Söz konusu suça herhangi bir suretle iştirak edilmesi mümkündür. Bu durumlarda TCK'nın 37-40 arasındaki hükümleri uygulanır.

Sistemde kalmaya devam etme hareketi açısından TCK 243 mütemadi bir suçtur. Hareketin yapılmasıyla suç tamamlanır ancak sona ermez. Sona erme anına kadar azmettirme hariç olmak üzere tüm iştirak türleri mümkündür¹⁶⁸.

2.1.10.3. İçtima

TCK'nın 43. maddesinde aynı suç işleme kararını icra ederken, farklı zamanlarda ancak aynı kişiye karşı suçun birden çok kez işlenmesi durumunda tek cezaya hükmolunacağı ancak cezanın dörtte birinden dörtte üçüne kadar arttırılacağı düzenlenmiştir. Failin tek bir suç işleme kararıyla aynı kişiye karşı bu suçu farklı zamanlarda birden çok kere işlemesi halinde TCK'nın 43. maddesinde düzenlenen zincirleme suç hükmü uygulanır.

Bir olay söz konusu olduğunda zincirleme suç hükümlerinin uygulanabilmesi için; birden fazla kez TCK'nın 243. maddesinin ihlal edilmiş olması, bu ihlallerin tek bir suç işleme kararı neticesinde gerçekleştirilmesi ve tüm ihlallerde mağdurun tek kişi olması gerekir¹⁶⁹. Bu ihlallerden bazıları tamamlanmış, bazıları ise teşebbüs aşamasında kalmış olsa dahi zincirleme suç hükümleri uygulanacaktır¹⁷⁰.

Aynı şekilde suçun temel şekli ile neticesi sebebiyle ağırlaşmış halinin de farklı zamanlarda aynı mağdura karşı birden fazla kez işlenmesi durumunda zincirleme suç hükümleri uygulanacaktır. Ancak tek bir fiille aynı mağdura karşı işlenen fiilin, suçun neticesi sebebiyle ağırlaşmış şeklini ihlal etmesi durumunda tek bir suçun varlığından söz edilecektir. Zira TCK 43/1 gereğince bir suçun temel şekli ile daha ağır veya daha az cezayı gerektiren nitelikli şekilleri, aynı suç sayılır.

Ancak, zincirleme suça ilişkin hükümlerin uygulanabilmesi için suçların değişik zamanlarda işlenmesi gerekir. Aynı anda işlenen suçlarda zincirleme suç hükümleri uygulanamaz. Burada değişik zamanlarda ifadesinden ne anlaşılması gerektiği önem arz etmektedir. Bu kavram dar yoruma tabi tutulmamalı, çok kısa aralıklarla işlenen fiiller de aynı zaman diliminde işlenmiş kabul edilmelidir¹⁷¹. Örneğin fail sisteme giriş yaptıktan hemen sonra herhangi bir sebeple sistemden çıkmak durumunda kalıyor ve tekrar giriş yapıyorsa burada failin sisteme girme eylemini aynı zaman diliminde işlediği kabul edilmeli ve zincirleme suç hükümleri uygulanmak yerine faile tek bir suçtan ceza verilmelidir. Ancak sistemden çıkmak zorunda kaldıktan yahut sistem tarafından dışarı atıldıktan sonra sisteme tekrar giriş yapması ile arasında belirli zaman dilimi söz konusu

¹⁶⁸ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s.295.

¹⁶⁹ DÖNMEZER, s. 663.

¹⁷⁰ ARTUK/GÖKCEN/YENİDÜNYA, s. 645.

¹⁷¹ HAKERİ, Hakan, Ceza Hukuku Genel Hükümler, 17. Baskı, Adalet Yayınevi, Ankara, 2014, s.

ise bu durumda eylemin tekliğinden söz edilemeyecek ve fail hakkında diğer şartların da varlığı halinde zincirleme suç hükümleri uygulanacaktır.

Sisteme girme veya sistemde kalma fiilleri seçimlik hareketler olduğundan failin önce sisteme girmesi ardından da sistemde kalmaya devam etmesi durumunda tek bir suç oluşmuş olacak, zincirleme suç hükümlerinin uygulanması söz konusu olmayacaktır. Ayrıca sistemde kalmaya devam etme fiili açısından suç mütemadi niteliktedir, failin sistemde çok uzun süre kalması da suçun tekliğini etkilemeyecektir.

TCK'nın 243. maddesinde düzenlenen suç tipine ilişkin olarak fıkri içtima hükümlerinin uygulanıp uygulanamayacağını belirlemek için öncelikle bu suç tipinin geçit suçu niteliği taşıyıp taşımadığı konusu irdelenmelidir. Geçitli suçun söz konusu olabilmesi için; suçların aynı fail tarafından işlenmesi, mağdurun aynı olması, failin söz konusu hareketleri ile hafiften ağıra giden bir süreç izlemesi, bu hareketle işlenen suçların korudukları hukuki yararlarının aynı olması, gerçekleşen neticelerin aynı harekete tek bir nedensellik bağı ile bağlanmaları ve failin kastının ilk harekete başladığı andan itibaren ağıra doğru giden tüm neticeleri derece derece gerçekleştirmeye yönelik bulunması gerekir¹⁷².

İçtima ile ilgili olarak çözülmesi gereken bir başka sorun ise failin bir bilişim sistemine giriş yaptıktan sonra, bu sistemden yararlanarak başka bir bilişim sistemine giriş yapması halidir. Bu duruma örnek olarak şirketlere yönelik olarak belirli hizmetler veren ve bu hizmetler dolayısıyla şirketlere ait bilişim sistemlerine giriş yapma yetkisi bulunan bir mağdura ait bilişim sistemine giriş yaptıktan sonra bu sistemdeki yetkileri kullanarak mağdurun erişim hakkı olan diğer sistemlere de giriş yapan failin durumu verilebilir. Fail burada ilk sisteme hukuka aykırı olarak girmiştir. İkinci sisteme giriş yaparken, ilk sistemdeki yetkileri kullanması failin eylemini hukuka uygun hale getirmeyecek, failin ikinci eylemi de hukuka aykırı olacaktır. TCK'nın 43/1. maddesinde düzenlenen zincirleme suç hükümlerinin uygulanabilmesi için failin tek bir suç işleme kararıyla aynı mağdura karşı birden çok kez aynı suçu işlemesi gerekir. Oysa olayda birden fazla mağdur vardır. TCK'nın 43/2. maddesinde düzenlenen aynı neviden fıkri içtimanın uygulanabilmesi için ise failin tek bir eylemle birden fazla mağdura karşı aynı suçu işlemesi gerekir. Oysa böyle bir durumda fail birden fazla eylem gerçekleştirmektedir. Dolayısıyla fail, iki farklı mağdura karşı iki farklı hukuka aykırı eylem gerçekleştirmiş olduğundan gerçek içtima hükümlerine göre her iki suçtan da cezalandırılması gerekecektir.

Doktrinde özellikle TCK'nın 244/2. maddesi ile 243/1. maddesi arasında geçitli suç durumunun bulunup bulunmadığı tartışma konusudur. Bazı yazarlar, TCK 244/2 maddesinde yer alan suçun işlenebilmesi için failin sisteme girmesinin zorunlu olduğunu, dolayısıyla geçitli suç kurallarının uygulanması gerektiğini belirtmektedir¹⁷³. Bazı yazarlar ise geçitli suç kurumunu kabul etmediklerinden ötürü burada da uygulanamayacağı

¹⁷² DÖNMEZER/ERMAN, s. 649-650.

¹⁷³ PARLAR, s. 21; SOYASLAN, Ceza Hukuku Özel Hükümler, s. 568;

görüşündedirler¹⁷⁴. Bazı yazarlar ise bu durumda fikri içtima hükümlerinin uygulanması gerektiği görüşündedir¹⁷⁵.

Dülger ise somut olayın özelliklerine göre belirleme yapılması görüşündedir. Yazara göre eylemler açısında zamansal farklılık yoksa eylem tek kabul edilerek yalnızca 244/2 maddesinden ceza verilmeli, failin farklı kastlarla hareket ettiğinin kabulüne imkân verecek ölçüde zamansal farklılık bulunması halinde ise her iki suçtan ayrı ayrı ceza verilmelidir. Yazara göre 244/2’de yer alan suçun her bir seçimlik hareketi için ayrı ayrı değerlendirme yapılmalıdır. Suçun işlenebilmesi için öncesinde sisteme girilmesinin zorunluluk olduğu durumlarda geçit suç söz konusu olacaktır. Örneğin sisteme veri yerleştirilmesi fiili için öncelikle sisteme girilmesi gerekir. Dolayısıyla burada sisteme hukuka aykırı olarak girme suçu cezalandırılmayan önceki hareket niteliğinde olacaktır¹⁷⁶.

Yargıtay da 243/1. ve 244/2. maddelerinin aynı suç işleme kararı kapsamında ihlal edilmesi durumunda yalnızca 244/2. maddesinden ceza verilmesi gerektiği görüşündedir¹⁷⁷.

Kanaatimizce her olay için failin kastı ve somut olayın diğer özellikleri göz önüne alınarak belirme yapılmalıdır. Örneğin bir bilişim sistemine en başından itibaren sistemdeki verileri bozmak için girilmesi durumunda fail tek bir hareketle hem bilişim sistemine ve hem de sistemdeki verileri bozma suçlarını işlemiş olacaktır. Bu durumda fikri içtima hükümleri uygulanmalıdır. Ancak sistemdeki verilerin bozulması için failin sisteme girmesi şart değildir. Failin sisteme girmeksizin de sistemdeki verileri yok edebileceği durumlar söz konusudur. Failin önce yakınında bulunduğu bir sisteme önce giriş yapması ardından da sisteme fiziksel olarak zarar vererek verileri yok etmesi durumunda her iki suçtan ayrı ayrı ceza verilmelidir. Sistemin güvenlik özellikleri gereği failin söz konusu verileri bozmak için öncelikle sisteme giriş yapmasının gerekli olduğu durumlarda ise sisteme giriş yapılmadan 244/2’deki suç da işlenemeyeceğinden burada 243/1’den ayrıca ceza verilmeyecektir, zira burada geçitli suç söz konusu olacaktır.

TCK’nın 245/A maddesinde düzenlenen suç ise amaç suç niteliği taşımaktadır. Fail hem 245/A hem de 243/1 maddelerini ihlal etti ise her iki suçtan da ayrı ayrı cezalandırılmalıdır¹⁷⁸.

Fail başka bir suçu örneğin özel yaşamın gizliliğini ihlal suçunu işlemek kastıyla bilişim sistemine girme veya kalma suçunu işlerse bu durumda her iki suçtan da ayrıca ceza verilmesi gerekir¹⁷⁹. Aynı şekilde failin bir bilişim sistemine girdikten sonra bilişim sistemini kullanmak suretiyle dolandırıcılık suçunu işlemesi durumunda da Yargıtay’a göre

¹⁷⁴ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 976.

¹⁷⁵ AKBULUT, s. 152; KOCA/ÜZÜLMEZ, s. 860-861;

¹⁷⁶ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 298.

¹⁷⁷ “...şikayetçi tarafından kendi adresine erişim sağlanıp sağlanmadığı, sanık tarafından adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığı Microsoft şirketinden sorulup, sonucuna göre katılana ait mail adresinin erişilmez kılındığı takdirde TCK.nun 244/2., mail adresine girildiği ancak; bu adrese erişimin engellenmemesi ve katılanın mail adresinde kalmaya devam ettiğinin tespiti halinde aynı yasanın 243/1. maddesi kapsamındaki suçun oluşacağı...” (8. Ceza Dairesi, 27.09.2017 gün, 2016/11236 E - 2017/10500 K. – UYAP sisteminden alınmıştır.)

¹⁷⁸ AKBULUT, s. 153.

¹⁷⁹ TEZCAN/ERDEM/ÖNOK, s. 1061.

her iki suçtan ayrı ayrı ceza verilecektir¹⁸⁰. Burada önem arz eden durum araç suç- amaç suç durumunda bulunan bu suçların icra hareketlerinin ne ölçüde örtüştüğüdür. Zira fiiller arasında tam bir örtüşme varsa bu durumda fikri içtima hükümlerine göre belirleme yapılmalıdır.

Failin bir başkasına ait bilişim sistemine girmesi ve buradaki verileri kaydetmesi durumunda TCK'nın 132. maddesi ile 243. maddesi arasında gerçek içtima uygulanacaktır¹⁸¹.

2.1.11. Soruşturma Usulü ve Yaptırım

TCK'nın 243/1. maddesinde bu suçun yaptırımını olarak bir yıla kadar hapis veya adli para cezası belirlenmiştir. Bu suç tipinde adli para cezası ve hapis cezası seçimlik yaptırım olarak düzenlenmiştir. Bu iki yaptırım seçimlik olarak düzenlendiği için iki yaptırımı birden hükmedilmesi mümkün değildir. Ayrıca TCK m. 50/2'de yer alan düzenleme dolayısıyla hapis cezasına hükmedilmişse; bu ceza artık adli para cezasına çevrilemeyecektir. Tekerrür hükümlerinin uygulanması halinde ise, TCK'nın 58/3. maddesi dolayısıyla hapis cezasına hükümlenilecek, adli para cezası verilemeyecektir.

Hapis cezasının üst sınırı olarak bir yıl belirlenmiştir. Alt sınır için bir belirleme yapılmadığından TCK'nın 49. maddesi göz önünde bulundurularak alt sınır bir ay olarak kabul edilecektir. Adli parasının da alt sınırı TCK'nın 61/9. maddesi dolayısıyla hapis cezasının alt sınırından az; üst sınırı da, hapis cezasının üst sınırından fazla olamayacaktır. Adli para cezasının alt sınırı beş gün, üst sınırı yedi yüz otuz gündür.

İkinci fıkrada düzenlenen hafifletici halin oluşması durumunda ise verilecek ceza yarı oranına kadar indirilecektir. Bu durumda indirim yapılması zorunlu olmakla birlikte yapılacak indirimin miktarı konusunda üst sınır konulmakla birlikte hâkime takdir hakkı tanınmıştır.

Üçüncü fıkrada düzenlenen neticesi sebebiyle ağırlaşmış halin oluşması durumunda ise verilecek ceza altı aydan iki yıla kadar hapis cezası olacaktır. Bu durumda adli para cezasına yer verilmemiş ve yalnızca hapis cezası öngörülmüştür. TCK'nın 244/2. maddesinde *“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*

¹⁸⁰ “...Somut olayda; sanığın, katılanlardan Ayhan Erkek'e ait "erkek 555 @.hotmail.com" MSN adresine şifresini kırmak suretiyle girdiği, diğer katılan Sinan Aktaş ile görüşüp kontör istediği ve katılan Sinan'ın diğer katılan Ayhan zannederek 30 adet 250'lik kontör kart numarasını MSN ile bahse konu mail adresine göndererek bilişim sistemine girme ve bilişim sistemini araç olarak kullanmak suretiyle dolandırıcılık suçlarını işlediğine dair kabulde isabetsizlik görülmüştür...” (15 CD. 16.04.2014 gün, 2014/6871 E- 7381 K. – UYAP sisteminden alınmıştır.)

¹⁸¹ “... Sanığın, eski eşi olan mağdura ait facebook şifresini bildiğini ve şifre kırma gibi bir eyleminin olmadığını beyan etmesi, mağdurun, şifresinin kırılarak facebook hesabına giriş yapıldığına dair iddialarını doğrulayan herhangi bir delil bulunmaması karşısında, sanığın sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakkı olmadığı halde sistemde kalmaya devam etme eyleminin TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ve mağdura ait içeriği özel mesajları okuyup, tarafı olmadığı haberleşme içeriklerini kaydetmesi eyleminin TCK'nın 132/1. madde ve fıkrasındaki haberleşmenin gizliliğini ihlal suçlarını oluşturacağı gözetilmeden...” (12 CD. 25.12.2019 gün, 2019/577 E- 2019/12248 K. – UYAP sisteminden alınmıştır.)

yıla kadar hapis cezası ile cezalandırılır.” denilmesi karşısında maddeler arasında bir orantısızlık söz konusu olmaktadır. Zira 243/3. maddede bilişim sistemine giriş yapan kişinin verilere taksirle zarar vermesi hali düzenlenirken 244/2. maddede fail verilere kasten zarar vermektedir. Buna karşın 244/2. maddede düzenlenen suçun yaptırımını alt sınır bakımından 243/2. maddeden düşüktür.

TCK’nın 246. maddesinde bilişim alanında suçların işlenmesi ile yararına haksız menfaat temin edilen tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir. Dolayısıyla TCK 243. maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunu’nun 11 ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

Üzerinde durulması gereken konulardan bir diğeri de suçun işlendiği yerin neresi olduğu hususudur. Zira bilişim suçlarında fail bir yerden, başka bir yerdeki bilişim sistemine erişerek de bu suçu işleyebilmektedir. Hatta suçun işlenmesi esnasında başka sunucular da aracı kılınabilmekte ve sisteme girme veya kalma fiillerinin oluşma evresinde pek çok farklı yerin yetkisi söz konusu olmaktadır. Uygulamada suçun işlendiği yerin bilişim sisteminin bulunduğu yer olduğu kabul edilmektedir. Doktrinde bu uygulamanın doğru olduğunu savunan yazarlar olduğu gibi¹⁸² failin bulunduğu yer mahkemesinin ve bilişim sisteminin bulunduğu yer mahkemesinin her ikisinin de yetkili olduğunu savunan yazarlar da vardır¹⁸³. Biz de bu suçun işlendiği yer olarak bilişim sisteminin bulunduğu yer mahkemesinin yetkili olduğu kanaatindeyiz.

Hemen hemen her bilişim suçu gibi TCK’nın 243/1. maddesinde yer alan suç da kimi zaman uluslararası olarak işlenebilmektedir. Yani bu suçların faili bir ülkede iken mağduru başka bir ülkede olabilmektedir. Ceza muhakemesinde geçerli olan kural ülkesellik ilkesidir¹⁸⁴. Bu ilke eylemlerin yapıldığı ülke kanuna tabi olmasıdır. Yani Türkiye sınırları içerisinde işlenen suçlarda yargılama yetkisi Türkiye’de söz olacaktır. Bunun haricinde faile göre şahsılık ilkesi gereğince, fiili işlediği sırada Türk vatandaşı olan fail fiilini ülke dışında işlemiş ise yargılaması Türkiye’de yapılamayacaktır. Zira TCK’nın 243/1. maddesinde yer alan suçun temel hali bir yıla kadar hapis cezası öngörmektedir. Oysa faile göre şahsılık ilkesine göre failin cezalandırılabilmesi için failin eyleminin temas ettiği suçun asgari haddinin bir yıl olması gerekmektedir¹⁸⁵.

Bilişim sisteme girme suçları CMK’nın 251. maddesi dolayısıyla basit yargılama usulünün uygulanması mümkün suçlardandır. Hâkim, önüne gelen uyuşmalıkta şartları değerlendirdikten sonra basit yargılama usulünü uygulayıp uygulamayacağına karar

¹⁸² DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s.301.

¹⁸³ AKBULUT, s. 156.

¹⁸⁴ ÖZTÜRK, Bahri, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Seçkin, Ankara, 2020, s. 39.

¹⁸⁵ SOYASLAN, Doğan, Ceza Muhakemesi Hukuku, Yetkin Yayınları, Ankara, 2020,

verecektir. Ancak basit yargılama usulünün uygulanması durumunda sonuç ceza dörtte bir oranında indirileceğinden, basit yargılama usulünü uygulamayan hakim gerekçesini de açıklamak durumunda olacaktır. Basit yargılama usulü derhal uygulama ilkesi gereğince hem ilk derece mahkemesince hem de üst derece mahkemelerce gözetileceğinden suç tarihine bakılmaksızın basit yargılama usulü uygulanacaktır¹⁸⁶.

CMK'nın 253/1-c maddesinde suça sürüklenen çocukların fail olması durumunda üst sınırı üç yılı geçmeyen hapis veya adli para cezasını gerektiren suçlar da uzlaştırma usulü kapsamında sayılmıştır. Dolayısıyla 243. maddenin ilk üç fıkrasında yer alan suçların failinin SSÇ olması durumunda mağdur veya suçtan zarar görenin de gerçek kişi ya da özel hukuk tüzel kişisi olması halinde öncelikle uzlaştırma usulüne başvurulacaktır.

Bu suç için dava zamanaşımı sekiz yıldır. (TCK m. 66/1-e)

Suçun soruşturması re'sen yapılacaktır.

2.2. Veri Nakillerini Sisteme Girmeksizin Teknik Araçlarla İzleme Suçu (TCK 243/4)

2.2.1.Genel Olarak

TCK'nın 243. maddesinin 4. fıkrası 6698 sayılı KVKK'nın 30. maddesi ile eklenmiştir. Söz konusu fıkra her ne kadar 243. maddeye eklenmiş de olsa bağımsız bir suç olarak değerlendirilmesi daha doğrudur. Zira TCK 243. maddesi bir bilişim sistemine girme başlığını taşıırken söz konusu maddenin 4. fıkrası bir bilişim sistemine girmeksizin veri nakillerinin izlenmesini düzenlemektedir. Hal böyleyken bu suçun 243. madde başlığı altında düzenlenmesi hatalıdır. Bu maddenin 243/A gibi ayrı bir madde olarak düzenlenmesi yerinde olacaktır.

Söz konusu fıkra ile bir bilişim sisteminin kendi içinde yahut başka bilişim sistemleri ile arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek suç olarak tanımlanmış ve yaptırım olarak bir yıldan üç yıla kadar hapis cezası belirlenmiştir.

Bu hüküm Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesinin 3. maddesi ile paralel olarak düzenlenmiştir. Yasadışı araya girme başlıklı madde şu şekildedir: “*Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dâhil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak geliştirilen araya girme fiilinin haksız yere ve kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun sahtekârlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir.*”

¹⁸⁶ ÜNVER, Yener, HAKERİ, Hakan, Ceza Muhakemesi Hukuku, Adalet Yayınevi, 2016, s. 88-97; ERCAN, İsmail, Ceza Muhakemesi Hukuku, Kuram Yayınevi, Kocaeli, 2017, s. 5-6.

Ülkemizdeki düzenleme ile sözleşmedeki düzenleme karşılaştırıldığında TCK'daki düzenlemenin daha kapsamlı olduğu görülmektedir. Zira sözleşme maddesinde bulunan kamuya kapalı olarak iletme şartı ve elektronik dalgalarla iletme ifadesi ülkemizdeki düzenlemede yer almamaktadır. Ayrıca TCK'da veri nakillerinin izlenmesi ifadesi yer alırken sözleşmede araya girme ifadesi yer almaktadır.

Sanal Ortamda İşlenen Suçlar Sözleşmesinin Açıklayıcı Raporu'nda bu suç ile ilgili olarak *“Bu hükümle veri iletişiminin gizliliği hakkının korunması amaçlanmaktadır. Suç, kişiler arasındaki sözlü telefon görüşmelerinin geleneksel yöntemlerle dinlenmesi ve kaydedilmesindeki iletişimin gizliliğinin ihlalini temsil etmektedir. İletişimin gizliliği hakkı Avrupa İnsan Hakları Konvansiyonunun 8. Maddesinde kutsal bir hak olarak gösterilmiştir. Madde 3'te tanımlanan suç bu ilkenin telefon, faks, e-posta ya da dosya transferi şeklindeki bütün elektronik veri transferi biçimlerine uygulanmasıdır.”* denilmektedir¹⁸⁷. Buradan da yola çıkarak bu hükmün konuluş amacının veri iletişimin gizliliğinin korunması olduğu sonucuna varılabilir.

2.2.2. Korunan Hukuki Yarar

Kanaatimizce bu suçla korunan hukuki yarar verilerin güvenliğidir. Bazı yazarlar ayrıca özel hayatın gizliliğinin de korunduğunu ifade etmektedirler¹⁸⁸.

Akbulut, bu suçla korunan hukuki yararın veri iletişiminin gizliliğinde, verileri üzerinde tasarruf yetkisi olan kişinin şekli çıkarının korunduğunu belirtmektedir¹⁸⁹.

2.2.3. Maddi Unsurlar

2.2.3.1. Fiil

Bu suçun oluşmasına sebebiyet veren fiil veri nakillerini sisteme girmeksizin teknik araçlarla izlemektir.

İzlemek sözcüğü sözlükte, birinin veya bir şeyin arkasından gitmek, takip etmek, gözlemek, incelemek gibi anlamlara gelmektedir¹⁹⁰.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunu'nun 2. maddesinin h bendinde ise izleme sözcüğü *“İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesini”* şeklinde tanımlanmıştır.

TCK'nın 243/4. maddesinde tanımlanan suçun oluşması için veri nakillerinin izlenmesi yeterlidir. Ayrıca bu verilerin öğrenilmesi, kaydedilmesi ya da bu verilere etki edilmesi gerekmez. Hatta failin bu verileri öğrenmesi, kaydetmesi ya da verilere etki etmesi hallerde özel hayata ve hayatın gizli alanına karşı suçlar ya da TCK'nın 244. maddesinde düzenlenen suçlar gündeme gelecektir.

¹⁸⁷ <https://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/>, 25.12.2019.

¹⁸⁸ TEZCAN/ERDEM/ÖNOK, s. 1062.

¹⁸⁹ AKBULUT, s. 159.

¹⁹⁰ <https://sozluk.gov.tr/>, E.T: 25.12.2019.

Yasa koyucu söz konusu suçun oluşabilmesi için veri nakillerinin teknik araçlarla izlenmesini aramıştır. Dolayısıyla teknik araçlar kullanılmadan yapılan izleme faaliyetleri bu suça sebebiyet vermeyecektir.

Bilişim sistemine herhangi bir şekilde bağlanılarak veri nakillerinin izlenmesi halinde ise bu suç oluşmaz. Zira yasa metni söz konusu fiilin bilişim sistemine girmeksizin işlenmesini aramıştır. Teamweaver ile bilgisayara bağlanması, casus yazılımlar kullanılması, sistemden veri aktarımına yarayan kamera, mikrofon vb. cihazlara ulaşılması durumunda bu suç oluşmayacaktır¹⁹¹.

Doktrinde bir görüşe göre veri nakil ağlarına girilmesi ancak verilerin yalnızca izlenmesi halinde de bu suç oluşur. Dülger veri nakil ağlarının bilişim sistemi olarak kabul edilemeyeceğini ancak veri nakilleri dahi bu suçun konusunu oluşturduğu için sistemler arasındaki nakillerin de bu suçun oluşturacağı görüşündedir¹⁹².

Dülger, veri iletimini koruyan şifrelerin teknik araçlarla kırılması ya da iletim protokollerinin bu araçlarla elde edilmesi durumunda da bu suçun oluşacağı görüşündedir¹⁹³. *Akbulut* ise, şifrelerin kırılması yoluyla sisteme dâhil olunması durumunda TCK 243/1 olacağı görüşündedir¹⁹⁴.

TCK 243/4'te düzenlenen bu suç aynı zamanda mütemadi bir suçtur. İzleme hareketi devam ettiği müddetçe suç da devam etmektedir.

2.2.3.2. Fail

Bu suçla ilgili olarak fail bakımından özellik arz eden bir durum yoktur, herkes bu suçun faili olabilir.

2.2.3.3. Mağdur

TCK'nın 243. maddesinde düzenlenen suçun mağduru herkes olabilir. Zira madde metninde özel bir belirleme yapılmamıştır. Bu suçun mağduru, suça konu olan veriler üzerinde hak sahibi olan kişi ya da kişilerdir.

Doktrinde veriler üzerinde tasarruf yetkisine sahip olan kişinin; alıcı verileri alıncaya yahut almak için çağırma hakkını elde edinceye kadar gönderici, bu andan itibaren ise alıcı olduğu söylenmektedir¹⁹⁵. Bu görüşe katılmak mümkün değildir. Veriler ister alıcıya ulaşmış olsun, ister olmasın gönderici ilk andan üzerinden veriler üzerinde hak sahibidir. Verileri bir kez geri döndürülemeyecek şekilde göndermiş olsa dahi söz konusu verilerin üçüncü kişiler tarafından izlenmesi ile göndericisinin de özel yaşamının gizliliği ve veri güvenliği ihlal edilmiş olacaktır. Aynı şekilde alıcının da henüz verilere erişmemiş olması bu veriler üzerinde hiçbir hakkı bulunmadığı anlamına gelmeyecek, veriler henüz alıcıya ulaşmamışken yapılan izleme hareketi de alıcının veri güvenliğini ve özel yaşamının

¹⁹¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 308; AKBULUT, s. 165-166; ÖZBEK/DOĞAN/BACAŞIZ/TEPE, s. 972.

¹⁹² DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 307.

¹⁹³ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 307.

¹⁹⁴ AKBULUT, s. 163.

¹⁹⁵ AKBULUT, s. 160;

gizliliğini ihlal edecektir. Dolayısıyla verilerin bir kişiden başka bir kişiye gönderildiği her durumda hem alıcı hem de gönderici bu suçun mağdurudur.

Türk hukukunda tüzel kişiler bir suçun mağduru olamazlar. Suçun konusunun tüzel kişilere ait veriler olması halinde tüzel kişiliği oluşturan kişiler bu suçun mağduru kabul edilir. Tüzel kişinin kendisi ise ancak suçtan zarar gören olabilir.

Suçun, kamu kurum ve kuruluşlarına ait veriler üzerinde işlenmesi durumunda ise suçun mağduru toplumu oluşturan tüm bireylerdir¹⁹⁶.

2.2.3.4. Suçun Konusu

Bu suçun konusu aktarım halindeki verilerdir. Bu suçun oluşabilmesi için verilerin sistemler arasında ya da sistemin kendi içinde aktarım halinde olması gerekir. Nakletme işlemi henüz başlamamışken yahut bu işlem tamamlandıktan sonra TCK 234/4. maddede düzenlenen suç gerçekleşemez.

Verilerin içinde bulunduğu depolama aygıtlarının nakil halinde olması durumu bu suç açısından veri nakli sayılmayacaktır.

Veri aktarımının nasıl yapıldığının bir önemi yoktur. Kablolu ya da kablosuz bağlantılar kullanılarak yapılıyor olabilir. İnternet aracılığıyla yapılan veri nakilleri de bu suçun kapsamındadır. Ayrıca Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde elektronik dalgalar aracılığıyla yapılan veri nakillerinin de bu suç kapsamında olacağı belirtilmiştir, her ne kadar TCK 243 bu hususu ayrıca belirtmediyse de ülkemizde de elektronik dalgalarla yapılan veri nakilleri bu suç kapsamındadır. Zira bilişim sistemleri arasında yapılan veri nakilleri kavramı elektronik veri nakillerini de kapsayacaktır¹⁹⁷.

Günümüzde verilerin iletimi sırasında uçtan uca şifreleme gibi metotlar kullanılmaktadır. Ancak TCK 243/4. maddede düzenlenen suç açısından aktarım konusu olan verilerin şifrelenmiş olmasının bir önemi yoktur. Veriler şifrelenmemiş olsa dahi hukuka aykırı olarak izlendikleri takdirde bu suç meydana gelecektir.

2.2.3.5. Netice

TCK 243/4 sırf hareket suçudur. Suçun oluşabilmesi için herhangi bir netice gerçekleşmesine gerek yoktur.

2.2.4. Manevi Unsurlar

Bu suçun taksirle işlenebileceği düzenlenmemiştir. Dolayısıyla bu suç yalnızca kasten işlenebilir bir suçtur.

Suçun oluşabilmesi için özel saik de aranmamıştır. Failin amacı ne olursa olsun kasten bu fiili gerçekleştirdiği takdirde suç oluşacaktır.

Fail hataya düşerek bu suçu işlediyse TCK 30/1 maddesinden yararlanacaktır.

¹⁹⁶ KOCA/ÜZÜLMEZ, s.863, AKBULUT, s. 160.

¹⁹⁷ AKBULUT, s.162.

2.2.5. Hukuka Aykırılık

Hukuka aykırılık bu suç açısından tipikliğe dâhil olan bir unsurdur çünkü madde metninde izlemenin hukuka aykırı olarak yapılması aranmıştır.

Görevin ifası kapsamında yapılan izlemeler bu suç için hukuka uygunluk sebebi sayılır. Örneğin CMK 135. maddesinde düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması tedbirini ifa eden görevliler bu suç kapsamında hukuka uygunluktan yararlanmış sayılır. Ayrıca PYSK 13/A maddesi kapsamında kayıp çocukların araştırılması amacıyla da telekomünikasyon yoluyla yapılan iletişim denetlenebilir.

PYSK Ek madde 7’de *”Polis ... ülke seviyesinde ve sanal ortamda istihbarat faaliyetlerinde bulunur, bu amaçla bilgi toplar, değerlendirir, yetkili mercilere veya kullanma alanına ulaştırır.”* denilmiştir. Polisin bu kapsamda yapacağı izleme faaliyetleri de hukuka uygunluk sebebi sayılacaktır. Benzer bir yetki, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu’nun 6. maddesinin g bendi ile Milli İstihbarat Teşkilatına ve Jandarma Teşkilat, Görev ve Yetkileri Kanunu Ek madde 5 ile jandarmaya verilmiştir.

2.2.6. Özel Görünüş Biçimleri

2.2.6.1. Teşebbüs

TCK’nın 243/4. maddesinde düzenlenen suç sırf hareket suçudur. Suçun tamamlanabilmesi için bir neticenin meydana gelmesi gerekmez. Failin yalnızca izleme hareketini yapması suçun oluşması için yeterlidir.

Fail izlemeye devam ettiği sürece suç gerçekleştiği için bu suç aynı zamanda kesintisiz suç niteliği taşımaktadır¹⁹⁸.

Bu suça teşebbüs teorik anlamda mümkün olsa da gerçekleşmesi oldukça güçtür. Failin teknik araçlarla izleme faaliyetine ilişkin tüm hazırlıkları tamamladıktan sonra, izlemeyi denemesi ancak başaramaması durumunda bu suça teşebbüsten söz edilebilir. Örneğin fail, teknik araçlarla veri nakillerini izlemek için harekete başlar ancak veri nakillerinin gerçekleştiği sistemdeki güvenlik önlemleri dolayısıyla bunu başaramazsa suç teşebbüs aşamasında kalmış olacaktır.

Veri nakillerini izlemek için teknik araçların temin edilmesi ise yalnızca hazırlık hareketi kapsamındadır. Bu teknik araçların temin edilmesi ancak kullanılmaması durumunda TCK’nın 243/4. maddesinde düzenlenen suça teşebbüs söz konusu olmayacaktır. Ancak bu durumda failin TCK 245/A maddesinden cezalandırılması mümkündür.

2.2.6.2. İştirak

TCK’nın 243/4. maddesinde düzenlenen suç iştirak açısından herhangi bir özellik arz etmez.

¹⁹⁸ AKBULUT, s. 168; KOCA/ÜZÜLMEZ, s. 865.

2.2.6.3. İçtima

Failin tek bir hareketle birden fazla bilişim sisteminden veri nakillerini izlemesi halinde aynı neviden fikri içtima söz konusu olacaktır.

Farklı zamanlarda aynı mağdura ait verilerin izlenmesi durumunda ise zincirleme suç hükümleri uygulanacaktır.

Fail izleme fiilini gerçekleştirirken aynı zamanda verilerin ele geçirilmesi, haberleşmenin gizliliğini ihlal, haberleşmenin engellenmesi ya da özel hayatın gizliliğini ihlal gibi suçları da işleyebilir. Bu durumlarda faile her bir suç için ayrı ceza verilmesi gerekir.¹⁹⁹

TCK 245/A maddesinde tanımlanan suç ise bu suçun hazırlık hareketleri kapsamındadır. Failin 243/4'teki suçu işlemesi durumunda ayrıca 245/A'dan sorumlu tutulmaması gerekir.

Doktrinde failin bu suçu işlemek için yasak program üretilip ayrıca bu programı kullanarak TCK 243/4'ü de işlemesi durumunda gerçek içtima kurallarınca sorumlu tutulması gerektiği belirtilmektedir²⁰⁰.

2.2.7. Yaptırım

Bu suçun cezası bir yıldan üç yıla kadar hapis cezasıdır. Soruşturma ve kovuşturulması re'sen yapılır. Bu suç için asliye ceza mahkemeleri yetkilidir.

CMK'nın 253/1-c maddesinde suça sürüklenen çocukların fail olması durumunda üst sınırı üç yılı geçmeyen hapis veya adli para cezasını gerektiren suçlar da uzlaştırma usulü kapsamında sayılmıştır. Dolayısıyla 243/4. maddede yer alan suçun failinin SSÇ olması durumunda mağdur veya suçtan zarar görenin de gerçek kişi ya da özel hukuk tüzel kişisi olması halinde öncelikle uzlaştırma usulüne başvurulacaktır.

2.3. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK 244/1-3)

2.3.1.Genel Olarak

Bilişim sistemleri ve bu sistemlerdeki verileri toplumsal yaşamımızın ayrılmaz bir parçası olmuş durumdadır. Dolayısıyla bu sistemlere ya da bu sistemlerde bulunan verilere karşı yapılacak olan saldırıların toplum hayatını belirli ölçülerde etkilemesi kaçınılmazdır. Yalnızca toplumsal anlamda değil, bireysel anlamda da bu tarz saldırıların zararları oldukça büyük olacaktır. Yasa koyucu da bilişim sistemlerini ve bu sistemlerdeki verileri koruma altına almak ve meydana gelebilecek olan tehlikelere karşı korumak için TCK'nın 244. maddesini düzenlemiştir.

¹⁹⁹ “Sanığın, ATM cihazına düzenek yerleştirmek suretiyle mağdurlara ait kart bilgilerini kopyalaması şeklinde sübutu kabul edilen eyleminin zincirleme şeklinde TCK'nın 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturduğuna ilişkin yerel mahkemenin kabul ve uygulamasında bir isabetsizlik görülmemiştir.” (Yargıtay 12. Ceza Dairesi, 17.01.2018 tarih 2017/1247 E - 2018/534 K – UYAP'tan alınmıştır.)

²⁰⁰ AKBULUT, s. 170.

TCK'nın 244. maddesinin ilk fıkrasında “Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.” denilerek bir bilişim sisteminin işleyişini engellemek ve bozmak, ikinci fıkrasında ise “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.” denilerek bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek, erişilemez kılmak, sisteme veri yerleştirmek ya da verileri başka bir yere göndermek suç olarak düzenlenmiştir. Söz konusu maddenin üçüncü fıkrasında bu fiillerin banka veya kredi kurumlarına ya da kamu kurum veya kuruluşlarına karşı işlenmesi halinde cezanın arttırılacağına ilişkin nitelikli hal düzenlenmiştir.

TCK'nın 244. maddesinin dördüncü fıkrasında ise “Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur.” denilerek bilişim sistemlerinin kullanılması yoluyla haksız yarar sağlama suçu düzenlenmiştir.

Görülmektedir ki TCK'nın 244. maddesi ile aslında birbiri ile bağlantılı olan üç farklı suç, tek bir başlık altında düzenlenmiştir. Aralarındaki benzerliğin daha fazla olması dolayısıyla söz konusu maddenin ilk iki fıkrası ve nitelikli hallerini içeren üçüncü fıkrası bu başlık altında incelenecek, son fıkrası ise ayrı bir başlık altında incelenecektir.

Mülga TCK'nın 525/b-1 maddesi ile TCK'nın 244/1 fıkrası, Mülga TCK'nın 525/a-2 maddesi ile de TCK'nın 244/2 fıkrası büyük oranda benzer düzenlemelerdir. Ayrıca Mülga TCK 525/c maddesinin de TCK 244. maddesi kapsamında kaldığı söylenebilir. Bir anlamda yeni TCK'daki bu düzenlemelerin Mülga TCK'daki düzenlemeler yerini almak için hazırlanmıştır. Yine de söz konusu düzenlemelerin birebir aynı olmadıkları unutulmamalıdır.

Söz konusu maddenin gerekçesinde ise sistemlere yöneltilen zarar verme fiillerinin özel bir suç hâline getirildiği, söz konusu düzenlemenin sistemin fiziksel varlığı ve işlemlerini sağlayan bütün diğer unsurlarını kapsadığı belirtilmiştir. Gerekçe göz önüne alındığında bilişim sistemi ifadesinden sistemin tüm unsurlarının anlaşılması gerektiği görülmektedir. Mala zarar verme suçunun yalnızca mal niteliği taşıyan şeylere verilen zararlara karşı uygulanabiliyor olması bu özel suç tipinin düzenlenmesini zorunlu hale getirmiştir.

Avrupa Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin 4. Maddesi “Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.” şeklindeyken, 5. Maddesi ise, “Taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.” şeklindedir. TCK'nın da 244. maddesinin 2. fıkrasının sözleşmenin 4. maddesinin, 1. fıkrasının ise sözleşmenin 5. fıkrasının karşılığı

olduğu söylenebilir. Görüldüğü üzere TCK düzenlemesinde sözleşmeden farklı olarak söz konusu fiillerin haksız olarak gerçekleşmesi şartı aranmamaktadır.

2.3.2. Korunan Hukuki Yarar

Bu suçla bilişim sistemlerinin hem yazılımları hem donanımları hem de bu sistemlerde bulunan veriler koruma altına alınmıştır. Bu suç tipiyle koruma altına alınan hukuki yarar sistem veya sistemde bulunan veriler üzerinde hak sahibi olan kişinin bu sistemlere ya da verilere hiçbir sorunla karşılaşmaksızın erişebilme ve kullanabilme hakkıdır. Dolayısıyla bu suç tipi sistemin ve içindeki verilerin güvenliğini de korumaktadır.

Dülger'e göre bu suç tipiyle korunan hukuki yarar genel olarak hak sahibinin sisteme ulaşmaktaki çıkarıdır. İlk fıkra sistemin işleyişini korumakta, ikinci fıkra ise sistemdeki verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliğini korumaktadır. Ayrıca verilerin başka yere gönderilmesinin suç olarak düzenlenmesi özel hayatın gizliliğini, sistemin işleyişinin engellenmesi ve bozulmasının suç olarak tanımlanması ile de haberleşme özgürlüğünü korumaktadır²⁰¹.

Bazı yazarlar her iki fıkra için ayrı ayrı belirleme yapmakta, ilk fıkrada bilişim sistemlerinin kullanıcı ve sahiplerinin sistemleri uygun bir biçimde kullanma hakkının²⁰², ikinci fıkrada ise bilgisayar verilerinin ve programlarının kasıtlı zarar verme girişimlerine karşı korunduğunu söylemektedir²⁰³. *Akbulut* ise, birinci fıkra ile sistemin kullanıcıları, işletmecileri ve sahipleri açısından sistemin arızasız şekilde çalışmasındaki yararın korunduğunu söylemektedir. İkinci fıkrada ise veriler üzerinde tasarruf yetkisi olan kişilerin verilerin bozulmadan, herhangi bir engelle karşılaşmadan ve verilerine müdahale edilmeden kullanmasındaki yararları koruma altına alınmıştır²⁰⁴.

Doktrinde bu suç tipiyle; malvarlığı hakkı ve bundan ziyade bilişim sistemlerinin zarar görmemesi, doğru ve işlevine uygun şekilde işlemesindeki toplumsal yararın korunduğu şeklinde bir görüş de mevcuttur²⁰⁵. Bir başka görüşe göre ise bu suç tipi bilişim sisteminin ve verilerin güvenliğini ayrıca mülkiyet hakkını korur²⁰⁶. *Erdoğan*'a göre bu suç tipi, sistemin toplum açısından güvenilir olmasını ve toplumsal menfaatler ile bilişim sisteminin güvenilirliğini korumaktadır²⁰⁷. Benzer mülkiyet hakkı ile toplumsal menfaati koruduğu²⁰⁸ şeklinde görüşler de vardır. Bu suç tipinin, mala zarar verme suçunun özel bir görünüş biçimi olduğunu savunan yazarlara göre ise bu suç tipiyle mülkiyet hakkı korunmaktadır²⁰⁹.

TCK'nın 244. maddesinin 2. fıkrası ile 135. ve 136. maddeleri arasındaki ayrımın yapılması da bu suç tipinin kapsamının ve koruduğu yararın belirlenmesi açısından önem arz

²⁰¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 313-315.

²⁰² ARTUK/GÖKCEN/YENİDÜNYA, s. 764.

²⁰³ ARTUK/GÖKCEN/YENİDÜNYA, s. 775.

²⁰⁴ AKBULUT, s. 181.

²⁰⁵ KOCA/ÜZÜLMEZ, s. 867.

²⁰⁶ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 980.

²⁰⁷ ERDOĞAN, s. 184.

²⁰⁸ YILMAZ, Sacit, 5237 SAYILI TCK'nın 244. MADDESİNDE DÜZENLENEN BİLİŞİM ALANINDAKİ SUÇLAR, TBBT, Y. 23, s. 92, s. 68.

²⁰⁹ TEZCAN/ERDEM/ÖNOK, s. 1064-1065.

etmektedir. TCK'nın 135. ve 136. maddeleri verilerin kendisini korurken 244/2. maddesi verilerin düzgün çalışmasını, varlığını, erişilebilirliğini ve doğruluğunu korumaktadır.

2.3.3. Maddi Unsurlar

2.3.3.1. Fiil

TCK'nın 244. maddesinin birinci ve ikinci fıkrasında tanımlanan suçlar seçimlik hareketlidir. Bu suç tipleri serbest hareketli olup yalnızca bir neticeyi meydana getirmeleri aranmıştır. Hareketlerin ne şekilde yapıldığının bir önemi yoktur. Kısacası TCK 244. maddesinin ilk iki fıkrasında düzenlenen suçlar seçimlik hareketli, serbest hareketli ve neticeli suç tipleridir.

TCK'nın ikinci fıkrasında yer alan hareketlerin yapılması sonucu, ilk fıkra da yer alan neticeler gerçekleşirse artık ilk fıkra hükmünün uygulanması gerekmektedir²¹⁰.

Unutulmamalıdır ki TCK'nın 244. maddesinin ilk iki fıkrasında yer alan fiiller zaman zaman birbirleriyle örtüşmektedirler. Fiilin farklı fıkralarda bulunan neticelere sebebiyet vermesi halinde içtima kuralları uygulanacaktır. Öte yandan aynı fıkra da bulunan farklı neticelere sebebiyet veren bir fiilin varlığı halinde ise olaya göre değerlendirme yapılmalı ve suçun hangi neticeye sebebiyet verdiği tam olarak irdelenmelidir.

2.3.3.1.1. Sistemin Engellenmesi ve Bozulması

TCK'nın 244. maddesinin ilk fıkrasında *“Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.”* denilmek suretiyle bu suçun iki farklı seçimlik hareketten birinin yapılması ile meydana geleceği düzenlenmiştir.

Bu suç açısından sistemin engellenmesi veya bozulması neticedir. Bu fiillerin ne şekilde meydana geldiği önemli değildir, önemli olan bu neticeleri meydana getirecek şekilde hareketlerde bulunulmasıdır.

2.3.3.1.1.1. Sistemin İşleyişinin Engellenmesi

Yargıtay'a göre sistemin işleyişinin engellenmesi bilişim sisteminin verimli çalışmasının engellenmesi, icra ettiği faaliyet ve sahip olduğu kapasitenin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesidir²¹¹.

Sistemin işleyişinin ne şekilde engellendiğinin bir önemi yoktur. Fiil bakımından serbest hareket söz konusudur. Önemli olan yapılan fiil neticesinde engellenmenin gerçekleşmesidir. Erişimin ne kadar süreyle engellendiğinin de bir önemi yoktur. Sistemde anlık bir kesinti yaratılmışsa dahi engellenme gerçekleşmiş sayılabilir. Gerçekten de bankalar, büyük şirketler ve önemli kamu kurumlarının sistemlerine yönelik bir saldırı sonucu oluşabilecek anlık kesintiler dahi büyük zararlara sebep olabilmektedirler.

²¹⁰ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 332;

²¹¹ *“...Sistemin işleyişinin “engellenmesi” ibaresi ile bilişim sistemin verimli çalışmasının önlenmesi, icra ettiği faaliyet ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi...”* (11. CD. 11.03.2013 gün, 2011/1801 E- 2013/3893K – UYAP'tan alınmıştır.)

Bir görüşe göre sistem çalışıyor ancak saldırı sonucunda yavaşlamışsa bu durumda sistemin engellenmesinden söz edilemez²¹². Ancak sistemdeki önemsiz düzeyde yavaşlamaları bir yana bırakırsak sistemde aksama yaratacak düzeydeki yavaşlatmaların engelleme sayılmaması söz konusu değildir. Zira böyle bir durumda da sistem kendisinden beklenen verimde bir çalışma yapamayacak ve sahip olduğu kapasitenin altında bir çalışma gösterecektir. Kısacası sistemin engellenmesinden söz edilebilmesi için sistemin tamamen durma noktasına gelmiş olması gerekmez, sistemin kendisinden beklenen faydayı gereği gibi yerine getirememesi durumunda da sistem engellenmiş olur.

Doktrinde bazı yazarlar TCK 244/1. maddesinde düzenlenen sistemin engellenmesi suçunun yalnızca sistemin soyut unsurlarını kapsadığını, somut unsurlara yönelik ızzar fiillerinin varlığı halinde ise mala zarar verme suçunun oluşacağını ifade etmektedirler²¹³. Oysa sistemin engellenmesi soyut unsurlara yönelik müdahale ile olabileceği gibi somut unsurlarına yönelik müdahale ile de gerçekleşebilir. Sistemin enerjisini kesmek, birtakım maddi unsurları sistemden ayırmak gibi fiiller neticesinde sistemin engellenmesi de sistemin engellenmesi suçunu oluşturacaktır. Burada failin kastının belirlenmesi de büyük önem arz etmektedir. Unutulmamalıdır ki bu suç tipiyle koruma altına alınan hukuki yarar yalnızca verilerin ya da soyut unsurların korunması olmayıp sistem üzerinde hak sahibi olan kişinin bu sistemi hiçbir sorunla karşılaşmaksızın kullanabilme hakkıdır.

TCK'nın 244/1. maddesinde düzenlenen bu suç tipi icrai ya da ihmali bir davranışla işlenebilir. İcrai bir davranışta bulunmakla yükümlü olan bir kimsenin bu yükümlülüğünü bilerek ihmal etmesi neticesinde veriler erişilemez kılınıyorsa bu durumda suç oluşmuştur.

2.3.3.1.1.2. Sistemin İşleyişinin Bozulması

Yargıtay'a göre sistemin işleyişinin bozulması; bilişim sistemine dâhil olan mekanik parçaların ya da bir yazılımın esasen yapması gereken, özgülendiği işi yapamayacak duruma getirilmesi ve sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi veya fiziki olarak dahi zarar verilmesidir. Yargıtay sistemin işleyişinin bozulmasını, sistemin engellenmesinin en üst hali olan durma noktasından da daha ileri bir sebebiyle olarak tanımlamıştır²¹⁴.

Sistemin işleyişinin bozulması yapması gereken bir şeyi yapmaması şeklinde olabileceği gibi yapması gerektiğinden farklı bir şeyi de yapması şeklinde olabilir.

Sistemin işleyişinin bozulması, sistemin somut unsurlarına zarar verilerek olabileceği gibi yalnızca soyut unsurlara yapılacak müdahalelerle de yapılabilir. Parçaların değiştirilmesi, verilerin değiştirilmesi, bazı verilerin silinmesi gibi yöntemlerle bilişim sisteminin işleyişi bozulabilir²¹⁵.

²¹² AKBULUT, s. 191.

²¹³ KOCA/ÜZÜLMEZ, s. 869-870.

²¹⁴ "...sistemin "bozulması" tabiri ile bilişim sistemine dâhil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi veya fiziki olarak dahi zarar verilmesi anlaşılmalıdır..." (11. CD. 08.05.2013 gün, 2011/13685 E- 2013/7446K – UYAP'tan alınmıştır.)

²¹⁵ AKBULUT, s. 194.

*Dölger'e göre bir bilişim sisteminin dâhili depolama biriminin kırılması da sistemin kendisinden beklenen işi bir daha yapamamasına sebebiyet verecek ve suç gerçekleşmiş olacaktır*²¹⁶.

Sistemin işleyişinin bozulmasının tamamen ya da kısmen olması önemsizdir.

Sistemin işleyişinin bozulması durumu zaman zaman sistemin işleyişinin engellenmesini de içine almaktadır. Ancak her engellenme fiili aynı zamanda bir bozulma değildir²¹⁷.

2.3.3.1.2. Verilerin Bozulması, Yok Edilmesi, Değiştirilmesi, Erişilmez Kılınması, Sisteme Veri Yerleştirilmesi, Var Olan Verilerin Başka Yere Gönderilmesi

2.3.3.1.2.1. Verilerin Bozulması

Bozmak sözcüğü, bir şeyi kendisinden beklenen işi yapamayacak duruma getirmek, zarar vermek anlamına gelmektedir²¹⁸. Bu durumda verilerin bozulması verilerin işlevlerini gerektiği gibi yerine getiremeyecek duruma sokulması ve verilere zarar verilmesi olarak tanımlanabilir.

Verilerin bozulmasının ne şekilde gerçekleşeceğinin bir önemi yoktur. Failin gerçekleştirdiği fiil neticesinde verilerin bozulması gerçekleşiyorsa bu TCK 244/2'nin oluşması için yeterlidir. Aynı zamanda verilerin tamamen veya kısmen kullanılamaz hale gelmesinin de önemi yoktur. Her iki durumda da bu suç gerçekleşmiş olacaktır.

Kimi zaman sistemin işleyişinin bozulması neticesine verilerin bozulması yoluyla da ulaşılabilir. Bu noktada fiilin hangi fıkra kapsamında kaldığının tespiti açısından failin kastı irdelenmelidir. Şayet fail sistemin işleyişini bozmak amacıyla verileri bozuyorsa ilk fıkra uygulanacak, failin nihai amacı yalnızca verileri bozmak ise ikinci fıkra uygulanacaktır²¹⁹.

2.3.3.1.2.2. Verilerin Yok Edilmesi

Yok etmek; ortadan kaldırmak, varlığına son vermek demektir²²⁰. Verilerin yok edilmesi de verilerin varlığına son verilmesi, verilerin ortadan kaldırılmasıdır.

Verilerin yok edilmesi fiilinin ne şekilde yapıldığı önemli değildir, önemli olan verilerin bilindik ve olağan yöntemlerle erişilemez hale getirilmesidir. Örneğin bir ögenin geri dönüşüm kutusuna gönderilmesi verilerin yok edilmesi olarak değerlendirilemez, zira bu veri basit ve olağan bir işlemle geri getirilebilir. Ancak verinin yazılım üzerinden tamamen kaldırılması yok edilme olarak tanımlanır. Günümüzde bu şekilde silinen verilerin de geri getirilmesi mümkündür. Zira bu veriler tam olarak silinmemekte, yalnızca yazılım tarafından üzerine yazılabilir olarak işaretlenmektedir. Fakat verilerin bu şekilde yani olağan yöntemlerin dışına çıkarak ve ancak belirli bir uzmanlık gerektiren işlemlerin uygulanması sonucu geri getirilebilecek şekilde silinmesi durumu verilerin yok edilmiş kabul edilmesi için yeterlidir. Aynı zamanda silinmiş bir verinin başka yedeklerinin

²¹⁶ DÖLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 322.

²¹⁷ KOCA/ÜZÜLMEZ, s.869-870, AKBULUT, s. 195.

²¹⁸ tdk.gov.tr, 24.01.2020.

²¹⁹ DÖLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 322-323.

²²⁰ tdk.gov.tr, 25.01.2020

bulunuyor olması da bu suçun oluşumunu etkilemeyecek, verilerin yok edilmesi fiili gerçekleşmiş sayılacaktır.

Verilerin geri dönülemez şekilde yok edilmesi gerekip gerekmediği konusu esasen doktrinde tartışmalıdır. Bazı yazarlar söz konusu verinin kayıtlı olduğu bellekten silinmesi suretiyle erişiminin mümkün olmayacak şekle getirilmesi gerektiği görüşündedirler. Ancak bu yazarlara göre de verilere bir şekilde tekrar ulaşabilme imkânının varlığı suçun oluşunu etkilemeyecek, veriye erişim için verilen komutun sonuçsuz kalması yeterli olacaktır²²¹. Benzer görüşteki bazı yazarlar da verilere normal yollardan ulaşılabilmesinin güçleştirilmesinin yeterli olduğunu, verilere bazı araç ve programlarla ulaşılabilir olmasının suçun oluşmasını engellemeyeceğini söylemektedir²²². Bazı yazarlar ise geri getirme imkânının varlığı halinde verilerin yok edilmesinin söz konusu olamayacağını, şartların varlığın varlığı halinde verilerin erişilemez kılınması suçunun kapsamına girebileceğini belirtmektedirler²²³.

Bilişim suçlarının pek çoğunda olduğu gibi verilerin yok edilmesi suçu da virüsler yoluyla işlenebilir. Ancak bu tarz virüslerin varlığının neticesinde gerçekleşecek durumların sistemi engellemek ya da bozmak kapsamında kalmayacak şekilde olması gerekir. Bu virüsler sistemi engellemek ve bozmaksızın sistemdeki verileri yok ediyorsa bu durumda bir bilişim sistemindeki verilerin yok edilmesi suçu gerçekleşecektir.

Verilerin yok edilmesi şeklindeki eylemin en sık karşılaşılan örneklerinden birisi kişilerin sosyal medya hesaplarına herhangi bir şekilde girdikten sonra buradaki paylaşımları silen kişinin eylemidir²²⁴.

Verilerin bulunduğu diskin zarara uğratılması yoluyla da verilerin yok edilmesi mümkündür. Bu verilerin herhangi bir yolla kurtarılması suçun oluşmasına engel değildir.

2.3.3.1.2.3. Verilerin Değiştirilmesi

Verilerin değiştirilmesi, var olan verilerin yerine yeni bir bilgi oluşmasıdır²²⁵.

Verilerin değiştirilmesinin ne şekilde yapıldığının bir önemi yoktur. Sistemdeki veri içeriğinin tamamının ya da bir kısmının değiştirilmesi de suçun oluşması için yeterlidir. Hatta bir verinin aynı sistem içindeki konumunun değiştirilmesi bile verilerin değiştirilmesi olarak ifade edilebilir.

Kimi zaman sistemde bulunan bir verinin yok edilmesi ya da sisteme yeni bir veri eklenmesi de sistemdeki verilerin değiştirilmesi anlamına gelecektir. Örneğin, bir yarışmaya katılma hakkı kazanan kişilerin listenin bulunduğu bir sistemde bu verilerden bir kişinin silinmesi ya da bu listeye yeni birinin eklenmesi de verilerin değiştirilmesi kabul edilebilecektir. Her ne kadar verilerin yok edilmesi ve sisteme veri yerleştirilmesi fiilleri

²²¹ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 987.

²²² DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 323-324. KOCA/ÜZÜLMEZ, s. 872.

²²³ AKBULUT, s. 197.

²²⁴ "...tüm etkinliklerini ve resimlerini silmek, çeşitli resimler eklemekten ibaret eyleminin, TCK.nun 244/2. maddesinde düzenlenen suçu oluşturacağı..." (Yargıtay 8. Ceza Dairesi, 04.03.2015 tarih, 2014/26276 E- 2015/12988 K – UYAP'tan alınmıştır.)

²²⁵ AKBULUT, s. 198.

de tıpkı verilerin değiştirilmesi gibi TCK 244'nın maddesinin 2. fıkrasında tanımlanıyor ve bu nitelemeler sonuç cezaya etki etmiyor olsa da suçun doğru tanımlanabilmesi açısından bu ayrımın yapılması önemlidir. Bu tarz olayların her biri kendi içerisinde değerlendirilmeli ve sistemdeki bir verinin yok edilmesi yahut sisteme yeni bir veri yerleştirilmesi fiilleri sistemdeki bilgilerin değişmesine, yeni bir bilgi oluşmasına sebebiyet veriyorsa işlenen suç verilerin değiştirilmesi suçu olarak kabul edilmelidir.

2.3.3.1.2.4. Verilerin Erişilemez Kılınması

Verilerin erişilemez kılınması, verilere ulaşma ve onları kullanabilme imkânının ortadan kaldırılmasıdır.

Verilerin erişilemez kılınmasının ne şekilde gerçekleştiğinin bir önemi yoktur. Bu neticeyi doğuran her türlü yöntemle işlenebilir. Verilerin erişilemez kılınmasının sürekli ya da geçici olması da bu açıdan önem arz etmez.

Bir veriye şifre konularak veri yetkilisinin erişiminin engellenmesi de verilerin erişilemez kılınması suçunu oluşturur²²⁶. Hatta yetkili kişinin kendi rızasıyla paylaşmış olduğu bir şifrenin değiştirilmesi de verilerin erişilemez kılınması olarak kabul edilecektir.²²⁷

Verilerin erişilemez kılınması fiili icrai ya da ihmali bir davranışla işlenebilir. İcrai bir davranışta bulunmakla yükümlü olan bir kimsenin bu yükümlülüğünü bilerek ihmal etmesi neticesinde veriler erişilemez kılınıyorsa bu durumda suç oluşmuştur²²⁸. Örneğin bir şirketteki bilişim sorumlusunun bu şirkete ait verilerin bulunduğu sunucuya yönelik bir saldırıyı tespit ettiği, buna rağmen kayıtsız kalarak verilerin ulaşılamaz duruma gelmesine sebebiyet verdiği durumda suç oluşur.

2.3.3.1.2.5. Sisteme Veri Yerleştirmek

Sisteme veri yerleştirmek, sistemde bulunmayan bir verinin sisteme dâhil edilmesidir. Örneğin bir bilişim sistemine yetkisiz olarak fotoğraf aktarmak bu suça sebebiyet verecektir.

Failin sisteme hukuka uygun olarak girme hakkı bulunduğu halde sisteme veri yerleştirme hakkı yoksa sisteme veri yerleştirmesi hukuka aykırı olacak ve yine suç oluşacaktır²²⁹.

²²⁶ "...Oluş ve tüm dosya kapsamına göre sanığın, bir süre nişanlı kaldığı müşteki Sevda Topkök'ün facebook hesabının şifresini kırarak, hesaba giriş şifresini değiştirip müştekinin erişimini engellemesi şeklinde gerçekleşen eyleminin TCK'nun 244/2. maddesinde düzenlenen bilişim sistemine erişimi engelleme, bozma, değiştirme suçunu oluşturduğu gözetilmeden suç vasfında hataya düşülerek yazılı şekilde TCK'nun 243/1. maddesi gereğince hüküm kurulması..." (Yargıtay 8. Ceza Dairesi, 16.04.2019 tarih, 2018/8369 E-2019/5454 K – UYAP'tan alınmıştır.)

²²⁷ "Şikayetçinin eski arkadaşı olan sanığın, şikayetçiye ait Facebook ve MSN adreslerine girerek şifrelerini değiştirmek suretiyle bir ay boyunca kullanıp şikayetçinin kullanmasına engel olmak, tüm etkinliklerini ve resimlerini silmek, çeşitli resimler eklemekten ibaret eyleminin, TCK'nun 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden, yazılı şekilde karar verilmesi..." (Yargıtay 8. Ceza Dairesi, 04.03.2015 tarih, 2014/26276 E- 2015/12988 K – UYAP'tan alınmıştır.)

²²⁸ AKBULUT, s. 201.

²²⁹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 328.

2.3.3.1.2.6. Sistemde Var Olan Verileri Başka Bir Yere Göndermek

Sistemde var olan verileri başka bir yere göndermek bir sistemde var olan verilerin başka bir sisteme aktarılmasıdır.

Göndermenin ne şekilde olduğunun bir önemi yoktur. İnternet ağı üzerinden ya da yerel bir ağ üzerinden veri aktarımı yapılabileceği gibi bir veri taşıma cihazı kullanılarak da aktarım sağlanabilir.

Sistemde var olan orijinallerinin verilerin yok edilerek başka sisteme aktarılması yoluyla (Kes-Yapıştır) verilerin gönderilmesi durumunda hem sistemde yer alan verilerin başka gönderilmesi hem de verilerin yok edilmesi neticeleri aynı anda oluşuyorsa da failin eylemi tek suç kabul edilerek TCK'nın 244/2. maddesi yalnızca bir kez uygulanır.

Başka yere gönderilen verilerin kişisel veri olması durumunda ise TCK'nın 244/2. maddesinin yanı sıra duruma göre 135. veya 136. maddesinde tanımlanan suçlar da oluşabilir. Bu durumlarda fikri içtima hükmüne göre sonuca gidilmeli ve cezası daha ağır olan TCK 135. ya da 136. maddelerinden olaya uyan suça göre ceza verilmelidir.

2.3.3.2. Fail

Bu suç tipinde fail açısından özel bir belirleme yapılmamıştır. Bu suçun faili herkes olabilir.

Bir kimsenin, başkalarının haklarını ihlal etmeksizin kendi sisteminin işleyişine yahut sistemdeki verilere müdahale etmesi ile suç oluşmaz. Ancak kişinin tasarruf yetkisi bulunsu dahi bir başkasının hak sahipliğine rağmen sisteme veya bu sistemdeki verilere kasten zarar vermesi durumunda bu suç oluşacaktır²³⁰. Aynı şekilde fail kendisine ait verileri erişilemez kılmak için bir başkasına ait verilere zarar verir yahut bu bir sistemin işleyişini engeller ya da bozarsa suç oluşacaktır.

Akbulut'a göre bir kimse kendi tasarrufu altında bulunan verileri bir başkasının veri taşıyıcısına kaydederse ve veri taşıyıcısının sahibi hukuka uygun şekilde bu verilere zarar verirse suç oluşmaz²³¹. Örneğin kendisine ait bir fotoğrafı arkadaşının cep telefonuna aktaran kişinin bu fotoğrafı daha sonra telefon sahibi tarafından silinirse suç oluşmayacaktır.

²³⁰ "...Suç tarihinde ... Lisesi müdür vekili olarak görev yapan sanığın, üç öğrenciye ait Türk Dili ve Edebiyatı öğretmeni tarafından 45 olarak belirlenen ve e-okul sistemine bu şekilde kaydedilen 2010-2011 yılı I. Dönem Türk Dili ve Edebiyatı dersi sözlü notlarını, Milli Eğitim Bakanlığı Ortaöğretim Kurumları Sınıf Geçme ve Sınav Yönetmeliğine göre belirlemesi münhasıran ilgili dersin öğretmenine ait olmasına rağmen, düşürmek istediği, bu amaçla 24/01/2011 günü idareci olması nedeni ile giriş izni bulunan e-okul sistemine girerek sözlü notlarını 30 olarak değiştirdiği, sözlü notlarının hüküm doğurup karneye işlenebilmesi için not çizelgesinin çıktısının alınarak ilgili öğretmen tarafından imzalanması gerektiği ve değiştirilmiş not çizelgesini ders öğretmenin imzalamaması nedeniyle sisteme tekrar girerek eski hale getirdiği iddia edilen somut olayda, sanığa isnat olunan eylemin 5237 sayılı TCK'nın 244/2. maddesinde düzenlenen bilişim sistemine hukuka aykırı olarak girmek suretiyle verilerin yok edilmesi veya değiştirilmesi suçunu oluşturabileceği..." (Yargıtay 5. Ceza Dairesi, 10/09/2019 Tarih, 2019/771 E, 2019/7782 K – UYAP'tan alınmıştır.)

²³¹ AKBULUT, s. 184.

2.3.3.3. Mağdur

Bilişim sisteminin engellenmesi ve bozulması suçunda mağdur bakımından özel bir belirleme yapılmamıştır. Herkes bu suçun mağduru olabilir. Bu suçun mağduru olmak için bilişim sisteminin maliki olmaya gerek yoktur. Bu suçun işlenmesiyle zarara uğrayan sistemler ya da veriler üzerinde tasarruf yetkisine sahip olan kişi bu suçun mağduru olacaktır. Örneğin bu suçun iş dünyasına yönelik hizmetler sunan bir bilişim sistemine karşı işlenmesi durumunda sistemin sahibi suçun mağduru olacaktır. Bu sisteme yönelik eylemler dolayısıyla işleri aksayan kişiler her ne kadar suçtan zarar görmüş olsalar da suçun mağduru kabul edilemeyecek ancak suçtan zarar gören sıfatıyla anılabileceklerdir.

Bu suçun bir bulut bilişim sistemine yönelik işlenmesi halinde duruma göre hem sistemin maliki kabul edilebilecek kişiler hem de sistemin kullanıcıları mağdur olacaklardır. Keza bu sistem üzerinde kullanıcıların da tasarruf yetkisine sahip olduğu veriler vardır. Aynı şekilde bir başkasına ait veri taşıyıcısına hukuka uygun şekilde verilerini kaydetmiş kişinin verileri, veri taşıyıcısının maliki tarafından silinir, yok edilir, değiştirilir ya da erişilemez kılınırsa veri taşıyıcısının maliki suçun faili olurken verileri sisteme kaydeden kişi suçun mağduru olacaktır. Ancak bu durumun söz konusu olabilmesi için veri taşıyıcısının verileri silme hakkının bulunmaması gerekir.

TCK'nın 135. ve 136. maddesinin aksine 244. madde açısından verilerin ilgilisi olan kişi bu suçun mağduru olmaz. Ancak duruma göre bu kişinin suçtan zarar gören olduğu kabul edilebilir.

Tüzel kişiler suçun mağduru olamazlar ancak suçtan zarar gören olabilirler.

Bu suç bir kamu kurum ve kuruluşuna ait bilişim sistemine yahut veriye karşı işlenirse toplumu oluşturan herkes bu suçun mağduru olur²³².

2.3.3.4. Suçun Konusu

TCK'nın 244. maddesinin ilk fıkrasında düzenlenen sistemi engelleme ve bozma suçunun konusu bilişim sistemidir. 244. maddenin ikinci fıkrasında yer alan verileri bozma, yok etme, değiştirme, erişilemez kılma ve başka yere gönderme suçunda ise suçun konusu bilişim sisteminde bulunan verilerdir. Ayrıca sisteme veri yerleştirilmesi durumunda ise sisteme yerleştirilen veriler bu suçun konusu olacaktır.

Doktrinde ayrıca bu suçun konusunun ilk fıkra açısından bilişim sisteminin işleyişi olduğu yönünde görüşler de mevcuttur²³³.

Koca ve Üzülmmez, ikinci fıkra açısından suçun konusunu oluşturan verilerin mutlak suretle bilişim sisteminin içerdiği veriler olması gerektiğini belirtmektedir. Yazarlara göre CD, flaş bellek, gibi verileri saklama araçlarında bulunan veriler suçun konusu olamayacaktır. Bu tarz verilere zarar verilmesi maksadıyla bu cihazlara zarar verilmesi durumunda mala zarar verme suçu oluşur²³⁴. Oysa bilişim sistemlerinde bulunan veriler de çeşitli dâhili belleklerde depolanmaktadır. Bu verilerin sistem tarafından okunması ile bir CD ya da flaş

²³² AKBULUT, s. 185.

²³³ KOCA/ÜZÜLMEZ, s. 868, AKBULUT, s. 188.

²³⁴ KOCA/ÜZÜLMEZ, s. 868-869.

bellek gibi harici veri taşıyıcısında bulunan verinin sistem tarafından okunması temelde aynı şeydir. Her ne kadar kanun metninde bir bilişim sisteminde bulunan veriler ifadesi kullanılmışsa da harici depolama cihazlarının da bir bilişim sisteminin parçası kabul edilmesi, dolayısıyla bu cihazlarda bulunan verilere yönelik zarar verme eylemlerinin de bu suç kapsamında sayılması gerekmektedir.

2.3.3.5. Netice

TCK'nın 244. maddesinin birinci ve ikinci fıkrasında tanımlanan suçlar seçimlik hareketlidir. Bu suç tipleri serbest hareketli olup yalnızca bir neticeyi meydana getirmeleri aranmıştır²³⁵.

Suçun oluşması açısından bir zararın ortaya çıkması gerekmez.

2.3.4. Manevi Unsurlar

TCK'nın 244. maddesinin ilk iki fıkrasında düzenlenen suçlar yalnızca kasten işlenebilir. Bu kast doğrudan kast olabileceği gibi olası kast da olabilir. Suçun oluşması için failin belirli bir amaçla hareket ediyor olması gerekmez. Kastın varlığı yeterlidir.

Suçun taksirli hali de düzenlenmediği için maddi unsurları bilmeksizin hareket eden failin fiili suç bu suçu oluşturmayacaktır. Failin kasten sistemdeki verileri yok ettiği yahut değiştirdiği durumda TCK'nın 244. maddesinde düzenlenen suç oluşacak, failin taksirli bir eyleminin neticesinde sistemdeki verilerin yok olması veya değişmesi durumunda ise 243/3. maddesi gündeme gelecektir. TCK'nın 243/3. maddesi ile TCK'nın 244. maddesi arasındaki temel fark failin verilerin zarar görmesine yönelik kastının bulunup bulunmadığı hususudur. Öte yandan TCK'nın 243/3. maddesinde düzenlenen suçun oluşması için failin sisteme kasten girdikten veya sistemde kalmaya kasten devam ettikten sonra sistemdeki verilere taksirle zarar vermesi gerekmektedir. Fail bir sisteme taksirle girdikten sonra buradaki verilere de taksirle zarar verirse bu durumda TCK'nın 244. maddesinde düzenlenen suç oluşmayacağı gibi 243/3. maddesinde düzenlenen suç da oluşmayacaktır.

Fail suçun kanuni tanımında yer alan unsurları bilerek ve isteyerek bu suçu işlemelidir. Fiilin işlenişi esnasında suçun yasal tanımındaki maddi unsurları bilmeyen fail bu hatasından yararlanır.

2.3.5. Hukuka Aykırılık

5651 sayılı yasa kapsamında internet üzerinden yapılan ve içeriği kanunda sayılı suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla hakkında erişimin engellenmesine karar verilebilir. Bu kanun kapsamında bir hâkim ya da gecikmesinde

²³⁵ “...tüm deliller birlikte değerlendirilerek katılanın kullandığı adı geçen programa erişilmez kılındığı takdirde TCK'nın 244/2, ancak; bu programa girişin engellenmemesi ve katılanın da programda kalmaya devam ettiğinin tespiti halinde aynı yasanın 243/1. maddesi kapsamındaki suçun oluşacağı dikkate alınıp sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmayla yazılı şekilde hüküm kurulması...” (Yargıtay 15. Ceza Dairesi, 20.11.2019 tarih, 2017/8891E- 2019/12369 K – UYAP'tan alınmıştır.)

sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilen erişimin engellenmesi kararının yerine getirilmesi suç oluşturmaz²³⁶.

CMK'nın 134. maddesi kapsamında yapılan çalışmalar da bu suç açısından görevin ifası niteliğinde olur ve hukuka uygunluk nedeni sayılır.

Sistem üzerinde hak sahibi olan kişi, sistemin işleyişinin engellenmesine ya da bozulmasına rıza göstermiş olabileceği gibi sistemde bulunan verilerin yok edilmesine, değiştirilmesine, erişilemez kılınmasına ya da sisteme veri yerleştirilmesine ve sistemde bulunan verilerin başka yere gönderilmesine rıza göstermiş olabilir. Örneğin bir şirkette sistem sorumlusu olarak çalışan bir kişi sistemde bulunan verilerin düzenli olarak yedeklenmesiyle görevlendirilmiş olabilir. Yine böyle bir işte çalışan bir kimse sistem güvenliğinden kaynaklanan çeşitli sebeplerden ötürü sistemin işleyişine engel dahi olabilir. Bu gibi durumlarda kendisine önceden verilmiş bir rıza dâhilinde ve bu rıza kapsamını aşmayacak şekilde hareket eden failin fiili suç oluşturmaz. Zira ilgilinin rızası burada hukuka aykırılığı kaldıracaktır. Fail kendisine verilen rızanın sınırlarını aşarak bu suçu işliyorsa artık eylemi hukuka aykırı hale gelecektir.

2.3.6. Suçun Nitelikli Hali

TCK'nın 244. maddesinin 3. fıkrasında ise söz konusu eylemlerin bir bankanın veya kredi kurumunun yahut bir kamu kurumu ya da kuruluşuna ait bilişim sistemi hakkında işlenmesi durumunda belirlenecek cezanın yarı oranında arttırılacağı düzenlenmiştir. Bu madde ile TCK'nın 244. maddesinde düzenlenen fiillerin banka veya kredi kurumları ile bir kamu kurum veya kuruluşuna ait bilişim sistemleri aleyhine işlenmesi durumu nitelikli hal olarak düzenlenmiştir²³⁷.

Bu nitelikli halin uygulanması yalnızca banka ve kredi kurumları ile kamu kurum ve kuruluşları ile sınırlıdır. Bunun dışında kalan şirketler, kurumlar ve derneklere yönelik olarak uygulanamaz. Kanunda bu nitelikli hal için sabit artırım sistemi kabul edilmiştir. Sisteme yönelik fiilin ne kadar süre devam ettiği ya da ne gibi zararlara neden olduğu gibi etkenler yapılacak olan artırım açısından bir özellik teşkil edemeyecektir. Ancak hâkim temel cezayı belirlerken bu durumları göz önünde tutabilecektir.

Doktrinde bu suçun kamu görevlisi ya da banka görevlisi tarafından işlenmesinin de nitelikli hal kapsamına alınması gerektiği savunulmaktadır. Bu görüşteki yazarlara göre kamu görevlileri ile banka görevlilerinin bu suçları işlemesi diğer kişilere nazaran daha kolaydır, dolayısıyla bu kişilerin fail olduğu suçlara ilişkin olarak özel bir düzenleme şarttır²³⁸. Kanaatimizce de böyle bir düzenleme yapılması yerinde olacaktır. Bunun yanı sıra hem bu suçun hem de diğer bilişim suçlarının sistem güvenliğinden sorumlu kişilerce işlenmesi durumu da nitelikli hal kabul edilmelidir. Çünkü bu kişiler kendi sorumlulukları

²³⁶ AKBULUT, s. 204, ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 994-995, KOCA/ÜZÜLMEZ, s. 873.

²³⁷ "...Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükümlenen cezanın üniversitenin kamu kurumu olması nedeniyle TCK'nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması..." (Yargıtay 8. Ceza Dairesi, 08.01.2014 tarih, 2012/33044 E, 2014/236 K – UYAP'tan alınmıştır.)

²³⁸ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 334; ERDOĞAN, 197.

altında olan bir sisteme karşı bu suçu işlemektedirler, bu durum bu kişilerin bu suçu işlemelerini kolaylaştırmadır. Bu kişiler sisteme ve verilere zarar verebilecek nitelikteki açıklara hâkimdir. Ayrıca sistemin güvenliği bu kişilere emanet edilmiştir. Burada fail sistem üzerinde hak sahibi olan kişilerin güvenliğini de zedelemektedir.

Bankacılık Kanunu'nun 3. maddesine göre banka sözcüğü mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını, kredi kuruluşu ise mevduat bankalarını ve katılım bankalarını ifade etmektedir. Yine aynı maddeye göre mevduat bankası, bu kanuna göre kendi nam ve hesabına mevduat kabul etmek ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini, katılım bankası ise bu Kanuna göre özel cari ve katılma hesapları yoluyla fon toplamak ve kredi kullandırmak esas olmak üzere faaliyet gösteren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini ifade etmektedir. Kalkınma ve yatırım bankası ise bu Kanuna göre mevduat veya katılım fonu kabul etme dışında; kredi kullandırmak esas olmak üzere faaliyet gösteren ve/veya özel kanunlarla kendilerine verilen görevleri yerine getiren kuruluşlar ile yurt dışında kurulu bu nitelikteki kuruluşların Türkiye'deki şubelerini ifade etmektedir.

Bir diğer nitelikli hal ise 3713 sayılı Terörle Mücadele Kanunu'nda düzenlenmiştir. 3713 sayılı Terörle Mücadele Kanunu'nun 4. maddesinde katalog olarak belirlen suçların ilgili yasanın 1 inci maddesinde ifade edilen hedefler doğrultusunda suç işlemek amacıyla kurulmuş bir terör örgütünün eylemleri çerçevesinde işlenmesi durumunda terör suçu sayılacağı düzenlenmiş ve TCK 244. maddesi de bu kapsamda sayılmıştır. İlgili yasanın 5. maddesinde ise yasanın 3.ile 4. maddelerinde belirtilen suçları işleyenler hakkında ilgili yasalar uyarınca belirlenecek hapis cezalarının ve adlî para cezalarının yarı oranında arttırılacağına yer verilmiştir. Maddeye göre bu şekilde belirlenecek cezalarda, gerek o fiil için, gerek her türden yaptırım için belirlen cezanın yukarı sınırının aşılabileceği belirtilmiştir. Öte yandan müebbet hapis cezası yerine, ağırlaştırılmış müebbet hapis cezasına hükmolunur denilmiştir. Bu sebeple söz konusu suçun terör faaliyeti çerçevesinde işlenmesi durumunda cezasının yarı oranında arttırılacağı da hükme bağlanmıştır.

2.3.7. Suçun Özel Görünüş Biçimleri

2.3.7.1. Teşebbüs

TCK'nın 244. maddesinin ilk iki fıkrasında düzenlenen bu suça teşebbüs mümkündür. Örneğin failin sistemdeki verileri yok etmek amacıyla sisteme virüs yüklemesi fakat bu virüsün anti virüs programınca tespit edilerek silinmesi durumunda failin fiili teşebbüs aşamasında kalmış olacaktır.

Fail sisteme belirli bir miktarda veri yerleştirmek amacıyla icra hareketlerine başlar ve verilerin bir kısmını yükledikten sonra eylemi yarıda kalırsa dahi teşebbüsten söz edilemez. Fail tamamlanmış suçtan cezalandırılır. Zira fail sisteme hedeflediğinden az bir miktarda da olsa veri yerleştirmiştir. Aynı durum diğer seçimlik hareket için de söz konusudur.

2.3.7.2. İştirak

TCK'nın 244. maddesinde tanımlanan suç iştirak açısından bir özellik arz etmez. İştirakin her türlü mümkün.

2.3.7.3. İçtima

Tek bir suç işleme kararı kapsamında, değişik zamanlarda aynı kişiye karşı bu suç birden fazla kez işlenirse bu durumda zincirleme suç hükümleri uygulanacaktır.

Bu suçun birden fazla kişiye karşı tek bir fiille işlenmesi durumunda da ise aynı neviden fikri içtima gündeme gelecektir. Örneğin birden fazla bilgisayara tek fiile virüs gönderilerek bu suç işleniyorsa bu durumda aynı neviden fikri içtima söz konusu olacaktır²³⁹.

TCK'nın 244. maddesinin ilk fıkrası ile ikinci fıkrası aynı anda gerçekleşebilir. Örneğin tek fiille hem veriler yok edilip hem de sistemin işleyişi engellenebilir. Bu durumda sorun fikri içtima hükümlerine göre çözülür. Dolayısıyla fail bu iki suçtan en ağır cezayı gerektiren ilk fiilden sorumlu tutulur²⁴⁰.

244. maddenin son fıkrası ise ilk iki fıkra da belirtilen fiillerin işlenmesiyle failin kendisi yahut bir başkası yararına haksız bir çıkar temin etmesinin başka bir suç oluşturmaması durumunda, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hüküm olunacağı düzenlenmiştir. Bu durumda 244. maddenin ilk iki fıkrasında tanımlanan suç 244. maddenin unsuru niteliğindedir. 244 maddenin 4. fıkrasının işlenmesi durumunda fail yalnızca bu fıkradan sorumlu tutulacaktır.

244. madde ile 243. maddenin aynı anda ihlal edilmesi durumunda ne olacağı hususunda farklı görüşler mevcuttur. Fikri içtima hükümlerinin uygulanması gerektiği görüşünün yanı sıra²⁴¹ 243. madde ile 244. madde arasında geçitli suç ilişkisi olduğunu savunan görüşler de mevcuttur²⁴². Bazı yazarlar ise geçitli suç kurumunu kabul etmediklerinden bu durumun failin kastına göre çözülmesi gerektiğini ifade etmektedir²⁴³. Dülger bu durumda her olay açısından ayrı ayrı, somut olayın özelliklerine göre değerlendirme yapılması gerektiği görüşündedir²⁴⁴.

Failin, mağdura ait bilişim sistemine girmesi ve bu sistemdeki içerikleri okuması durumunda 244. maddede düzenlenen suçlar oluşmayacak fail yalnızca 243/1. madde ile durumun özelliğine göre TCK 132. veya 136. maddelerden cezalandırılacaktır.²⁴⁵

²³⁹ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 337-338.

²⁴⁰ AKBULUT, s. 210.

²⁴¹ AKBULUT, s. 211.

²⁴² ARTUK/GÖKCEN/YENİ DÜNYA, s. 767.

²⁴³ ÖZBEK/DOĞAN/BACAŞIZ/TEPE, Türk Ceza Hukuku Özel Hükümler, s. 976.

²⁴⁴ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s.388.

²⁴⁵ "... Sanığın, eski eşi olan mağdura ait facebook şifresini bildiğini ve şifre kırma gibi bir eyleminin olmadığını beyan etmesi, mağdurun, şifresinin kırılarak facebook hesabına giriş yapıldığına dair iddialarını doğrulayan herhangi bir delil bulunmaması karşısında, sanığın sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakkı olmadığı halde sistemde kalmaya devam etme eyleminin TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme ve mağdura ait içeriği özel mesajları okuyup, tarafı olmadığı haberleşme içeriklerini kaydetmesi eyleminin TCK'nın 132/1. madde ve fıkrasındaki haberleşmenin gizliliğini ihlal suçlarını oluşturacağı gözetilmeden, delillerin takdirinde ve suç vasfında yanılığa düşülerek, sanık hakkında TCK'nın 244/2. madde ve fıkrasındaki sistemi engelleme, bozma, verileri yok etme veya değiştirme ve TCK'nın 136/1. madde ve fıkrasındaki verileri hukuka aykırı olarak verme veya ele geçirme suçlarından mahkumiyet kararı verilmesi..." (Yargıtay 12. Ceza Dairesi, 25.12.2019 tarih, 2019/577 E - 2019/12248 K – UYAP'tan alınmıştır.)

244. maddenin ilk iki fıkrasında düzenlenen suçun işlenmesi yoluyla sahte belge düzenlenmesi halinde ise ne olacağına dair doktrinde farklı görüşler mevcuttur. Bazı yazarlara göre bu durumda fikri içtima kuralları uygulanarak fail en ağır cezayı gerektiren suçtan sorumlu tutulacaktır²⁴⁶.

TCK'nın 245/A maddesinde düzenlenen suç amaç suç niteliği taşımaktadır. Fail hem 245/A hem de 244 maddelerini ihlal etti ise her iki suçtan da ayrı ayrı cezalandırılmalıdır. Yani bu iki suçun aynı anda gerçekleşmesi durumunda gerçek içtima uygulanacaktır.

Doktrinde en çok tartışılan konulardan birisi de 244. madde ile 151. maddede düzenlenen mala zarar verme suçu arasındaki ilişkidir. Zira 244. maddenin gerekçesinde "*Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızzar fiilleri özel bir suç hâline getirilmiştir.*" denilmektedir. Doktrinde bazı yazarlar bu 244. maddenin 151. maddeye göre özel norm niteliğinde olduğunu savunurken bir kısım yazarlar ise bu görüşe karşı çıkmaktadır²⁴⁷.

244. maddede düzenlenen suçlar ile mala zarar vermenin birlikte işlenmesi durumunda failin kastına göre hareket edilmesi gerekmektedir. Örneğin fail bir sistemi engellemek amacıyla sistemin somut unsurlarına zarar veriyorsa bu durumda yalnızca 244. maddede düzenlenen suçtan sorumlu tutulmalıdır. Fail yalnızca veri taşıyıcıya zarar vermek amacıyla hareket etmesine rağmen fiili sonucunda veri taşıyıcı içerisinde bulunan verilerin zarar görmesi halinde ise fail yalnızca mala zarar verme suçundan sorumlu tutulacaktır. Zira burada failin kastı yalnızca mala zarar verme suçuna yöneliktir.

TCK'nın 124. maddesinde düzenlenen haberleşmenin engellenmesi suçuyla 244. maddesinde düzenlenen suçun birlikte gerçekleşmesi durumunda ise fikri içtima uygulanır²⁴⁸.

Failin sisteme bir veri yerleştirerek bir kişinin suç işlediği izlenimine sebep olması durumunda suçun diğer unsurları da varsa 267. maddede düzenlenen iftira suçu ya da 271. maddede düzenlenen suç uydurma suçu da oluşabilir. Bu durumda farklı neviden fikri içtima uygulanmalıdır. Doktrinde de bu yönde görüşler vardır²⁴⁹.

2.3.7. Soruşturma Usulü ve Yaptırım

TCK'nın 244. maddesinin ilk fıkrasında düzenlenen suçların cezası bir yıldan beş yıla kadar hapis cezası, ikinci fıkrasında düzenlenen suçların cezası ise altı aydan üç yıla kadar hapis cezasıdır.

TCK'nın 244. maddesinin ilk iki fıkrasında düzenlenen suçlar re'sen soruşturulur. Suçtan zarar görenlerin davaya bu sıfatla katılması mümkündür.

²⁴⁶ AKBULUT, s. 211.

²⁴⁷ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 338, ERDOĞAN, s. 237.

²⁴⁸ AKBULUT, s. 212, ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 996.

²⁴⁹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 338.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11 ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

TCK'nın 246. maddesinde *“Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.”* denilmektedir. Dolayısıyla TCK'nın 244. maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

CMK'nın 253/1-c maddesinde suça sürüklenen çocukların fail olması durumunda üst sınırı üç yılı geçmeyen hapis veya adli para cezasını gerektiren suçlar da uzlaştırma usulü kapsamında sayılmıştır. Dolayısıyla 244/2. maddede yer alan suçta failinin SSÇ olması durumunda mağdur veya suçtan zarar görenin de gerçek kişi ya da özel hukuk tüzel kişisi olması halinde öncelikle uzlaştırma usulüne başvurulacaktır.

2.4. Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK 244/4)

2.4.1. Genel Olarak

TCK'nın 244. maddesinin son 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 adli para cezasına hükmolunur.”* denilmek suretiyle bilişim sistemleri aracılığıyla haksız yarar sağlama suçu düzenlenmiştir. Bu suç tipi düzenlenirken maddenin ilk iki fıkrasına atıf yapılmıştır.

Doktrinde TCK'nın 244. maddesinin son fıkrasında yapılan düzenlemenin ilk iki fıkrada yer alan suç tipinin cezasını arttıran bir nitelikli hal olduğu yönünde görüşler mevcut²⁵⁰ olduğu gibi bu fıkrayı ayrı bir suç tipi olarak değerlendiren pek çok yazar yazar vardır.²⁵¹ Kanaatimizce bu fıkranın koruduğu hukuki yararın ilk iki fıkradan ayrıştığı da göz önüne alındığında bu fıkrayı ayrı bir suç olarak değerlendirmek gerekmektedir.

TCK'nın 244/4. maddesinde düzenlenen bu suçun işlenebilmesi için gerekli olan eylem unsuru 244. maddenin ilk iki fıkrasında düzenlenmiştir. Dolayısıyla bu suç bileşik suçtur²⁵². TCK'nın 42. maddesinde de birinin diğerinin unsurunu oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denileceği ve bu tür suçlarda içtima hükümlerinin uygulanmayacağı hükme bağlanmıştır.

Mülga TCK'nın 525 b/2 maddesi *“Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir.”*

²⁵⁰ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 989-994.

²⁵¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 339-355; AKBULUT, s.217-267; KOCA/ÜZÜLMEZ, s. 876.

²⁵² KOCA/ÜZÜLMEZ, s. 876, AKBULUT, s. 217-218.

şeklindeydi. Ancak burada suç tipinin oldukça geniş tutulmuş olması uygulamada birtakım zorluklara yol açmaktaydı. Yeni TCK'da bu suç tipi dört farklı suça bölünmüştür. Bu suçlar; bilişim sistemleri aracılığıyla haksız yarar sağlama suçu, banka ve kredi kartlarının kötüye kullanılması suçu ve dolandırıcılık ile hırsızlık suçlarının bilişim yoluyla işlenmesi şeklindeki nitelikli halleridir.

Madde metninde bu suç tipinin söz konusu eylem neticesinde başka bir suç oluşturmaması halinde gündeme geleceği düzenlenmiştir. Madde gerekçesinde ise *“bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.”* denilmek suretiyle bir çelişki durumu oluşturulmuştur. Keza madde metni eylemin başka bir suç oluşturmamasını ararken gerekçede daha ağır bir cezadan söz edilmiştir. Yani gerekçe esas alınacak olursa eylem daha az cezayı gerektiren bir suç oluşturuyorsa dahi fail bilişim sistemleri aracılığıyla haksız yarar sağlama suçundan cezalandırılacaktır. Oysa madde metni esas alınacak olursa eylem daha az bir cezayı gerektiren başka bir suç oluşturuyorsa bu durumda fail o suçtan ceza alacak ve artık bilişim sistemleri aracılığıyla haksız yarar sağlama suçundan cezalandırılmayacaktır. Hiç şüphe yok ki burada madde metni esas alınmalıdır. Zira madde gerekçesi madde metninin yorumlanabilmesi için yol gösterici nitelikte olmakla birlikte bağlayıcı değildir. Aksine, madde metninin uygulanması bir zorunluluktur. Dolayısıyla TCK'nın 244. maddesinin 4. fıkrasında düzenlenen bilişim sistemleri aracılığıyla haksız yarar sağlama suçu tali norm niteliğinde kabul edilmeli ve madde metni esas alınarak evvela başka bir suç oluşup oluşmadığı değerlendirilmeli, eylemin başka hiçbir suç oluşturmaması halinde fail bu suçtan cezalandırılmalıdır. Ancak failin eyleminin daha az cezayı gerektiren bir suç oluşturmaması durumunda 244/4. maddenin uygulanamayacak olması ceza adaleti açısından sorun teşkil etmektedir. Madde metninde bir değişiklik yapılarak failin eyleminin daha ağır cezayı gerektiren bir suç oluşturmaması halinde o suçun, aksi durumda ise TCK'nın 244/4. maddesinde düzenlenen suçun oluşması sağlanabilir. Kaldı ki yasa koyucu bu şekilde özel bir düzenleme yapmasa dahi suçun tali niteliği madde metninden çıkarıldığı takdirde fikri içtima hükümlerince de aynı sonuca varılacaktır.

Bu suç ile benzer nitelikte bir düzenleme Sanal Ortamda İşlenen Suçlar Sözleşmesinin 8. maddesinde yer almaktadır. Bilgisayarlarla bağlantılı dolandırıcılık başlıklı madde *“Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiği, bunların kendi iç hukukunda cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir: Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle; a. bilgisayar sistemlerine veri girişi yapma, verileri değiştirme, silme veya engelleme; b. bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunma”* şeklindedir. Ancak 244/4. maddesi suçun maddi menfaat sağlama amacıyla işlenmesini aramamış, suç neticesinde bir çıkar elde edilmesini yeterli görmüştür. Bu bakımdan sözleşmenin 8. maddesinden ayrılmaktadır. Aynı şekilde sözleşmenin aksine 244/4. maddesinde hile veya sahtekârlık niyetiyle fiillerin işlenmesi de aranmamıştır.

2.4.2. Suçla Korunan Hukuksal Değer

Fail bu suç tipinde gerçekleştirilen eylemler neticesinde bir yarar elde etmelidir. Bu yararın maddi bir yarar mı olması gerektiği yoksa maddi manevi her türlü yararı mı kapsadığı hususunda farklı görüşler mevcuttur.

Bu yararın maddi manevi her türlü yararı kapsadığını savunan görüşe göre²⁵³ kişinin işe girmesi ya da bir beklentisinin karşılanması gibi manevi çıkarlar da bu kapsamda değerlendirilecektir.

Bu suçu malvarlığına yönelik bir suç olarak değerlendiren görüş ise bu suçla korunan hukuki yararın da malvarlığı olduğunu söylemektedir²⁵⁴. Ancak bu suç bilişim suçları bölümünde düzenlenmiştir. Hatta bu suçun malvarlığına yönelik suçlar olan dolandırıcılık, hırsızlık, güveni kötüye kullanma ve benzeri suçlardan birinin oluşması durumunda fail TCK 244/4'ten sorumlu tutulmayacaktır. Dolayısıyla bu görüşe katılmak mümkün değildir.

Madde metninde de bir yarardan söz edilmiş bunun maddi ya da manevi bir çıkar olması ile ilgili bir sınırlama yapılmamıştır. Kanaatimizce maddi manevi her türlü çıkar bu suç kapsamında yarar sayılacaktır. Ancak suç tipinde bu yönde bir sınırlama bulunmasa dahi uygulamada bu yarar genellikle maddi nitelikte bir yarardır.

Bu suç tipi ile korunan hukuki yararın, kişilerin maddi ve manevi haklarının korunması olduğu görüşündeyiz. Doktrinde de korunan hukuki yararı özel hayatın gizliliğinin yanı sıra malvarlığına yönelik saldırıların da önlenmesi gibi geniş bir yelpazede değerlendirilerek kişilerin maddi ve manevi haklarına yönelik saldırıların önlenmesi olarak ifade edilmiştir²⁵⁵.

2.4.3. Maddi Unsurlar

2.4.3.1. Fiil

Bu suç “Bir bilişim sisteminin işleyişini engelleyen veya bozan ya da Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen ve bu suretle kendisinin veya başkasının yararına haksız bir çıkar sağlayan kişinin eyleminin başka bir suç oluşturmaması halinde iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.” şeklinde okunabilir²⁵⁶. Dolayısıyla bu suç açısından fiil TCK'nın ilk iki

²⁵³ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 341; ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 994. KOCA/ÜZÜLMEZ, s. 881.

²⁵⁴ AKBULUT, s.230; KOCA/ÜZÜLMEZ, s. 881.,

²⁵⁵ ARTUK/GÖKCEN/YENİDÜNYA s. 775.

²⁵⁶ “...5237 sayılı TCK'nın 244/4 maddesi gereğince suç oluşabilmesi için; bir bilişim sistemindeki verilen bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması ya da sisteme veri yerleştirilmesi ve bu şekilde haksız çıkar sağlanmasının başka bir suç oluşturmaması gerektiği, somut olayda ise herhangi bir sisteme müdahalenin söz konusu olmadığı, sanığın bankaya müracaat ederek derneğin kaşesi ile tanzim ettiği sahte talimat ile dernek adına internet hesabı açılmasını sağladığı ve bu şekilde elde ettiği şifre ile internet hesabından kendi hesabına havale gönderdiği, bu eylemin haricinde bankaya sahte imzalar içeren ödeme talimatları ile başvurarak dernek hesabından nakit para çektiği, bu haliyle sanığın bankayı araç olarak kullanarak şikayetçi dernek hesabından haksız menfaat temin ettiği anlaşılmakla, sanığın 5237 sayılı TCK'nın 158/1-f maddesi gereğince nitelikli dolandırıcılık suçundan mahkumiyetine hükmedilmesi gerektiği

fikrasında tanımlanan fiillerin işlenmesi suretiyle haksız yarar elde edilmesidir. Burada fail bu eylemlerden birini ya da bir kaçını işleyebilir. Her hâlükârda tek bir suç oluşacaktır. Ayrıca failin gerçekleştirebileceği hareketler seçimlik olarak sayıldığından bu suç seçimlik hareketli bir suçtur.

Failin, 244. maddenin ilk iki fıkrasındaki fiilleri işlemesinin yanı sıra çıkar elde etmesi gerektiğinden bu suç bağıli hareketli bir suç niteliğindedir²⁵⁷. Fail burada kendisi ya da bir başkası yararına haksız bir çıkar sağlayabilir. Önemli olan bir yarar sağlanması ve bu yararın içeriğinin haksız olmasıdır.

TCK'nın 244. maddesinde tanımlanan suç ile hırsızlık suçu zaman zaman birbirine karıştırılmaktadır. Zilyedinin rızası olmaksızın bir taşınır malın bulunduğu yerden alınması suretiyle menfaat temin edilmesi halinde TCK'nın 141. ve devamı maddelerinde yer alan hırsızlık suçu oluşacaktır. 244/4. maddede düzenlenen suçun oluşması için failin 244. maddenin ilk iki fıkrasında düzenlenen eylemler işleyerek menfaat temin etmesi gerekmektedir²⁵⁸.

Bu suç tipinin en sık rastlanan örneklerinden birisi de ATM'lere fiziksel şiddet uygulanması yoluyla içindeki paraların alınmasıdır²⁵⁹. Ancak bu durumda hırsızlık suçu da oluşabileceğinden ayırımın iyi yapılması ve eylemin hırsızlık suçuna vücut vermesi durumunda tali norm niteliğinde bulunan 244/4. maddeden işlem yapılmaması gerekir.

Bu suç icrai ya da ihmali hareketle işlenebilir. Fail, yükümlülüğü bulunmasına rağmen bunu yerine getirmiyor ve bu yolla bir çıkar elde ediyorsa bu durumda ihmali hareketle bu suç işlenmiş olacaktır.

2.4.3.2. Fail

Bu suç tipinde fail açısından özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun faili herkes olabilir.

Veriler üzerinde tasarruf yetkisine sahip kişi ya da sistemin sahibi de bu suç işleyebilir. Aynı şekilde sistemi kullanması için kendisine izin verilmiş olan bir kimse de bu suçun

gözetilmeksizin, suç vasfında hataya düşülerek hüküm kurulması..."(Yargıtay 15. Ceza Dairesi, 30/10/2018 Tarih, 2015/13311 E, 2018/7255 K – UYAP'tan alınmıştır.)

²⁵⁷ AKBULUT, s. 234.

²⁵⁸ "...Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği, bu itibarla; sanıkların Knight Online oyunundaki "Gavurboğan" isimli karakteri hukuka aykırı bir şekilde ele geçirmesi eyleminin, 5237 sayılı TCK'nın 244/2-4. maddesindeki bilişim suçunu oluşturacağı gözetilmeksizin suç vasfında yanılıya düşülerek yazılı şekilde nitelikli hırsızlık suçundan hüküm kurulması..." (Yargıtay, 13. Ceza Dairesi, 06.11.2018 Tarih, 2018/1272 E, 2018/15168 K – UYAP'tan alınmıştır.)

²⁵⁹ "Sanıkların Oyakbank ATM'nin çalışmasındaki aksaklığı fark ederek, çeşitli zamanlarda para çekme işlemi sırasında ATM'ye fiziki müdahalede bulunmak suretiyle cihazın para bloke edilmiş gibi işlem görmesini sağlayıp, çektikleri paranın hesaptan düşmesini engelleyerek menfaat elde ettiklerinin iddia ve kabul olunması karşısında eylemlerinin 765 sayılı TCK'nın 525/b-1 (5237 sayılı TCK'nın 244/4) maddesindeki "bilişim sistemini engellemek veya yanlış biçimde çalışmasını sağlamak suretiyle yarar sağlamak" suçuna uygun bulunduğu gözetilmeden yazılı şekilde 765 sayılı TCK'nın 525/b-2. maddesinden hüküm kurulmak suretiyle eksik ceza tayini" (Yargıtay 11. Ceza Dairesi 2010/6346 E - 2012/3544K – UYAP'tan alınmıştır.)

faili olabilir. Önemli olan burada 244. maddenin ilk iki fıkrasında tanımlanan fiillerin işlenmesi suretiyle haksız bir çıkarın elde edilmiş olmasıdır.

Bu suçun dolaylı fail olarak da işlenmesi mümkündür²⁶⁰. Kişi kendisi suç tanımında yer alan fiilleri işlemek yerine bunları üçüncü bir kimseyi kullanarak ona işletiyorsa bu durumda dolaylı fail olacaktır. Burada aracı kişinin suç işleme kastı bulunmamalıdır. Zira bu kişinin de kastı varsa artık dolaylı faillik değil şeriklik durumu söz konusu olacaktır.

2.4.3.3. Mağdur

Bu suç tipinde mağdur açısından özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun mağduru herkes olabilir.

Mağdur bilişim sisteminin ya da verilerin sahibi ya da kullanıcısı olabileceği gibi duruma göre üçüncü bir kişi de olabilir²⁶¹. Örneğin bir pozisyona yerleşmek maksadıyla iş başvurusunda bulunan iki kişiden birinin, diğerinin başvuru evraklarını değiştirerek ya da silerek o kişinin işe alınmamasını sağlaması durumunda evrakları değiştiren ya da silen kişi fail, bu sebepten dolayı işe alınmayan kişi ise mağdur durumundadır.

Bu suçu malvarlığına yönelik bir suç olarak tanımlayan görüşe göre mağdur da malvarlığında azalma olan kimsedir. Ancak bu suçun neticesinde elde edilen yararın maddi bir yarar olma zorunluluğu bulunmadığı için bu mağdur malvarlığında azalma olabileceği gibi manevi bir hakkı zarara uğratılan kimse de olabilir.

Öte yandan bu suçun bir mağdur olmadan da işlenmesi yahut tüm toplumun zararına olarak işlenmesi de mümkündür. Örneğin bir kimsenin kamuya ait bilişim sistemine girerek askerliğini yapmadığı halde yapmış gibi göstermesi yahut haksız bir şekilde tecil edilmesini sağlaması durumunda doğrudan bir kişinin hakkı zarara uğratılmış olmasa da toplum bu durumdan zarar görmüştür. Aynı şekilde kişinin bilişim sistemine girerek devamsızlıktan kaldığı bir derse ilişkin verileri değiştirmesi ve bu suretle dersi geçmesi durumunda zarara uğratılan bir kimseden söz edilemeyecek ancak ortada haksız bir çıkar olacaktır. Dolayısıyla bu durumda suç doğrudan bir mağdura karşı olmaksızın işlenmiş kabul edilecektir.

2.4.3.4. Konu

Suçun konusu failin sağladığı hukuka aykırı yarardır. Bu yararın maddi bir yarar mı olması gerektiği yoksa maddi manevi her türlü yararı mı kapsadığı hususunda farklı görüşler mevcuttur. Yukarıda da belirttiğimiz gibi madde metninde bu suçun işlenmesi neticesinde elde edilen çıkarın maddi bir çıkar olması şartı yoktur²⁶². Dolayısıyla maddi ya da manevi her türlü hukuka aykırı yarar bu suçun konusunu oluşturabilir.

²⁶⁰ AKBULUT, s. 231.

²⁶¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s.342;

²⁶² “...Bu madde anlamında haksız çıkar yalnızca maddi yararları içermeyip, herhangi bir yararın elde edilmesi suçun oluşması için yeterlidir. Suçun oluşabilmesi için failin sağladığı çıkarın haksız olduğunu bilmesi gerekir. Buradaki haksızlık suçun maddi unsurlarından çıkara ilişkin bir nitelendirme olduğu için kusur değil, kast kapsamındadır ve suç kasten işlenebilir.

2.4.3.5. Netice

Madde metninde failin TCK'nın 244. maddesinin ilk iki fırcasında düzenlenen fiilleri işleyerek haksız bir yarar elde etmesi aranmıştır. Dolayısıyla bu suç açısından netice de bu haksız yararadır. Bu suç neticeli bir suçtur. Failin gerçekleştirdiği eylem neticesinde yarar elde edememesi durumunda bu suç tamamlanmış olmaz.

Bu fıkra açısından elde edilen yararın sonucunda mağdurun bir zarara uğraması gerekip gerekmediği hususu tartışmalıdır. Bu suçun zarar suçu olduğunu söyleyen görüşe göre suçun oluşması için bir başkasının malvarlığında kayıp oluşmalıdır. Dolayısıyla bu suç bir zarar suçudur²⁶³. Ancak daha önce de belirttiğimiz gibi bu görüşe katılmıyoruz. Dolayısıyla bu suç tipi açısından bir zarar aranmaz. Bu suç bir zarar suçu değildir.

Öte yandan bu suç tehlike suçu da değildir. Zira failin bu çıkarı sağlamış olması gerekir. Fail çıkar üzerinde hâkimiyet kuramadıysa yahut bu çıkar gerçekleşmediyse suç tamamlanmış sayılmayacaktır.

2.4.4. Manevi Unsurlar

Bilişim sistemleri aracılığıyla haksız yarar sağlama suçu yalnızca kasten işlenebilen bir suçtur. Bu suçun taksirle işlenen hali kanunda düzenlenmediği için taksirle işlenmesi mümkün değildir.

Madde metninde failin suç tipinde yer alan eylemler neticesinde haksız bir yarar elde etmesi aranmıştır. Failin en baştan itibaren bu haksız yararı elde etmek maksadıyla hareket etmesi gerekip gerekmediği hususunda farklı görüşler mevcuttur. Azınlıkta kalan görüşe göre madde metninde failin hangi amaçla hareket ettiği önemsenmemiştir. Fail suç tipinde belirtilen hareketleri kasten işledikten sonra haksız bir yarar elde etme amacı olmasa dahi böyle bir yarar elde ediyorsa bu suçun oluşması için yeterlidir. Zira bu suç tipinde amaç aranmamış, neticenin gerçekleşmesi yeterli sayılmıştır²⁶⁴. Doktrindeki diğer görüşe göre ise failin yalnızca suç tipinde belirlenene eylemleri kasten yapması yeterli olmayacak, ayrıca failin haksız yarar elde etme kastıyla da hareket ediyor olması gerekecektir²⁶⁵. Bu görüşe göre bu suç için özel kast aranmaktadır.

Gerçekten de kanun metninde failin başlangıçtan itibaren böyle bir amaç ile hareket ediyor olması aranmamıştır. Hatta Sanal Ortamda İşlenen Suçlar Sözleşmesinin 8. maddesinde “*maddi bir menfaat sağlamak için*” denilmiş olmasına rağmen TCK'nın 244/4.

Somut olayda suç tarihinde Tekirdağ Emniyet Müdürlüğünde Asayiş Şube Müdürü olarak görev yapan sanığın kendisine bağlı olan Aranan Şahıslar Büro Amirliğine gelerek atış eğitimine gitmek için bürodan ayrılmak üzere olan tanık Ender Tozçöken'in kullandığı şahıs sorgulama sistemi açık olan bilgisayardan, tanık anlatımları ve bir bilişim sistemi olan PolNet kayıtlarına göre Özkan Kartal isimli şahsa ait silah ruhsatı almasına engel sicil kaydını saat 15:24'te iptal ettiği, PolNet bilişim sistemine girilerek kaydın silinmesi sonucu ... isimli kişiye Bakırköy Kaymakamlığının 18.05.2009 tarihli olurları ile silah taşıma ruhsatı verilerek başkasına haksız bir çıkar sağlanması şeklindeki eylemin TCK'nun 244/2-son maddesindeki “bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme” suçunu oluşturduğu gözetilmeden, yazılı biçimde hüküm kurulması...” (Yargıtay 8. Ceza Dairesi, 12.04.2016 Tarih, 2015/14782 E, 2016/4928 K – UYAP’tan alınmıştır.)

²⁶³ AKBULUT, s. 235.

²⁶⁴ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 351; ERDOĞAN, s. 257;

²⁶⁵ KOCA/ÜZÜLMEZ, s. 883.

maddesinde böyle bir ifadeye yer verilmemiştir. Bu bakımdan failin maddi ya da manevi bir çıkar sağlama amacını en başından itibaren taşıyor olması gerekmez. Suç neticesinde bu yararın elde edilmiş olması yeterlidir.

2.4.5. Hukuka Aykırılık

Bu suç tipinde failin elde ettiği yararın haksız olması aranmıştır. Fail, hak sahibinin rızasına dayanarak hareket ediyorsa elde ettiği yarar da haksız bir yarar olmaktan çıkacak dolayısıyla hukuka aykırılık da ortadan kalkacaktır. Burada önemli olan söz konusu rızanın kim tarafından verildiğidir. Örneğin bir bilişim sisteminin maliki, bu tarz bir fiil için rıza gösterse dahi sistemdeki verilerin malikinin farklı olması ve bu kişinin rızasının bulunmaması durumunda eylem hukuku uygun hale gelmeyecektir. Önemli olan burada rıza vermeye yetkili olan kişinin rıza vermesidir. Bu kişi de her olay için ayrı ayrı tespit edilmelidir.

Rızanın varlığı hususunda hataya düşüldü ise bu durumda TCK'nın 30. maddesi gündeme gelecektir.

2.4.6. Özel Görünüş Biçimleri

2.4.6.1. Teşebbüs

Bu suç teşebbüs açısından bir özellik arz etmez. Ancak failin kastının en baştan itibaren ne olduğu iyi tespit edilmelidir.

Bu suç TCK'nın 244. maddesinin ilk iki fıkrasında yer alan fiillerin işlenmesi sonucu haksız bir yarar elde edilmesiyle gerçekleşir. Fail en baştan itibaren haksız bir yarar elde etmek kastıyla hareket ediyorsa fakat ilk iki fıkradaki fiillerden birisini tamamladıktan sonra haksız yararı elde edemeden eylem bir şekilde yarıda kalırsa bu halde 244/4. maddeye teşebbüsten sorumlu tutulmalıdır. Ancak failin kastının bu olmadığı ya da belirlenemediği durumda fail 244. maddenin ilk fıkrasındaki hareketi tamamlar ve bir yarar elde edilemezse eylemine uyan fıkradan, bu hareketleri de tamamlayamazsa eylemine uyan fıkraya teşebbüsten sorumlu tutulmalıdır. Öte yandan failin haksız yarar elde etme kastının olup olmadığı çoğu zaman belirlenemez. Yine de her olay kendi içinde değerlendirilerek bir sonuca gidilmeli ve bu kast belirlenebiliyorsa ona göre sonuca gidilmelidir.

2.4.6.2. İştirak

Bu suç iştirak açısından bir özellik arz etmez. TCK'nın iştirake ilişkin hükümleri uygulanır.

2.4.6.3. İçtima

Bu suç tali suç niteliğindedir. Yani ancak failin fiilinin başka bir suç oluşturmaması halinde uygulanabilir. Her ne kadar madde gerekçesinde *“bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturmaması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.”* denilmişse de yukarıda da belirttiğimiz üzere madde metni esas alınmalı ve daha ağır ya da daha hafif bir cezayı gerektiriyor olmasına bakılmaksızın başka

bir suçu oluştuyorsa o suçtan hüküm kurulmalı, başka bir suçu oluşturmuyorsa faile bu suçtan ceza verilmelidir.

Bu suçun zincirleme suç şeklinde işlenmesi mümkündür. Fail 244. maddenin ilk iki fıkrasında yer alan fiilleri bir suç işleme kararı kapsamında değişik zamanlarda icra ederek hukuka aykırı yarar elde ediyorsa burada zincirleme suçtan söz edilir. Ancak fail değişik zamanlarda ilk iki fıkradaki hareketleri icra ediyor ve bu hareketlerin yalnızca sonuncusunda haksız yarar elde ediliyorsa burada tek bir bilişim sistemleri aracılığıyla haksız yarar sağlama suçu oluşacaktır. Zira failin kastı en baştan itibaren haksız yarar sağlamaktır ve bu yararı elde etmek için değişik zamanlarda ilk iki fıkrada yer alan eylemleri icra etmek durumunda kalmış, nihayetinde bu yararı elde etmiştir. *Burada zincirleme suçtan değil olsa olsa kesintisiz suçtan söz edilebilir.* Bu durumda ceza adaletinin sağlanabilmesi için hâkim alt sınırdan uzaklaşarak ceza tayinine gitmelidir.

Zincirleme suçtan söz edilebilmesi için failin her bir hareketi neticesinde belirli miktarlarda haksız yarar elde etmesi gerekmektedir. Burada failin kastının en baştan belirli bir miktar olmasının önemi yoktur. Fail her bir eylemi neticesinde belirli bir miktarda haksız yarar elde ediyorsa bu yeterlidir.

TCK'nın 244/4. maddesinde düzenlenen bu suç bileşik suç olduğu için TCK'nın 244. maddesinin ilk iki fıkrasıyla arasında içtima hükümleri uygulanmaz. Zira TCK'nın 42. maddesinde de birinin diğerinin unsurunu oluşturması dolayısıyla tek fiil sayılan suça bileşik suç denileceği ve bu tür suçlarda içtima hükümlerinin uygulanmayacağı hükme bağlanmıştır.

Bu suçla başka herhangi bir suç arasında fikri içtima hükümlerinin uygulanması ise mümkün değildir. Zira yukarıda da açıkladığımız üzere bu suç tali suç niteliğindedir ve ancak fail başka bir suçtan cezalandırılmıyorsa gündeme gelecektir.

TCK'nın 245/A maddesinde düzenlenen suç ise amaç suç niteliği taşımaktadır. Fail hem 245/A hem de 244/4 maddelerini ihlal etti ise her iki suçtan da ayrı ayrı cezalandırılmalıdır. Yani gerçek içtima uygulanacaktır.

2.4.7. Nitelikli Haller

Bu suçun nitelikli hali 3713 sayılı Terörle Mücadele Kanunu'nda düzenlenmiştir. 3713 sayılı Terörle Mücadele Kanunu'nun 4. maddesinde katalog olarak belirlen suçların ilgili yasanın 1 inci maddesinde ifade edilen hedefler doğrultusunda suç işlemek amacıyla kurulmuş bir terör örgütünün eylemleri çerçevesinde işlenmesi durumunda terör suçu sayılacağı düzenlenmiş ve TCK 244/4. maddesi de bu kapsamda sayılmıştır. İlgili yasanın 5. maddesinde ise yasanın 3.ile 4. maddelerinde belirtilen suçları işleyenler hakkında ilgili yasalar uyarınca belirlenecek hapis cezalarının ve adlî para cezalarının yarı oranında arttırılacağına yer verilmiştir. Maddeye göre bu şekilde belirlenecek cezalarda, gerek o fiil için, gerek her türden yaptırım için belirlen cezanın yukarı sınırının aşılabileceği belirtilmiştir. Öte yandan müebbet hapis cezası yerine, ağırlaştırılmış müebbet hapis cezasına hükmolunur denilmiştir. Bu sebeple 244/4. maddede düzenlenen suçun terör faaliyeti çerçevesinde işlenmesi durumunda cezasının yarı oranında arttırılacağı da hükme bağlanmıştır.

2.4.8. Soruşturma Usulü ve Yaptırım

TCK'nın 244. maddesinin 4. fıkrasında düzenlenen bu suçun cezası iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasıdır. Burada hapis cezası ve adli para cezası seçimlik olmayıp, bu suçu işleyen fail hakkında her iki cezaya birden hükmedilecektir.

TCK'nın 142/2-e maddesinde düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun yaptırımı ise beş yıldan on yıla kadar hapis cezasıdır. Bilişim sistemlerinin veya verilerin güvenliğine zarar vererek haksız bir menfaat elde eden faile verilecek cezanın bilişim sistemlerini yalnızca aracı olarak kullanan failden daha az ceza alabilmesine yol açacak bu durum acilen değişikliğe gidilerek düzeltilmelidir.

TCK'nın 244. maddesinin son fıkrasında düzenlenen bu suç re'sen soruşturulur.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10. 11. ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

TCK'nın 246. maddesinde bilişim alanında suçların işlenmesi ile haksız bir menfaat temin eden tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir. Dolayısıyla TCK'nın 244/4. maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

2.5. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK 245)

2.5.1. Genel Olarak

Günümüzde alışveriş yapma alışkanlıkları hızla değişmekte, insanlar para yerine taşınması daha kolay olan kredi kartları ve banka kartları ile alışveriş yapmayı tercih etmektedirler. İnternet üzerinden alışverişin de yaygınlaşması ile banka ve kredi kartlarının alışverişlerde kullanılması pek çok kişi için kaçınılmaz denilecek düzeye ulaşmıştır. Ayrıca kişilerin banka hesaplarında bulunan paraları en kolay ve en hızlı şekilde çekmelerinin yolu da banka kartlarını kullanarak ATM'lerden para çekmektir. Banka ve kredi kartlarına duyulan ihtiyacın artması sonucu bu kartlar yaygınlaşmış, bununla birlikte bu kartların kullanması ya da sahtelerinin üretilmesi yoluyla işlenen suçlar da ortaya çıkmıştır. Bu durumu gören kanun koyucu bu konuda bir düzenleme yapmak ihtiyacı duymuştur. Banka ve kredi kartlarının kullanılmasını bağımsız bir suç olarak ilk kez 5237 sayılı TCK'da yer almıştır.

5237 sayılı Kanunun 245. maddesinde bu suç düzenlenmeden önce bu suç tipine girebilecek olaylar Yargıtay tarafından hırsızlık, dolandırıcılık ya da 525/b-2 maddesi kapsamında değerlendirilmekteydi²⁶⁶. Ancak hem doktrinde hem de uygulamada farklı görüşler ve durumlarla karşılaşılıyordu ve bu konuda düzenli bir uygulamaya rastlamak mümkün değildi. Sanal Ortamda İşlenen Suçlar Sözleşmesinde de bu konuyla ilgili bir düzenleme yoktu. Kanun koyucu uygulamada karşılaşılan bu karışıklıkları gidermek için

²⁶⁶ AKBULUT, s. 270.

5237 sayılı TCK ile yeni bir suç tipi ihdas etti. TCK'nın 245. maddesinde düzenlenen bu suçun hırsızlık, dolandırıcılık, sahtecilik suçları, güveni kötüye kullanma gibi suçların banka ve kredi kartları kullanılarak işlenen halleri olduğu ifade edilmiştir²⁶⁷. Bu husus madde gerekçesinde de *“Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür.”* denilerek ifade edilmiştir.

Söz konusu 245. maddenin gerekçesinde de bu durum *“Madde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır. Banka kartı, bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kart, saptanan ve kart sahibince bilinen bir numara marifetiyle, banka görevlisinin yardımı olmadan, kart sahibinin kendi hesabından para çekmesini sağlamaktadır. Kredi kartları ise, banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince, kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araçtır. İşte bu kartların kötüye kullanılmaları, söz konusu maddede suç olarak tanımlanmıştır.”* denilmek suretiyle ifade edilmiştir.

TCK'nın 245. maddesi *“Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.”* şeklindedir. İkinci fıkrasında ise *“Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.”* denilmiş ve üçüncü fıkrasında ise *“Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.”* hükmüne yer verilmiştir.

Maddenin ilk üç fıkrası incelendiğinde ilk fıkranın başkalarına ait gerçek banka ve kredi kartlarının geçerli bir rıza olmaksızın kullanılarak yarar sağlanmasını; ikinci fıkrada ise sahte banka ve kredi kartlarının başkalarına ait banka hesaplarıyla ilişkilendirilmek suretiyle üretilmesi, satılması, devredilmesi, satın alınması ve kabul edilmesini son fıkrada ise sahte olarak üretilen veya üzerinde sahtecilik yapılan banka ve kredi kartlarının kullanılarak yarar sağlanmasının suç olarak düzenlediği görülür. Dolayısıyla TCK'nın 245. maddesinin ilk suç fıkrasında üç ayrı suç tanımlanmıştır. Çalışmamızda da her üç suç tipi farklı bir başlık altında incelenecektir.

4. fıkrada *“Birinci fıkrada yer alan suçun; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına*

²⁶⁷ AKBULUT, s. 276; KOCA/ÜZÜLMEZ, s. 887; ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 999.

olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.” denilmek suretiyle birinci fıkrada düzenlenen suç ilişkin şahsi cezasızlık sebebine yer verilmiştir. Son fıkrada ise “Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.” denilerek yine birinci suça ilişkin olarak etkin pişmanlıkla ilgili belirleme yapılmıştır.

2.5.2. Başkasına Ait Banka veya Kredi Kartlarını Kullanarak Yarar Sağlama Suçu

2.5.2.1. Korunan Hukuki Değer

Madde gerekçesinde bu suçun hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının ratio legis’lerinin tümünü de içeren bu fiillerin içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirildiği belirtilmiştir. Bu suçlardan hırsızlık, dolandırıcılık ve güveni kötüye kullanma suçları TCK’nın ikinci kitabının kişilere karşı suçlar başlıklı ikinci kısmının malvarlığına karşı suçlar başlıklı onuncu bölümünde; sahtecilik suçları ise ikinci kitabın topluma karşı suçlar başlıklı ikinci kısmının kamu güvenine karşı suçlar başlıklı aldığı dördüncü bölümde düzenlenmiştir. Her ne kadar banka ve kredi kartlarının kötüye kullanılması suçları bilişim suçları bölümünde düzenlenmiş olsa da bu suç bir malvarlığına ilişkin bir suçtur. 245. maddenin son fıkrasında da birinci fıkraya giren suçlarla ilgili olarak malvarlığına karşı suçlarla ilişkin etkin pişmanlık maddesinin uygulanacağını düzenlenmesi bu durumu pekiştirmiştir. 245. maddenin ilk fıkrasında düzenlenen başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçu da kişilerin malvarlığını korumaktadır. Yine madde gerekçesinde bu husus “banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır.” denilerek ifade edilmiştir.

Doktrinde de genel olarak bu suçla malvarlığının korunduğuna ilişkin görüşler mevcuttur²⁶⁸. Öte yandan bu suçla banka ve kredi kartlarının kötüye kullanılmasının önlenmesi ve bu kartlarla yapılan alışverişin kişiye ait gerçek bir kartla yapıldığına olan güvenin korunması²⁶⁹, kamuya duyulan güvenin korunması²⁷⁰ ve bankacılık sistemine ve ticari yaşama duyulan güven²⁷¹ gibi hukuki değerlerin de korunduğu ifade edilmektedir. Dolayısıyla bu yazarlara göre bu suç tipi ile birden fazla hukuki değer korunmaktadır.

2.5.2.2. Maddi Unsurlar

2.5.2.2.1. Fîil

TCK’nın 245. maddesinde düzenlenen suç “Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa” oluşacaktır. Dolayısıyla bu suçun oluşması için

²⁶⁸ KOCA/ÜZÜLMEZ, s. 887-888; TEZCAN/ERDEM/ÖNOK, s. 1072; AKBULUT, s. 276; DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku 357-359.

²⁶⁹ KOCA/ÜZÜLMEZ, s. 888.

²⁷⁰ GÜL, s. 126.

²⁷¹ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s.999-1000; TEZCAN/ERDEM/ÖNOK, s. 1072.

failin, kart hamilinin rızası bulunmaksızın kartı kullanarak ya da bir başkasına kullandırarak yarar sağlaması gerekir.

Fail hem kartı kullanmalı ya da başkasına kullandırtmalı hem de yarar sağlamalıdır. Kanunda düzenlenen suçun oluşması için tek bir hareketin yeterli olmadığı, birden fazla hareketin hepsinin yapılmasının arandığı hallerde birden fazla hareketli suçlardan söz edilir²⁷². Bu itibarla inceleme konusu suç birden fazla hareketli bir suçtur. Failin kartı kullanması ya da kullandırması ile yarar elde edilmesi arasında bağlantı bulunması gerekir.

Failin yararı kendisine sağlaması durumunda suç oluşur ancak bu yarar kendisine sağlaması şart değildir. Zira madde metninde de açıkça bu yararın bir başkasına da sağlanabileceği ifade edilmiştir. Önemli olan bu yararın sağlanmış olmasıdır.

Bu yararın fiilen ele geçirilmiş olması gerekmez. Failin yarar üzerinde tasarruf edebilecek konuma gelmesi bu suçun oluşması açısından yeterlidir²⁷³.

Bu suç kullanma veya kullandırtma hareketleri bakımından seçimlik hareketlidir. Kartın ne şekilde kullanılacağı ya da kullandırılacağı ya da yararın ne şekilde elde edileceği hususunda ise bir sınırlama yoktur. Bu açıdan serbest hareketli bir suçtur.

Banka Kartları ve Kredi Kartları Kanunu’nun üçüncü maddesinin d ve e bentlerine göre banka kartı “*Mevduat hesabı veya özel carî hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlayan kartı*”, kredi kartı ise “*Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fizikî varlığı bulunmayan kart numarasını*” ifade etmektedir. Bu tanımlamaların dışında kalan kartlar banka veya kredi kartı sayılamayacağından bu kartların maddede belirtilen şekilde kullanımında dahi bu suç oluşmayacaktır. Zira madde metninde genel olarak kartlardan değil, banka veya kredi kartlarından söz edilmektedir. Bu kartların belirli noktalarda ödeme aracı olarak kullanılabilmesi de bu durumu değiştirmeyecektir. Bu kartlara ilişkin olarak gerçekleşen fiiller söz konusu olduğunda olayın özelliklerine göre TCK 244/4 ya da 142/2-e maddelerini uygulanması söz konusu olabilecektir.

Suçun oluşması için kullanılacak ya da kullandırılacak banka veya kredi kartının başkasına ait bir banka veya kredi kartı olması gerekir. Bir kimsenin kendi kartını kullanması ya da bir başkasına kullandırması durumunda suç oluşmaz. Esasen bir kimsenin kendi kartını başkasına kullandırttığı durumda bu kartı kullanan kişi başkasına ait bir banka veya kredi kartını kullanıyor durumdadır ancak kart hamilinin rızası bulunduğu için yine suç oluşmayacaktır. Zira suçun oluşması için başkasına ait banka veya kredi kartının kullanılması veya kullandırılması tek başına yeterli olmayıp kart hamilinin rızasının da bulunmaması gerekir. Bu rıza varsa yine suç oluşmaz.

Söz konusu banka veya kredi kartlarının ne şekilde ele geçirildiği bu suç açısından önemli değildir. Zira madde metninde “*her ne suretle olursa olsun ele geçiren veya elinde bulunduran*” ifadesine yer verilmiştir. Fail bu kartı bulmuş ya da çalmış olabileceği gibi

²⁷² DÖNMEZER/ERMAN, s. 86.

²⁷³ AKBULUT, s. 295; ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1009-1010; TEZCAN/ERDEM/ÖNOK, s. 1075.

kart, hamili tarafından rıza ile verilmiş de olabilir. Yine kartı hamiline teslim etmekle görevli olan kişinin bu kartı kendisine verilmesi gereken kişinin rızası olmaksızın kullanması suretiyle de suç oluşabilir. Kart failin eline hata sonucu da geçmiş olabilir. Önemli olan failin kart hamilinin rızası bulunmaksızın bu kartı kullanarak ya da kullandırarak yarar elde etmesidir. Hatta fail söz konusu banka veya kredi kartını rıza ile vermiş olsa bile failin kendisine verilen yetkinin sınırlarını aşması durumunda yine suç oluşacaktır. Örneğin kartı sadece saklaması için verilen fail bu kartı kullanırsa suç oluşur. Hatta belirli bir miktar para çekmesi için kendisine verilen kartı kullanarak belirlenen miktarın üzerinde bir miktarda para çekilmesi durumunda da suç oluşacaktır.

Dülger'e göre suç tipinde geçen ele geçirmek ifadesi daha çok kişinin kartı hukuka aykırı olarak elde etmesi, elinde bulundurmamak ifadesi ise kişinin kartı önceden hukuka uygun bir şekilde elde etmiş olmasına rağmen sonradan bu suç için kullanması anlamına gelmektedir²⁷⁴.

Failin başkasının kullandığı banka veya kredi kartından ötürü sorumlu tutulabilmesi için kullandırtma iradesinin bulunması gerekir. Bu irade dolaylı faillik ya da şeriklik şeklinde ortaya çıkabilir. Kişi kartı kullanması dışında bir amaçla üçüncü kişiye veriyorsa ve bu üçüncü kişi kartı kullanarak yarar sağlıyorsa bu durumda kartı veren kişinin kullandırtma iradesinden söz edilemeyeceğinden onun failliği de söz konusu olmayacak, yalnızca kartı kullanan kişinin failliğinden söz edilebilecektir. Ancak kişi kartı kullanması amacıyla bir başkasına veriyorsa ya da aldatmak veya zorlamak suretiyle bu kişinin farkında olmadan kartı kullanmasını sağlıyorsa bu durumda kullandırtmak fiili gerçekleşmiş olduğundan kişi fail olarak bu suçtan sorumlu tutulacaktır.

Bir görüşe göre failin bir kartı çalarak bir başkasına satması ya da bedelsiz olarak vermesi, sattığı ya da verdiği kişinin de bunu kullanması ve yarar elde etmesi durumunda da 245/1 oluşmuştur. Çünkü fail kullandırtma eylemini gerçekleştirmiştir²⁷⁵. Burada taraflar arasında müşterek faillik vardır.

Banka Kartları ve Kredi Kartları Kanunu'nda banka kartı için “... *sağlayan kartı*”, kredi kartı için ise “... *sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını*” ifadesi kullanılmıştır. Dolayısıyla sadece fiziki varlığı bulunan kartlar değil sanal kartlar da bu suç tipi anlamında kredi kartı sayılacak ve sanal kartlara yönelik olarak bu fiilin işlenmesi durumunda da suç oluşacaktır. Ayrıca her ne kadar yalnızca kredi kartları için kart numarasından söz edilmiş, banka kartları için böyle bir belirme yapılamamış olsa da fiziki varlığı bulunan banka kartının failin elinde olması şart değildir. Fail, fiziki varlığı bulunan ancak elinde bulunmayan banka kartının numarasına sahipse ve bu numarayı kullanarak kart hamilinin rızası hilafına kullanarak yarar elde ederse yine suç oluşacaktır²⁷⁶.

²⁷⁴ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 372.

²⁷⁵ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 374.

²⁷⁶ “...Banka veya kredi kartlarının kötüye kullanılması suçunun oluşabilmesi için 5464 sayılı Kanun'un 3. maddesi uyarınca kartın fiziken kullanımı gerekmeyip kart bilgilerinin kullanılması yeterli olduğu cihetle; sanığın müştekinin kart bilgilerini birden fazla kez kullanarak toplam 2.520,00 TL'lik cep telefonu faturalarını ödemesi şeklindeki eyleminin 5237 sayılı TCK'nın 245/1, 43/1. maddelerinde belirtilen suçu oluşturduğu gözetilmeden aynı Kanun'un 142/2-e maddesi gereği cezalandırılmasına karar

Fiziki varlığı bulunsun ya da bulunmasın kredi kartlarının numaralarının kullanılması suretiyle yarar elde edilmesi durumunda da suç oluşacaktır.

Doktrinde bazı yazarlar kartların fiziksel olarak kullanılması gerektiğini, yalnızca numaralarının kullanılması durumunda 245/1. maddede düzenlenen suçun oluşmayacağını ifade etmektedirler²⁷⁷. Bazı yazarlar ise kredi kartlarında kart numarası ifadesine de maddede yer verildiğini, dolayısıyla bu kartlar açısından fiziksel olmayan kullanımların da geçerli olduğunu ancak banka kartlarının bu şekilde kullanılamayacağını ifade etmektedir²⁷⁸. Bazı yazarlar ise fiziki olmayan kullanımların da 245/1 anlamında bir kullanım olduğunu, dolayısıyla suçun oluşacağını belirtmektedirler²⁷⁹.

Belirtmek gerekir ki Banka Kartları ve Kredi Kartları Kanunu'nun 3. maddesinin e bendinde yer alan "*fizikî varlığı bulunmayan kart numarasını*" ifadesi sanal kartlar için kullanılmıştır. Sanal kart, basılı olmayan ve fiziki bir varlığı bulunmayan, asıl karta ya da banka hesabına bağlı olarak oluşturulabilen, limiti de kullanıcısının belirleyebileceği bir karttır. Dolayısıyla bu suç basılı banka kartlarının, basılı kredi kartlarının ya da sanal kartların kullanılması suretiyle işlenebilir. Ancak bu kullanmanın illa fiziksel bir kullanma olmasına yani ATM'den ya da POS cihazlarından geçirilerek kullanılmasına gerek yoktur. Bu kartların numaraları kullanılarak internet üzerinden yapılan alışverişlerde de bu kartlar kullanılmış sayılır. Bu durum hem kredi kartları hem de banka kartları için geçerlidir.

Öte yandan bir kart numarasının değil de internet bankacılığının kullanılması durumunda 245/1. değil duruma göre 244/4. ya da 142/2-e maddeleri gündeme gelecektir. Zira TCK'nın 245/1. maddesinde banka veya kredi kartlarının kullanılması aranmış olup internet bankacılığı üzerinden bu kartlar kullanılmadan da işlem yapılması mümkündür.

Ayrıca bu suçun oluşması için gerçek bir banka kartı ya da gerçek bir kredi kartı bulunmalıdır. Sahte olarak üretilen bir kartın kullanılması durumunda 245/1. maddede tanımlanan suç değil 245/3. maddede tanımlanan suç oluşur.

2.5.2.2.2. Fail

TCK'nın 245. maddesinde düzenlenen başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunda faile ilişkin özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun faili herkes olabilir.

Bir kimsenin hamili olduğu banka kartını kullanması suretiyle bu suç oluşmaz. Kişinin, banka ve kredi kartlarını kendisine tanımlanan limitleri aşacak şekilde kullanması durumu da bu suça sebebiyet vermez. Bu durum ancak bir hukuki ihtilaf yaratır. Öte yandan bu kart hamilinin sistemi engellemek, bozmak; verileri bozmak, yok etmek, değiştirmek ya da erişilemez kılmak; sisteme veri yerleştirmek ya da var olan verileri başka bir yere göndermek gibi fiilleri işleyerek haksız bir menfaat elde etmesi durumunda 244/4. maddesinde tanımlanan suç gerçekleştirilecektir. Yine kart hamili kendi kullanımında bulunan

verilmesi..."(Yargıtay 2. Ceza Dairesi, 08.06.2020 Tarih, 2020/5865 E, 2020/5291 K – UYAP'tan alınmıştır.)

²⁷⁷ KOCA/ÜZÜLMEZ, s. 895; ÖZBEK/DOĞAN/BACAŞIZ/TEPE, s. 1008.

²⁷⁸ ÖZBEK s. 1032.

²⁷⁹ AKBULUT, s. 294; MAHMUTOĞLU, s.872.

bu kartları farklı suçların işlenmesinde kullanabilir. Bu suçlara örnek olarak özellikle Banka Kartları ve Kredi Kartları Kanunu'nun 36. maddesinde düzenlenen sahte belge düzenlenmesi suçu ve yine aynı Kanunun 37. maddesinde düzenlenen gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik suçu verilebilir. Ancak kart hamilinin yalnızca kendisine ait banka veya kredi kartlarını kullanarak 245. maddede tanımlanan suçu işlemesi mümkün değildir.

Bir kimsenin kendisine ait banka veya kredi kartını kaybettiğini ya da çaldırdığını beyan ederek bizzat kullanması ya da başkasına kullandırması durumunda da yukarıda belirtilen Gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik suçu oluşur. Bu durumda kartını bu şekilde kullandıran kart hamili gibi kartı kullanan kişiler de TCK'nın 245/1. maddesinden değil Banka Kartları ve Kredi Kartları Kanunu'nun 37/1. maddesinden cezalandırılırlar.

Tüzel kişiler suçun faili olamazlar ancak TCK'nın 246. maddesinde de belirtildiği üzere bu suçun işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirleri uygulanacaktır.

2.5.2.2.3. Mağdur

TCK'nın 245. maddesinde düzenlenen başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunda mağdura ilişkin özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun mağduru herkes olabilir.

Bu suç bir zarar suçudur. Bu suçun mağduru ise banka ve kredi kartlarının kullanılması dolayısıyla malvarlığı zarara uğrayan kimsedir. Bu kimse çoğu zaman maddede belirtilen ifadeyle kart sahibi ya da kartın kendisine verilmesi gereken kişidir. Bu kimsenin kim olduğu iyi tespit edilmelidir. Banka Kartları ve Kredi Kartları Kanunu'nun 3. maddesinin j bendinde kart hamilinin tanımı, banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişi olarak yapılmıştır. TCK'nın 245. maddesinde ise kart hamili ifadesi değil kart sahibi veya kartın kendisine verilmesi gereken kişi ifadesi kullanılmıştır. Kartın mülkiyeti ise bu kartları çıkaran kuruluşlara aittir. Bu durum suçun mağdurunun kim olduğuna ilişkin problem yaratmıştır. Ancak doktrinde de genel olarak ifade edildiği üzere²⁸⁰ TCK 245/1. maddesinde kullanılan kart sahibi veya kartın kendisine verilmesi gereken kişi ifadesi kart hamilini ifade etmektedir. Banka Kartları ve Kredi Kartları Kanunu'nun TCK'dan sonra düzenlenmiş olması sebebiyle böyle bir çelişki ortaya çıkmıştır. Bu durum 245. maddede yapılacak olan bir değişiklik ile giderilebilecektir.

245/1. maddede yer alan kart sahibi veya kartın kendisine verilmesi gereken kişi ifadesi kart hamili şeklinde okunduğunda bu suçun mağduru olarak banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişi görülecektir. Ancak suçun mağduru tüzel kişi olamayacağından suçun tüzel kişinin zararına olarak işlenmesi durumunda tüzel kişi suçtan zarar gören olarak kabul edilecek, tüzel kişinin ortağı ya da maliki ise suçun mağduru olacaktır.

²⁸⁰ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1006; KOCA/ÜZÜLMEZ, s. 890; AKBULUT, s. 281.

Suçtan zarar gören kişi olaya göre kartın hamili değil de kartı çıkaran kuruluş da olabilir. Böyle bir durumda suçun mağduru bu kuruluş olacaktır. Tüzel kişiler suçun mağduru olamayacaklarından bu tüzel kişiliğin ortakları suçun mağduru olarak kabul edilecektir. Dolayısıyla bu suçun işlenmesi dolayısıyla malvarlığı zarara uğrayan kimse olaya özgü olarak tespit edilmeli, bu kimsenin kartın hamili olması durumunda kart hamili; kartı çıkaran banka veya finans kuruluşu olması durumunda bu kuruluş mağdur olarak kabul edilmelidir. Her ikisinin de zararı varsa bu suçun mağduru olarak hem kart hamili hem de kartı çıkaran kuruluş kabul edilecektir. Özellikle kartın kaybolması ve çalınması ihtimali ile ilgili olarak Banka Kartları ve Kredi Kartları Kanunu'nun 12. maddesinde yer alan *"Kartın ya da 16 ncı maddede belirtilen bilgilerin kaybolması veya çalınması halinde kart hamili, yapacağı bildirimden önceki yirmidört saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan yüzelli YeniTürk Lirası ile sınırlı olmak üzere sorumludur. Hukuka aykırı kullanımın, hamilin ağır ihmaline veya kastına dayanması veya bildirimin yapılmaması hallerinde bu sınır uygulanmaz."* düzenlemesi dolayısıyla söz konusu maddede belirtilen durum gerçekleştiğinde hem kart hamilinin hem de kartı çıkaran kuruluşun zarara uğraması, dolayısıyla da suçun mağduru olması söz konusudur. Elbette suçun mağduru tüzel kişiler olamayacağından mağdur bu tüzel kişiliğin ortakları olacaktır. Yargıtay banka veya kredi kartı henüz hamiline teslim edilmeden önce kartı ele geçirerek menfaat temin edilmesi halinde suçtan zarar gören olarak banka ve finans kurumunu kabul etmektedir²⁸¹.

Doktrinde bu suçun mağduru olarak genellikle kart hamili kabul edilmiştir²⁸². Öte yandan doktrinde bu suçun mağdurunun 5464 sayılı yasadaki düzenleme gereği banka ve finans kurumu da olabileceğine ilişkin görüşler de mevcuttur²⁸³. Ayrıca bu suçun mağduru olarak kart hamilini kabul eden ancak banka ya da kredi kurumunu da suçtan zarar gören olarak kabul eden görüşler de mevcuttur²⁸⁴.

2.5.2.2.4. Konu

TCK'nın 245/1. maddesinde yer alan bu suçun meydana gelebilmesi için failin, başkasına ait banka veya kredi kartını, kart hamilinin rızası bulunmaksızın kullanması ve suretle kendisine yahut bir başka kimseye yarar sağlaması gerekir. Bu suçun konusu, sağlanan bu yararadır. Bu yarar malvarlığına ilişkin bir değer, çoğu zaman da paradır. Ekonomik bir değeri olmayan bir yarar bu suçun konusu olamaz.

Doktrinde bu suçun konusunun yarar olduğunu söyleyen görüşün²⁸⁵ yanı sıra genellikle bu suçun konusunun banka ve kredi kartları olduğu ifade edilmektedir²⁸⁶. Bazı yazarlar ise

²⁸¹ *"Banka ya da finans kuruluşları tarafından üretilen, banka veya kredi kartlarının ya da kart bilgilerinin, kartın hamile tesliminden önce ele geçirilerek menfaat temin edilmesi halinde, suçtan zarar görenin kartı üreten banka ya da finans kuruluşları olacağı cihetle"* (Yargıtay 15. Ceza Dairesi, 07/10/2020 tarih, 2020/5469 E - 2020/9598 K – UYAP'tan alınmıştır.)

²⁸² AKBULUT, s. 280-284; ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s.1006. TEZCAN/ERDEM/ÖNOK, s.1073; KOCA/ÜZÜLMEZ, s. 890.

²⁸³ GÜL, s. 128.

²⁸⁴ TEZCAN/ERDEM/ÖNOK, s. 1073.

²⁸⁵ KOCA/ÜZÜLMEZ, s. 891.

²⁸⁶ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1002; TEZCAN/ERDEM/ÖNOK, s. 1073.

suçun konusunun hem banka ve kredi kartı hem de malvarlığına ilişkin bir değer olduğunu ifade etmektedir²⁸⁷.

2.5.2.2.5. Netice

Bu suçun oluşması için başkasına ait banka veya kredi kartı kullanılarak ya da kullandırılarak bir yarar sağlanması gerekir. Dolayısıyla bu suç için netice sağlanan yararlıdır. Yarar elde etmeksizin bu suç gerçekleşmez ancak bu suça teşebbüs edilmiş olur.

Suçun tamamlanması için yarar elde edilmesi gerekir. Bu yararın karşılığı olarak mağdur da zarara uğrar. Dolayısıyla bu suç bir zarar suçudur.

2.5.2.3. Manevi Unsurlar

TCK'nın 245. maddesinin ilk fıkrasında düzenlenen suç yalnızca kasten işlenebilir. Bu suçun failin taksirli bir hareketi ile işlenmesi olası değildir.

Failin, kart sahibinin rızasının bulunduğu hususunda hataya düşmesi sonucu suç tipinde belirtilen fiili işlemesi durumunda TCK 30/1 maddesi gereğince hatasından yararlanır. Suçun taksirli hali de olmadığından cezalandırılmaz.

Bu suç açısından failin hangi saik ile hareket ettiğinin bir önemi yoktur. Fail kendisine yarar sağlamaktan ziyade mağdura zarar vermek amacıyla da bu suçu işleyebilir. Örneğin haksız kazanç elde ettiğini düşündüğü bir kimseye ait banka kartını ya da kredi kartını, kart hamilinin rızası olmaksızın kullanarak bir yardım kuruluşuna bağış yapan kişi de bu suçu işlemiştir. Zira failin saiki önemsenmediği gibi yararın bizzat faile sağlanması da gerekmez.

2.5.2.4. Hukuka Aykırılık

Bu suçun oluşması için failin, kart sahibinin ya da kartın kendisine verilmesi gereken kişinin rızası hilafına hareket etmesi gerekir. Kart hamilinin rızası varsa bu durumda suç oluşmaz. Bu durum madde metninde açıkça belirtilmiştir ancak belirtilmeseydi dahi böyle bir rızanın varlığı durumunda eylemin suç niteliğinden bahsedilemeyecekti.

Hakkın kullanması da bu suç açısından bir hukuka uygunluk sebebidir²⁸⁸. Veli ya da vasiinin kendisine tanınan hak kapsamında malları üzerinde tasarruf yetkisine sahip olduğu kişiye ait kartları kullanması durumunda hakkın kullanılması hali gerçekleşecek ve fiil hukuka uygun olacaktır²⁸⁹. Ancak doktrinde bu hukuka uygunluk sebebini kabul etmeyen yazarlar da vardır²⁹⁰.

2.5.2.5. Suçun Özel Görünüş Biçimleri

2.5.2.5.1. Teşebbüs

Failin, başkasına ait banka kartını ya da kredi kartını kart hamilinin rızası olmaksızın kullanarak yarar elde etmesi durumunda suç tamamlanmış olur. Fail kartı kullanma

²⁸⁷ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.368-369.

²⁸⁸ KOCA/ÜZÜLMEZ, s. 897.

²⁸⁹ AKBULUT, s. 296.

²⁹⁰ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1010.

hareketine henüz başlamadıysa teşebbüsten de söz edilemez. Failin kartı kullanmaya yönelik harekete başlaması ancak söz konusu kartı kullanmadan eylemini elinde olmayan sebeplerden ötürü tamamlayamaması durumunda ise suç teşebbüs aşamasında kalmış olur.

Failin banka kartını ya da kredi kartını kullanması ancak yararı elde edememesi durumunda da suç teşebbüs aşamasında kalmıştır.²⁹¹

Fail kartı bir şekilde ele geçirmiş ancak kullanmaya başlamamışsa bu durumda TCK'nın 245/1. maddesine teşebbüsten söz edilemeyecek ancak kartın ele geçiriliş şekli bir başka suçu oluşturuyorsa örneğin kart hırsızlık sonucu ele geçirilmişse bu suçtan dolayı fail sorumlu tutulacaktır.

2.5.2.5.2. İştirak

Bu suç, failin kendisine ait banka veya kredi kartını kullanması ya da kullandırması yoluyla işlenir. Burada kullandırmanın şekli önem arz etmektedir. Şayet fail kartı aralarında birlikte suç işleme iradesi bulunan bir kimseye kullandırıyor ise bu durumda müşterek faillik söz konusu olacaktır. Ancak fail bir kimseyi kandırarak, tehdit ederek ya da aldatarak bu kimseye kartı kullandırıyor ise bu durumda dolaylı faillik söz konusu olacak ve kartı kullanan kişinin bir sorumluluğu bulunmayacaktır.

Müşterek failliğin söz konusu olduğu durumlarda müşterek failler hem 245/1. maddeden hem de kartın ele geçirilmesi başka bir suçun neticesinde oluyorsa bu suçtan dolayı birlikte fail olacaklardır. Örneğin bir failin kartı hırsızlık sonucu ele geçirilerek diğer faile vermesi ve bu failin de kartı kullanması durumunda her iki müşterek fail de hem hırsızlık hem de TCK'nın 245/1. maddesinde düzenlenen suçtan sorumlu olacaklardır.

Yararın fail tarafından başka bir kişiye sağlanması durumunda en baştan itibaren birlikte hareket etme kararı varsa müşterek faillik söz konusu olacak ancak böyle bir durum yoksa o halde TCK'nın 165. maddesinde düzenlenen suç eşyasının kabul edilmesi suçu oluşabilecektir²⁹².

Bir suç işleme kararı kapsamında faillerden birinin suç konusu kartı hırsızlık yoluyla ele geçirmesi, diğerinin de bu kartı kullanarak yarar elde etmesi durumunda müşterek faillik gündeme gelecek ve her iki fail de hem hırsızlık hem de 245/1. maddede düzenlenen bu suçtan sorumlu olacaklardır²⁹³.

2.5.2.5.3. İctima

TCK'nın 245/1. maddesinde düzenlenen başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunun zincirleme suç şeklinde işlenmesi mümkündür. Bunun için bir suç işleme kararı kapsamında değişik zamanlarda aynı kişiye karşı, başkasına ait

²⁹¹ “müştekilerin kredi kartı ve kişisel bilgilerini elde ettikten sonra kredi kartlarından nakit avans çekilerek, müştekilerin hesaplarına aktarılması, buradan cepbank yöntemiyle faillerin kullandığı cep telefonlarına para transferi yapılarak ATM lerden çekilmesi suretiyle haksız kazanç elde edilmesi şeklindeki eylemlerin TCK.nun 245/1. madde ve fıkrasında düzenlenen başkasına ait banka veya kredi kartlarının kötüye kullanılması suçunu oluşturduğu, menfaat temin edilememesi halinde TCK.nun 35. maddesinin uygulanması gerektiği” (Yargıtay 8. Ceza Dairesi, 25.02.2019 tarih 2017/20222 E - 2019/2585 K – UYAP’tan alınmıştır.)

²⁹² DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 408.

²⁹³ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 409. ERDOĞAN, s. 321.

banka veya kredi kartlarını kullanarak yarar sağlama suçunun işlenmesi gerekir. Ancak bu noktada suçun mağdurunun kim olduğunun belirlenmesi önem arz etmektedir. Zira suçun mağduru kart hamili kabul edildiğinde bir hamilin kullanımında olan farklı bankalara ait kartların kullanılması durumunda da zincirleme suç hükümleri uygulanacaktır. Suçun mağduru banka kabul edildiğinde ise bu kez aynı bankaya ait farklı hamiller adına çıkarılmış kartların kullanımı zincirleme suç hükümleri kapsamında sayılacaktır.

Yargıtay henüz hamiline teslim edilmemiş kartların mağdurunun banka olduğunu kabul etmekte ve farklı kişiler adına çıkarılmış olsa da aynı bankaya ait bu tarz kartların kullanılması durumunda zincirleme suç hükümlerinin uygulanmasına hükmetmektedir²⁹⁴. Kartların hamiline teslim edilmiş olması durumunda ise bu kez mağduru kart hamili kabul etmekte ve zincirleme suç hükümlerini bu şekilde uygulamaktadır²⁹⁵.

Eylemin hem TCK 245/1. maddesini hem de 244/4. maddesini ihlal etmesi durumunda faille yalnızca başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçundan ceza verilmelidir. Zira 244/4. maddede düzenlenen suç tali niteliktedir. Failin bu suçtan cezalandırılabilmesi için hareketinin başka bir suç oluşturmaması gerekir.

Failin mağduru, kendisine ait olan bir banka kartını ya da kredi kartını kullanmaya zorlayarak fail ya da bir başkası lehine yarar elde etmesi durumunda fail başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçundan değil yağma suçundan cezalandırılmalıdır. Burada fail söz konusu kart kullandırtma fiilini işlemektedir ancak başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunun oluşması için failin, bir başka kişiye ait kartı kullandırtması gerekmektedir. Oysa burada fail mağdura, mağdurun kendisine ait olan bir kartı kullandırtmıştır. Burada mağdur “*kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden ya da malvarlığı itibarıyla büyük bir zarara uğratacağından bahisle tehdit ederek veya cebir kullanılarak*” fail lehine yarar sağlamaktadır²⁹⁶. Ancak failin bir kimseye yönelik olarak söz konusu cebir ve tehdit fiillerini işleyerek bu kişiyi üçüncü bir kimseye ait olan banka kartını ya da kredi kartını kullanmaya zorlarsa burada başkasına ait

²⁹⁴ “...Oluşa ve tüm dosya kapsamına göre; sanığın Kargonet A.Ş isimli dağıtım kargo firmasında kurye olarak çalıştığı, mağdur Garanti Bankası A.Ş tarafından katılanlara gönderilen kredi kartlarını teslim etmeyerek katılanların bilgisi ve rızası dışında bu kartlarla şifresiz nakit çekim işlemleri gerçekleştirdiği şeklindeki eylemleri bakımından; sanığın aynı suç işleme kararının icrası kapsamında farklı zamanlarda mağdur Garanti Bankası A.Ş’ye yönelik başkasına ait banka veya kredi kartının izinsiz kullanılması suretiyle yarar sağlama suçunu işlediğinin anlaşılması karşısında; sanık hakkında tek bir 5237 sayılı TCK’nın 245/1. maddesinden kurulan hükümde TCK’nın 43/1 maddesi gereğince zincirleme suç hükümleri uygulanarak verilecek cezadan artırım yapılması gerekirken, katılan sayısınca ceza verilmesi suretiyle yazılı şekilde fazla ceza tayini...” (Yargıtay 8. Ceza Dairesi 27.10.2020 tarih, 2020/6266 E - 2020/17557K – UYAP’tan alınmıştır.), “...Banka ya da finans kuruluşları tarafından üretilen, banka veya kredi kartlarının ya da kart bilgilerinin, kartın hamile tesliminden önce ele geçirilerek menfaat temin edilmesi halinde, suçun mağduru ilgili banka olması...” (Yargıtay 8. Ceza Dairesi, 18.01.2016 tarih 2015/14822E - 2016/441K – UYAP’tan alınmıştır.)

²⁹⁵ “...5237 sayılı Türk Ceza Kanunu’nun 245/1. maddesinde düzenlenen banka veya kredi kartının kötüye kullanılması suçunun mağduru kart sahibi olup, başkalarına ait kredi kartlarını kötüye kullanmak suçundan doğrudan zarar görmeyen Efes Varlık Yönetim A.Ş.’nin davaya katılma hakkı bulunmadığından katılan vekilinin temyiz isteminin CMUK’nın 317. maddesi gereğince REDDİNE...” (Yargıtay 8. Ceza Dairesi 15.06.2020 tarih, 2019/24444 E - 2020/13331K – UYAP’tan alınmıştır.)

²⁹⁶ AKBULUT, s. 290.

banka veya kredi kartlarını kullanarak yarar sağlama suçu oluşacaktır. Fail, dolaylı fail olarak sorumlu tutulacak; kartı kullanması için zorlanan kimse ise suça konu eylemi özgür iradesi ile gerçekleştirmemiş olduğundan eyleminden sorumlu tutulamayacaktır.

Aynı mağdura ait banka veya kredi kartının farklı zamanlarda ve birden fazla kez kullanılması durumuna fail zincirleme suç hükümlerine göre sorumlu tutulacaktır.²⁹⁷ Aynı bankaya ait olsa bile farklı hamillerin kullanımında olan banka kartlarının kullanılması durumunda zincirleme suç hükümleri uygulanamaz.²⁹⁸

Kartın hamili hileli davranışlarla aldatılarak kendisine ait banka ve kredi kartlarını kullanmak suretiyle fail lehine yarar sağlarsa bu durumda dolandırıcılık suçu gündeme gelecek ve fail başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçundan sorumlu tutulmayacaktır²⁹⁹. Ancak failin, mağduru aldatarak banka ve kredi kartını alması daha sonra kendisinin kullanması ya da başkasına kullandırması durumunda başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçu da gündeme gelecek, sorun içtima hükümleri kapsamında çözülecektir.

Başkasına bir banka veya kredi kartının hırsızlık suretiyle ele geçirilmesi ve sonrasında kullanılarak ya da kullandırılarak yarar sağlanması durumunda başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunun yanı sıra hırsızlık suçu da oluşacaktır. Doktrinde de hem bu suç için hem de kartın ele geçiriliş şekline ilişkin olabilecek yağma, güveni kötüye kullanma dolandırıcılık gibi diğer suçlar için ayrı ayrı ceza verilmesi gerektiği savunulmaktadır³⁰⁰. Öte yandan doktrinde bu durumda tüketen norm-tüketilen norm ilişkisinin bulunduğunu belirterek failin yalnızca 245/1 maddesinden cezalandırılması gerektiği yönünde görüşler de mevcuttur³⁰¹. Yargıtay uygulamasında ise kartın ele geçiriliş biçiminin bir başka suç oluşturmaması durumunda bu suçtan ayrıca ceza verilmektedir³⁰². Biz de bu durumda gerçek içtima uygulanması gerektiği görüşündeyiz.

²⁹⁷ “Müştekilerin mail adreslerine bankalardan gönderilmiş gibi kredi kartı başvuru formları gönderip, müşteri kart hamilleri tarafından bu formlar doldurularak kart ve kişisel bilgilerinin paylaşılması üzerine faillerce kredi kartlarından internet siteleri üzerinden alışverişler yapılması şeklindeki eylemlerin TCK.nun 245/1. madde ve fıkrasında düzenlenen başkasına ait banka veya kredi kartlarının kötüye kullanılması suçunu oluşturduğu, birden fazla ve farklı zamanlarda harcama olması halinde TCK.nun 43/1.madde ve fıkrasının uygulanması gerektiği...” (Yargıtay 8. Ceza Dairesi, 25.02.2019 tarih 2017/20222 E - 2019/2585 K – UYAP’tan alınmıştır.)

²⁹⁸ “TCK.nun 245/1. maddesinde düzenlenen suçun mağdurunun kredi veya banka kartı sahibi kişi olduğu gözetilerek mağdur sayısınca uygulama yapılması gerektiği gözetilmeden yazılı şekilde teselsül hükümleri uygulanarak 1 kez TCK.nun 245/1, 43. maddeleri uyarınca uygulama yapılması” Yargıtay 8. Ceza Dairesi, 15.12.2016 tarih, 2016/3559 E- 2016/11448 K – UYAP’tan alınmıştır.)

²⁹⁹ AKBULUT, s. 290.

³⁰⁰ ÖZBEK/DOĞAN/BACAŞIZ/TEPE, s. 1017-1018; KOCA/ÜZÜLMEZ, s. 899-902; AKBULUT, s.301.

³⁰¹ TEZCAN/ERDEM/ÖNOK, s. 1081.

³⁰² “...TCK'nın 245. maddesinde düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun yasadaki düzenleniş şekli göz önüne alındığında bileşik suç olarak düzenlenmediği, banka veya kredi kartının hukuka aykırı olarak ele geçirilmesi durumunda oluşabilecek hırsızlık, yağma, güveni kötüye kullanma, dolandırıcılık gibi suçlar ile banka veya kredi kartlarını kötüye kullanma suçu arasında gerçek içtima kuralı uygulanarak failin her bir suçtan ayrı ayrı cezalandırılabilmesi, yasa maddesinde geçen “her ne surette olursa olsun” ifadesi banka veya kredi kartlarının sadece hukuka uygun yollardan ele geçirilmesini kapsadığı, bunun sonucu olarak somut olay incelendiğinde; sanığın yardımcı olmak bahanesiyle katılanın banka kartını alıp şifresini öğrendikten sonra hesapta para olmadığını söyleyip katılana kendi kartı yerine

Yukarıda internet bankacılığı kullanılarak yarar sağlama eylemlerinin başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunu değil hırsızlık suçunu oluşturduğunu ifade etmiştik. Başkasına ait banka kartlarının ya da kredi kartlarının numaralarının ele geçirilerek yarar sağlanması durumunda ise hem kişisel verilerin ele geçirilmesi suçundan hem de başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçundan hüküm kurulmalıdır. Doktrinde de bu yönde görüşler bulunmaktadır ³⁰³.

Kart hamili, gerçek durum öyle olmaksızın kartı kaybettiğini kartı çıkartan banka veya finans kurumuna bildirir ve kartın kullanıma kapatılmasına kadar geçen sürede kartı kullanır ya da bir başkasına kullandırtırsa kartın başkasına ait olması şartı gerçekleşmediği için nitelikli dolandırıcılık suçu oluşur³⁰⁴. Fail başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçundan sorumlu olmaz.

Başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunun işlenebilmesi amacıyla bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa sunulması, satın alınması ya da başkalarına verilmesi veya bulundurulması durumunda bu fiilleri işleyen fail TCK 245/A maddesinden de sorumlu tutulur. Bu fiilleri işleyen fail ayrıca başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunu da işlerse her iki fiilden ayrı ayrı cezalandırılacaktır.

2.5.2.6. Şahsi Cezasızlık Sebebi

TCK'nın 245. maddesinin 4. fıkrasında bu suçun, haklarında ayrılık kararı verilmemiş eş zararına, üstsoy ya da altsoyunun ile bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın zararına ya da aynı konutta beraber yaşayan kardeşlerden birinin, zararına işlenmesi durumunda, fail hakkında cezaya hüküm olunmayacağına ilişkin düzenleme yapılarak suçun faili ile mağduru arasında belirtilen derecede akrabalık bağı olması durumunda ceza verilmemesini sağlayan bir düzenlemeye yer verilmiştir. Bu düzenleme yağma ve nitelikli yağma hariç malvarlığına ilişkin suçlarda söz konusu olan TCK 167/1. maddesinin aynısıdır.

TCK'nın 245/1. maddesinde düzenlenen suç 4. fıkarda sayılı olan kişiler tarafından işlendiğinde yine suç oluşacak ancak bu kimseler şahsi cezasızlık sebebi dolayısıyla cezalandırılmayacaktır. Söz konusu suçun bu fıkarda sayılı kişilerle iştirak halinde bulunan kimseler tarafından işlenmesi durumunda ise bu kimseler şahsi cezasızlık sebebinden yararlanamayacaktır.

katılanın yaşlı olması ve gözlerinin iyi görmemesinden yararlanıp el çabukluğu ile başka bir şahsa ait banka kartını verdiği ve katılan uzaklaştıktan sonra katılana ait kart ile ATM'den para çektiğinin anlaşılması karşısında, sanığın katılana ait banka kartını katılanın rızasına aykırı olarak elinde tutmuş olması, ekonomik değeri bulunduğu konusunda kuşku bulunmayan menkul mal niteliğindeki banka kartı ile başka bir ATM cihazına gidip para çekmesi şeklinde gerçekleştirdiği eylemlerinde banka veya kredi kartının kötüye kullanılması suçu yanında hırsızlık suçu da oluşacağı gözetilmeyip sanığın TCK'nın 141/1. maddesinde düzenlenen hırsızlık suçundan mahkumiyeti yerine, yazılı şekilde dolandırıcılık suçundan beraatine karar verilmesi..." (Yargıtay 15. Ceza Dairesi, 30/10/2018 Tarih, 2015/13009 E, 2018/7317 K – UYAP'tan alınmıştır.)

³⁰³ AKBULUT, s.301-302.

³⁰⁴ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.370.

Söz konusu suçun birden fazla mağdurunun olması ve failin yalnızca mağdurlardan biriyle fıkra da şahsi cezasızlık sebebi olarak belirtilen kapsamda akrabalık ilişkisinin bulunması durumunda fail şahsi cezasızlık sebebinden yararlanamayacak, cezalandırılacaktır.

Maddede haklarında ayrılık kararı verilmemiş eşler sayıldığına göre boşanmış durumda olan kimseler arasında bu suçun işlenmesi durumunda şahsi cezasızlık sebebi uygulanmayacaktır. Ancak fiilen ayrı yaşasalar hatta aralarında boşanma davası bulunsa dahi haklarında ayrılık kararı verilmemiş eşler açısından bu şahsi cezasızlık sebebi uygulama alanı bulacaktır. Öte yandan bu fıkra açısından şahsi cezasızlık sebebinin oluşabilmesi için eş olma durumunun resmi olarak bulunması gerekir. Nikâhsız birliktelikler ya da resmi nikâh olmayan evlilikler bu madde kapsamında şahsi cezasızlık sebebi olarak değerlendirilemez.

4. fıkranın b bendi açısından hısımlığın kaçınıcı dereceden olduğunun önemi yoktur. Birkaç kuşak önce ya da sonra olması bu bent açısından bir fark teşkil etmez.

Evlilik sona erdikten sonra da kayın hısımlığı açısından şahsi cezasızlık sebebinin bulunup bulunmadığı hususu tartışmalıdır. Kayın hısımlığını düzenleyen Türk Medeni Kanunu'nun 18. maddesine göre bir eşin kan hısımları ile diğer eş aynı dereceden ve aynı türden kayın hısımları olurlar. Hatta bu hısımlık söz konusu evlilik sona ermiş olsa dahi varlığını korur. Bu madde göz önüne alındığında kendisini meydana getiren evlilik sona ermiş olsa bile şahsi cezasızlık sebebinin uygulanması gerekir. Doktrinde de benzer yönde görüşler mevcuttur³⁰⁵. Öte yandan aksi yönde görüş belirten yazarlar da vardır.

Suçun evlat edinilen tarafından evlat edinenin zararına olarak ya da evlat edinen tarafından evlat edinilenin zararına işlenmesi durumunda fail şahsi cezasızlık sebebinden yararlanacaktır.

Kardeşler arasında şahsi cezasızlık sebebinin uygulanabilmesi için ise bu kardeşlerin aynı konutta beraber yaşıyor olması şartı aranmıştır.

Doktrinde kayın hısımları bakımından aynı konutta yaşama gibi bir şart bulunmazken daha yakın olan kardeşler arasında böyle bir şart aranması eleştirilmiştir³⁰⁶.

Fail aralarında şahsi cezasızlık sebebinin olduğunu sanarak bu fiili işlerse hatasından yararlanır. Örneğin annesinin zannederek başka bir kişinin kartını kullanan fail TCK 245/1. maddesinden sorumlu olmayacaktır.

Fail ile suçun zararına işlendiği kişi arasında şahsi cezasızlık sebebi varsa fail bunu bilmeseyse bile bu durumdan faydalanır. Örneğin başkasına ait olduğunu zannederek dedesine ait olan kartı kullanan kişi bu hatasından yararlanacaktır.

2.5.2.7. Etkin Pişmanlık

TCK'nın 245. maddesinin son fıkrasında “*Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır*” denilmek suretiyle 245/1. maddede düzenlenen suça ilişkin etkin pişmanlık hükmüne yer

³⁰⁵ TEZCAN/ERDEM/ÖNOK, s. 871.

³⁰⁶ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.361.

verilmiştir. Maddenin ilk halinde olmayan bu fıkra 6.12.2006 tarihinde yapılan değişiklikle maddeye eklenmiştir.

Bu fıkranın yollama yaptığı TCK 168. maddesi “(1) *Hırsızlık, mala zarar verme, güveni kötüye kullanma, dolandırıcılık, hileli iflâs, taksirli iflâs suçları tamamlandıktan sonra ve fakat bu nedenle hakkında kovuşturma başlamadan önce, failin, azmettirenin veya yardım edenin bizzat pişmanlık göstererek mağdurun uğradığı zararı aynen geri verme veya tazmin suretiyle tamamen gidermesi halinde, verilecek cezanın üçte ikisine kadar indirilir.*(2) *Etkin pişmanlığın kovuşturma başladıktan sonra ve fakat hüküm verilmezden önce gösterilmesi halinde, verilecek cezanın yarısına kadar indirilir.* (3) *Yağma suçundan dolayı etkin pişmanlık gösteren kişiye verilecek cezanın, birinci fıkraya giren hallerde yarısına, ikinci fıkraya giren hallerde üçte birine kadar indirilir.* (4) *Kısmen geri verme veya tazmin halinde etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır.*(5) *Karşılıksız yararlanma suçunda, fail, azmettiren veya yardım edenin pişmanlık göstererek mağdurun, kamunun veya özel hukuk tüzel kişisinin uğradığı zararı, soruşturma tamamlanmadan önce tamamen tazmin etmesi halinde kamu davası açılmaz; zararın hüküm verilinceye kadar tamamen tazmin edilmesi halinde ise, verilecek ceza üçte birine kadar indirilir. Ancak kişi, bu fıkra hükmünden iki defadan fazla yararlanamaz.”* şeklindedir.

Yollama dolayısıyla TCK’nın 245/1. maddesinde düzenlenen suçu işleyen fail, azmettiren ya da yardım eden suç tamamlandıktan fakat bu nedenle hakkında kovuşturma başlamadan önce bizzat pişmanlık gösterir ve mağdurun uğradığı zararı aynı geri vererek ya da tazmin suretiyle giderirse verilecek ceza üçte ikisine kadar indirilecektir. Kovuşturma başladıktan sonra henüz hüküm verilmemişken pişmanlık gösterip zararı gideren failin, azmettirenin ya da yardım edenin cezası ise yarı oranında indirilecektir.

Etkin pişmanlık koşullarının varlığı halinde cezanın indirilmesi zorunludur, bu durum hâkimin takdirine bırakılmamıştır.

Failin, azmettirenin ya da yardım edenin etkin pişmanlık hükmünden yararlanabilmesi için bizzat pişmanlık göstererek zararı gidermesi gerekir. Fail başkası tarafından zorlandığı için zararı giderirse etkin pişmanlık söz konusu olmayacaktır. Ancak zararın bizzat fail tarafından giderilmesi gerekmez. Fail pişmanlık gösterdikten sonra fail adına bir yakını da bu zararı giderebilir. Bu durumda da fail etkin pişmanlık hükmünden yararlanacaktır.

Zararın kısmen giderilmesi halinde ise etkin pişmanlık hükümlerinin uygulanabilmesi için, ayrıca mağdurun rızası aranır. Mağdur etkin pişmanlık hükümlerinin uygulanmasını kabul ederse zararı kısmen gidermiş olan fail, azmettiren ya da yardım eden etkin pişmanlık hükmünden yararlanır.

Etkin pişmanlık hükümlerinden yararlanılabilmesi için pişmanlığın bizzat gösterilmesi gerekir. Bu sebeple zararın suç ortaklarından yalnızca biri tarafından giderilmesi durumunda diğer suç ortakları etkin pişmanlık hükmünden yararlanmayacaktır. Birden çok suç ortağından her biri zararın tamamının giderilmesi hususunda çaba gösterdiyse etkin pişmanlık hükümlerinden hepsi yararlanır. Ancak zararın giderilmesi hususunda çaba göstermeyen suç ortakları etkin pişmanlıktan yararlanamaz.

2.5.2.8. Soruşturma Usulü ve Yaptırım

Başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunun cezası üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. Bu suçu işleyen faile hem hapis cezası hem de adli para cezası verilecektir, yaptırımlar seçimlik değildir. Adli para cezasının alt sınırı TCK'nın 52. maddesi gereğince 5 gündür.

Bu suçun yaptırımının 142/2-e maddesi için öngörülen yaptırım karşısında düşük kalması ceza adaleti açısından sıkıntı yaratmaktadır. Hırsızlık suçunda fail yalnızca mağdurun malvarlığına yönelik bir saldırıda bulunurken banka ve kredi kartlarının kullanması durumunda mağdurun malvarlığının yanı sıra banka ve kredi kartlarına duyulan güveni de zedelemiş olacak, buna rağmen daha az alacaktır. Bu husustaki sorunun giderilmesi için 245/1. maddesinde düzenlenen suçun cezasının arttırılması gerektiği görüşündeyiz.

TCK'nın 245. maddesinin ilk fıkrasında düzenlenen bu suç re'sen soruşturulur.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

CMK'nın 171. maddesi ile etkin pişmanlık hükümlerinin ya da şahsi cezasızlık sebeplerinin varlığı halinde Cumhuriyet savcısına kovuşturmaya yer olmadığı kararı verebilme imkanı tanınmıştır. TCK'nın 245/4. maddesinde de 245/1. maddede tanımlanan suç için şahsi cezasızlık sebebi düzenlenmiştir. Olayda şahsi cezasızlık sebebi varsa Cumhuriyet savcısı dava açıp açmamak hususunda takdir yetkisine sahip olacaktır.

TCK'nın 246. maddesinde bilişim alanında suçların işlenmesi sonucu *haksız bir menfaat* elde eden tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir. Dolayısıyla TCK 245/1. maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

2.5.3. Sahte Banka Veya Kredi Kartı Üretmek, Satmak, Devretmek, Satın Almak veya Kabul Etmek Suçu

2.5.3.1. Korunan Hukuki Değer

TCK'nın 245. maddesinin gerekçesinde 245. maddede yer alan suçların esasen hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının tümünün konuluş amaçlarını da içerdiği ve bu fiillerin işlenmesi dolayısıyla yaşanan duraksamaların ve içtihat farklılıklarının önüne geçilebilmesi maksadıyla bağımsız suç hâline getirildikleri belirtilerek 245. maddede tanımlanan suçların söz konusu maddede sayılan suçların özel bir görünümü oldukları vurgulanmıştır. 245. maddenin ikinci fıkrasında düzenlenen suç ise daha çok sahtecilik suçunun özel bir görünümü niteliğindedir³⁰⁷. Bu düzenleme yapılmadan önce Yargıtay kredi kartları konusundaki sahtecilik fiillerini özel belgede sahtecilik olarak

³⁰⁷ SOYASLAN, Ceza Hukuku Özel Hükümler, s. 683.

kabul ediyor ancak bu durum kanunilik ilkesine aykırı olduğu gerekçesi ile eleştiriliyordu³⁰⁸.

Bu suç ile korunan hukuki değer ise banka ve kredi kartlarının güvenilirliğinin korunmasıdır.

2.5.3.2. Maddi Unsurlar

2.5.3.2.1. Fiil

Bu suçun oluşması açısından söz konusu hareketler sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmektir. Bu hareketler seçimlik olarak belirtilmiş olup bunlardan yalnızca birinin yapılmasıyla dahi suç oluşacaktır. Bu hareketlerden bir kaçının yapılması durumunda da tek fiil olacaktır. Ancak bunun için bu hareketlerin konusu olan sahte banka ve kredi kartlarının aynı kartlar olması gerekir. Örneğin failin bir sahte kredi kartını başka bir hesapla ilişkilendirerek üretmesi ardından da bu kartı devretmesi durumunda iki seçimlik hareket gerçekleşmiş olmasına rağmen tek suç oluşacak fakat bu hareketlerin fazlalığı cezanın belirlenmesinde göz önüne alınacaktır. Fail bir kredi kartını üretilip bir başkasın ürettiği başka bir kredi kartını da satın alırsa bu durumda iki farklı suç konusu var olduğundan iki ayrı suç olduğu kabul edilecek ve faile her iki hareketinden dolayı ayrı ayrı ceza verilecektir.

Banka veya kredi kartı dışında başka bir kartın sahte olarak üretilmesi durumunda bu suç oluşmaz.

Sahte banka veya kredi kartı üretilmesi için bir kartın tamamen sahte olarak üretilmiş olması gerekmez. Var olan bir banka veya kredi kartında değişiklik yapılarak bu kart sahte kart haline de getirilebilir³⁰⁹.

Bu suçta sebebiyet verebilecek tüm hareketler madde metninde sayılmıştır. Bu sebeple bu suç bağlı hareketli bir suçtur³¹⁰.

Sahte belgelerle banka veya finans kurumuna başvurularak kart çıkarılması halinde de 245/2. maddede düzenlenen suç oluşur³¹¹. Ancak bu kart çıkarılmadan durumun anlaşılması halinde 245/2. maddeye teşebbüsten değil Banka Kartları ve Kredi Kartları Kanunu'nun 37/2. maddesinde düzenlenen "*Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler.*" hükmünden sorumlu

³⁰⁸ TEZCAN/ERDEM/ÖNOK, s. 1075.

³⁰⁹ SOYASLAN, Ceza Hukuku Özel Hükümler, s. 683; AKBULUT, s.318, TEZCAN/ERDEM/ÖNOK, s.1076.

³¹⁰ ERDOĞAN, s. 334; DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.385.

³¹¹ "...Kabul ve uygulamaya göre de; başkasına ait aslı ele geçmeyen sürücü belgesi ve nüfus cüzdan fotokopileriyle bankalara başvurup sahte kredi kartı sözleşmeleri düzenleterek üretilen sahte kartları teslim almak şeklindeki eylemlerin mağdur banka sayısınca, küll halinde TCK.nun 245/2 ve 43. maddelerindeki suçu oluşturduğu ve başkasına ait kimlik belgeleriyle düzenlenen sahte kredi kartlarına ait sözleşmelerin de TCK.nun 245/2. maddesi kapsamında değerlendirilmesi gerektiği gözetilmeden yazılı şekilde hükümler kurulması suretiyle fazla ceza tayini..." (Yargıtay 8. Ceza Dairesi, 12.11.2018 Tarih, 2018/5486 E, 2018/12580 K – UYAP'tan alınmıştır.)

tutulurlar. Yargıtay da bu görüştedir³¹². Ancak doktrinde sahte belgelerle başvuru yapılarak kartın üretilmesinin sağlanması durumunda da 245/2. maddesinde düzenlenen suçun oluşmayacağını zira bu durumda üretilen kartın sahte bir kart olmadığı yönünde görüşler mevcuttur³¹³. Bazı yazarlar ise sahte belge ibraz etmek suretiyle kart çıkarılması durumunda failin belgenin niteliğine göre özel veya resmi belgede sahtecilik suçundan, ayrıca 245/2. maddede düzenlenen suçtan sorumlu tutulması gerektiğini belirtmektedir³¹⁴. Benzer görüşte olan başka yazarlar ise belgenin resmi belge olması halinde failin hem resmi belgede sahtecilik suçundan hem de 245/2. maddeden, belgenin özel belge olması durumunda ise yalnızca 245/2. maddeden ceza verilmesi gerektiğini savunmaktadır³¹⁵. Gerçekten de TCK'nın içtima başlıklı 212. maddesinde "*Sahte resmi veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması halinde, hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunur.*" denilmiştir. Dolayısıyla failin sahte belgelerle banka veya finans kurumuna başvurarak kart çıkartması halinde gerçek içtima hükümlerinin uygulanması kanuni bir zorunluluktur.

Doktrinde sanal kartın oluşturulması durumunda da bu suçun oluşacağı ifade edilmektedir³¹⁶. Ancak sanal kartlar genellikle internet bankacılığı kullanılarak üretilmektedir. Fail, mağdurun internet bankacılığını kullanarak bir sanal kart oluşturduğu durumda bu kartın sahte bir kart olup olmadığı iyi değerlendirilmelidir. Bu durumda fail önce mağdura ait internet bankacılığı şifrelerini ele geçirerek kişisel verilerin ele geçirilmesi suçunu işlemiş sonra da sisteme girerek sanal kartlar oluşturmuştur. Bu kartlar henüz kullanılmadığından 244. maddenin 2. ve 3. fıkraları ile 245/2. madde değerlendirilmelidir. Bu kartların kullanılarak yarar sağlanması durumunda ise suç 244/4. ya da 245/3. maddelerde düzenlenen suç olacaktır.

Satmak, sözlükte bir malın bedeli karşılığında alıcıya verilmesi olarak tanımlanmaktadır³¹⁷. Öyle ise bir değer karşılığında sahte banka veya kredi kartının alıcıya verilmesiyle de bu suç oluşur. Satın almak ise, bir mal için belirlenmiş olan bedeli ödeyerek edinmek, mubayaa etmektir³¹⁸. Satmak ve satın almak fiilleri karşılıklı olarak yapılır. Bu durumda hem kartı satan fail hem de satın alan fail ayrı ayrı cezalandırılacaktır.

³¹² "...Sanığın, katılan Yılmaz Yayar adına, bilgisi ve rızası olmaksızın sahte kredi kartı sözleşmesi düzenlediğinin ve üretilen kredi kartını kullandığının iddia edildiği olayda; Finansbank tarafından gönderilen kredi kartına ait 19/12/2011 tarihli kredi kartı sözleşmesini imzalaması eylemi yönünden; 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 37/2. maddesinde yer alan "kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler" şeklindeki düzenlemenin sözleşmenin imzalanmasını da kapsayacak aşamaya kadar uygulanabileceği, kredi kartı sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde 5237 sayılı TCK'nın 245/2. maddesinin, sahte üretilen bu kartın kullanılarak menfaat temin edilmesi halinde ise 245/3. maddesine temas eden suçu oluşturacağı..." (Yargıtay 11. Ceza Dairesi, 14.09.2020 tarih 2018/3105 E - 2020/4396K – UYAP'tan alınmıştır.)

³¹³ SOYASLAN, Ceza Hukuku Özel Hükümler, s. 683-684;

³¹⁴ AKBULUT, s. 321-323.

³¹⁵ GÜL, s. 158-162.

³¹⁶ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s. 386; GÜL, s. 156.

³¹⁷ <https://sozluk.gov.tr>, E.T. 09.03.2020.

³¹⁸ <https://sozluk.gov.tr/>, E.T. 09.03.2020.

Devretmek ise bir malın mülkiyetini, bir mal üzerindeki hakkı başkasına geçirmek anlamına gelir³¹⁹. Devretmek fiili bir bedel olmaksızın kartın mülkiyetinin başkasına geçirilmesi şeklinde olur. Kabul etmek, bir armağanı almak demektir³²⁰. Fail burada bir bedel ödemeksizin kendisine armağan edilen bir kartı kabul etmektedir. Devretmek ve kabul etmek fiilleri de karşılıklı olarak yapılan fiiller olup kartı devreden ve kabul eden faillerin her ikisi de cezalandırılacaktır.

2.5.3.2.2. Fail

TCK'nın 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçunda fail açısından özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun faili herkes olabilir. Bu suçun failinin belirli bir konuda uzman olan bir kime olmasına gerek yoktur.

Fıkarda sayılan fiillerden satmak-satın almak, devretmek-kabul etmek gibi fiiller çok failli suç niteliği taşımaktadır³²¹. Bu fiillerin gerçekleşmesi durumunda hareketin iki tarafı da bu suçu işlemiş olacaktır.

2.5.3.2.3. Mağdur

Sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu özel bir sahtecilik suçu niteliğindedir. Sahtecilik suçları ise topluma karşı işlenen suçlardır. Dolayısıyla bu suç da topluma karşı işlenen bir suç niteliğinde olup suçun mağduru toplumu oluşturan herkeştir. Ancak unutulmamalıdır ki bu suçun oluşması için sahte kartların üretilmesi, satılması ya da satın alınması veya devredilmesi, kabul edilmesi gibi fiiller tek başına yeterli olmayıp suçun konusu sahte kartın başkalarına ait banka hesaplarıyla ilişkilendirilmesi gerekir. Söz konusu sahte kartların kullanılması durumunda ise bu suç değil 3. fıkradaki suç oluşacaktır. Dolayısıyla her ne kadar bu kartlar başkalarına ait hesaplarla ilişkilendirilse dahi hesap sahiplerinin bir zararı yoktur. Ancak kartı üreten banka ve finans kurumu kartlar kullanılmasa dahi zarara uğramıştır zira bu kartlar bankanın güvenilirliğini sarsmıştır. Dolayısıyla bu suçun mağduru banka ve finans kurumudur. Tüzel kişiler mağdur olamayacakları için suçtan zarar gören olarak kabul edilirler.

Doktrinde de suçun mağduru olarak banka ve finans kurumunu kabul eden yazarlar³²² olduğu gibi suçun mağduru olarak toplumu oluşturan herkesi kabul eden yazarlar da vardır³²³.

2.5.3.2.4. Konu

Bu suçun konusu başkalarına ait banka hesaplarıyla ilişkilendirilerek meydana getirilmiş sahte banka veya kredi kartlarıdır. Suç bu kartların üretilmesi, satılması, devredilmesi, satın alınması veya kabul edilmesi ile oluşur. Suçun oluşması için söz konusu fiillerin sahte

³¹⁹ <https://sozluk.gov.tr/>, E.T. 09.03.2020.

³²⁰ <https://sozluk.gov.tr/>, E.T. 09.03.2020.

³²¹ AKBULUT, s.314.

³²² ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1010; GÜL, s. 130.

³²³ AKBULUT, s. 314.

banka veya kredi kartları üzerinde işlenmesi yetmez, bu kartların başkalarına ait banka hesaplarıyla da ilişkilendirilmesi gerekir.

Başkalarının hesaplarıyla ilişkilendirilmeden oluşturulan banka veya kredi kartları üzerinde bu fiillerin işlenmesi durumunda TCK'nın 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu oluşmaz. Ancak başkalarına ait hesaplarla ilişkili olmasa da banka veya kredi kartları kullanılarak bir kişinin aldatılması yoluyla yarar sağlanması halinde dolandırıcılık suçu değerlendirilmelidir³²⁴.

2.5.3.2.5. Netice

Bu suçun gerçekleşmesi için herhangi bir neticenin meydana gelmesi aranmaz. Bir netice ya da zarar aranmadığı için bu suç soyut tehlike suçudur.

Bu suçun oluşması için netice aranmadığı için aynı zamanda sırf hareket suçudur³²⁵. Bu kartların kullanılması suretiyle yarar sağlanması durumunda artık 245/2 değil 245/3. maddede tanımlanan suç oluşacaktır.

2.5.3.3. Manevi Unsurlar

TCK'nın 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçu yalnızca kasten işlenebilen bir suçtur. Suçun taksirli şekline yer verilmemiştir. Suçun oluşması için failin fıkra da sayılı fiilleri bilerek işlemesi gerekir.

Suçun oluşması için herhangi bir amaç ya da saikle işlenmesi gerekmez. Failin amacı ya da saiki ne olursa olsun fıkra da sayılan fiilleri işlediği takdirde suç oluşacaktır.

Failin bu fiilleri bilerek işlemesi de aranmadığından suç olası kastla da işlenebilir³²⁶.

2.5.3.4. Hukuka Aykırılık

Bu suça ilişkin olarak herhangi bir hukuka uygunluk sebebi bulunmamaktadır.

2.5.3.5. Suçun Özel Görünüş Biçimleri

2.5.3.5.1. Teşebbüs

Failin suç tipinde belirtilen fiilleri yapmaya başlaması ancak elinde olmayan sebeplerle bu hareketi tamamlayamaması durumunda suç teşebbüs aşamasında kalmış olacaktır³²⁷.

³²⁴ KOCA/ÜZÜLMEZ, s. 907; AKBULUT, s. 316.

³²⁵ AKBULUT, s. 317.

³²⁶ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1023; AKBULUT, s. 324.

³²⁷ "...Sanıklara yüklenen sahte kart üretmeye teşebbüs suçunda, sanıkların 09.03.2013 günü saat 16.46'da Yapı ve Kredi bankası Bayramyeri şubesine ait ATM' ye kart kopyalama aparatını yerleştirdikleri, daha sonra saat 20.35' te sanık Veysel'in gelerek aparatı söktüğü ve montuna sakladığı, uzaklaşacakları sırada takipte bulunan emniyet güçleri tarafından durdurulmak istendiğinde kaçtıkları daha sonra yakalandıklarında sanık Veysel'de üzerinde 8 GB'lık hafıza kartı takılı ATM giriş haznesi, diğerinin üzerinde kart okuyucu ele geçtiği, bu materyaller üzerinde inceleme yapan bilirkişinin raporunda ATM'de işlem yapanların görüntüleri ile kart bilgilerine rastlandığının anlaşılması ve henüz kart üretildiğine veya üretilmeye teşebbüs edildiğine ilişkin dosyada delil bulunmaması karşısında, eylemlerinin TCK'nun 136, 43. maddelerinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek suçunu oluşturduğu gözetilmeden, suç vasfında yanılığa düşülerek yazılı şekilde aynı yasanın 245/2. ve 35. maddeleri uyarınca

Örneğin failin sahte kart satın almak için harekete geçmesi ancak hareket tamamlanmadan yakalanması durumunda suç teşebbüs aşamasında kalmış kabul edilecektir.

Bu suç soyut tehlike suçu olduğundan bir neticenin de gerçekleşmesi aranmaz. Dolayısıyla failin kartı yalnızca satın alması ya da devralması suçun tamamlanması için yeterlidir. Failin ayrıca bu kartı kullanması gerekmez. Kaldı ki kartın kullanılması durumunda bu suç değil 245/3. maddede düzenlenen suç oluşacaktır.

2.5.3.5.2. İştirak

Bu suçla ilişkin olarak tüm iştirak hallerinin gerçekleşmesi mümkündür.

Bir failin kart satması bir başka failin de bu kartı satın alması durumunda her iki fail de ayrı ayrı bu suçu işlemiş olacak, aralarında bir şeriklik durumundan söz edilemeyecektir. Ancak faillerden birinin bu kartları üretmesi bir başka failin de bu kartların satışını yapması durumunda müşterek faillik söz konusu olacaktır.³²⁸

Bir kimsenin faili bu suçu işlemeye azmettirmesi ya da suçun işlenmesine yardım etmesi mümkündür.

Failin bu suçun işlenmesinde bir başkasını araç olarak kullanması durumunda dolaylı faillik söz konusu olacaktır.

Sahte banka veya kredi kartlarının üretilmesi fiili bir cihazın kullanımı suretiyle olabilir. Böyle bir durumun varlığı halinde bu cihazı faile sağlayan kişi bu suç açısından yardım eden konumunda olacaktır. Ancak aynı fiil 245/A maddesinde de düzenlenmiştir ve bu suçun yardım edeni olan kişi 245/A maddesi açısından fail kabul edilecektir. Dolayısıyla bu durumda bu kişi yardım eden değil, 245/A maddesinin faili olarak cezalandırılmalıdır.³²⁹

2.5.3.5.3. İctima

Failin farklı zamanlarda TCK'nın 245/2. maddesinde tanımlı fiilleri işlemesi durumunda zincirleme suç hükümleri gündeme gelecektir. Failin aynı anda ya da kısa aralıklarla söz konusu fiilleri işlemesi durumunda zincirleme suçtan söz edilmeyecek, tek bir suç gerçekleşmiş kabul edilecektir.

Failin kısa aralıklarla aynı bankaya ya da finans kurumuna ait birden fazla banka veya kredi kartını sahte olarak üretmesi durumunda zincirleme suç söz konusu olmayacak, tek bir suçtan dolayı sorumlu olacaktır.

Doktrinde bazı yazarlar suçun mağdurunu toplumu oluşturan herkes olarak kabul etmekte ve banka sayısınca suç oluştuğu kabulünü eleştirmektedir³³⁰. Bu yazarlara göre kartların aynı bankaya ya da farklı bankalara ait olmasının bir önemi yoktur. Kartların farklı zamanlarda üretilmesi durumunda zincirleme suç hükümleri uygulanmalıdır.

hükümler kurulması,...” (Yargıtay 8. Ceza Dairesi, 19.12.2018 Tarih, 2018/8124 E, 2018/14646 K – UYAP’tan alınmıştır.)

³²⁸ AKBULUT, s. 325.

³²⁹ AKBULUT, s.325.

³³⁰ AKBULUT, s. 326.

Fail bu suçu işlemek amacıyla TCK'nın 245/A maddesi kapsamında kalan fiilleri işler sonra da bu cihazı kullanarak 245. maddesinin 2. fıkrasındaki suçu işlerse her iki suçtan da ayrı ayrı cezalandırılmalıdır.

Fail 245/2. maddedeki suçu işleyerek elde ettiği kartı kullanarak bir yarar elde ederse hem 245/2. maddeden hem de 245/3. maddeden dolayı cezalandırılmalıdır³³¹. Zira fail 245/2. maddede tanımlanan fiilleri işledikten sonra bu kartları kullanarak yarar elde etmiştir. Bu durumda birden fazla hareket vardır. Oysa TCK'nın 44. maddesine göre fikri içtimaa hükmedilebilmesi için tek fiil ile birden fazla suçun işlenmesi gerekir. Öte yandan bazı yazarlar bu durumda yalnızca 245/3. maddeden dolayı cezalandırma yapılması gerektiğini savunmaktadır³³².

Failin ATM cihazlarına bir düzenek yerleştirerek kart sahiplerinin bilgilerini kopyalaması halinde TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme suçu oluşur. Bu bilgilerin kullanılması suretiyle ayrıca sahte banka veya kredi kartları üretilirse TCK'nın 244/2. maddesinde düzenlenen suç oluşur. Böyle bir durumda fail her iki suçtan ayrı ayrı cezalandırılır. Sahte olarak oluşturulan bu kartların kullanılması suretiyle menfaat temin edilmesi halinde ise TCK'nın 245/3. maddede düzenlenen suç oluşur.

Failin ATM cihazlarına bir düzenek yerleştirerek banka ve kredi kartı kullanıcılarının manyetik şerit bilgilerini ele geçirmeye çalışması ancak bu düzeneğin fark edilmesi dolayısıyla bilgileri ele geçirememesi durumunda yalnızca TCK'nın 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirme suçuna teşebbüsten cezalandırılır. Çünkü fail bu aşamada herhangi bir kopyalama faaliyetinde bulunmamış, yalnızca kişisel bilgileri ele geçirmeye çalışmıştır.³³³

Banka Kartları ve Kredi Kartları Kanunu'nun 38. maddesinin ilk fıkrası “*Bu Kanunun 4 üncü maddesinde belirtilen izinleri almaksızın kartlı sistem kuran, kredi kartı çıkaran veya üye işyeri anlaşması yapan veya ticaret unvanları, her türlü belgeleri, ilân ve reklamları veya kamuoyuna yaptıkları açıklamalarda bu işlerle uğraştıkları izlenimini yaratacak söz ve deyimleri kullanan gerçek kişiler ile tüzel kişilerin görevlileri bir yıldan üç yıla kadar hapis ve bin güne kadar adli para cezası ile cezalandırılırlar.*” şeklindedir. Bu maddede sahte kart üretilmesinden değil, izin alınmaksızın kart üretilmesinden söz edilmektedir. Bir kartın, kart çıkarmak için gerekli izinleri almaksızın üretilmiş olması sahte olması anlamına gelmez. Dolayısıyla izin alınmaksızın kart üretilmesi durumunda bu Kanunun 38/1. maddesinden cezalandırma yoluna gidilmelidir. Failin sahte banka veya kredi kartı üretmesi durumunda ise 245/2. maddeden cezalandırma yapılmalıdır.

³³¹ KOCA/ÜZÜLMEZ, s. 908; GÜL, s. 165; AKBULUT, s.326-327.

³³² TEZCAN/ERDEM/ÖNOK, s. 1080-1081.

³³³ “*sanığın bankanın ATM cihazlarına yerleştirdiği düzenekle, işlem yapmaya gelen kişilere ait kartların manyetik şerit bilgilerini kopyalamak ve şifrelerini elde etmeye çalışması halinde ise eyleminin TCK'nın 136, 35. ve 43/2. maddelerinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmeye teşebbüs suçunu oluşturacağı gözetilmeden eksik araştırmayla yazılı şekilde hüküm kurulması*” (Yargıtay 8. Ceza Dairesi, 27.10.2020 tarih 2019/23499 E - 2020/17559 K – UYAP'tan alınmıştır).

2.5.3.6. Soruşturma Usulü ve Yaptırım

TCK'nın 245/2. maddesinde düzenlenen sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek suçunun cezası üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezasıdır. Bu suçu işleyen faile hem hapis cezası hem de adli para cezası verilecektir, yaptırımlar seçimlik değildir. Adli para cezasının alt sınırı TCK'nın 52. maddesi gereğince 5 gündür.

TCK'nın 245. maddesinin 2. fıkrasında düzenlenen bu suç re'sen soruşturulur.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

TCK'nın 246. maddesinde bilişim alanında suçların işlenmesi neticesinde haksız bir yarar elde eden tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir. Dolayısıyla TCK 245/2. maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

2.5.4. Sahte Banka ve Kredi Kartlarını Kullanarak Yarar Sağlama Suçu

2.5.4.1. Korunan Hukuki Değer

Sahte banka ve kredi kartlarını kullanarak yarar sağlama suçu TCK'nın 245. maddesinin 3. fıkrasında düzenlenmiştir. Bu suçun meydana gelebilmesi için sahte oluşturulan veya üzerinde sahtecilik yapılan bir kart bulunmalı ve fail bu kartı kullanmak suretiyle kendisine veya başkasına yarar sağlamalıdır.

Bu suçla korunan hukuki değer hem malvarlığı hem de banka ve kredi kartlarına duyulan güvendir. Bu suç da tıpkı 245. maddenin ilk fıkrasında düzenlenen suçlar gibi malvarlığına karşı bir suçtur. Bu suçun işlenmesi ancak bir yarar sağlaması ile oluşur ve bu yararın karşılığı olarak mağdur bir zarara uğrar. Bu düzenleme ise, bu zararı önlemeyi amaçlar. Ayrıca bu suçun işlenmesi neticesinde kişilerin banka ve kredi kartlarına duydukları güven azalacaktır. Bu suç ile birlikte bu güven de koruma altına alınmıştır.

Doktrinde bu suçun malvarlığını³³⁴ ve banka ve kredi kartlarının doğruluğuna ilişkin güveni³³⁵ koruduğu ifade edilmektedir. Bazı yazarlar ise bu suçla hem malvarlığının hem de bilişim alanının güvenliğinin ve kamu güveninin korunduğunu ifade etmektedirler³³⁶.

2.5.4.2. Maddi Unsurlar

2.5.4.2.1. Fiil

TCK'nın 245. maddesinin 3. fıkrasında tanımlanan suç sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanması suretiyle gerçekleşir. Ancak bu yeterli değildir. Ayrıca yarar elde edilmesi gerekir. Hem söz konusu kartın kullanılması

³³⁴ AKBULUT, s. 330; DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 357-359.

³³⁵ KOCA/ÜZÜLMEZ, s. 909.

³³⁶ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1052.

hem de yarar elde edilmesi gerektiğinden bu suç çok hareketli bir suçtur. Failin bu kartı ne şekilde temin ettiğinin bir önemi yoktur. Fail bu kartı kendisi üretmiş, bir başkasından almış yahut tesadüf sonucunda ele geçirmiş olabilir. Önemli olan failin bu kartı kullanması ve bu suretle bir yarar elde etmesidir.

Bu kartın ne şekilde kullanılacağı ya da yararın ne şekilde elde edileceği hususunda bir sınırlama yoktur. Bu açıdan söz konusu suç serbest hareketli bir suçtur.

Failin bu suçun işlenmesinde kullandığı kart sahte olarak oluşturulmuş bir kart olabileceği gibi üzerinde sahtecilik yapılmış bir kart da olabilir. Üzerinde sahtecilik yapılmış kart deyiminden var olan, gerçek bir banka veya kredi kartının manyetik şeritlerinin değiştirilmesi, başka bir karta ait verilerin kopyalanması vb. yollarla oluşturulmuş kart anlaşılır.

245. maddenin 2. fıkrasından farklı olarak bu fıkra tanımlanan suç açısından söz konusu kartların gerçek bir hesapla ilişkilendirilmesi şart değildir. Tamamen hayali kişiler adına oluşturulmuş kart bilgilerinin kullanılması suretiyle de bu suç gerçekleştirilir.

Yararın bizzat fail tarafından elde edilmesi gerekmez. Fail kendisine yarar sağlayabileceği gibi bir başkasına da yarar sağlayabilir. Bu husus madde metninde de “*kendisine veya başkasına yarar sağlayan kişi*” denilerek ifade edilmiştir. Bu yararın mutlaka failin ya da yarar sağladığı üçüncü kişinin eline tamamen geçmiş olması gerekmez, önemli olan üzerinde hâkimiyet kurabilecek duruma gelmiş olmasıdır.

Sahte belgelerle banka ve finans kurumu başvurularak kart çıkarılıp kullanılması durumunda, bu kart gerçek bir kişinin hesabıyla ilişkilendirilerek çıkarıldıysa hem 245. maddenin 2. fıkrasındaki suç hem de 3. fıkrasındaki suç, bu kart hayali kişilerin bilgilerinin kullanıldığı belgelerle kart çıkartılıp kullanılması durumunda ise yalnızca 245. maddenin 3. fıkrasındaki suç oluşacaktır³³⁷.

2.5.4.2.2. Fail

TCK’nın 245/3. maddesinde düzenlenen sahte banka ve kredi kartlarını kullanarak yarar sağlama suçu için fail açısından özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun faili herkes olabilir.

Fail 245. maddenin 2. fıkrası neticesinde kartı üreten, satılan alan ya da devralan kişi olabilir. Ancak böyle bir şart yoktur. Fail TCK’nın 245/2. maddesinde düzenlenen suç işlemeden de bu suçun faili olabilir.

2.5.4.2.3. Mağdur

TCK’nın 245. maddesinde düzenlenen başkasına ait banka veya kredi kartlarını kullanarak yarar sağlama suçunda mağdura ilişkin özel bir belirleme yapılmamıştır. Dolayısıyla bu suçun mağduru herkes olabilir.

Bu suç malvarlığına ilişkin bir suçtur ve suçun tamamlanması için failin bir yarar sağlaması gerekir. Bu yararın sağlanabilmesi de bir başka kimsenin malvarlığında azalma olması

³³⁷ AKBULUT, s. 336.

gerekir. İşte bu suçun mağduru da malvarlığında azalma olan bu kimsedir. Bu kimsenin kim olduğu her olayın özelliğine göre tespit edilmelidir. Bu kimse kart hamili ya da banka veya finans kuruluşu olabileceği gibi bunların dışında bir kimse de olabilir.

2.5.4.2.4. Suçun Konusu

TCK'nın 245/3. maddesinde tanımlanan suçun oluşması için failin, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya bir başkasına yarar sağlaması gerekir. Bu suçun konusu, sağlanan bu yarardır. Bu yarar malvarlığına ilişkin bir değer, çoğu zaman da paradır. Ekonomik bir değeri olmayan bir yarar bu suçun konusu olamaz. Bu suçun malvarlığına ilişkin bir suç olması da konusunun ekonomik değer taşıyan yarar olduğu kanaatini güçlendirmektedir.

Doktrinde bazı yazarlar bu suçun konusunun sahte oluşturulan veya üzerinde sahtecilik yapılmış olan banka veya kredi kartları olduğunu söylemektedirler³³⁸. Bazı yazarlar ise bu suçun konusunun hem yarar hem de banka ve kredi kartları olduğunu ifade etmektedir³³⁹.

2.5.4.2.5. Netice

Suçun oluşması için yarar sağlanması gerekir. Bu itibarla söz konusu suç bir zarar suçudur.

2.5.4.3. Manevi Unsurlar

TCK'nın 245. maddesinin 3. fıkrasında tanımlanan bu suç yalnızca kasten işlenebilir. Suç tipinde taksirle işlenebileceğine dair bir ifade yer almadığı için bu suçun taksirle işlenmesi mümkün değildir. Bu suçun oluşabilmesi için sahte kredi veya banka kartlarını bilerek kullanmalı ve yarar sağladığını bilmelidir.

Bu suç tipinde herhangi bir saik ya da amaç aranmamıştır. Failin bu suçu kasten işlemesi yeterlidir. Fail her ne sebepten işlerse işlesin, suç tipinde yer alan fiilin gerçekleşmesiyle suç tamamlanmıştır.

Bu suç olası kastla da işlenebilir³⁴⁰.

2.5.4.4. Hukuka Aykırılık

Bu suç için geçerli olabilecek herhangi bir hukuka uygunluk sebebi yoktur. İlgilinin rızası, kanun hükmünü ifa gibi hukuka uygunluk sebepleri bu suç açısından geçerli olmayacaktır.

2.5.4.5. Suçun Özel Görünüş Biçimleri

2.5.4.5.1. Teşebbüs

Bu suça teşebbüs mümkündür. Fail sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağladığında suç tamamlanmış olur. Elverişli hareketlerle suçun icrasına başlamasına rağmen elinde olmayan sebeplerle suçu tamamlayamadığında suç teşebbüs aşamasında kalmış olacaktır. Failin eylemi kendi elinde olmayan sebeplerle tamamlayamamış olması gerekir. Fail, suçun icra hareketlerine başlar ancak suçu tamamlaması mümkün olmasına rağmen suç

³³⁸ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1026;

³³⁹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s.368-369.

³⁴⁰ AKBULUT, s.337.

tamamlamaktan kendi isteği ile vazgeçerse, teşebbüsten dolayı da ceza verilmez. Bu durumda gönüllü vazgeçme hükmü uygulanır.

Failin sahte ya da üzerinde sahtecilik yapılmış olan banka kartını veya kredi kartını kullanmak için elverişli hareketler yapması ama bir sebepten ötürü bu fiilini tamamlayamaması durumunda teşebbüs söz konusu olacaktır. Aynı şekilde failin söz konusu kartları kullanması ancak yarar elde edememesi durumunda da suç teşebbüs aşamasında kalmış olacaktır. Zira bu suçun tamamlanması için kartların kullanılarak yararın elde edilmiş olması şarttır.

Failin yalnızca sahte oluşturulmuş veya üzerinde sahtecilik yapılmış bir karta sahip olması bu suçun teşebbüs aşamasında kalmış olduğu anlamına gelmez. Fail bu kartları kullanmak ve yarar elde etmek için harekete geçmiş ancak bir sebepten ötürü suçu tamamlayamamış olduğunda teşebbüsten söz edilir. Öte yandan failin bu sahte kartları kendisinin üretmesi ayrıca başkasına ait bir banka hesabıyla ilişkilendirmesi durumunda henüz kullanmamış olsa dahi 245/2. maddedeki suç oluşmuş olacaktır.

2.5.4.5.2. İştirak

Bu suç iştirak açısından bir özellik göstermez. TCK'da düzenlenen müşterek faillik, azmettirme, yardım etme gibi iştirak türleri gerçekleştirilebilir. Bu durumlarda TCK'nın ilgili maddeleri uygulanacaktır.

Bu suçun işlenmesi neticesinde yararın fail tarafından başka bir kişiye sağlanması durumunda en baştan itibaren birlikte hareket etme kararı varsa yararın kendisine sağlandığı kişi başka hiç bir hareket yapmasa bile bu yararı kabul ederek müşterek fail olacaktır. Fail ile yararın kendisine sağlandığı kişi arasında önceden bir antlaşma yoksa fakat bu kişi yararı yine de kabul ediyorsa. TCK'nın 165. maddesinde düzenlenen suç eşyasının kabul edilmesi suçu oluşacaktır.

2.5.4.5.3. İctima

Fail aynı bankaya veya finans kuruluşuna ait bir ya da birden fazla kartı, değişik zamanlarda kullanarak yarar elde ederse suç zincirleme suç şeklinde işlenmiş olacaktır. Burada aynı kart birden çok kez kullanılmış olabileceği gibi aynı bankaya ait farklı kartlar da kullanılmış olabilir. Ancak fail farklı banka veya finans kuruluşlarına ait kartları kullanarak bu suç işlerse bu durumda mağdur sayısı kadar suç oluşacaktır. Zira zincirleme suçtan söz edilebilmesi için suç tipinde belirtilen fiilin aynı mağdura karşı işlenmesi gerekir. Yargıtay da bu görüştedir³⁴¹.

Fail, başkalarına ait banka hesaplarıyla ilişkili sahte banka veya kredi kartları ile ilgili olarak hem 245. maddenin 2. maddesini hem de 3. maddesini ihlal ediyor olabilir. Bu

³⁴¹ “...sanığın, aynı banka tarafından mağdura tahsis edilen iki bankamatik kartı ile değişik zamanlarda para çekme ve harcama yapma şeklindeki eylemlerinin Türk Ceza Kanunu’nun 245/1, 43. maddelerine uyan zincirleme suç oluşturacağı gözetilmeden...” (Yargıtay 8. Ceza Dairesi, 16.06.2016 tarihli, 2015/11765E - 2016/8081K – UYAP’tan alınmıştır.)

durumda faile her iki suçtan da ceza verilmelidir³⁴². Yargıtay da bu görüştedir³⁴³. Çünkü burada tek fiil değil, birden fazla fiil dolayısıyla birden fazla suç vardır. Öte yandan doktrinde 245/2. maddesinde düzenlenen suçun 245/3. maddesinde düzenlenen suç için geçit suç olduğunu, dolayısıyla yalnızca 245/3. maddeden ceza verilmesi gerektiğini savunan yazarlar da vardır³⁴⁴.

Bu suç için fikri içtima ise söz konusu değildir. Çünkü sahte banka ve kredi kartlarını kullanarak yarar sağlama suçu tali nitelikte bir suçtur. Madde metninde “*fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde*” denilerek bu durum açıkça ifade edilmiştir. Dolayısıyla fiil daha ağır cezayı gerektiren bir suç oluşturuyorsa faile bu suçtan ceza verilecek ancak cezası daha az olan başka bir suç söz konusu ise fail sahte banka ve kredi kartlarını kullanarak yarar sağlama suçundan cezalandırılacaktır. Esasen kanun koyucu madde metnine bu ifadeyi koymamış olsa dahi fikri içtima hükmü dolayısıyla aynı sonuca ulaşacaktık. Çünkü kanun koyucu TCK’nın 44. maddesinde “*İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır.*” hükmüne yer vermiştir. Ancak bu durumda sahte banka ve kredi kartlarını kullanarak yarar sağlama suçunun daha özel norm niteliğinde olması dolayısıyla uygulamada problem yaşanacaktı.

Bu suç ile aynı anda gerçekleşebilecek suç tipine örnek olarak dolandırıcılık verilebilir³⁴⁵. Dolandırıcılık suçunun temel halinin cezası sahte banka ve kredi kartlarını kullanarak yarar sağlama suçundan daha düşüktür. Fiilin aynı anda basit dolandırıcılık ve sahte banka ve kredi kartlarını kullanarak yarar sağlama suçunu oluşturması durumunda faile sahte banka ve kredi kartlarını kullanarak yarar sağlama suçundan ceza verilmelidir. Dolandırıcılık suçunun daha ağır cezayı gerektiren nitelikli hallerinin oluşması durumunda ise faile bu suçtan ceza verilecek, sahte banka ve kredi kartlarını kullanarak yarar sağlama tali norm niteliğinde olduğundan uygulanmayacaktır.

Fail bu suçu işlemek amacıyla TCK’nın 245/A maddesi kapsamında kalan fiilleri işler sonra da bu cihazı kullanarak TCK’nın 245. maddesinin 3. fıkrasındaki suçu işlerse her iki suçtan da ayrı ayrı cezalandırılmalıdır.

2.5.4.6. Soruşturma Usulü ve Yaptırım

TCK’nın 245/3. maddesinde düzenlenen sahte banka ve kredi kartlarını kullanarak yarar sağlama suçunun cezası dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. Bu suçu işleyen faile hem hapis cezası hem de adli para cezası verilecektir, yaptırımlar seçimlik değildir. Adli para cezasının alt sınırı TCK’nın 52. maddesi gereğince 5 gündür.

TCK’nın 245. maddesinin 3. fıkrasında düzenlenen bu suç re’sen soruşturulur.

³⁴² AKBULUT, s.341; GÜL, 165;

³⁴³ “...Türk Ceza Kanunu’nun 245/2 ve sahte oluşturulan kartın kullanımının aynı maddenin 3. fıkrasındaki birbirinden bağımsız suçları oluşturacağı gözetilip sahte kart üretmek suçundan da davalar açılması sağlanarak tüm deliller birlikte değerlendirilmesi...” (Yargıtay 8. Ceza Dairesi, 28.10.2020 tarih, 2020/2414 E- 2020/17684 K – UYAP’tan alınmıştır.)

³⁴⁴ SOYASLAN, Ceza Hukuku Özel Hükümler, s. 687.

³⁴⁵ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1030; KOCA/ÜZÜLMEZ, s. 911.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

TCK'nın 246. maddesinde *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükümlenir."* denilmektedir. Dolayısıyla TCK'nın 245/3. maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

2.6. Yasak Cihaz ve Programlar (TCK 245/A)

2.6.1. Genel Olarak

Günümüzde gelişen teknoloji ile birlikte pek çok suç bilişim sistemleri üzerinden işlenebilir hale gelmiş ve bu durumun sonucu olarak da TCK'da bilişim suçları ile bazı suçların bilişim yoluyla işlenebilen nitelikli halleri düzenlenmiştir. Ancak teknolojinin gelişimi ile bu suçların varlığı caydırıcılık açısından yeterli olmamış bir de bu suçların işlenmesi için hazırlık hareketi teşkil edebilecek cihaz ve programların temini de suç olarak düzenlenmiştir. Söz konusu cihaz ve programların bu suçların işlenmesini oldukça kolaylaştırıyor olması hiç şüphe yok ki bu düzenlemenin ardında yatan en önemli sebeptir. Zira bu cihaz ve programları temin eden kimse, bu alanda hiçbir uzmanlığı olmasa dahi bu suçları işleyebilir hale gelmektedir.

TCK'nın ilk halinde olmayan 245/A maddesi yukarıda açıklanan gerekçeler dolayısıyla 6698 sayılı Kişisel Verilerin Korunması Kanun'un 30. maddesinin 5. fıkrası ile eklenmiştir. *"Yasak cihaz veya programlar"* başlığını taşıyan söz konusu maddeye göre *"Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır."*

Söz konusu maddenin gerekçesinde *"Son olarak 5237 sayılı Kanuna "Yasak cihaz veya programlar" başlıklı 245/A maddesinin eklenmesi öngörülmüştür. Böylece bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bir bilişim suçunun işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran faillerin cezalandırılması amaçlanmaktadır. Mezkûr Sözleşmenin 6'ncı maddesiyle sözleşmeci taraflar, bilişim alanında suç işlenmesini kolaylaştıran cihazların kötüye kullanılmasını cezalandırmaya davet edilmektedir. Bilişim suçları ile bilişim sistemleri araç kılınarak işlenen suçlarla etkin ve caydırıcı bir şekilde mücadele edebilmek için bu tür eylemlerin suç ve ceza politikaları bakımından sınırlandırılması ve yaptırıma bağlanmasında yarar görülmektedir. Maddede tanımlanan suçun oluşumunda kişinin suç işleme kastı dikkate alınmak zorundadır. Buna göre, bu tür*

cihaz ve programların, bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır. Ayrıca, failin cezalandırılabilmesi bakımından söz konusu cihaz, program, şifre veya güvenlik kodunun suçun işlenmesine elverişli olması gerekir.” denilmiştir.

Gerekçede görüldüğü üzere düzenlemede Sanal Ortamda İşlenen Suçlar Sözleşmesinin 6. maddesi bu suç için temel alınmıştır.

Bu suçun oluşabilmesi için bu yasak cihaz ve programları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran faillerin söz konusu suçları işleme kastıyla hareket etmesi aranmıştır. Fail bilişim yoluyla işlenen suçlardan birini ya da doğrudan bilişim suçlarından birini işlemek maksadında olmalıdır. Sistemlerin güvenliklerinin test edilmesi amacıyla bu cihaz ve programların yapılması ya da oluşturulması durumunda suç teşkil etmeyeceği de gerekçede özellikle vurgulanmıştır.

Gerekçede vurgulanan son husus ise söz konusu yasak cihaz ve programların hedef suçları işlemeye elverişli olması gerektiğidir, bu suçları işlemeye elverişli olmayan cihaz ve programların yapılması ya da oluşturulması da bu suçun oluşmasına sebebiyet vermeyecektir.

Söz konunu Sanal Ortamda İşlenen Suçlar Sözleşmesinin “Cihazların kötüye kullanımı” başlıklı 6. maddesinde “*Taraflardan her biri, kasten ve haksız yere gerçekleştirildiği zaman, aşağıdakilerin kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:*

a. aşağıda belirtilenlerin 2 ila 5. maddelerde belirtilmiş herhangi bir suçun işlenmesi için kullanılmaları amacıyla üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı veya başka şekilde erişilebilir hale getirilmesi:

i. bir bilgisayar programı da dâhil olmak üzere, öncelikli olarak yukarıda belirtilen 2 ila 5. maddelerde belirtilmiş herhangi bir suçu işlemek amacıyla tasarlanmış veya uyarlanmış bir cihaz;

ii. bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişimi mümkün kılan bir bilgisayar şifresi, erişim kodu veya benzer bir veri.

ve

b. yukarıda paragraf a.i veya ii' de atıfta bulunulmuş bir öğeye, 2 ila 5. maddelerde belirtilmiş herhangi bir suçun işlenmesi için kullanılması amacıyla bulundurma. Taraflardan biri, yasa gereği cezai sorumluluğun doğması için bahsi geçen öğelerden belli bir sayıda bulundurulmasını şart koşabilir.

İşbu madde, bu maddenin 1. paragrafında atıfta bulunulan üretme, satma, kullanım amaçlı tedarik, ithalat, dağıtma veya başka şekilde erişilebilir hale getirme veya bulundurmanın, 2 ila 5. maddeler uyarınca suç işlemek maksadıyla gerçekleştirilmemesi durumunda, örneğin bir bilgisayar sisteminin yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde, cezaî yükümlülük doğuracağı şeklinde yorumlanmayacaktır.

3. Taraflardan her biri, çekincenin işbu maddenin 1.a.ii paragrafında sözü edilen öğelerin satışı, dağıtımı veya başka şekilde erişilebilir hale getirilmesiyle alakalı olmaması kaydıyla, işbu maddenin 1.paragrafını uygulamama hakkını saklı tutabilir.” denilmiştir.

Sözleşme ile madde metni karşılaştırıldığında büyük oranda aynı oldukları görülecektir. Sözleşme söz konusu cihaz ve programların “üretimi, satışı, kullanım amaçlı tedarik edilmesi, ithal edilmesi, dağıtımı” şeklinde fiilleri saydıktan sonra “veya başka şekilde erişilebilir hale getirilmesi” denilerek düzenleme kapsamını oldukça geniş tutmuştur. 245/A maddesi düzenlenirken de sözleşmede yazılı fiillerin yanı sıra nakledilmesini, sevk edilmesini, depolanmasını, satışa arz edilmesini, satın alınmasını, başkalarını verilmesini ve bulundurulmasını da suç saymıştır. Görüldüğü gibi TCK’daki düzenleme sözleşmeye nazaran hem daha kapsamlı hem de belirlilik ilkesine daha uygundur.

Sözleşmede “bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişimi mümkün kılan bir bilgisayar şifresi, erişim kodu veya benzer bir veri” şeklinde bir sınırlama mevcutken madde metnimizde herhangi bir sınırlama yapılmaksızın bir şifre veya güvenlik kodunun belirtilen amaçla yapılması veya oluşturulması suç sayılmıştır.

Sözleşmede “Bilişim Alanında Suçlar” bölümünde yer alan suçların işlenmesi maksadıyla yasak cihaz ve programların yapılması ve oluşturulmasının suç olarak düzenlenmesi öngörülmüşken kanunumuzda bununla yetinilmeyerek bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen tüm suçları bu suç için amaç suç olarak kabul etmiştir. Sözleşmede “Taraflardan biri, yasa gereği cezai sorumluluğun doğması için bahsi geçen öğelerden belli bir sayıda bulundurulmasını şart koşabilir.” denildiyse de kanunumuzdaki düzenlemede böyle bir sınırlamaya yer verilmemiş, öğelerden kaç tane bulundurulursa bulundurulsun suç kabul etmiştir.

Madde başlığının “Yasak Cihaz veya Programlar” olması ise doktrinde eleştirilmiştir. Söz konusu eleştiride TCK sistematğinde madde başlıkları belirlenirken fiil unsuru ön plana çıkarılmış olmasına rağmen 245/A maddesinin başlığının belirlenmesinde ise konu unsurunun esas alınmasının hatalı olduğu belirtilmiştir. Gerçekten de madde başlığı, maddede yer alan suçun içeriğini yansıtmaktan ziyadesiyle uzaktır. Ayrıca söz konusu cihazların ya da programların yasak olup olmadıklarına dair bir ibare de madde metninde geçmemektedir. Buna rağmen madde başlığında söz konusu cihazların yasaklı olduğuna dair bir ibare bulunmaktadır. Ortada bir yasaklama kararı ise yoktur. Yazarlar, bunun yerine “suçta kullanılacak cihaz ve programların üretilmesi, yayılması veya bulundurulması” başlığını önermişlerdir³⁴⁶. Bu suç için önerilen bir diğer başlık ise “program veya cihazların kötüye kullanılması” şeklindedir³⁴⁷. Bu suçun başlığının “Suçta Kullanılacak Yasak Cihaz ve Programların İmal Edilmesi, Ticareti, Dolaşıma Sokulması ve Bulundurulması” şeklinde düzenlenmesi suça uygun olacaktır.

2.6.2. Suçla Korunan Hukuki Yarar

Bu suçla korunan hukuki değer bilişim sistemlerinin güvenliği ve güvenilirliğidir. Zira bu suçla söz konusu cihaz ve programların yapılması veya oluşturulması engellenerek bilişim

³⁴⁶ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1034.

³⁴⁷ AKBULUT, s. 348.

sistemlerine yönelik suçlar ile bilişim sistemlerinin araç olarak kullanıldığı suçların işlenmesinin de engellenmesi amaçlanmıştır. Bilişim sistemine yönelik suçların engellenmesindeki amaç hiç şüphesiz bilişim sistemlerinin güvenliğini korumaktır. Bilişim sistemlerinin araç olarak kullanıldığı suçlarda ise bilişim sisteminin güvenilirliğinin zedelendiği açıktır. Bu düzenlemeyle bunun önüne geçilmek istenmiştir.

Doktrinde bu suçla korunan hukuki değere ilişkin farklı görüşler mevcuttur.

Bir görüşe göre bu suçla toplum güvenliği korunmaktadır. Bunun yanı sıra kişilerin özel hayatı, malvarlığı ve haberleşme özgürlükleri de bu suçla koruma altına alınmıştır³⁴⁸.

Bir başka görüşe göre bu suçla bilişim sistemlerinin güvenliği, güvenilirliği ve kamu düzen ve güvenliği koruma altına alınmıştır³⁴⁹.

Bir diğer görüşe göre ise bu suçla kamunun bilişim sistemlerine yönelik güveni korunmaktadır³⁵⁰.

Benzer şekilde bazı yazarlar da bilişim sistemlerine karşı toplumda oluşan güvenin ve bu suçlarla işlenebilecek suçlarla korunan diğer hukuksal değerlerin korunduğunu ifade etmiştir³⁵¹.

Bazı yazarlar ise bu suçla bilişim sistemlerinin güvenliği ve güvenilirliğinin, bunlarla bağlantılı olarak da kişilerin kendini özgürce geliştirebilme hakkının korunduğunu ayrıca bilişim teknolojisi kullanıcılarının uğrayacakları zararlar bakımından malvarlığı değerlerinin de yine bu suçla koruma altına alındığını belirtmektedir. Bu yazarlara göre korunan hukuki değer karma niteliklidir³⁵².

2.6.3. Maddi Unsurlar

2.6.3.1. Fiil

Bu suçun oluşması için suç konusu cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması gerekir. Görüldüğü gibi suç tipinde birden çok fiil seçimlik olarak sayılmıştır, bu sebeple bu suç tipi seçimlik hareketli bir suçtur. Bu hareketlerden yalnızca birisinin yapılmasıyla dahi suç oluşacaktır. Bu hareketlerden birkaçı aynı konu üzerinde yapılırsa dahi tek bir suç oluşacaktır ancak bu durumda temel cezanın belirlenmesinde göz önüne alınacaktır.

Madde metninde suçun işlenebileceği hareketler sıra ile sayılmıştır. Bu nedenle suç bağlı hareketli bir suçtur³⁵³.

Depolamak ve bulundurmamak fiilleri bakımından temadi bir suç niteliği arz etmektedir³⁵⁴.

³⁴⁸ GÜL, s. 240.

³⁴⁹ AKBULUT, s. 349.

³⁵⁰ KOCA/ÜZÜLMEZ, s. 913.

³⁵¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 456.

³⁵² ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1034.

³⁵³ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1037; AKBULUT, s. 355.

³⁵⁴ KOCA/ÜZÜLMEZ, s. 914.

İmal etmek, ham maddeyi işleyerek bir mal üretmektir³⁵⁵. Bir cihazın, bir bilgisayar programının, bir şifrenin veya bir güvenlik kodunun üretilmesi ile suç oluşur.

İthal etmek ise bir ülkeye başka ülkelerden mal getirmek anlamındadır. Doktrinde cihaz üretimi için kullanılacak parçaların ayrı ayrı ithal edilerek Türkiye’de birleştirilmesinin ithal etme kapsamında değerlendirilmeyeceği ifade edilmişse de³⁵⁶ failin bu durumda da cihaz imal etmek fiilinden sorumlu tutulması gerekmektedir. İthal etmenin söz konusu olabilmesi için suça konu bilgisayar programı, şifre ya da sair güvenlik kodunun fiziksel olarak sınır kapısından geçirilmesi şart olmayıp internet üzerinden temin edilmesi durumunda da bu suç gerçekleşecektir³⁵⁷.

Sevk etmek; göndermek, götürmek demektir. Bir cihazın, bilgisayar programının, güvenlik kodunun ya da şifrenin gönderilmesi ile suç oluşur. Suç konusunun yurt dışından getirilmesi ithal etmek şeklinde ayrıca düzenlenmiştir ancak yurt içinden yurt dışına gönderilmesi ya da yurt içinde bir yerden başka yere gönderilmesi durumları da sevk etmek kapsamında kalmaktadır³⁵⁸.

Nakletmek, nakil işini yapmak, bir yerden başka bir yere geçirmek, iletmek demektir³⁵⁹. Bilgisayar programının, şifrenin ya da güvenlik kodunun ağlar vasıtasıyla başka yere gönderilmesi de nakletmektir³⁶⁰.

Depolamak, saklamak veya korumak amacıyla ambara koymak, depo etmek, biriktirmek, ambarlamak ya da bir bellek cihazına veriyi yerleştirmek veya saklamak anlamındadır³⁶¹. Bir cihazın fiziksel olarak belirli bir yerde saklanması depolamak olurken bir bilgisayar programının, şifrenin ya da güvenlik kodunun depolanması bir bellek cihazına saklanması şeklinde olmaktadır. Bulundurmak ise var olmasını, hazır bulunmasını sağlamak, eksik etmemek anlamına gelmektedir³⁶². Depolamak ve bulundurmak hemen hemen aynı anlama gelmekle birlikte bulundurmak fiilinin depolamak fiilini de kapsadığı söylenebilir. Depolamak fiili daha ziyade birden fazla cihazı, bilgisayar programını, şifreyi ya da sair güvenlik kodunu bulundurmak anlamına gelmektedir. Ancak tek bir cihazın, bilgisayar programının, şifrenin ya da sair güvenlik kodunun depolanması da mümkündür. Burada ayırt edici olan saklama ve koruma amacının bulunmasıdır.

Vermek; satış amacı gütmeksizin bir cihazı, bilgisayar programını, şifreyi ya da güvenlik kodunu teslim etmek kabul etmek ise bu suç konusunu teslim almaktır.

Satmak ve satın almak ise bir bedel karşılığında cihazı, bilgisayar programını, şifreyi ya da güvenlik kodunu teslim etmek ve teslim almaktır. Satışa arz etmek, satışa çıkarmak ya da satmak için ortaya koymak demektir. Doktrinde de ifade edildiği üzere satışa arz etmek

³⁵⁵ <https://sozluk.gov.tr/> 31.03.2020.

³⁵⁶ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1038.

³⁵⁷ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1038.

³⁵⁸ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1038.

³⁵⁹ <https://sozluk.gov.tr/> 31.03.2020.

³⁶⁰ AKBULUT, s.356.

³⁶¹ <https://sozluk.gov.tr/> 31.03.2020.

³⁶² <https://sozluk.gov.tr/> 31.03.2020.

fiilinin gerçekleşmesi için somut bir alım satım ilişkisinin varlığı şart değildir³⁶³. Suça konu cihazın, programın, şifrenin ya da sair güvenlik kodunun satılacağına dair bir ilan vermek, ürünü bu amaç için teşhir etmek gibi fiiller satışa arz etmeye örnek verilebilir.

2.6.3.2. Fail

Bu suç tipi düzenlenirken faille ilgili özel bir belirleme yapılmamıştır. Fail herhangi biri olabilir. Suçun faili söz konusu yasak cihaz ve programları “imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran” kimsedir.

Satmak ve satın almak, kabul vermek ve vermek gibi fiiller çok faille işlenmektedir. Bu fiillerin işlenmesi durumunda her iki taraf da fail olacaktır. Çok failli suçlar birleşme ve karşılaşma suçları şeklinde iki ayrı şekilde işlenebilirler. Birleşme suçlarında faillerin amaçları aynı yöndeyken karşılaşma suçlarında birden çok fail aynı suçta değişik bir neden ile karşılaşmaktadır³⁶⁴. Satmak ve satın almak, kabul etmek ve vermek fiilleri açısından 245/A maddesinde düzenlenen suç da bir karşılaşma suçudur.

2.6.3.3. Mağdur

Bu suçun işlenmesi sırasında belirli bir kişiye yönelen bir saldırı söz konusu değildir³⁶⁵. Dolayısıyla bu suçun mağduru toplumu oluşturan herkeştir.

2.6.3.4. Konu

Bu suçun söz konusu olabilmesi için bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun söz konusu suçların işlenebilmesi için yapılması veya oluşturulması gerekmektedir. Madde metninde sayılan fiiller ancak böyle bir program, şifre, cihaz ya da güvenlik kodu söz konusu ise bu suçun oluşmasına sebebiyet verecektir. Dolayısıyla bu suçun konusu cihaz, bilgisayar programı, şifre veya sair güvenlik kodudur.

Cihazın sözlük anlamı; aygıt, alet, takımdır³⁶⁶. Fiziksel varlığı olan şeyler için kullanılır³⁶⁷. Kart bilgilerini kopyalamaya yarayan encoder cihazı ve kartların manyetik şerit bilgilerini kopyalamaya yarayan, şifrelerini ele geçirmeye yarayan, bu kartların ATM’lere sıkışmasını sağlayan cihazlar da bu suçun konusudur³⁶⁸.

Bu suçun konusunu oluşturan cihazlar genellikle bu suç için özel olarak geliştirilen cihazlar olmakla birlikte doktrinde bu cihazların ileri teknoloji gerektiren cihazlar olması gerekmediği, örneğin bir kameranın da kartların şifresini öğrenmek amacıyla özel olarak tasarlanmış olması durumunda bu suçun konusu olabileceği ifade edilmiştir³⁶⁹.

Doktrinde, ATM’den çekilen paraların sıkışmasını sağlayan bir düzeneğin bu madde kapsamında değerlendirilmeyeceği, zira böyle bir düzenek kullanılarak suç işlenmesi

³⁶³ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1039.

³⁶⁴ HAKERİ, s.507

³⁶⁵ KOCA/ÜZÜLMEZ, s.

³⁶⁶ <https://sozluk.gov.tr/>, 30.03.2020.

³⁶⁷ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1035.

³⁶⁸ GÜL, s. 240.

³⁶⁹ ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 1035.

durumunda bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu değil basit hırsızlık suçunun oluşacağı ifade edilmiştir³⁷⁰.

Bilgisayar programları ise yukarıda geniş şekilde anlattığımız kötü amaçlı yazılımlardır.

Şifre, harf sayı ya da sembollerden oluşan dijital kilittir. Gizli kalması istenen bilgi, belge ve sistemleri koruyan bir anahtar görevi görür³⁷¹. Bu şifreleri kıran yazılımlar bilgisayar programı olduğundan yine bu suç kapsamında kalırlar. Örneğin bir sistemin ücret karşılığında kullanıcılarına belirli hizmetler sunduğu ve bu hizmetleri kullanmaları için de bir şifre verdiği, bu şifrenin de özel bir algoritma vasıtasıyla her kullanıcı için ayrı ayrı oluşturulduğu durumda failin söz konusu algoritmayı keşfederek bir şifre oluşturması ve bu şifreyi kullanarak bilişim sistemine girmesi halinde söz konusu şifre bu suçun konusunu teşkil edecektir ve fail şifreyi oluşturduktan sonra sisteme girse de girmese de 245/A maddesinden cezalandırılacaktır. Yine de kanun koyucunun şifre ifadesini ile neyi kast ettiğini daha açık bir şekilde ifade etmesi belirlilik ilkesi açısından daha yerinde olurdu.

Sair güvenlik kodu ise güvenlik amaçlı kullanılan; ses ve biyolojik verilerdir. Göz taraması, parmak izi, avuç içi tanıma, yüz tanıma gibi teknolojiler de günümüzde güvenlik kodu olarak kullanılmaktadır³⁷². Bunların dışında da güvenlik kodları mevcuttur. Örneğin bir QR kod ya da bir desen de güvenlik kodu olarak kullanılabilir. Burada sair ifadesi “şifre veya sair” şeklinde kullanılmış olup şifre dışında kalan güvenlik kodlarını ifade etmek amacı taşımaktadır³⁷³.

Doktrinde de cihaz ve bilgisayar programı ifadelerinin rahatlıkla anlaşılabilir olmasına rağmen şifre ve güvenlik kodlarının neyi ifade ettiğinin belirsiz olduğu ifade edilerek bu durum eleştirilmiştir³⁷⁴.

Bilişim alanında suçlar bölümünde yer alan suçların yanı sıra “Eğitim ve öğretim hakkının engellenmesi”, “Kamu hizmetlerinden yararlanma hakkının engellenmesi”, “Hakaret”, “Haberleşmenin gizliliğini ihlal”, “Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması”, “Özel hayatın gizliliğini ihlal”, “Kişisel verilerin kaydedilmesi”, “Verileri hukuka aykırı olarak verme veya ele geçirme”, “Verileri yok etmeme”, “Halk arasında korku ve panik yaratmak amacıyla tehdit”, “Suç işlemeye tahrik”, “Suçu ve suçluyu övmeye”, “Halkı kin ve düşmanlığa tahrik veya aşıllama”, “Kanunlara uymamaya tahrik”, “Müstehcenlik” ve “Kumar oynanması için yer ve imkân sağlama” gibi suçların işlenmesi amacıyla söz konusu yasak cihaz, program, şifre veya sair güvenlik kodunun yapılması veya oluşturulması durumunda suç oluşacaktır. Madde gerekçesinde “Maddede tanımlanan suçun oluşumunda kişinin suç işleme kastı dikkate alınmak zorundadır.” denilmiştir. Bu durum suçun manevi unsuruyla olduğu kadar konu unsuruyla da ilgilidir. Zira bu suçun oluşması için suça konu olan cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun belirtilen suçların işlenmesi maksadıyla yapılmış ve oluşturulmuş olması gerekir.

³⁷⁰ GÜL, s. 241.

³⁷¹ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 457.

³⁷² DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 457.

³⁷³ KOCA/ ÜZÜLMEZ, s. 914.

³⁷⁴ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1035.

Sistemin test edilmesi ya da benzeri amaçlarla bir cihazın bilgisayar programının, şifrenin veya sair güvenlik kodunun yapılması ya da oluşturulması durumunda suç oluşmayacaktır.

Yine madde gerekçesinde de belirtildiği üzere suça konu cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun suçun işlenmesine elverişli olması gerekir. Aksi halde suç oluşmaz.

2.6.3.5. Netice

Bu suç soyut tehlike suçudur. Bu suçun oluşması için herhangi bir neticenin meydana gelmesine gerek yoktur. Bir zarar oluşması da gerekmez. Yalnızca madde metninde sayılan fiillerin yapılmasıyla suç oluşmuş olur. Dolayısıyla sırf hareket suçudur.

2.6.4. Manevi Unsurlar

TCK'nın 245. maddesinde düzenlenen yasak cihaz ve programlar suçu yalnızca kasten işlenebilir bir suçtur. Madde metninde taksirle işlenebilir haline yer verilmediği için bu şekilde işlenmesi mümkün değildir.

Bu suçun oluşabilmesi için kastın yanında amaç unsuru da aranmıştır. Fail, suç konusunu bilişim alanında suçlar bölümünde düzenlenen suçlar ya da bilişim sistemlerinin araç olarak kullanıldığı diğer suçlardan birini işlemek maksadıyla almalıdır. Amaç unsurunun da arandığı bu suçun olası kastla işlenmesi mümkün değildir. Fail, bu amaçlarla oluşturulmuş bir cihazı, bilgisayar programını, şifreyi ya da güvenlik kodunu bilerek imal etmeli, ithal etmeli, sevk etmeli, nakletmeli, depolamalı, kabul etmeli, satmalı, satışa arz etmeli, satın almalı, başkalarına vermeli ya da bulundurmalıdır.

Faillin söz konusu cihazı, bilgisayar programını, şifre veya sair güvenlik kodunu ne amaçla aldığıнын belirlenmesi suçun oluşması açısından önemlidir. Bu tarz cihazlar, programlar, şifreler ve güvenlik kodları teknik özellik arz ettiğinden bilirkişi incelemesine başvurulabilir. Bunun dışında failin beyanları, yakalanış şekli, suç konusunun hazırlanış şekli vb. durumlar göz önüne alınarak değerlendirilmelidir³⁷⁵.

Fail amaç suçu gerçekleştirmese dahi söz konusu suçlardan birini işleme amacıyla olması yeterlidir.

Failin hataya düşmesi durumunda TCK'nın 30/1 maddesi uygulama alanı bulacaktır.

2.6.5. Hukuka Aykırılık

CMK'nın 134. maddesinde “*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*” düzenlenmiştir. Söz konusu koruma tedbirinin hayata geçirilmesi için de birtakım cihazlar, bilgisayar programları, güvenlik kodları ve şifreler kullanılmaktadır. Bu amaçla bu cihazların, bilgisayar programlarının, güvenlik kodlarının veya şifrelerin imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya

³⁷⁵ GÜL, s. 241.

bulundurulması suç oluşturmaz. Burada kanun hükmünün yerine getirilmesi söz konusudur³⁷⁶.

Madde gerekçesinde “*Buna göre, bu tür cihaz ve programların, bilişim sistemlerinin güvenliğini test etmek amacıyla yapılması veya oluşturulması halinde belirtilen suç oluşmayacaktır.*” denilmektedir. Doktrinde bu durum için ilgilinin rızasının söz konusu olduğu da ifade edilmiştir³⁷⁷. Keza sistem güvenliğinin sağlanması amacıyla pek çok şirket bu tarz testleri bilerek ve isteyerek yaptırmaktadır.

Bu tür cihaz ve programların, şifrelerin ya da güvenlik kodlarının yetkili makamların izni ile imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması suç da oluşturmaz. Zira bu durumda kanunen verilmiş bir hakkın kullanılması söz konusudur³⁷⁸.

Bunların dışında kalan hukuka uygunluk sebeplerinin bu suç açısından gerçekleşmesi mümkün değildir.

2.6.6. Suçun Özel Görünüş Biçimleri

2.6.6.1. Teşebbüs

Bu suçun oluşması için imal etmek, ithal etmek, sevk etmek, nakletmek, depolamak, kabul etmek, satmak, satışa arz etmek, satın almak, başkalarına vermek veya bulundurmak fiillerinin birinin tamamlanması yeterlidir. Failin elverişli hareketlerle bu fiillerden birinin icrasına başlamasına rağmen elinde olmayan bir sebepten ötürü söz konusu fiili tamamlayamaması durumunda eylem teşebbüs aşamasında kalmış olacaktır. Failin kendi isteğiyle fiili tamamlamaktan vazgeçmesi durumunda ise gönüllü vazgeçme hükmü söz konusu olacaktır.

Bulundurmak ve depolamak fiilleri kesintisiz suç niteliği arz etmektedir. Fail bu fiillerinden birini çok az bir süre dahi gerçekleştirdiyse suç tamamlanmıştır³⁷⁹.

2.6.6.2. İştirak

Bu suç iştirak açısından bir özellik arz etmez, tüm iştirak türleri bu suç açısından mümkündür.

2.6.6.3. İçtima

Bu suç seçimlik hareketli bir suçtur. Failin söz konusu hareketlerden birini yapmasıyla suç oluşacaktır ancak failin aynı suç konusu üzerinde birden fazla hareketi gerçekleştirmesi durumunda da tek suç söz konusu olacaktır. Örneğin failin aynı cihazı önce imal etmesi ardından da satması durumunda tek suçtan söz edilecektir.

Failin aynı anda birden fazla cihazı, bilgisayar programını, şifreyi ya da sair güvenlik kodunu imal etmesi, satması, satın alması, satışa arz etmesi, ithal etmesi, sevk etmesi,

³⁷⁶ AKBULUT, s. 359, ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1039.

³⁷⁷ ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s. 1040.

³⁷⁸ AKBULUT, s. 359.

³⁷⁹ KOCA/ ÜZÜLMEZ, s. 915-916.

nakletmesi, depolaması, başkalarına vermesi, kabul etmesi ya da bulundurması durumunda da tek suç oluşacaktır. Bu hareketlerin çok kısa bir aralıkta gerçekleşmesi de durumunda da tek bir suç söz konusu olacaktır.

Failin farklı zamanlarda suça konu fiilleri gerçekleştirmesi durumunda ise zincirleme suç hükümleri değerlendirilecektir.

TCK'nın 245/A maddesinde düzenlenen suç bir araç suç niteliğindedir. Failin bu suçun yanı sıra amaçladığı suçu da işlemesi durumunda her iki suçtan da ceza alması gerekir. Örneğin kişisel verilerin ele geçirilmesi maksadıyla bir bilgisayar programı imal eden sonra da bu programı kullanarak bu verileri elde eden fail hem TCK'nın 245/A maddesinden hem de 135. maddesinden sorumlu olacaktır.

Fikir ve Sanat Eserleri Kanunu'nun *"Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri"* başlıklı 72. maddesinde *"Bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde bulunduran kişi altı aydan iki yıla kadar hapis cezasıyla cezalandırılır."* denilmiştir. Ayrıca Elektronik İmza Kanunu'nun *"İmza oluşturma verilerinin izinsiz kullanımı"* başlıklı 16. maddesi de *"Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adli para cezasıyla cezalandırılırlar. Yukarıdaki fıkra da belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır."* şeklindedir. Her iki maddede düzenlenen suç da TCK'nın 245/A maddesine göre özel nitelik arz etmektedir. Dolayısıyla failin bu fiilleri işlemesi durumunda yalnızca ilgili maddeden hüküm kurulacak, faile ayrıca 245/A maddesinden ceza verilmeyecektir.

2.6.7. Soruşturma Usulü ve Yaptırım

TCK'nın 245/A. maddesinde düzenlenen yasak cihaz ve programlar suçunun cezası bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. Bu suçu işleyen faile hem hapis cezası hem de adli para cezası verilecektir, yaptırımlar seçimlik değildir. Adli para cezasının alt sınırı TCK'nın 52. maddesi gereğince 5 gündür.

TCK'nın 245/A maddesinde düzenlenen bu suç re'sen soruşturulur.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 11. ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

TCK'nın 246. maddesinde *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* denilmektedir. Dolayısıyla TCK'nın 245/A maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, tüzel kişilere özgü güvenlik tedbirleri uygulanacaktır.

ÜÇÜNCÜ BÖLÜM

Dolayısıyla Bilişim Suçları

3.1. Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık Suçu (142/2-e)

3.1.1. Genel Olarak

TCK'nın “*Kişilere Karşı Suçlar*” Başlıklı 2. Kısımın Onuncu Bölümünde, “*Malvarlığına Karşı Suçlar*” başlığı altında yer alan 141. maddesinde zilyedinin rızasını almaksızın bir başka kimseye ait taşınır bir malı, kendisine yahut bir başka kimseye yarar temin etmek amacıyla bulunduğu yerden alan kimseye bir yıldan üç yıla kadar hapis cezası verileceği düzenlenerek hırsızlık suçunun temel hali düzenlenmiş, nitelikli hırsızlık başlıklı 142. maddesinin 2. fıkrasının e bendinde ise hırsızlık suçunun “*Bilişim sistemlerinin kullanılması suretiyle*” işlenmesi halinde beş yıldan on yıla kadar hapis cezasına hükmolunacağı düzenlenmiştir.

Günümüzde teknoloji hızla ilerlemiş ve bankacılık sistemleri günlük hayatın vazgeçilmez bir unsuru olmuştur. Bununla birlikte internet bankacılığı ortaya çıkmış ve bankacılık sistemini oldukça kolaylaştırması dolayısıyla hızla yaygınlaşmıştır. Bu işlemlerin bu kadar kolay yapılabilmesi beraberinde birtakım güvenlik problemlerini de ortaya çıkarmış ve kötü niyetli kimselerin bu sistemleri kullanarak hırsızlık fiillerini işlemeleri sonucunu doğurmuştur. Bu durumun bir sonucu olarak da hırsızlık suçunun bilişim sistemlerinin kullanılması suretiyle işlenmesi bir nitelikli hal olarak kabul edilmiştir.

765 sayılı Mülga TCK'da benzer nitelikte bir suç bulunmamaktaydı. Bu yasa döneminde 525 b/2 maddesinde düzenlenmiş olan hukuka aykırı yarar sağlamak suçu yeni TCK'da düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu da kapsayacak şekilde uygulanıyordu. ESKİ TCK 525 b/2 maddesi, yeni TCK düzenlemesinde ise 142/2-e, 158/1-f, 244/4, 245 maddelerinde düzenlenecek şekilde dörde ayrılmıştır³⁸⁰.

3.1.2. Korunan Hukuki Yarar

Hırsızlık suçu ile korunan hukuki yarar zilyetlik ve mülkiyet hakkıdır. Bu kavramlardan hareketle genel olarak malvarlığına ilişkin değerleri koruduğu açıktır.

Doktrinde bu suçun koruduğu hukuki yararı yalnızca zilyetlik olarak kabul eden yazarlar³⁸¹ olduğu gibi yalnızca mülkiyet hakkı olduğunu da kabul eden görüşler³⁸² bulunmaktadır. Ayrıca bu suçun koruduğu hukuki yararın mülkiyet hakkı olduğunu ve bu suçla malın bulunduğu yerden alınmasına karşı korunduğunu kabul eden görüşler³⁸³ olduğu gibi bu suçun hem zilyetliği hem de mülkiyet hakkını koruduğunu kabul eden yazarlar³⁸⁴ da vardır.

³⁸⁰ DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s.461.

³⁸¹ SOYASLAN, Ceza Hukuku Özel Hükümler, s. 389.

³⁸² ÖZBEK/DOĞAN/BACAKSIZ/TEPE, s. 610; DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku s.463.

³⁸³ TEZCAN/ERDEM/ÖNOK, s. 695.

³⁸⁴ KOCA/ÜZÜLMEZ, s.554-555.

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu da aynı şekilde malvarlığını korumaktadır.

3.1.3. Maddi Unsurlar

3.1.3.1. Fiil

Hırsızlık suçunun oluşması için gerekli olan eylem taşınır bir malı, kendisine yahut başka bir kimseye menfaat sağlamak gayesiyle bulunduğu yerden almaktır. Yani bu suçun oluşması için bir taşınır mal olmalı, bu mal alınmalı ve alınma eylemi rıza dışı olmalıdır. Söz konusu taşınır eşya mağdurun egemenlik alanından çıkıp failin egemenlik alanına girdiğinde eylem tamamlanmış olur ve suç oluşur. Başka bir hareketin yapılmasına gerek yoktur. Ayrıca bir neticenin oluşması da aranmaz. Dolayısıyla bu suç sırf hareket suçudur.

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunda da bilişim sistemleri aracılığıyla malvarlığını temsil eden verilerin alınması aktarılması suretiyle suç tamamlanır. 142/2-e maddesinden söz edebilmek için failin bilişim sistemlerini kullanması gerekir. Örneğin ATM cihazına düzenek yerleştirilmesi durumunda TCK'nın 141. maddesi gündeme gelecektir³⁸⁵.

Bu suçun tamamlanması için asıl zilyedin söz konusu mal üzerindeki haklarını kullanamayacak duruma gelmesi ve failin bu malvarlığı değeri üzerinde tasarruf imkânı sağlaması yeterlidir. Örneğin fail, mağdura ait banka hesabından kendi hesabına parayı aktardığı anda suç tamamlanmış olacak, ayrıca failin bu parayı kullanması ya da çekmesi aranmayacaktır. Hatta havale işlemi tamamlandıktan çok kısa süre sonra banka tarafından işlem iptal edilerek paraya bloke koyulsa dahi suç tamamlanmıştır.

3.1.3.2. Fail

Bu suç fail açısından herhangi bir özellik arz etmez, herkes bu suçun faili olabilir.

3.1.3.3. Mağdur

Bu suç mağduru olmak açısından herhangi nitelik aranmamaktadır. Herkes bu suçun mağduru olabilir.

Bu suçun oluşması için başkasına ait bir malın alınması suretiyle yarar sağlanması gerekir. Failin sağladığı bu yarar karşısında malvarlığında zarar oluşan kimse bu suçun mağdurdur. Bu kimsenin kim olduğu olaya göre belirlenmelidir. Örneğin bir kimsenin banka hesabından başka bir hesaba havale yapılması yoluyla hırsızlık suçu işlendiğinde mağdur hesap sahibi olacaktır. Öte yandan hesap sahibi ile banka arasında yapılan bir sözleşme dolayısıyla bu tip bir hırsızlık fiilinden bankanın sorumlu tutulacağı

³⁸⁵ “...Tüm dosya içeriğine göre; sanığın ATM cihazına yerleştirdiği düzenek sebebiyle katılanın banka kartının cihazda sıkıştığı, arıza uyarısı gelmesinden şüphelenen katılanın banka görevlisine haber vermesi üzerine suça konu aparatın ve aparatın içine takılmış olan kartın ele geçirildiği somut olayda; sanığın eyleminin TCK'nın 141/1. maddesinde tanımlanan hırsızlığa teşebbüs suçunu oluşturduğu gözetilmeden, aynı Kanun'un 142/2-e maddesi uygulanmak suretiyle yazılı şekilde hüküm kurulması...” (YARGITAY 2. Ceza Dairesi, 06/03/2019 Tarih, 2017/5412 E - 2019/4230 K – UYAP'tan alınmıştır.)

kararlařtırıldıysa bu durumda bankanın mağdurluđu kabul edilecektir. Tüzel kişiler suçun mağduru olamayacağı için banka suçtan zarar gören olarak kabul edilecektir.

3.1.3.4. Konu

Hırsızlık suçunun konusu başkasına ait taşınır maldır.

Bilişim sistemlerinin kullanılması suretiyle işlenen hırsızlık suçunun konusu ise para, hisse senedi, altın vb. gibi menkul değerleri temsil eden veridir. Burada suç konusu olan verinin herhangi bir veri olmayıp para vb. değerleri temsil eden veri olması gerekir³⁸⁶. Bunun dışındaki verilerin ele geçirilmesi durumunda bu suç oluşmaz. Örneğin kişisel bilgilerin ele geçirilmesi durumu TCK'nın 135. maddesinde ayrı bir suç olarak düzenlenmiştir. Bunun gibi özel bir suç tipi olarak düzenlenmeyen ancak para vb. değerleri de temsil etmeyen verilerin ele geçirilmesi durumunda ise TCK'nın 244. maddesinin 2. fıkrasında yer alan suçun değerlendirilmesi gerekecektir.

Hırsızlık suçunda bir malın zilyedinden çalınmasıyla da suç oluşacağı ifade edilmekte ve ancak suçun malın maliki tarafından zilyedine karşı işlenemeyeceği ifade edilmektedir³⁸⁷. Bilişim yoluyla işlenen hırsızlık suçunda ise böyle bir durum söz konusu değildir. Zira bu suçun konusu malvarlığını temsil eden verilerdir. Örneğin bir kimsenin banka hesabında bulunan para onun kabul edilecektir. Diğer malvarlığı unsurlarında olduğu gibi kişinin emaneten verdiği bir eşyayı gidip zilyedinden geri alması gibi bir durum söz konusu olamayacaktır. Bir kimsenin borç para verdiği kimseye karşı bu suçu işlemesi durumunda ise ancak alacağın tahsili için hırsızlık suçu söz konusu olabilecektir.

3.1.3.5. Netice

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu, malvarlığını temsil eden verilerin alınmasıyla tamamlanır. Ayrıca bir neticenin meydana gelmesi aranmaz.

Suçun oluşması için söz konusu malvarlığının fail tarafından “kendisine veya başkasına bir yarar sağlamak maksadıyla” alınması gerekir. Failin böyle bir yarar sağlaması durumunda mağdur da malvarlığı açısından zarara uğrayacaktır. Dolayısıyla bu suç zarar suçudur. Ancak suçun oluşması için bu yararın oluşması şart değildir. Zira madde metninde eşyanın “kendisine veya başkasına bir yarar sağlamak maksadıyla” alınması şartı aranmış ancak bu yararın sağlanmış olmasını şart koşmamıştır. Madde metninde, başka suçlarda örneğin TCK 245/1. maddesindeki suçta olduğu gibi “kendisine veya başkasına bir yarar sağlarsa” ifadesi bulunsaydı bu durumda bir neticenin de gerçekleşmesi aranacaktı.

³⁸⁶ “...Verilerin hukuka aykırı olarak ele geçirilip, bundan da yarar sağlanmasının; ekonomik değer taşısa dahi veriyi taşınır mal haline getirmeyeceği, bu itibarla; Knight Online oyunundaki katılana ait karakterin hukuka aykırı bir şekilde ele geçirilmesi eyleminin, 5237 sayılı TCK'nın 244/2-4. maddesindeki bilişim suçunu oluşturacağı gözetilmeksizin, suç vasfında yanılığa düşülerek yazılı şekilde TCK'nın 142/2-e maddesi gereğince hırsızlık suçundan hüküm kurulması...” (YARGITAY, 2. Ceza Dairesi, 13/01/2020 Tarih, 2019/11010 E, 2020/568K – UYAP'tan alınmıştır.)

³⁸⁷ KOCA/ÜZÜLMEZ, s. 555-556.

3.1.4. Manevi Unsurlar

Hırsızlık suçu yalnızca kasten işlenebilir. Failin, suçun kanuni tanımındaki unsurları bilerek hareket etmesi gerekir. Dolayısıyla hırsızlık suçunun bir nitelikli hali olan bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu da yalnızca kasten işlenebilir bir suçtur. Bu suçun taksirle işlenmesi mümkün değildir.

Fail bir başka kimseye ait veriler üzerinde alma fiilini işlediğini biliyorsa bu suçun oluşması için yeterlidir. Bu verilerin kime ait olduğunu bilmesi gerekmez. Her ne kadar bilişim sistemlerinde genelde kişilere ait isim bilgileri yer alsın da bunun yer almamasının bir önemi yoktur. Örneğin Kripto para cüzdanı (blockchain wallet) söz konusu olduğunda anonimlik durumu daha yüksektir. Ancak fail kime ait olduğunu bilmeseydi dahi bir başkasına ait olduğunu bildiği bir hesaptan para aktarımı yapıyorsa hırsızlık fiili oluşmuştur. Söz konusu hesabın bir kişiye ait olduğunu düşünerek hırsızlık fiilini işlemesi ancak hesabın başka bir kimseye ait olması da bu durumu değiştirmeyecektir.

Öte yandan fail kendisine ait olduğunu zannederek başkasına veriler üzerinde alma fiilini işlerse bu durumda hatasından yararlanacaktır. Zira bu durumda failin kastı da yoktur ve bu suçun taksirle işlenen hali düzenlenmemiştir.

Fail, mağdurun rızası olduğunu zannederek alma fiilini işlerse de bu hatasından yararlanır. Rızanın yokluğu madde metninde de arandığından tipikliğin olumsuz unsurunu oluşturmaktadır³⁸⁸.

Suçun oluşması için ayrıca failin kendisine veya başkasına yarara sağlamak amacıyla hareket etmesi gerekir. Ancak suçun oluşması açısından failin başlangıçta hedeflediği artışa kavuşması şart değildir, bu amaçla hareket etmiş olması suçun oluşması açısından yeterlidir.

3.1.5. Hukuka Aykırılık

Hırsızlık suçunun oluşabilmesi için failin, zilyedinin rızası olmadan bir malı alması gerekir. Dolayısıyla bu suç açısından rıza bir hukuka uygunluk sebebi olarak kabul edilebilir. Öte yandan rızanın varlığı madde metninde de bir unsur olarak yer almıştır. Dolayısıyla rızanın varlığı halinde eylem tipikliği de yitirecektir.

Bir kimse öldüğünde malvarlığı kendiliğinden mirasçılara geçer. Bu sebeple hesap sahibinin ölmesi halinde hesap bilgilerini bir şekilde bilen mirasçının bu hesaptaki paralar üzerinde tasarrufta bulunması suç oluşturmaz.

3.1.6. Suçun Özel Görünüş Biçimleri

3.1.6.1. Teşebbüs

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun oluşması için para ya da benzeri bir değeri temsil eden bir verinin zilyedinin rızası olmaksızın alınması gerekir. Alma eyleminin tamamlanmasıyla suç da tamamlanmış olur. Failin icra hareketlerine

³⁸⁸ KOCA/ÜZÜLMEZ, s.586.

başlaması ancak bir şekilde alma eylemi tamamlanamadan suçun yarıda kalması durumunda suç teşebbüs aşamasında kalmış kabul edilir.

Failin parayı hesabına transfer etmesi ancak bu parayı çekememesi ya da bu paraya bloke konulması suçun teşebbüs aşamasında kalmasına sebep olmaz³⁸⁹. Bu suçun tamamlanması için alma eyleminin gerçekleşmiş olması yeterlidir.

3.1.6.2. İştirak

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu iştirak açısından bir özellik göstermez. İştirakin her türlü suçu bu suç açısından mümkündür. İştirakin varlığı halinde TCK'nın 37, 38, 39, 40 ve 41. maddeleri uygulanacaktır.

TCK'nın 40/1. maddesinde kasten ve hukuka aykırı olarak işlenen bir fiilin varlığı halinde suçun işlenişine iştirak eden kişilerin şahsi sebepler göz ardı edilerek kendi kusuruna göre cezalandırılacağı düzenlenmiştir. Bu bakımdan müşterek faillerden biri ile mağdur arasında TCK'nın 167. maddesinde düzenlenen suçun yakın akrabalar arasında işlenmesinden kaynaklı şahsi cezasızlık sebebi varsa yalnızca bu fail bu maddeden yararlanacak, diğer failler cezalandırılacaktır.

3.1.6.3. İçtima

Failin tek bir suç işleme kararı kapsamında aynı mağdura ait verilerinden belirli aralıklarla kendi hesabına veri aktarımı yapması durumunda zincirleme suç hükümleri uygulanacaktır.

Failin bir bankanın sistemine girerek aynı anda birden fazla mağdurun hesabından kendi hesabına tek bir hareket ile para aktarması durumunda aynı neviden fikri içtima hükmünün tartışılması gerekir. Ancak failin tek tek failleri değil doğrudan bankanın sistemini hedef alması durumunda ise tek bir suçun olduğu kabul edilmelidir³⁹⁰.

Yeni TCK'nın yürürlüğe girmesinden sonra bazı fiillerin TCK'nın 244/4. fıkrasındaki suç mu yoksa 142/2-e maddesindeki suç mu oluşturduğu konusunda farklı görüşler ortaya çıkmıştır. İlgili Ceza Genel Kurulu Kararında üzere TCK'nın 244/4 maddesi tali nitelikte bir madde olduğu vurgulanmış, dolayısıyla 244/4 ile 142/2-e suçlarının her ikisine uyan eylemlerle ilgili olarak TCK'nın 142/2-e maddesi uygulanması gerektiği belirtilmiştir³⁹¹.

Bir kimsenin hesabından internet bankacılığı yoluyla başka bir kimsenin hesabına para aktarılması durumunda TCK'nın 142/2-e maddesinde düzenlenen bilişim sistemlerinin

³⁸⁹ “Suça konu telefon bedelinin katılan tarafından sanığın adına kayıtlı posta çeki hesabına yatırılması neticesinde sanığın haksız menfaati temin etmesinden sonra, savcılık yazısına istinaden bu hesaba bloke konulması karşısında, sanığın eyleminin teşebbüs aşamasında kalmayıp atılı suçun tamamlandığı dikkate alınarak, sanık hakkında tamamlanmış suç hükümlerine göre ceza tayin edilmesi gerekirken...” Yargıtay 15. Ceza Dairesi, 11/06/2020 tarih 2017/30420E - 2020/5447K UYAP’tan alınmıştır.

³⁹⁰ DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s. 474.

³⁹¹ “...Ayrıca maddede ‘başka bir suçu oluşturmaması halinde’ denilerek ‘tali norm’ niteliğinde bir düzenleme yapılmıştır. Yani bilişim sistemleri aracılığıyla bir çıkar sağlandığında öncelikle bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık, zimmet gibi asli (birinci derecede) olan önce uygulanması gereken bir başka suçun oluşup oluşmadığı tartışılmalı eylem başka bir suçu oluşturmamışsa o zaman Türk Ceza Kanunu’nun 244/4. maddesi irdelenmelidir...” (Yargıtay Ceza Genel Kurulu, 17.11.2009 tarih ve 2009/11-193 E 2009/268 K - UYAP’tan alınmıştır.)

kullanılması suretiyle hırsızlık suçu söz konusu olacaktır³⁹². Ancak bir kimseye ait banka kartı veya kredi kartı bilgilerinin kullanılması suretiyle başka bir hesaba para aktarımı yapılması durumunda TCK'nın 245/1. maddesi uygulanacaktır. Zira banka veya kredi kartlarının kullanılması yoluyla haksız yarar elde edilmesini düzenleyen 245/1 maddesi 142/2-e maddesine nazaran daha özel nitelikte bir düzenlemedir.

Failin mağdurun internet bankacılığına giriş yaptıktan sonra buradan kendi hesabına ya da bir başka hesaba havale yapması durumunda failin banka sistemine girmiş olması dolayısıyla ayrıca 243 ya da 244. maddeden ceza verilmez. Failin buradaki eylemi bir bütün olarak hırsızlık suçunu oluşturmaktadır³⁹³.

3.1.7. Suçun Gece Vakti İşlenmesi

TCK'nın 143. maddesi "*Hırsızlık suçunun gece vakti işlenmesi halinde, verilecek ceza yarı oranında artırılır.*" hükmüne yer vermektedir. Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu da hırsızlık suçunun nitelikli hallerinden biridir. Dolayısıyla bu suçun gece vakti işlenmesi durumunda da verilecek ceza yarı oranında arttırılacaktır.

TCK'nın tanımlar başlıklı 6. maddesinin e bendine göre "*Gece vakti deyiminden; güneşin batmasından bir saat sonra başlayan ve doğmasından bir saat evvele kadar devam eden zaman süresi*" anlaşılmalıdır.

3.1.8. Daha Az Cezayı Gerektiren Haller

3.1.8.1. Hırsızlık Suçunun, Paydaş veya Elbirliği İle Malik Olunan Mal Üzerinde İşlenmesi

TCK'nın 144. maddesinin 1. fıkrasının a bendinde "*hırsızlık suçunun; paydaş veya elbirliği ile malik olunan mal üzerinde, ... işlenmesi halinde, şikayet üzerine, fail hakkında iki aydan bir yıla kadar hapis veya adli para cezasına hükmolunur.*" düzenlemesi yer almaktadır.

Daha az cezayı gerektiren bu halin bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunda da meydana gelmesi mümkündür. Örneğin birden fazla kişi bir bankaya başvurarak ortak banka hesaba açabilmekte hatta bunun için aralarında kan bağıının varlığı dahi aranmamaktadır. Bu durumda hesap sahiplerinden birisi, diğerlerinin bilgisi olmaksızın söz konusu hesaptan aktarım yaparsa bu durumda TCK'nın 144/1-a maddesinin uygulanması gerekecektir.

Bu halin varlığı durumunda suçun soruşturması da şikâyete bağlı hale gelecektir.

³⁹² "...katılanın banka hesabına internet bankacılığı yoluyla girip başkalarına ait kredi kartlarına para havale ederek çekmekten ibaret eylemlerin, suç tarihi itibarıyla 5237 sayılı TCK'nın 142/2-e maddesinde öngörülen "bilişim suretiyle hırsızlık" suçunu oluşturacağı gözetilmeden, suç vasfında yanılığa düşülerek yazılı şekilde, TCK'nın 244/4 ve 43. maddeleri uyarınca mahkumiyet hükümleri kurulması..." (Yargıtay 8. Ceza Dairesi, 27.01.2020 tarih, 2019/27768 E, 2020/1040 K – UYAP'tan alınmıştır.)

³⁹³ "...Sanığın, müştekinin bilgisi ve rızası dışında İş Bankası Mustafakemalpaşa Şubesinde bulunan hesabındaki parasını, internet bankacılığı kullanılarak, kendi hesabına havale etmek suretiyle çalması şeklindeki eyleminin, 5237 sayılı TCK'nın 142/2-e maddesinde düzenlenen "bilişim sistemlerinin kullanılması suretiyle hırsızlık" suçunu oluşturduğu gözetilmeden; sanık hakkında ayrıca aynı Kanun'un 244/2, 244/3 maddeleri gereğince cezalandırılmasına karar verilmesi..." (Yargıtay 2. Ceza Dairesi, 01/07/2020 Tarih, 2020/13398 E, 2020/7421 K – UYAP'tan alınmıştır.)

3.1.8.2. Hırsızlık Suçunun Bir Hukuki İlişkiye Dayanan Alacağı Tahsil Amacıyla İşlenmesi

TCK'nın 144. maddesinin 1. fıkrasının b bendinde “*hırsızlık suçunun; ... bir hukuki ilişkiye dayanan alacağı tahsil amacıyla, işlenmesi halinde, şikâyet üzerine, fail hakkında iki aydan bir yıla kadar hapis veya adli para cezasına hükmolunur.*” düzenlemesi yer almaktadır.

Bu halin söz konusu olabilmesi için fail ile mağdur arasında bir borç ilişkisi olmalıdır. Bu borç ilişkisi hukuk düzeni tarafından korunan bir borç ilişkisi olmalıdır³⁹⁴. Ancak bu borcun tahsil kabiliyeti bulunan bir borç olmasına gerek yoktur. Örneğin zamanaşımına uğramış bir borç da söz konusu olduğunda yine bu hüküm uygulanacaktır³⁹⁵.

Müşterek faillik durumunda faillerinden yalnızca birisi için böyle bir borç ilişkisi mevcutsa bu fail söz konusu indirimden yararlanacak, diğer failler yararlanamayacaktır³⁹⁶.

Bu halde soruşturma ve kovuşturma yapılması için mağdurun şikâyeti aranmaktadır.

3.1.8.3. Malın Değerinin Az Olması

TCK'nın 145. maddesinde “*Hırsızlık suçunun konusunu oluşturan malın değerinin azlığı nedeniyle, verilecek cezada indirim yapılabileceği gibi, suçun işleniş şekli ve özellikleri de göz önünde bulundurularak, ceza vermekten de vazgeçilebilir.*” denilmek suretiyle cezanın indirilmesine ya da ceza verilmemesine ilişkin bir düzenleme yapılmıştır.

Suç konusunun değerinin az olması fiili hırsızlık suçu olmaktan çıkarmaz. Yalnızca bu durumda hâkime cezayı indirmek ya da ceza vermekten tamamen vazgeçmek hususunda takdir hakkı tanınmıştır. Yani hâkim bu takdir yetkisini kullanarak faile ceza vermekten vazgeçiyorsa beraat değil ceza verilmesine yer olmadığına dair karar vermelidir.

3.1.9. Şahsi Cezasızlık Sebebi veya Cezada İndirim Yapılmasını Gerektiren Şahsi Sebep

TCK'nın 167. maddesinde “*Yağma ve nitelikli yağma hariç, bu bölümde yer alan suçların; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.*

(2) *Bu suçların, haklarında ayrılık kararı verilmiş olan eşlerden birinin, aynı konutta beraber yaşamayan kardeşlerden birinin, aynı konutta beraber yaşamakta olan amca, dayı, hala, teyze, yeğen veya ikinci derecede kayın hısımlarının zararına olarak işlenmesi halinde; ilgili akraba hakkında şikâyet üzerine verilecek ceza, yarısı oranında indirilir.*” hükmüne yer verilmiştir.

3.1.10 Etkin Pişmanlık

Bu suça ilişkin etkin pişmanlık hükmüne TCK'nın 168. maddesinde yer verilmiştir. Bu maddeye göre hırsızlık suçunu tamamlayan fail, azmettiren ya da yardım eden henüz

³⁹⁴ KOCA/ÜZÜLMEZ, s. 610; ÖZBEK/DOĞAN/BACAĞIZ/TEPE, s.634.

³⁹⁵ TEZCAN/ERDEM/ÖNOK, 731-732; KOCA/ÜZÜLMEZ, s. 610.

³⁹⁶ KOCA/ÜZÜLMEZ, s. 610.

hakkında kovuşturma başlamadan önce mağdurun zararını giderirse verilecek ceza üçte ikisine kadar indirilecektir.

Fail, kovuşturma başladıktan sonra henüz hüküm verilmemişken zararı giderirse verilecek ceza yarısına kadar indirilecektir.

Bu durumlar zararın tamamen giderilmesi hali için söz konusudur. Kısmen geri verme halinde bu hükümlerin uygulanabilmesi için mağdurun rıza göstermesi gerekir. Zararın tamamen giderilmesi halinde ise mağdurun rızası aranmaz.

Suçun iştirak halinde işlenmesi durumunda zararın giderilmesine katılmayan fail, azmettiren ya da yardım eden etkin pişmanlıktan yararlanamaz. Her bir suç ortağının kendi pişmanlığını ortaya koyması gerekir.

3.1.11. Soruşturma Usulü ve Yaptırım

Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun cezası beş yıldan on yıla kadar hapis cezasıdır.

Bu suç re'sen soruşturulur.

5235 Sayılı Adli Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 10. 11. ve 12. maddeleri dolayısıyla görevli mahkeme asliye ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiği yer mahkemesidir.

TCK'nın 169. maddesinde “*Hırsızlık, güveni kötüye kullanma ve dolandırıcılık suçlarının işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*” denilmektedir. Dolayısıyla TCK'nın 142/2-e maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, TCK'nın 60. maddesinde düzenlenen tüzel kişilere hakkında güvenlik tedbirleri uygulanacaktır.

3.2. Bilişim Sistemlerinin Kullanılması Suretiyle Dolandırıcılık Suçu (158/1-f)

3.2.1. Genel Olarak

TCK'nın “*Kişilere Karşı Suçlar*” Başlıklı 2. Kısımın Onuncu Bölümünde, “*Malvarlığına Karşı Suçlar*” başlığı altında yer alan 157. maddesinde “*Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişiye bir yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası verilir.*” denilerek dolandırıcılık suçunun temel hali düzenlenmiş, nitelikli dolandırıcılık başlıklı 158. maddesinin 1. fıkrasının f bendinde ise dolandırıcılık suçunun “*Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle*” işlenmesi halinde üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunacağı düzenlenmiştir.

158/1-f maddesinde her ne kadar banka ve kredi kurumlarının araç olarak kullanılması da nitelikli hal sayıldıysa da çalışmamızın konusu itibarıyla bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu incelenecektir.

Bu suçla failin, bilişim sistemlerini kullanarak, hileli davranışlar sonucu mağduru aldatması ve bu yolla mağdurun zararına sebep olarak kendine ya da başkasına yarar sağlaması suç olarak düzenlenmiştir.

Günümüzde bilişim sistemlerinin oldukça gelişmesi ve bu sistemlerle sesli, görüntülü ve yazılı iletişim kolaylaşması dolayısıyla bu günlük hayatta ilişkinin önemli bir kısmı bu sistemler aracılığıyla yapılır olmuştur. Alışverişlerin internet üzerinden yapılabilmesinin yanı sıra internet üzerinden para transferinin yapılabilmesini dolayısıyla ticari yaşam da bilişim sistemleri üzerinden işlemeye başlamıştır. Bilişim sistemleri kullanılarak yapılan alışverişler, kişiler açısından hem daha az maliyetli hem de daha az zahmetli olduğu için günlük yaşamın vazgeçilmez bir unsuru olmuştur. Bu sistemlerin bu kadar yaygınlaşmasının bir sonucu olarak dolandırıcılık fiilleri de bilişim sistemleri aracılığıyla işlenmeye başlamıştır. Gerçekten de bu sistemlerin kolay ulaşılabilir ve güven veren yapısı dolayısıyla bu sistemler aracılığıyla kişilerin aldatılması daha kolaydır. Ayrıca bu sistemler kullanılarak failin birden fazla kişiye çok daha kolay ulaşım imkânı bulması da bilişim sistemlerinin kullanılması suretiyle işlenen dolandırıcılık fiillerine ayrı bir boyut katmaktadır. Tüm bu sebepler dolayısıyla, bilişim sistemlerini kullanan kişilerin bu sistemleri güven içinde kullanması, iradelerinin ve malvarlıklarının korunması amacıyla bu nitelikli hal düzenlenmiştir.

Madde gerekçesinde “*Dolandırıcılık suçunun, bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenmesi de, birinci fıkranın (f) bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin ya da birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir.*” denilerek bu suçun bilişim sistemlerinin, kişilerin aldatılmasını kolaylaştıran unsuru dolayısıyla bir nitelikli hal olarak düzenlendiği vurgulanmıştır.

Dolandırıcılık suçunun basit hali 5271 sayılı CMK’nın 253. maddesi uyarınca uzlaşma kapsamında olmasına rağmen nitelikli hallerinde böyle bir durum söz konusu değildir.

3.2.2. Korunan Hukuki Yarar

Bu suçla kişilerin malvarlıkları, kişiler arası iyi niyet ve güven duygusu ve kişinin özgür iradesi korunmaktadır. Bu husus madde gerekçesinde de “*Dolandırıcılık, hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kişinin kendisine veya başkasına yarar sağlamasıdır. Bu bakımdan dolandırıcılık suçu, kişilerin malvarlığına karşı işlenen bir suçtur. Söz konusu suç tanımı ile kişilerin sahip bulunduğu malvarlığı hakkının korunması amaçlanmıştır. Ayrıca, bu suçun işlenişi sırasında hileli davranışlar ile kişiler aldatılmaktadır. Aldatıcı nitelik taşıyan hareketlerle, kişiler arasındaki ilişkilerde var olması gereken iyi niyet ve güven ihlâl edilmektedir. Bu suretle kişinin irade serbestisi etkilenmekte ve irade özgürlüğü ihlâl edilmektedir.*” denilmek suretiyle ifade edilmiştir.

3.2.3. Maddi Unsurlar

3.2.3.1. Fiil

Dolandırıcılık suçunun gerçekleşmesi için failin hileli davranışlarla bir başkasını aldatarak bu kişinin ya da bir başkasının zarara uğramasına sebep olmasını ve kendisine ya da bir başkasına yarar sağlamasını aramıştır. Dolayısıyla dolandırıcılık suçunun gerçekleşebilmesi için fail birtakım hileli davranışlarda bulunmalı ve mağduru aldatmalıdır. Fail bu hileli davranışları sonucunda kendisi ya da bir başkası lehine yarar sağlamalıdır. Bu yarar mağdurun ya da bir başkasının aleyhine olmalıdır. Bu yarar ile zarar arasında illiyet bağılı bulunmalıdır.

Bu suç madde gerekçesinde de belirtildiği üzere çok hareketli bir suçtur. Zira bu suçun oluşması için tek bir hareket yeterli değildir. Hileli davranışlar sergilenmesi, bu yolla mağdurun aldatılması ve zarara uğratılması failin de kendisi ya da bir başkası için yarar sağlaması gibi birden fazla hareketin tamamının gerçekleşmesi gerekir.

Bu suç açısından basit bir hile suç unsuru olarak kabul edilmemekte, failin mağduru aldatabilecek nitelikli bir hile yapması aranmaktadır. Ancak doktrinde bu hilenin mağduru aldatmış olmasının yeterli olduğu, objektif olarak aldatmaya elverişli bir fiilin yapılmasının yani hilenin belirli bir ağırlığa ulaşmasının şart olmadığı yönünde görüşler de vardır³⁹⁷. Bu görüş kanunda hilenin varlığının arandığını bu davranışların objektif olarak kandırmaya elverişli olmasının aranmadığı ifade etmiştir.

Öte yandan uygulamada hukuki uyumsuzluk kabul edilebilecek pek çok durumun da dolandırıcılık suçu kapsamında şikâyet edildiği görülmektedir. Örneğin kişinin kırmızı rengini sipariş verdiği ürünün bordo renginin gelmesi, ürünün kusurlu olması gibi durumlar zaman zaman dolandırıcılık suçunu oluşturduğu zannıyla şikâyet edilmektedir. Belirtmek gerekir ki bu tür durumlarda aldatıcılık unsuru gerçekleştirmemiş olduğundan dolandırıcılık suçu oluşmayacaktır. Elbette failin oldukça pahalı bir ürünü sattığı izlenimini uyandırdıktan sonra bunun yerine çok düşük kalitede bir ürün göndermesi durumunda dolandırıcılık suçu değerlendirilmelidir. Benzer şekilde kişiler arasında bir ticari ilişkinin gerçekleşmesi ancak daha sonra taraflardan birinin caymak istemesi ya da bir kimsenin borcunu ödememek için “sonra veririm, şu an yanımda yok” gibi basit nitelikte ve aldatmaya elverişli olmayan yalanlar söylemesi de dolandırıcılık suçunu oluşturmaz. Ancak internet siteleri üzerinden ilan vererek ödemeyi aldıktan sonra ürünü göndermeyen failin eylemi bilişim sistemlerinin kullanılması suretiyle dolandırıcılık olarak değerlendirilmektedir³⁹⁸.

³⁹⁷ TEZCAN/ERDEM/ÖNOK, s. 813.

³⁹⁸ “... İbrahim Varol ismiyle "www.sahibinden.com" adlı internet sitesinde dizüstü bilgisayar satışı için ilan veren sanığın, bu ilanı görüp kendisini telefonla arayan katılanla, bilgisayarların 1500 Lira bedelle satışı konusunda anlaşması, bir süre sonra katılanı telefonla arayarak bilgisayarları kargoya verdiğini söyleyip, bedelini vereceği hesap numarasına yatırmasını istemesi üzerine, bildirdiği banka hesabına 1500 Lira yatıran katılana sözde alışverişe konu bilgisayarları göndermemesi şeklinde gerçekleşen olayda; sanığın hem bilişim sistemini araç olarak kullanmak hem de basın ve yayın aracının sağladığı kolaylıktan yararlanmak suretiyle suçu işlediği anlaşıldığından, sanığın bu eylemi ile TCK'nun 158. maddesinin 1. fıkrasının (f) bendinde düzenlenen "bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık" ve aynı fıkranın (g) bendinde düzenlenen "basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak

Dolandırıcılık suçunun bilişim sistemleri kullanılarak işlenmesi ise nitelikli hal olarak düzenlenmiştir. Bu nitelikli halin oluşması için bilişim sistemlerinin kullanılarak gerçek bir kişinin aldatılmış olması aranır. Hileli hareket bir bilişim sistemine yöneltilemez. Sistemde yer alan açıklar kullanılarak haksız bir yararın sağlanması durumunda TCK 142/2-e ya da TCK'nın 244/4. maddelerinde düzenlenen suçlardan birisi oluşur.

Bu suç genellikle internet üzerinden aldatıcı nitelikte satılık eşya ilanı verilmesi ve bu ilana aldanarak irtibat kuran kişilerden haksız yararın temin edilmesi şeklinde işlenmektedir.

Fail ile mağdurun internet üzerinden görüştüktan sonra yüz yüze de bir araya gelip konuşmaları ve bunun akabinde failin mağduru kandırarak yarar sağlaması durumunda basit dolandırıcılık suçu oluşacaktır.

Bu icrai bir davranışla işlenebileceği gibi ihmali bir davranışla da işlenebilir. Bu husus da madde gerekçesinde *“Hile, icrai bir davranışla gerçekleştirilebileceği gibi; karşı tarafın içine düştüğü hatadan, bir konuda yanlış bilgi sahibi olmasından yararlanarak da, yani ihmali davranışla da, gerçekleştirilebilir. Ancak, bu durumda kişinin, hataya düşen karşı tarafı bilgilendirmek konusunda yükümlülüğünün olması gerekir. Hataya düşen kişi ile hukukî ilişkide bulunulan durumlarda, böyle bir yükümlülük vardır. Ayrıca, muhatabın belli bir husustaki hatası karşısında kişinin ihmali davranışının, örneğin susmasının, bir beyan, açıklama değerini taşıması gerekir.”* denilmek suretiyle ifade edilmiştir. Örneğin bir ürünü satan kişinin aldatmak için başka bir çaba göstermemesine rağmen, mağdurun ürünle ilgili düştüğü bir yanılgıyı düzeltmeyerek ürünün satışını gerçekleşmesi durumunda dolandırıcılık suçu ihmali davranışla işlenmiş olacaktır.

3.2.3.2. Fail

Bu suç fail açısından herhangi bir özellik arz etmez, herkes bu suçun faili olabilir. Bir başkasını aldatarak kendine veya başkasına yarar sağlayan kişi bu suçun failidir.

Failin, mağdurun belirli bir dereceden yakını olması durumunda TCK'nın 167. dolayısıyla ceza verilmeyecek ya da cezasında indirim yapılacaktır. Fail ile mağdur arasında bir borç ilişkisinin bulunması durumunda ise TCK'nın 159. maddesi dolayısıyla failin cezası indirim yapılacaktır.

3.2.3.3. Mağdur

Bu suç mağduru olmak açısından herhangi nitelik aranmamaktadır. Herkes bu suçun mağduru olabilir.

Dolandırıcılık suçlarında da mağdur gerçek bir kişidir. Aldatıcı hareket gerçek bir kişiye yönetilmeli ve onun aldatılması yoluyla yarar sağlanmalıdır.

Bu suçun oluşması için failin *“hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak”* bir yarar elde etmesi aranmıştır. Yani yarar aldatılan kişinin malvarlığı aleyhine olabileceği gibi bir başkasının malvarlığı aleyhine de olabilir. Bu

suretiyle dolandırıcılık" olmak üzere dolandırıcılık suçunun iki farklı nitelikli halinin olduğu, bu durumda suçun daha ağır cezayı içeren nitelikli hali olan "bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık" suçundan hüküm kurulması gerektiği kabul edilmelidir..." (Yargıtay Ceza Genel Kurulu, 17.01.2017 tarih, 2015/15-867 E- 2017/13 K – UYAP'tan alınmıştır.)

durumda hem aldatılan kişinin hem de malvarlığı zarara uğratılan kişinin mağdur olarak kabul edilmesi gerekir. Öte yandan doktrinde yalnızca aldatılan kişinin mağdur kabul edilmesi gerektiği, bu aldatma hareketi neticesinde malvarlığı zarara uğrayan kişinin ise bu suçtan ötürü zarar gören olduğu kabul edilmektedir³⁹⁹.

3.2.3.4. Konu

Bu suçun konusu yarardır.

Bu suçun işlenmesi neticesinde elde edilecek yarar maddi nitelikte bir yarar olmalıdır. Bu yarar doğrudan para temin edilmesi şeklinde olabileceği gibi fail, mağduru kandırarak telefonuna TL yükletebilir, faturalarını ödeyebilir, kendisine bir ürün satın aldırabilir. Önemli olan ekonomik olarak ölçülebilen bir yararın temin edilmiş olmasıdır.

3.2.4. Manevi Unsurlar

Dolandırıcılık suçu yalnızca kasten işlenebilir. Failin, suçun kanuni tanımındaki unsurları bilerek hareket etmesi gerekir. Fail, hileli davranışları bilerek yapmalı, bu davranışlarla bir başkasını bilerek zarara uğratmalı ve kendisine ya da bir başkasına bilerek yarar sağlamalıdır.

Dolandırıcılık suçunun bir nitelikli hali olan bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu da yalnızca kasten işlenebilir bir suçtur. Bu suçun taksirle işlenmesi mümkün değildir.

Doktrinde bu suçun olası kast ile de işlenebileceği belirtilmiştir⁴⁰⁰.

3.2.5. Hukuka Aykırılık

3.2.6. Suçun Özel Görünüş Biçimleri

3.2.6.1. Teşebbüs

Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu failin aldatıcı hareketlerinin neticesinde kendisi ya da başkası lehine yarar sağlamasıyla tamamlanır. Suçun icra hareketlerine başlanmasına rağmen bu yararın sağlanamaması durumunda suç teşebbüs aşamasında kalmış olacaktır⁴⁰¹. Örneğin failin bir kimse ile bir şekilde bilişim sistemleri üzerinden iletişime geçmesi ve bu kişiyi aldatmaya yönelik hareketlerde bulunması ama bu kişinin aldanmaması ya da aldatılan kişinin durumu anlaması henüz suç tamamlanmadan anlaması halinde suç teşebbüs aşamasında kalacaktır. Suçun hazırlık hareketleri tamamlanıp henüz icra hareketlerine başlanmadan önceki aşamada ise suçun teşebbüs

³⁹⁹ KOCA/ÜZÜLMEZ, s. 688-689.

⁴⁰⁰ KOCA/ÜZÜLMEZ, s.698.

⁴⁰¹ “...Sanığın, olay tarihinde arkadaşı adına kayıtlı Vodafone Vınn hattından internete girmek suretiyle katılan Ali Nihat Keskin'in email ve buna bağlı oluşturduğu facebook hesabının şifresini kırmak suretiyle katılanın izni ve bilgisi olmaksızın erişim sağladığı ve katılanın erişimini şifresini değiştirerek engellediği, ardından da arkadaş listesinde bulunan şikayetçi Fevzi Aktan'dan internet bankacılığı ile para göndermesini istediği, şikayetçi Fevzi'nin şüphelenip katılan Ali Nihat'ı araması ile hesabının ele geçirildiğini öğrendiği ve parayı göndermediği, bu suretle sanığın bilişim sistemine hukuka aykırı olarak girmek suretiyle verilerin yok edilmesi veya değiştirilmesi ve teşebbüs aşamasında kalan bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçlarını...” (YARGITAY 15. Ceza Dairesi, 17/04/2018, 2017/31912 Esas, 2018/2652 Karar Sayılı Kararı – UYAP’tan alınmıştır.)

aşamasında kaldığı kabulü yanlış olacaktır. Failin mağduru aldatması, mağdurun da aldanarak malvarlığında tasarrufta bulunması buna rağmen failin bu yararı elde edememesi durumunda da teşebbüs gerçekleşmiş olacaktır.

Failin kendisini iletişime geçtiği kişilerin arkadaşımı gibi tanıtmak suretiyle bu kişilerin bilgilerini alması ancak bunları bir şekilde kullanamaması durumunda bu hareket hazırlık hareketi olarak kabul edilecek ve fail henüz suçun icrasına başlamamış olacağından suçun teşebbüs aşamasında kaldığını kabul etmek yanlış olacaktır. Çünkü failin bu hareketleri ne amaçla yapmış olduğunun tespiti mümkün değildir⁴⁰². Elbette bu durumda failin bu bilgileri ele geçirmesi ayrı bir suçu oluşturuyorsa bu suçtan ceza alacaktır.

Failin internet üzerinden ürün satmak için ilan vermesi, bu ilanda aldatıcı niteliklerin bulunması ve mağdurun da bu ilana inanarak para göndermesi ancak failin söz konusu ürünü göndermemesi durumunda bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu oluşur. Ancak failin söz konusu aldatıcı hareketlerde bulunmasına rağmen mağdurun bir şekilde durumu anlayarak parayı göndermemesi durumunda suç teşebbüs aşamasında kalmış olacaktır. Öte yandan mağdurun parayı göndermesi fakat bu para failin hesabına yattıktan sonra banka tarafından paraya bloke konulması durumunda artık suç tamamlanmış kabul edilecektir. Mağdurun bu para henüz failin hesabına yatmadan durumu anlayıp işlemi iptal etmesi durumunda da yine suç teşebbüs aşamasında kalmış olacaktır. Örneğin faile para göndermek amacıyla EFT talimatı veren mağdurun henüz işlem gerçekleşmeden durumu anlayarak EFT işlemini iptal etmesi durumunda suç teşebbüs aşamasında kalmıştır.

Bu suça ilişkin olarak gönüllü vazgeçme de mümkündür. Fail suçun icra hareketlerine başladıktan sonra, henüz yarar elde edilmeden suçu işlemekten vazgeçerse bu durumda gönüllü vazgeçme söz konusu olacaktır. Ancak yararın elde edilmesiyle suç tamamlanmış olacağından bu aşamadan sonra gönüllü vazgeçme mümkün olmayacak failin elde ettiği yararı iade etmesi durumunda etkin pişmanlık hükümleri değerlendirilecektir.

3.2.6.2. İştirak

Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçu iştirak açısından bir özellik göstermez. İştirakin her türlü bu suç açısından mümkündür. İştirakin varlığı halinde TCK'nın 37, 38, 39, 40 ve 41. maddeleri uygulanacaktır.

3.2.6.3. İçtima

Failin tek bir suç işleme kararı kapsamında aynı suçu, aynı mağdura karşı birden fazla kez ve değişik zamanlarda işlemesi durumunda zincirleme suçtan söz edilecektir. Failin tek bir suç işleme kararı kapsamında, ilk hareketin devamı niteliğinde yaptığı fiiller ayrı bir suç oluşturmayacak ve faile tek bir tamamlanmış dolandırıcılık suçundan ceza verilecektir.

Failin tek bir aldatıcı hareketle birden fazla mağduru aldatarak zarara uğratması ve bu şekilde yarar elde etmesi durumunda ise aynı neviden fikri içtima söz konusu olacaktır.

⁴⁰² DÜLGER, Bilişim Suçları Ve İnternet İletişim Hukuku, s.481.

Failin, haksız yararı sağlamak için mağdur ile iletişim kurduğu ve mağdurun iradesini aldatıcı hareketlerle yanıltılarak bir yarar elde ettiği durumda dolandırıcılık suçu oluşur. Bu suç tipini diğer suçlardan ayıran en önemli unsur aldatma unsurudur. Ortada iradesi yanıltılan bir mağdurun bulunmadığı durumda dolandırıcılık suçundan değil hırsızlıktan söz edilecektir.

Fail, mağduru aldatıp banka ve kredi kartı bilgilerini ele geçirmek suretiyle haksız bir yarar kendisi elde ediyorsa bu durumda banka ve kredi kartlarının kötüye kullanılması suçu oluşur. Fail mağdurun kart bilgilerini değil internet bankacılığı şifresini öğrenir ve bu suretle yarar elde ederse hırsızlık suçu söz konusu olacaktır.⁴⁰³ Mağdurun iradesinin yanıltılması sonucu fail lehine haksız yararın sağlanması gerçekleşiyorsa bu durumda dolandırıcılık suçu oluşacaktır. Örneğin failin mağduru kandırarak kendisine belirli bir miktar paranın havale yapılmasını sağlaması durumunda dolandırıcılık suçu söz konusu olacaktır.

Failin, bir kimsenin sosyal paylaşım sitesi hesabını ele geçirmesi durumunda TCK 244/2. maddesinde düzenlenen suç oluşur. Daha sonra bu sosyal medya hesabını kullanarak hesap sahibinin arkadaşları ile iletişime geçmesi ve kişilerden yarar temin etmesi durumunda dolandırıcılık suçundan söz edilecektir. Her ikisinin birlikte gerçekleşmesi durumunda faile her iki suçtan ayrı ayrı ceza verilmelidir.

Failin bu suçu işlerken kimliğinin ortaya çıkmasını engellemek amacıyla bir başkasına ait kimlik bilgilerini kullanması durumunda TCK'nın 136. maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçu, sahte telefon hatta kullanması durumunda sahtecilik suçları ya da 5809 sayılı Elektronik Haberleşme Kanunu'nun 56/4. maddesi ile aynı Kanunun 63. maddesi değerlendirilmelidir⁴⁰⁴. Failin mağdurlara ait kişisel bilgiler ile kredi kartı bilgilerini elde etmesi şeklinde eylemi de başlı başına TCK'nın 136. maddesinde düzenlenen suçu oluşturacaktır.⁴⁰⁵

TCK'nın 212. maddesinde “*Sahte resmi veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması halinde, hem sahtecilik hem de ilgili suçtan dolayı ayrı ayrı cezaya hükmolunur.*” hükmü yer almaktadır. Bu hüküm dolayısıyla failin sahte belgeler kullanarak dolandırıcılık suçu işlemesi durumunda gerçek içtima söz konusu olacaktır.

3.2.7. Suçun Daha Az Cezayı Gerektiren Hali

TCK'nın 159. maddesinde “*Dolandırıcılığın, bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi halinde, şikâyet üzerine, altı aydan bir yıla kadar hapis veya adli para*

⁴⁰³ “...Faillerin, müşterilerin banka hesaplarına internet bankacılığı aracılığıyla girip paraların başkasının banka hesabına transfer edilmesi şeklindeki eylemlerinin, TCK.nun 142/2-e madde ve fıkrasında düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu...” (Yargıtay 8. Ceza Dairesi, 25.02.2019 tarih 2017/20222 E - 2019/2585 K – UYAP’tan alınmıştır.)

⁴⁰⁴ GÜL, s.271.

⁴⁰⁵ “Müştekilere ait kişisel ve kredi kartı bilgilerinin elde edilerek bankalara ait çağrı merkezlerinin aranması ve sorgulama yapılması şeklinde gerçekleşen eylemleri ise TCK.nun 136. maddesinde düzenlenen kişisel verileri hukuka aykırı olarak ele geçirmek suçunu oluşturduğu...” (Yargıtay 8. Ceza Dairesi, 25.02.2019 tarih 2017/20222 E - 2019/2585 K – UYAP’tan alınmıştır.)

cezasına hükmolunur.” denilmek suretiyle suçun daha az ceza verilmesini gerektiren nitelikli hali düzenlenmiştir.

Fail ile mağdur arasında bir borç ilişkisinin bulunması bu suçun oluşmasını engellemez. Fail, tam olarak alacağı miktarınca yarar elde etse dahi hileye başvurarak mağduru zarara uğratması ve bir yarar elde etmesi dolayısıyla dolandırıcılık suçunu işlemiş olacaktır. Hukuk düzeninde kişinin hakkını hukuk düzeni yoluyla elde etmesi esastır. Dolayısıyla kanun koyucu bu hali de suç kapsamında tutmuş ancak haksızlık içeriğinin daha az olmasını da gözeterek failin cezasında indirim yapmıştır.

3.2.8. Şahsi Cezasızlık Sebebi veya Cezada İndirim Yapılmasını Gerektiren Şahsi Sebep

TCK’nın 167. maddesinde “*Yağma ve nitelikli yağma hariç, bu bölümde yer alan suçların; a) Haklarında ayrılık kararı verilmemiş eşlerden birinin, b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın, c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.*

(2) Bu suçların, haklarında ayrılık kararı verilmiş olan eşlerden birinin, aynı konutta beraber yaşamayan kardeşlerden birinin, aynı konutta beraber yaşamakta olan amca, dayı, hala, teyze, yeğen veya ikinci derecede kayın hısımlarının zararına olarak işlenmesi halinde; ilgili akraba hakkında şikâyet üzerine verilecek ceza, yarısı oranında indirilir.” hükmüne yer verilmiştir.

3.2.9. Etkin Pişmanlık

Bu suça ilişkin etkin pişmanlık hükmüne TCK’nın 168. maddesinde yer verilmiştir. Bu maddeye göre dolandırıcılık suçunu tamamlayan fail, azmettiren ya da yardım eden henüz hakkında kovuşturma başlamadan önce mağdurun zararını giderirse verilecek ceza üçte ikisine kadar indirilecektir.

Fail, kovuşturma başladıktan sonra henüz hüküm verilmemişken zararı giderirse verilecek ceza yarısına kadar indirilecektir.

Bu durumlar zararın tamamen giderilmesi hali için söz konusudur. Zararın kısmen giderilmesi halinde bu hükümlerin uygulanabilmesi için mağdurun rıza göstermesi gerekir. Zararın tamamen giderilmesi halinde ise mağdurun rızası aranmaz.

Suçun iştirak halinde işlenmesi durumunda zararın giderilmesine katılmayan suç ortakları etkin pişmanlıktan yararlanamaz. Her bir suç ortağının kendi pişmanlığını ortaya koyması gerekir.

3.2.10. Soruşturma Usulü ve Yaptırım

Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık suçunun cezası üç yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezasıdır. Ayrıca bu suç için verilecek hapis para cezasının alt sınırı dört yıldan, adli para cezası ise suçtan elde edilen yararın iki katından az olamayacaktır. Bu suç tipinde adli para cezası ve hapis cezası birlikte verilecektir. Bu yaptırımlar seçimlik değildir.

Bu suç re'sen soruřturulur. Dolandırıcılık suçunun bir hukuki ilişkiye dayanan alacağı tahsil amacıyla işlenmesi halinde ise suçun soruřturulması řikâyete baėlı olacaktır. Bu durumda suçun cezası altı aydan bir yıla kadar hapis veya adlî para cezası olacaktır. Faile ya hapis cezası ya da adli para cezası verilecektir, bu yaptırımlar seçimlik olarak düzenlenmiştir.

5235 Sayılı Adlî Yargı İlk Derece Mahkemeleri İle Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunu'nun 10. 11. ve 12. maddeleri dolayısıyla görevli mahkeme ağır ceza mahkemesi, yetkili mahkeme ise 5271 sayılı CMK 12. maddesi dolayısıyla suçun işlendiėi yer mahkemesidir.

TCK'nın 169. maddesinde “*Hırsızlık, güveni kötüye kullanma ve dolandırıcılık suçlarının işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.*” denilmektedir. Dolayısıyla TCK'nın 142/2-e maddesinde düzenlenen suçun işlenmesi suretiyle haksız menfaat temin eden tüzel kişilere, TCK'nın 60. maddesinde düzenlenen tüzel kişiler hakkında güvenlik tedbirleri uygulanacaktır.

SONUÇ

Gelişen teknoloji ile birlikte çağımızda internet ve bilişim sistemleri yaşamımızın vazgeçilmez bir unsuru olmuştur. Bilişim sistemlerinin hayatımızdaki bu yadsınamaz yeri karşısında kötü niyetli kimseler de faaliyetlerini bilişim alanlarına yöneltmiş, hem ülkemizde hem de uluslararası alanda kanun koyucular da bu faaliyetleri engellemek amacıyla birtakım yasal düzenlemeler yapmıştır. İlk olarak 1991 yılında 3756 sayılı kanunla 765 sayılı TCK'ya eklenen bilişim suçları 5237 sayılı TCK'da da düzenlenmiştir.

Bu çalışmada 5237 sayılı TCK'da düzenlenen bilişim suçları ile bilişim yoluyla işlenebilen diğer suçlar inceleme konusu yapılmış, bu suçların hangi suçlar olduğu konusunda uygulamada yaşanan tereddütler giderildikten sonra, suçlarla ilgili olarak uygulamada yaşanan karışıklıklara çözüm önerileri getirilmeye çalışılmış, bilişim suçlarının yetersiz kaldıkları noktalar vurgulanarak bu alanlarda yapılabilecek değişikliklere değinilmiş, son olarak da bu suçların yaptırımlarındaki dengesizlikler ortaya konularak bu hususta düzenlemeler önerilmiştir.

Bilişim Suçları bir üst kavram olarak değerlendirildiğinde bu kavramın alt başlıkları “doğrudan bilişim suçları” ve “dolayısıyla bilişim suçları” olacaktır. Çalışmamızın başlığında bu ifadeler yerine benzer kavramları karşılayan ancak suçların ayrımının daha net yapılmasına imkân tanıyan “bilişim suçları” ve “bilişim yoluyla işlenen suçlar” kavramlarını tercih ettik. Gerçekten de bilişim suçları TCK'nın İkinci Kitabının onuncu bölümünde yer alan suçları ifade etmektedir. Bu suçlar düzenleniş şekilleri gereği yalnızca bilişim sistemleri vasıtasıyla işlenebilirler. Ancak Yargıtay tarafından “dolayısıyla bilişim suçları” olarak ifade edilen, çalışmamızda bilişim yoluyla işlenen suçlar ifadesini tercih ettiğimiz bilişim sistemlerinin kullanılması suretiyle hırsızlık, bilişim sistemlerinin kullanılması suretiyle dolandırıcılık, kişisel verilerin hukuka aykırı olarak ele geçirilmesi ve benzeri suçlar bilişim yoluyla işlenebilecekleri gibi bilişim sistemleri haricinde de işlenebilmektedir. Bu suçlar bilişim yoluyla işlendikleri takdirde bilişim suçları gibi sınıflandırılacak, bilişim sistemlerinin kullanılmadığı durumlarda ise bu kategoride değerlendirilmeyecektir.

Çalışmamızın ilk bölümünün ikinci kısmında bilişim suçlarının sıklıkla karşılaşılan işlenme şekillerini değerlendirdik. Bu işlenme yöntemlerinin virüsler, solucanlar vb. gibi önemli bir kısmı yazılım kategorisinde değerlendirilebilecek türdendir ve bilişim sistemlerindeki açıklardan yararlanarak kötücül amaçları gerçekleştirmeye çalışmaktadır. Ancak yemleme adı verilen yöntem gibi bir kısım yöntemler yazılımdan ziyade bilişim sistemlerinin kullanıcılarını hedef almakta ve bu kullanıcılara karşı sosyal mühendislik faaliyetleri geliştirerek kötücül amaçlarına ulaşmaktadır. Çalışmamızın ana konusu olmamakla birlikte bilişim suçlarının ve bilişim yoluyla işlenen suçların ne şekillerde işlendiği hususunun da belirlenmesi önemli olduğundan bu yöntemler arasındaki farklılıklara da değinilmiştir.

Bilişim sistemlerinin kendilerine has bu işleniş şekilleri dolayısıyla bu suçların soruşturmasında ve kovuşturmasında da yeni yöntemler geliştirilmesine ve uzmanlaşmanın sağlanmasına ihtiyaç duyulmaktadır. Uygulamada adli kolluk birimleri içerisinde hemen hemen her il merkezinde “siber suçları soruşturma birimleri” kurulmuş durumdadır. Yine de bu birimlerde çalışan uzman personel sayısının yetersiz oluşu, hâkim ve Cumhuriyet savcılarının da bu birimlerin yapabilecekleri işlemler hakkında yeterince bilgiye sahip olmaması sebebiyle soruşturma ve kovuşturma aşamalarında yaşanan eksiklikler pek çok zaman suçların ve suçluların ortaya çıkarılarak cezalandırılması konusunda gecikmelere sebep olmaktadır.

Günümüzde özellikle büyükşehir adliyeleri ile dosya ve fiziki koşulları itibarıyla bürolaşmaya müsait olan bazı ağır ceza merkezlerinde Cumhuriyet Başsavcılıkları bünyelerinde “Bilişim Suçları Soruşturma Büroları” kurulmuştur. Cumhuriyet Başsavcılıkları bir bütün olmakla birlikte bilişim suçlarının soruşturulması amacıyla kurulmuş özel bürolar bulunması, bu bürolarda çalışan Cumhuriyet savcıları ve diğer personelin bilişim suçları alanında uzmanlaşmış olması gibi etkenler bilişim suçlarının soruşturulmasını kolaylaştırmakla birlikte iş bölümlerindeki birtakım aksaklıklar dolayısıyla bu bürolar da yetersiz kalmaktadır. Bununla birlikte yalnızca bilişim suçlarının değil bilişim alanında işlenen bütün suçların soruşturulmasında birtakım özel usullere başvurulması gerekmektedir. Günümüzde artık tehdit, hakaret gibi nispeten düşük cezalara sahip ve uzlaştırma usulüne tabi suçlardan nitelikli hırsızlık, nitelikli dolandırıcılık gibi suçlara varıncaya dek pek çok suç bilişim sistemleri vasıtasıyla işlenmekte ve hem Cumhuriyet Başsavcılıklarında hem de mahkemelerde iş yükünün büyük bir kısmını bu suçlar oluşturmaktadır. Bu duruma rağmen çoğu zaman bilişim suçları büroları yalnızca TCK’nın “Bilişim Alanında Suçlar” başlıklı bölümünde düzenlenen suçlara bakmakta, bilişim yoluyla işlenen diğer suçlara ilişkin soruşturmalar ise genel bürolar tarafından yürütülmektedir. Bu bürolarda çalışan ve iş yükünün belirli bir kısmı bilişim suçları olan, geri kalan kısmı ise diğer suçlardan oluşan Cumhuriyet savcıları zaman zaman bu suçların soruşturmasında yetersiz kalmakta ve yine bu suçlarla ilgili olarak ilgili kolluk birimlerinin siber suçları soruşturma birimlerine soruşturmada görev vermekten imtina etmektedir. Kovuşturma aşamasında ise iş yüzdelerinin az bir kısmı bilişim suçları ve bilişim sistemlerinin kullanılması suretiyle işlenen suçlardan oluşan ceza hâkimleri bu suçların kovuşturulması konusunda uzman olmadıklarından ötürü dosyalar uzamaktadır. Açıklanan problemin çözümü için İl Emniyet Müdürlüklerinde ve İl Jandarma Komutanlıklarında çalışan uzman personel sayısı artırılarak bilişim suçlarının soruşturma aşamalarında bu personele görev verilmelidir. Cumhuriyet Başsavcılıkları bünyesinde kurulan “Bilişim Suçları Bürosunun” yanı sıra yine Cumhuriyet Başsavcılıkları bünyesinde “Bilişim Yoluyla İşlenen Suçları Soruşturma Büroları” kurulmalı ve TCK ile diğer kanunlarda tanımlanan, TCK’nın “Bilişim Alanında Kalan Suçlar” başlıklı bölümünde düzenlenen suçların dışında kalan diğer suçlar bu bürolar vasıtası ile soruşturulmalıdır. Kovuşturma aşamasında ise bilişim suçlarına ve bilişim yoluyla işlenen suçlara bakan ihtisas mahkemeleri kurulmalı, bu sayede ilgili mahkeme hâkimlerinin de bu suçlar konusunda bilgili kimseler olmaları sağlanmalıdır.

Çalışma konumuzun ilk bölümün son kısmında ise bilişim suçları ile bilişim yoluyla işlenen suçları inceleyerek bu suçların uygulanması ve yorumlanması bakımından yaşanan birtakım sıkıntılara yönelik çözüm önerileri getirdik.

İnceleme konusu yapılan ilk suç TCK'nın 243/1. maddesinde düzenlenen “Bilişim Sistemlerine Girme veya Kalma” suçudur. 2016 yılında yapılan değişikliğe kadar bu suç “bilişim sistemlerine girme ve kalma” suçu şeklindeydi. 2016 yılında “ve” bağlacının “veya” olarak değiştirilmesi ile birlikte uygulamada yaşanan bir kısım tereddütler giderilmekle birlikte bu suç tipinin eylem unsuru da değişmiş oldu. Buna rağmen suçun başlığında herhangi bir değişikliğe gidilmeyerek suç başlığı “bilişim sistemlerine girme suçu” olarak bırakıldı. Yapılan değişiklikle birlikte suçun seçimlik hareketli bir suç olması, eylem unsurunun “bilişim sistemine girmek” ya da “bilişim sistemlerinde kalmaya devam etmek” şeklinde olması karşısında suçun başlığı yetersiz kalmış durumdadır. Bu sorunun giderilebilmesi için madde başlığının “Bilişim Sistemine Girme veya Kalma Suçu” suçu olarak değiştirilmesi gerektiği düşüncesindeyiz. Öte yandan “Bilişim Sistemine Hukuka Aykırı Olarak Girme veya Kalma Suçu” ya da “Bilişim Sistemlerinde Hukuka Aykırı Olarak Bulunmak” gibi başlıkların da bu suç tipi için uygun başlıklar olduğunu düşünüyoruz.

Bilişim Sistemine Girme veya Kalma suçunun seçimlik unsurlarından bilişim sistemine girme eyleminin yalnızca icrai bir davranışla işlenebileceği hususunda şüphe yoktur. Ancak doktrindeki yaygın görüşün aksine bilişim sisteminde kalma suçunun ihmali bir davranışla işlenebileceği gibi icrai bir davranışla da işlenebileceği görüşündeyiz. Yukarıda açıklandığı üzere bir kişinin hukuka uygun olarak girdiği bir sistemde kalmaya devam etmesi için özel bir çaba harcaması ve bunun hukuka aykırı olması durumu da mümkündür. Failin, hukuka uygun olarak girdiği bilişim sisteminde hukuka aykırı olarak kalmaya devam etmek için özel bir çaba göstermesi durumunda suç icrai bir davranışla işlenmiş olacaktır.

TCK'nın 243. maddesinin 2. fıkrasında ise bu suçun bedeli karşılığında yararlanılabilen bir sistem hakkında işlenmesi halinde cezanın yarı oranına kadar indirileceği düzenlenmiştir. Kullanıcıların büyük bir kısmı bedeli karşılığında yararlanılabilecek bu sistemlere bu bedeli ödmeden girmenin yollarını aramakta hatta bu durum siber suçlu olarak tanımlanamayacak kişilerin dahi ilgisini çekmektedir. Bilişim sistemleri konusunda uzman olmayan kişilerin dahi bu sistemlere girmek konusunda hevesli olması bu sistemlerin diğer sistemlere nazaran korunmaya muhtaçlık yönlerini artırmaktadır. Bu sebeple bu nitelikli halin bir indirim sebebi olarak düzenlenmesi eleştirilmekte, bu durumun artırım maddesi yapılması gerektiği yönünde görüşler ileri sürülmektedir. Kanaatimizce “Bedeli Karşılığında Yararlanılabilen Bilişim Sistemlerine Girme veya Kalma” şeklindeki eylemin bir artırım ya da indirim maddesi olarak düzenlenmesi yerine kendisine ait yaptırım bulunan ayrı bir suç olarak düzenlenmesi gerekmektedir. Bu suçun alt sınırı temel halinden az üst sınırı ise temel halinden fazla olmalıdır. Gerçekten de bu eylemler zaman zaman bilişim sistemleri konusunda yeterince bilgisi olmayan bir kimsenin gerçekleştirdiği, failin eylemi kasten işlemesine rağmen eylemin sonuçlarını kavrama yetisinin bulunmadığı şekillerde gerçekleşmektedir. Bu gibi durumlarda genellikle bilişim sistemine girilmiş olması dolayısıyla mağdur, yalnızca muhtemel bir kazançtan olmakta bunun dışında bir

zarara uğramamaktadır. Bu gibi bir durumda temel cezadan daha az bir ceza tayini yerindedir. Ancak meydana gelen netice kimi zaman 243/1. maddesinde düzenlenen suçtan daha ağır olabilmektedir. Bu gibi durumlarda da cezanın arttırılması uygundur. Bu sebeple 243/1. maddesinin cezasının bir yıla kadar hapis veya adli parası olduğu da göz önüne alınarak, 243/2. maddesinin yaptırımının “6 aydan 2 yıla kadar hapis veya adli para cezası” olarak düzenlenmesi ve bu konuda hâkime takdir hakkı tanınması gerekmektedir.

243/3. maddesinde ise 243/1. maddede düzenlenen eylemin neticesinde sistemin içerdiği verilerin değişmesi ve zarar görmesi halinde verilecek ceza altı aydan iki yıla kadar hapis cezası olarak düzenlenmiştir. Bu suçun işlenmesi için failin sisteme girmek yönünden kasten, verileri değiştirmek ya da yok etmek yönünden ise taksirle hareket etmesi gerekmektedir. 244/2. maddesinde ise verilerin kasten değiştirilmesi ve yok edilmesi hali düzenlenmiş ve bu halin yaptırımı olarak da altı aydan üç yıla kadar hapis cezası öngörülmüştür. Kanaatimizce bu iki suçun yaptırımları konusunda bir orantısızlık bulunmaktadır. Bu orantısızlığın giderilerek yaptırımlar arasında dengenin sağlanması gerekmektedir.

243. maddenin 4. fıkrasında ise “Veri Nakillerini Sisteme Girmeksizin Teknik Araçlarla İzleme Suçu” düzenlenmiştir. Bu suçun işlenmesi için veri nakillerinin “sisteme girmeksizin” izlenmesi gerekmektedir. Madde başlığının “bilşim sistemine girme” olarak düzenlendiği hususu da göz önüne alındığında bu suçun 243. maddede düzenlenmesi yersizdir. Bu suç tipi eylem, netice, korunan hukuki yarar ve konu itibarıyla 243. maddede düzenlenen suçtan tamamen ayrılmaktadır. Bu sebeple 243/4. maddesi yerine 243/A gibi ayrı bir madde başlığı olarak düzenlenmesi daha yerinde olacaktır.

Çalışma konumuz kapsamındaki bir diğer suç ise 244. maddede düzenlenen Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçudur. 244/1. maddesinde bilişim sisteminin işleyişini engellemek veya bozmak fiillerine yönelik yaptırım düzenlenirken 244/2. maddesinde ise bir bilişim sistemindeki verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak ile sisteme veri yerleştirmek ve var olan verileri başka bir yere göndermek fiilleri yaptırıma bağlanmıştır.

243. maddenin ve 244. maddenin aynı anda ihlal edilmesi durumunda ne olacağı hususunda yukarıda da açıkladığımız üzere farklı görüşler mevcuttur. Kanaatimizce bu durumda geçitli suç hükümleri uygulanmalı ve yalnızca 244. maddeden dolayı cezalandırma yapılmalıdır. Hâkim, bu durumda temel cezayı belirlerken 243. maddenin de ihlal edilmiş olmasını alt sınırdan uzaklaşma gerekçesi yapabilecektir. 244. madde ile 151. maddenin aynı anda ihlal edilmesi durumunda ise kanaatimizce failin kastına göre hareket edilmelidir. Fail sistemin somut unsurlarına zarar vermek gayesindeyse 151. maddeden aksi halde ise 244. maddeden sorumlu tutulmalıdır.

244. maddenin 3. fıkrasında ise bu suçun bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde verilecek cezanın yarı oranında arttırılacağı düzenlenmiştir.

244. maddenin son fıkrasında ise Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu düzenlenmiştir. Doktrinde bu suçun da ayrı bir maddede düzenlenmesi gerektiği yönünde

görüşler bulunmaktadır. Bu fıkranın koruduğu hukuki yararın ilk iki fıkradan ayrıştığı da göz önüne alındığında bu fıkrayı ayrı bir suç olarak değerlendirmek gerektiği yönündeki görüşe katılmaktayız.

244. maddenin son fıkrasında düzenlenen bu suç, maddi ve manevi her türlü yararı kapsamaktadır. Bu suçun mağduru belirli bir kişi olabileceği gibi toplumun tamamı da bu suçun mağduru olabilecektir. Bu suç açısından fiil, TCK'nın 244. maddesinin ilk iki fıkrasında tanımlanan fiillerin işlenmesi suretiyle haksız yarar elde edilmesidir. Dolayısıyla bu suç bağlı hareketli bir suç niteliğindedir. Bu suçun bir mağdur olmadan da işlenmesi yahut tüm toplumun zararına olarak işlenmesi de mümkündür. Bir kimsenin kamuya ait bilişim sistemine girerek askerliğini yapmadığı halde yapmış gibi göstermesi yahut haksız bir şekilde tecil edilmesini sağlaması durumunda doğrudan bir kişinin hakkı zarara uğratılmış olmasa da toplum bu durumdan zarar görmüştür.

TCK'nın 244/4. maddesinde düzenlenen bu suçun yaptırımı ise iki yıldan altı yıla kadar hapis cezası olarak belirlenmiştir. 244/4. maddede düzenlenen suçu işleyen fail hem sistemin ya da sistemdeki verilerin güvenliğine yönelik bir saldırı düzenlemekte hem de haksız bir yarar elde etmektedir. TCK'nın 142/2-e maddesinde düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunun yaptırımının beş yıldan on yıla kadar hapis cezası olduğu da göz önüne alındığında 244/4. maddedeki suçun yaptırımının değiştirilmesi gerekmektedir.

Türk Ceza Kanunu'nun 244/4. maddesinde düzenlenen suç tali niteliktedir. Fail; eyleminin başka bir suçu oluşturmaması halinde TCK'nın 244/4. maddesinden cezalandırılacak, eylemi başka bir suçu oluşturduğu takdirde ise bu suçtan cezalandırılacaktır. Madde gerekçesinde failin eyleminin daha ağır bir cezayı gerektirmesi halinde o suçtan ceza verileceği, aksi durumda ise 244/4. maddesinin uygulanacağı düzenlenmiştir. Ancak madde gerekçesi bağlayıcı nitelikte olmayıp ancak maddenin yorumlanması esnasında yol gösterici niteliktedir. Ceza adaletinin sağlanması açısından 244/4. maddede değişikliğe gidilerek maddeye “daha ağır cezayı gerektiren” ibaresi eklenmelidir. Bu durum hem kafa karışıklığını giderecek hem de ceza adaleti açısından daha doğru sonuçlar doğuracaktır.

TCK'nın 245. maddesinde ise Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu düzenlenmiştir. Bu suç uygulamada sıklıkla bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu ile karıştırılmaktadır. Suçun konusu banka ve kredi kartlarıdır. Banka ve Kredi Kartları kullanılarak yapılan para aktarımlarında TCK'nın 245. maddesinde düzenlenen bu suç söz konusu olacakken banka ve kredi kartları kullanılmadan, örneğin mağdurun internet bankacılığı hesabı ele geçirilerek yapılan para aktarımında hırsızlık suçu oluşacaktır. Bu suçun oluşması için suç konusu kartın fiziki olarak mevcut olması gerekmez, sanal kartların kötüye kullanılması da bu suçu oluşturacaktır. Bu suçun oluşması için failin bizzat kendisine yarar sağlaması da gerekmez. Fail bir yardım kuruluşuna dahi yarar sağlasa bu suç oluşacaktır. Önemli olan failin banka veya kredi kartlarını kullanarak kendisine veya bir başkasına yarar sağlamasıdır. 245. maddenin 4. fıkrasında bu suç ile ilgili olarak şahsi cezasızlık sebebi düzenlenmiştir. Fail, aralarında şahsi cezasızlık sebebinin olduğunu sanarak bu suçu işlerse, gerçekte böyle bir durum olmasa bile hatasından yararlanacaktır. Yine aynı maddenin 5. fıkrasında TCK'nın 167. maddesine atıf

yapılarak bu suç açısından etkin pişmanlık hükümlerine yer verilmiştir. Etkin pişmanlık hükümlerinin uygulanabilmesi için zararın bizzat fail tarafından giderilmesi gerekmez. Fail pişmanlık gösterdikten sonra fail adına bir yakını da bu zararı giderebilir.

245. maddenin 2. fıkrasında “Sahte Banka Veya Kredi Kartı Üretmek, Satmak, Devretmek, Satın Almak veya Kabul Etmek Suçu” düzenlenmiştir. Bu suç hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının tümünün ratio legis’lerine sahip olan bir suç tipi olarak düzenlenmiştir. Fail, sahte belgeler hazırlayarak banka ve finans kurumuna başvurur ve bu başvurusu neticesinde ilgili kurum tarafından banka veya kredi kartı düzenlenirse, failin bu eylemi yine TCK’nın 244/2. maddesinde düzenlenen suç oluşturacaktır. Bu durumda fail ayrıca sahtecilik suçundan cezalandırılmalıdır. Doktrinde bir sanal kartın sahte olarak oluşturulması durumunda da bu suçun oluşacağı ifade edilmektedir. Ancak sanal kartların genellikle internet bankacılığı kullanılarak oluşturulması karşısında failin, mağdura ait internet bankacılığı hesabını ele geçirip ardından sanal kart oluşturması şeklindeki eylemi hem TCK’nın 136. ve 244/2-3. hem de 245/2. maddelerinde düzenlenen suçları oluşturacak, bu durumda 136. madde ile 245. madde arasında gerçek içtima uygulanırken 244. madde ile 245. madde arasında fikri içtima hükümleri uygulanacaktır.

245. maddenin 3. fıkrasında “Sahte Banka ve Kredi Kartlarını Kullanarak Yarar Sağlama Suçu” düzenlenmiştir. Bu suçun faili 245. maddenin 2. fıkrası neticesinde kartı üreten, satın alan ya da devralan kişi olabilir. Ancak böyle bir şart yoktur. Fail TCK’nın 245/2. maddesinde düzenlenen suç işlemeyen de bu suçun faili olabilir.

245. maddenin 3. fıkrasında düzenlenen suç tali nitelikte olduğundan, bu suç açısından içtima hükümlerinin uygulanması söz konusu değildir. Çünkü bu suç “fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde” söz konusu olacak, tali nitelikte bir suçtur.

Failin ATM cihazlarına bir düzenek yerleştirerek kart sahiplerinin bilgilerini kopyalaması halinde TCK’nın 136. maddesinde bulunan suç, bu bilgileri kullanmak suretiyle sahte banka veya kredi kartları üretmesi durumunda ise TCK’nın 244/2. maddesinde düzenlenen suç oluşur. Sahte olarak oluşturulan bu kartların kullanılması suretiyle menfaat temin edilmesi halinde ise TCK’nın 245/3. maddesinde düzenlenen suç oluşur. Fail, bu durumda üç suçtan da gerçek içtima hükümlerine göre cezalandırılır.

TCK’nın 245/A maddesinde ise “Yasak Cihaz ve Programlar” başlıklı suç düzenlenmiştir. Söz konusu suçun başlığının hatalı olarak belirlendiği kanaatindeyiz. TCK sistematığında suçların isimlendirilmesi yapılırken fiil unsuru dikkate alınmasına rağmen bu suçta suçun konusu göz önüne alınarak isimlendirme yapılmıştır. Bu suçun başlığının “Suçta Kullanılacak Yasak Cihaz ve Programların İmal Edilmesi, Ticareti, Dolaşıma Sokulması ve Bulundurulması” şeklinde olabileceği kanaatindeyiz.

Türk Ceza Kanununda nitelikli hal olarak düzenlenen bilişim yoluyla işlenebilen suçlar ise Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık Suçu ve Bilişim Sistemlerinin Kullanılması Suretiyle Dolandırıcılık suçudur.

Bilişim Sistemlerinin Kullanılması Suretiyle Hırsızlık Suçu TCK’nın 142/2-e maddesinde düzenlenmiştir. Bu suç, hırsızlık suçunun bilişim sistemleri kullanılarak işlenmesi

durumunu düzenleyen nitelikli halidir. Bir olayda failin eyleminin hem 244/4. maddesine hem de 142/2-e maddesine uyması durumunda fail, 142/2-e maddesinden cezalandırılacaktır. Bu, hem fikri içtima hükümlerinin gereğidir hem de 244/4. maddesinin tali nitelikte olmasının bir sonucudur. Fakat bir kimsenin banka veya kredi kartları kullanılarak işlenen bir eylem söz konusu olduğunda fail 142/2-e maddesinden değil 245/1 maddesinden sorumlu tutulacaktır. Zira 245. madde, 142/2-e maddesine göre özel nitelikte bir maddedir. Ancak 142/2-e maddesinde öngörülen ceza miktarının 245/1 maddesinde öngörülen ceza miktarından yüksek olması dolayısıyla cezalandırma konusunda adaletsizlik yaşanmaktadır. Zira hırsızlık suçunda fail, yalnızca mağdurun malvarlığına yönelik bir saldırıda bulunurken, banka ve kredi kartlarının kullanması durumunda mağdurun malvarlığının yanı sıra banka ve kredi kartlarına duyulan güveni de zedelemiş olacak, buna rağmen daha az ceza alacaktır. Bu husustaki sorunun giderilmesi için 245/1. maddesinde düzenlenen suçun cezasının arttırılması gerektiği görüşündeyiz.

Türk Ceza Kanunu'nun Bilişim Alanında Suçlar başlıklı onuncu bölümüne yeni bir madde eklenerek bu bölümde düzenlenen suçların bilişim sistemlerinin güvenliğinden sorumlu olan kişiler tarafından işlenmesi durumunda temel cezada artırım yapılacağının düzenlenmesi gerekmektedir. Gerçekten de bu kişilerin bilişim sistemlerine erişimleri ve bu bölümde düzenlenen suçları işlemeleri diğer kişilere nazaran daha kolaydır. Bunun yanı sıra bu sistemlerin güvenlikleri bizzat onlara emanet edilmiştir. Bilişim suçlarının bu kimseler tarafından işlenmesi halinde fail, hem sistemin güvenliğine duyulan güveni zedelemiş, hem bir zarara sebep olmuş hem de mağdur tarafından kendisine duyulan güveni zedelemiştir. Bu sebeplerle failin sistemin güvenliğinden sorumlu olan kişi olması durumu özel nitelik arz eden bir durumdur.

Bilişim Sistemlerinin Kullanılması Suretiyle Dolandırıcılık Suçu ise TCK'nın 158. maddesinin 1. fıkrasının f bendinde düzenlenmiştir. Bu suç, dolandırıcılık suçunun bilişim sistemleri kullanılarak işlenmesi durumunu düzenleyen nitelikli halidir.

Uygulamada bilişim sistemlerinin kullanılması suretiyle hırsızlık ve dolandırıcılık suçları ile banka ve kredi kartlarının kötüye kullanılması suçunun ve güveni kötüye kullanma suçunun sıklıkla karıştırıldığı görülmektedir. Fail, bir banka ve kredi kartını kullanarak yarar sağlıyorsa bu durumda özel düzenleme olması sebebiyle banka ve kredi kartlarının kötüye kullanılması suçu oluşacaktır. Fail, mağdurun malvarlığı değerini, mağdurun zilyetliğine müdahale ederek ele geçiriyorsa hırsızlık suçu söz konusu olacaktır. Fail, hileli hareketler kullanarak mağduru, malvarlığı değerini kendi rızası ile vermeye ikna ediyorsa bu durumda dolandırıcılık suçu oluşacaktır. Fail, mağdurun rızaen verdiği bir malvarlığı değerini iade etmiyorsa bu durumda güveni kötüye kullanma suçu söz konusu olacaktır. Bu malvarlığının banka ve kredi kartı olması ve failin de bu kartı kullanması durumunda ise güveni kötüye kullanma suçu değil, yine banka ve kredi kartlarının kötüye kullanılması suçu olacaktır. Ayrıca fail, tehdit ve cebir kullanarak mağduru bir malvarlığı değerini vermeye zorluyorsa bu durumda yağma suçu oluşacaktır. Yağma suçunun işlenmesi sırasında bilişim sistemlerinden yararlanılmış olması suçun niteliğini değiştirmeyecektir.

KAYNAKÇA

Ak, B. (2009). Türkiye’de sağlık bilişimi, bir kişisel değerlendirme ve uluslararası bir başarı öyküsü: CorTTex. Akademik Bilişim, 11-13. https://ab.org.tr/ab09/kitap/ak_AB09.pdf adresinden alındı.

Akarşlan, H. (2015). Bilişim Suçları. Ankara: Seçkin Yayıncılık

Akbulut, B. (2017). Bilişim Alanında Suçlar. Ankara: Adalet Yayınevi

Altuğ, Ş. (2018). Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri (CMK – TCK – Özel Yasalar). Ankara: Yargıtay Cumhuriyet Başsavcılığı

Artuk. M. E., Alşahin. M. E. (2021). Kriminoloji. Ankara: Adalet Yayınevi

Artuk. M. E., Gökçen ,A. ve Yenidünya, A. C. (2014). Ceza Hukuku Genel Hükümler. Ankara: Adalet Yayınevi

Artuk. M. E., Gökçen ,A. ve Yenidünya, A. C. (2014). Ceza Hukuku Özel Hükümler. Ankara: Adalet Yayınevi

Aslay, F . (2017). Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi . International Journal of Multidisciplinary Studies and Innovative Technologies , Volume 1 Issue 1 , 24-28 . <https://dergipark.org.tr/tr/pub/ijmsit/issue/32341/359378> adresinden alınmıştır.

Avrupa Konseyi Siber Suç Sözleşmesi – Açıklayıcı Memorandum [İ nternet ve Hukuk Platformu - İ v H P- çevirisi]. <https://www.eralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/>. Erişim Tarihi, 25.12.2019.

Bassham, L. E., Polk, W. T. (1992). Threat Assessment of Malicious Code and External Attacks (No. NISTIR-4939). National Inst Of Standards And Technology Gaithersburg Md. <https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir4939.pdf> adresinden alınmıştır.

Bilgisayarların tarihi!(10.03.2011). <https://www.milliyet.com.tr/teknoloji/bilgisayarlarin-tarihi-1362416>. Erişim Tarihi, 13.08.2020.

Bilgisayar Kuşakları. <https://bembilgisayar.com/bilgisayar-kusaklari>. Erişim Tarihi, 02.04.2020.

Bozdoğan Akbulut, B. (2000). Bilişim Suçları. Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 8(1-2 (Milenyum Armağanı)), 545-555. <https://dergipark.org.tr/en/pub/suhfd/issue/26619/280658> adresinden alınmıştır.

Canbek, G , Sağiroğlu, Ş . (2013). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma . Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi , 22 (1),. <https://dergipark.org.tr/tr/pub/gazimmfd/issue/6671/88359> adresinden alınmıştır.

Canpolat, C. Yabancıların İadesi: Türkiyeden Yabancı Devlete İadenin Şartları Yönünden Bir İnceleme, Türkiye Adalet Akademisi Dergisi, 43, 2020, s. 315-350

Çerezler - Web Sitelerinin Bilgisayarınızda Depoladığı Bilgiler. <https://support.mozilla.org/tr/kb/cerezler-web-sitelerinin-bilgisayarinizda-depoladi>. Erişim Tarihi, 24.03.2020.

Çernobil virüsü 4 milyar dolar yedi. (28.04.1999). <https://www.hurriyet.com.tr/ekonomi/cernobil-virusu-4-milyar-dolar-yedi-39076290>. Erişim Tarihi, 25.03.2020.

Chrome’u Silen Zararlı Yazılım!. <https://shiftdelete.net/chrome-silen-zararli-yazilim-efast-browser-64976>. Erişim Tarihi, 25.03.2020.

CIH (Çernobil) virüsü. <https://answers.microsoft.com/tr-tr/protect/forum/all/cih-%C3%A7ernobil-vir%C3%BCs%C3%BC/a1de04f7-d8eb-4d94-9e70-60c5b775affb>. Erişim Tarihi, 25.03.2020.

Cohen. F. Computer Viruses - Theory and Experiments. <https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html>. Erişim Tarihi, 23.03.2020.

Değirmenci, O. (2004). Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi. TBB Dergisi, (58), 195-208.

Demircan. K. (2015) “Chrome Taklidi Yapan Bilgisayar Virüsüne Dikkat >> Efast Virüsü Chrome’u Silip Yerine Geçiyor”. <https://khosann.com/chrome-taklidi-yapan-bilgisayar-virusune-dikkat-efast-virusu-chromeu-silip-yerine-geciyor/>

Denial of Service (DoS) Saldırıları ve Korunma Yöntemleri. [https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/denial-of-service-\(dos\)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri](https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri). Erişim Tarihi, 26.03.2020.

Department of Justice U.S. Attorney’s Office Western District of Pennsylvania (2019) Siemens Contract Employee Intentionally Damaged Computers by Planting Logic Bombs into Programs He Designed. <https://www.justice.gov/usao-wdpa/pr/siemens-contract-employee-intentionally-damaged-computers-planting-logic-bombs-programs>. Erişim Tarihi, 25.03.2020.

Dönmez, A. (2001). Bilgisayarcı matematikçiler. Doğu Üniversitesi Dergisi, Cilt 2, Sayı 2, 2001, s.30. <http://journal.dogus.edu.tr/index.php/duj/article/view/214> adresinden alınmıştır.

Dönmezer, S. ve Erman, S. (2019). Nazari ve Tatbiki Ceza Hukuku, C. II, İstanbul: Der Yayınları

Dülger, M. V. (2018). Bilişim Suçları ve İnternet İletişim Hukuku. Ankara: Seçkin Yayıncılık

Dülger, M. V. (2020). Ceza Hukuku Genel Hükümler. İstanbul:Hukuk Akademisi

Dülger, M. V., & Mодоğlu, G. (2014). Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet ve İletişim Hukuku Uygulama Rehberi (Cybercrimes, Investigations and Trials for Cybercrimes and Internet Telecommunication Law). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564591 adresinden alınmıştır.

Eniac nedir, ne işe yarar? (10.06.2017). <https://www.hurriyet.com.tr/gundem/eniac-nedir-ne-ise-yarar-40485962>. Erişim Tarihi, 14.08.2020.

Er, Y. (2019). Logic (Mantık) Bombası Nedir?. <https://teknodestek.com.tr/logicmantik-bombasi-nedir/>

Ercan, İ. (2017). Ceza Hukuku Genel Hükümler. Kocaeli: Kuram Kitap

Ercan, İ. (2017). Ceza Muhakemesi Hukuku. Kocaeli: Kuram Kitap

Erdağ, A. İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). Gazi Üniversitesi Hukuk Fakültesi Dergisi, 14(2), 275-303.

Erdoğan, Y. (2013). Türk Ceza Kanunu’nda Bilişim Suçları. İstanbul: Legal Yayıncılık

ESET Cyber Security. <https://help.eset.com/ecs/6/tr-TR/>.

Fidye Yazılımı (Ransomware) Nedir?. 27.02.2019. <https://www.isnet.net.tr/BlogIcerik/Fidye-Yazil%C4%B1m%C4%B1-Ransomware-Nedir-isnet-blog>. Erişim Tarihi, 25.03.2020.

Fidye yazılımı 'WannaCry' Türkiye dahil 99 ülkede binlerce bilgisayarı etkiledi. (12 Mayıs 2017). <https://www.bbc.com/turkce/39899848>. Erişim Tarihi, 24.03.2020.

First Computer Virus. <https://history-computer.com/Internet/Maturing/Thomas.html>. Erişim Tarihi, 23.03.2020.

Gonzalez Redondo, F. A. (2011). The Contribution of Leonardo Torres Quevedo to Lighter-Than-Air Science and Technology. The International Journal for the History of Engineering & Technology, 81(2), 212-232. <https://www.tandfonline.com/doi/pdf/10.1179/175812111X13033852943237?needAccess=true> adresinden alınmıştır.

GÖKBULUT, İ. Bilgisayar Uygulamaları. İstanbul Üniversitesi Açık Ve Uzaktan Eğitim Fakültesi. http://auzefkitap.istanbul.edu.tr/kitap/sivilhava_ao/bilgisayaruygulamalari.pdf, adresinden alınmıştır.

Gül, A. (2018). Doğrudan/Dolaylı Bilişim Suçları. Ankara: Seçkin Yayıncılık

Güryuva, Y. (2019). Uluslararası Siber Güvenlik Ve Siber Ortamdaki Tehditlerin Fiziksel Bir Savaşa Dönüşme Olasılığı. Ankara: Yayımlanmış Yüksek Lisans Tezi

Hakeri, H. (2014). Ceza Hukuku Genel Hükümler. Ankara: Adalet Yayınevi

İphone'de Arka Kapı Talebine Karşı Direniş. (23.02.2016). <https://www.dw.com/tr/iphonedede-arka-kap%C4%B1-talebine-kar%C5%9F%C4%B1-direni%C5%9F/a-19067503>. Erişim Tarihi, 24.03.2020.

Johansen, A. G. (2019). What is ransomware and how to help prevent ransomware attacks. <https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html>. Erişim Tarihi, 04.03.2020.

Johnson, M. (2013). Cyber crime, security and digital intelligence. Gower.

Karakehya, H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. TBMM Dergisi, (81), 1-24.

Karakehya, H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. TBB Dergisi, (81), 1-24. (<http://tbbdergisi.barobirlik.org.tr/m2009-81-498> adresinden alınmıştır.)

Kaspersky Resmi Blogu. <https://www.kaspersky.com.tr/blog/>.

Kaspersky Kaynak Merkezi. <https://www.kaspersky.com.tr/resource-center>.

Kaspersky IT Encyclopedia. <https://encyclopedia.kaspersky.com>.

Keser, H . (2019). Bilgisayarın Evrimi . Ankara University Journal of Faculty of Educational Sciences (JFES) , 24 (2) , 411-422. <https://dergipark.org.tr/en/pub/aubfd/issue/47781/604335> adresinden alınmıştır.

- Ketizmen, M. (2006) Türk Ceza Hukukunda Bilişim Suçları. Ankara: Doktora Tezi.
- Kılıç, Ç. (2019). Dünden Bugüne Fidyeye Yazılımların (Ransomware) Gelişimi ve Geleceği. İstanbul: Yayımlanmış Yüksek Lisans Tezi.
- Koca, M. ve Üzülmez, İ. (2018). Türk Ceza Hukuku Özel Hükümler. Ankara: Adalet Yayınevi
- Kunter, N. (1954). Suçun Maddi Unsurları Nazariyesi. İstanbul: İsmail Akgün Matbaası.
- Küçükşille, E. U., Yalçınkaya, M. A., ve Uçar, O. (2014). Siber saldırılarda istismar kitlerinin kullanımı üzerine bir analiz ve savunma önerileri. (<https://iscTurkey.org/assets/files/2016/03/isc2014-29.pdf> adresinden alınmıştır.)
- Küçükşille, E. U., Yalçınkaya, M. A., & Uçar, O. (2014). Siber saldırılarda istismar kitlerinin kullanımı üzerine bir analiz ve savunma önerileri. 7. In Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı [7th International Conference on Information Security and Cryptology] (pp. 17-18). <https://iscTurkey.org/assets/files/2016/03/isc2014-29.pdf> adresinden alınmıştır.
- Mahmutoğlu, F. Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71(1), 855-889.
- Naroğlu, M. Konrad Zuse ve Makineleri. Bilgisayar Mühendisleri Odası Dergisi. [<https://dergi.bmo.org.tr/bilisim-tarihi/turkiyede-internetin-tarih-onesi-uzerine-prof-dr-levent-toker-ile-roportaj> adresinden alınmıştır.]
- NSA, Torvalds'dan Linux'a yazılımsal açık koymasını istedi. (18.11.2013). <https://www.donanimhaber.com/NSA-Torvaldsdan-Linuxa-yazilimsal-acik-koymasini-istedi--52657>. Erişim Tarihi, 24.03.2020.
- Olta lama (Phishing). <https://www.eset.com/tr/phishing/>. Erişim Tarihi, 25.03.2020.
- Özbek, V. Ö., Doğan, K. ve Bacaksız, P. (2020). Türk Ceza Hukuku Genel Hükümler. Ankara: Seçkin Yayıncılık.
- Özbek, V. Ö., Doğan, K., Bacaksız, P. ve Tepe, İ. (2018). Türk Ceza Hukuku Özel Hükümler. Ankara: Seçkin Yayıncılık.
- Özbek, V. (2007). Banka Veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245) . Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi , Cilt 9 Özel Sayı , 1019-1063. (<https://dergipark.org.tr/en/pub/deuhfd/issue/46938/589018> adresinden alınmıştır.)
- Özgenç, İ. (2020). Türk Ceza Hukuku Genel Hükümler. Ankara: Seçkin
- Öztürk. B. (2020). Nazari ve Uygulamalı Ceza Muhakemesi Hukuku. Ankara: Seçkin
- Öztürk, C., Tekerek, M., Yılmaz, A. S., “Bilgi Güvenliği Endüstrisinin Ülkelere Göre Karşılaştırması” in Sağiroğlu, Ş., Alkan, M., Akyıldız, E., Akleylek, S. (2016). Bilgi Güvenliği ve Kriptoloji Konferansı Bildiri Kitabı, <https://www.iscTurkey.org/assets/files/isc-BildiriKitabi2016.pdf> adresinden alınmıştır.
- Parlar, A. (2015). Türk Ceza Hukukunda Bilişim Suçları. Ankara: Bilge Yayınevi

RED SHELL Spyware - "Holy Potatoes! We're In Space?!" Integrated And Removed It After Complaints.

https://www.reddit.com/r/Steam/comments/8pud8b/psa_red_shell_spyware_holy_potatoes_were_in_space/. Erişim Tarihi, 24.03.2020.

Samet, R. Kötü Amaçlı Yazılımlar ve Analizi in Sağiroğlu, Ş., Alkan, M., (2018). Siber Güvenlik ve Savunma Farkındalık Ve Caydırıcılık. Ankara: Grafiker Yayınları. <https://acikerisim.sirt.edu.tr/xmlui/handle/20.500.12604/883> adresinden alınmıştır.

Semiz, M. (2020). İctihatlar ve Uygulamadan Örnekleriyle Bilişim Suçları ve Soruşturma Yöntemleri. Ankara: Adalet Yayınevi

SNYDER. D. (2010) The Very First Viruses: Creeper, Wabbit And Brain. <https://infocarnivore.com/the-very-first-viruses-creeper-wabbit-and-brain>. Erişim Tarihi, 20.03.2020.

Soyaslan, D. (2018). Ceza Hukuku Özel Hükümler. Ankara: Yetkin Yayınları

Soyaslan, D. (2020). Ceza Muhakemesi Hukuku. Ankara: Yetkin Yayınları

T.C. Ulaştırma ve Altyapı Bakanlığı. “CRYPTOLOCKER VİRÜSÜ HAKKINDA BİLGİ NOTU”. <https://www.uab.gov.tr/uploads/pages/cryptolocker-virusu-hakkinda-bilgilendirme/74bc0128f065b41.pdf> Erişim Tarihi, 24.03.2020.

TCP/IP PROTOKOLÜ Nedir. <http://www.bilgisayarnedir.com/tcp-ip-protokolu-nedir.html>. Erişim Tarihi, 03.04.2020.

Tezcan, D., Erdem, M. R. ve Önok, R. M. (2019). Teorik ve Pratik Ceza Özel Hukuku. Ankara: Seçkin Yayıncılık

The Virus Encyclopedia. <http://virus.wikidot.com/>.

Türk Dil Kurumu Sözlükleri, <https://sozluk.gov.tr/>.

Türk Dil Kurumu Sözlüğü, <http://www.tdk.gov.tr/>.

Türkiye’de İnternet. <http://www.internetarsivi.metu.edu.tr/tarihce.php>. Erişim Tarihi, 03.04.2020.

Türkiye’de İnternetin 25. Yılı Etkinliği Sitesi, <http://internet.org.tr/>, Erişim Tarihi, 03.04.2020.

Uysal, D. (2020). Dijital ve Sanal Yansımalar Wolfgang Hohlbein'in "Im Netz der Spinnen" ve "Das Netz" Adlı Romanları. Ankara:İksad Uluslararası Yayınevi, <https://iksadyayinevi.com/wp-content/uploads/2020/04/D%C4%B0J%C4%B0TAL-VE-SANAL-YANSIMALAR-WOLFGANG-HOHLBEIN%E2%80%99IN-%E2%80%99CIM-NETZ-DER-SPINNEN%E2%80%9D-VE-%E2%80%9CDAS-NETZ%E2%80%9D-ADLI-ROMANLARI.pdf> adresinden alınmıştır.

U. S. Cyber Security & Infrastructure Security Agency . “RANSOMWARE GUIDANCE AND RESOURCES” <https://www.us-cert.gov/Ransomware>. Erişim Tarihi, 24.03.2020.

Ünver Y. ve Hakeri, H. (2016). Ceza Muhakemesi Hukuku. Ankara: Adalet Yayınevi

Virüs, Solucan ve Truva Atı (07.09.2013). <https://bidb.itu.edu.tr/sevir-defteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1>. Erişim Tarihi, 23.03.2020.

Virüslerin Tarihçesi. (26 Temmuz 2018). <https://www.yeniduzen.com/viruslerin-tarihcesi-104990h.htm>. Erişim Tarihi, 25.03.2020.

Weisman, S. (2020). What are Denial of Service (DoS) attacks? DoS attacks explained. <https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html>. Erişim Tarihi, 25.03.2020.

What is spyware?. <https://www.avast.com/c-spyware>. Erişim Tarihi, 24.03.2020.

Yalman, Y. (2018). BÖLÜM 9: Siber Terör, Terörizm ve Mücadele in Sağiroğlu, Ş., Alkan, M., (2018). Siber Güvenlik ve Savunma Farkındalık Ve Caydırıcılık. Ankara: Grafiker Yayınları. <https://acikerisim.siiert.edu.tr/xmlui/handle/20.500.12604/883> adresinden alınmıştır.

Yılmaz, S. (2011). 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar. Türkiye Barolar Birliği Dergisi, (92), 62-100.

ÖZGEÇMİŞ

Muhammed Burak Güngör, [REDACTED] 2013 yılında başladığı Kocaeli Üniversitesi Hukuk Fakültesinden 2017 yılında mezun oldu.

2017-2018 yıllarında Bursa Barosu'nda avukatlık stajını tamamladı.

2018 yılında Hâkim-Savcı Adayı olarak Bursa Adliyesinde göreve başladı. 2020 yılında Cumhuriyet Savcısı olarak Gölköy Adliyesine atanmış olup halen buradaki görevine devam etmektedir.

